UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES "ARAGÓN"

"NECESIDAD DE CREAR UN TIPO PENAL EN EL DISTRITO FEDERAL QUE REGULE EL ACCESO A SISTEMAS INFORMÁTICOS"

T E S I S

PARA OBTENER EL TÍTULO DE :

L I C E N C I A D O E N D E R E C H O

P R E S E N T A :

CHRISTIAN GUILLERMO HONIGMANN CAMARILLO

ASESOR:
LIC. MARISELA VILLEGAS PACHECO

BOSQUES DE ARAGÓN ESTADO DE MÉXICO 2006

DEDICATORIAS

A mis padres por su gran amor que dan y que profesan con su ejemplo, por ser mi motor que mi impulsa a seguir adelante.

A mi hermana Shantal por su gran cariño y por que sigamos siempre juntos a cada instante.

A toda mi familia que me apoyo en cada uno de los grandes momentos de mi vida, en especial éste cuando culmino mi carrera profesional.

AGRADECIMIENTOS

A Dios por permitirme llegar a este momento.

A mi madre por darme la vida, por acompañarme siempre, por su amor, por su dedicación.

A mi padre por su gran apoyo en todo momento, por ser un ejemplo a seguir.

A mi hermana Shantal por ser como una amiga para mí, por todos esos lindos momentos que hemos pasado juntos.

A mis tíos Irma, Elia, Noe, Juan, Enriqueta, Lourdes, Moisés, Roció, Luis; a mis primos Daniel Juan Carlos, Alejandro, Omar, Eric; Karla, Verónica y EriKa, a mi sobrino Juan Ramón.

A mis abuelos Luis Honigmann, José Pacheco, Maria del Carmen y Enriqueta Rodríguez.

A la Lic. Marisela Villegas Pacheco por apoyarme y aconsejarme en la elaboración de mi tesis y en la impartición de sus cátedras.

A mis amigos: Edgar, Christian, Moisés; Salvador, Efraín, Rodrigo David, Manuel, Iván, Juan Carlos; a mis amigas: Bárbara, Ana Maria, Margarita, Mirna; Lourdes y Cinthya por compartir grandes momentos con todos ustedes.

A la UNAM, por ser ella mi verdadera casa de conocimiento.

A la FES –ARAGON por darme la oportunidad de encontrar a grandes profesores y amigos, ser mi mar de posibilidades.

NECESIDAD DE CREAR UN TIPO PENAL EN EL DISTRITO FEDERAL QUE REGULE EL ACCESO A SISTEMAS INFORMÁTICOS.

CAPÍTULO II EL DELITO

I N T R O D U C C I Ó N.

La información tiene gran importancia como base de todo proceso cognoscitivo y como motor impulsor de desarrollo de actos individuales y sociales, traduciéndose en progreso; la información requería de un esfuerzo rutinario de cálculo y gestión, como respuesta a esto el hombre desarrollo herramientas que fueron evolucionando hasta llegar a los sistemas de tratamiento de la información, creando las computadoras, estas máquinas trajeron consigo la ciencia y la tecnología de la informática.

En los últimos años, sin embargo con la creación de dispositivos informáticos más pequeños y fáciles de maniobrar, el ritmo de difusión de las aplicaciones informáticas parece adquirir mayor relevancia, junto con los beneficios que tiene el empleo de sistemas informáticos en el ámbito administrativo, laboral, jurídico, industrial o de la vida cotidiana, también trajo consigo perjuicios, la informática no es buena ni mala en si misma, sino que se crearon los llamados delitos informáticos.

Al poder tener acceso a dispositivos que caben en la palma de la mano o computadoras portátiles se hizo vulnerable la información como: filiación, fecha de nacimiento, etc., o más particulares como: raza, religión, historial clínico, cuentas bancarias, etc., por medio de registros parroquiales, civiles, culturales deportivos, médicos, laborales o administrativos, apoyándose claro en sistemas informáticos para su disposición instantánea y puedan ser empleados para otros fines. Con la difusión de Internet se crea un forma más sencilla de obtener datos sin necesidad de introducirse directamente a una computadora, y ahora con los sistemas de interconexión inalámbricas aún es mucho más sencillo.

Los sistemas informáticos pueden manejar tanto archivos públicos como privados, los titulares de estos datos tienen la facultad de exigir ciertos derechos como son: disposición de la información en cualquier momento, permitiendo alterar, ampliar o cancelar estos datos; el derecho de ser usados conforme al fin y no por otros sujetos o instancias como fiscales o policíacas.

El objeto de este presente trabajo es que se cree un tipo penal que regule el acceso ilícito a sistemas informáticos en el Distrito Federal dada la relevancia que esto puede representar.

El primer capítulo, abarca los conceptos generales como son la informática, el Derecho Informático y por supuesto los delitos informáticos para poder comprender este presente trabajo, así también como influyen los sistemas informáticos en la vida cotidiana.

El segundo capítulo es El Delito, por ser de gran importancia para la elaboración del presente trabajo, este estudio se elaboró conforme a la doctrina clásica.

El tercer capítulo es titulado Régimen Jurídico, se trata el tema de organismos internacionales, legislación extranjera y por supuesto nuestra legislación aplicada a los delitos informáticos en su ámbito federal y los Códigos penales de algunos de los estados de la Republica Mexicana.

El capítulo cuarto, toca el punto medular del trabajo de tesis ya que se describen las conductas ilícitas de acceso a sistemas informáticos, la seguridad

informática y organismos vinculados con el combate y vigilancia de estos ilícitos.

El método de estudio que se utilizó en el Capítulo I es el deductivo por hablar de las generalidades e histórico por los antecedentes; el Capítulo II utilizo el método deductivo y analítico; el Capítulo III llevará el método exegético por ser el régimen jurídico y el Capítulo IV empleando el método deductivo y analítico, basándome en un tipo de estudio explicativo y descriptivo, a través de la investigación documental.

El objetivo primordial es proponer la creación de un tipo penal en el Distrito Federal que sancione el acceso ilícito a sistemas informáticos, planteando la siguiente hipótesis ¿Qué si es necesaria la creación de un tipo penal en el Distrito Federal que regule el acceso indebido a sistemas informáticos?

CAPÍTULO PRIMERO.
CONCEPTOS GENERALES.

1.1. INFORMÁTICA.

1.1.1. CONCEPTO.

Desde que el hombre tuvo la necesidad de contar, se tuvo que enfrentar al cálculo y la gestión en respuesta a esto, desarrolló máquinas que le ayudaran a solucionar estas tareas, con el paso del tiempo evolucionaron hasta desarrollar las computadoras u ordenadores.

La palabra informática es una acepción relativamente nueva derivada de los vocablos información y automática, sugerida por Phillipe Dreyfus[1] en el año mil novecientos sesenta y dos; el término se origina de la fusión de estos dos vocablos y hace alusión a la combinación de conocimientos científicos y de técnicas que hacen posible el tratamiento automático y lógico de la información por medio de computadoras.

Mora y Molino[2] lo definen como: "el estudio que delimita las relaciones entre los medios (equipo), los datos y la información necesaria en la toma de decisiones desde el punto de vista de un sistema integrado".

---

[1] Cfr. Téllez Valdez Julio. *Derecho Informático*. Ed. MC. Graw Hill. México. 2004. p.5.
[2] Ídem.

Pierre Conso define a la informática como: “la ciencia del tratamiento racional especialmente por medio de máquinas automáticas, de la información, considerada como soporte de los conocimientos humanos y de las comunicaciones, en los campos técnico, económico y social”[3].

El propio Philipe Dreyfus menciona su concepto de informática y la define como: “la ciencia del tratamiento automático o automatizado de la información, primordialmente mediante las computadoras”.[4]

Ahora señalaremos el concepto de sistema informático que es: conjunto de elementos necesarios para la realización y explotación de aplicaciones informáticas, es decir cualquier medio electrónico que organice, distribuya o almacene datos de cualquier tipo.

Por otra parte es necesario establecer la diferencia entre cibernética e informática lo cual es en que la primera emplea métodos científicos para explicar fenómenos de la naturaleza o en la sociedad y la forma de representación del comportamiento humano de forma simulada a través de una máquina, y la segunda estudia básicamente a las computadoras, sus elementos y la utilización de las mismas, la cibernética se apoya en la informática para su desarrollo.

[3] Pierre. Conso. *Informática y Gestión.* Ed. Técnicos Asociados. Buenos Aires. 1990. p.9.
[4] Ídem.

La informática tiene amplias aplicaciones dentro de las cuales destacan, almacenamiento de un gran volumen de información, realización de tareas repetitivas sobre una gran cantidad de datos, tratamiento de la información geográficamente, por ejemplo: sucursales bancarias; rapidez y precisión en la realización de cálculos matemáticos y científicos; manipulación de datos comunes para múltiples procesos.

1.1.2. ANTECEDENTES.

La primera herramienta que se utilizó para contar fueron los dedos de las manos y hasta la fecha lo seguimos utilizando, esta es la razón por lo que ocupamos el sistema decimal para representar números; en la cultura maya se usaban montones de piedras para representar cantidades, y algunas culturas usaban tablillas de arcillas o de cera; los asirios hacían agujeros en la arena colocando semillas en montoncitos; los griegos utilizaban tableros de cobre o mármol para el cálculo.[5]

El ábaco fue la primera máquina de cálculo y la seguimos utilizando hoy en día; la palabra ábaco encuentra su raíz etimológica en fenicia de la palabra abak (tabla lista cubierta de arena); estas tabletas de arcilla tienen una antigüedad de cuatro mil años, utilizadas para llevar registros de cuentas y prestamos en esa época, el Código de Hammurabi, ya mencionaba referencias de negocios como contratos, inventarios, ventas y otros tipos de operaciones; este instrumento esta compuesto de varias ranuras o varillas en las que se

[5] Cfr. Sánchez Solana Antonio Miguel. *Fundamentos de Informática*. Ed. Alfa-Omega Zima. México. 1999. p. 290.

encuentran pequeñas piezas con significado de unidades, decenas y centenas para realizar sumas y restas de forma fácil; regularmente se atribuye el crédito de la invención a los babilónicos, aunque aparece en varias culturas de la antigüedad, como en la India y Roma.[6]

El ábaco chino se inventó en el año 1200 d.C. aproximádamente y estaba formado por alambres y siete cuentas en cada uno, dos a un lado con valor de cinco y otras cinco al otro lado; el ábaco que hoy conocemos apareció a finales del Imperio Romano y sirve para multiplicar, dividir, restar y sumar. [7]

En el año 1614, John Naiper crea un método llamado tablas de logaritmos, a través de las cuales se podían realizar multiplicaciones en forma sencilla y rápida; las multiplicaciones se traducen en sumas y las divisiones en restas; Naiper era ayudado por su compañero H. Briggs para crear las tablas y sus algoritmos.[8]

Basándose en el método de Naiper, el inventor inglés William Oughtred construyo en 1621 el primer prototipo de regla de cálculo, el instrumento se basaba en la medición de longitudes entre dos pequeñas reglas que guardan relación de operandos y resultados, por consiguiente era un sistema analógico.[9]

---

[6] Ídem.
[7] Cfr. Téllez Valdez Julio *Derecho Informático* .Ed. MC Graw Hill. México. 2004. p.6
[8] Ibidem. p.291.
[9] Ibidem. pp.291-292.

Blaise Pascal, desarrolla el primer modelo de calculadora mecánica en 1642; consistía en un sistema de ruedas engranadas, en cada una estaban marcados los dígitos del cero al nueve; cada vez que completaba una vuelta la siguiente a la izquierda caminaba un elemento y así sucesivamente, dando como resultado la suma de varias cantidades; más adelante Gottfried Leibniz convierte la máquina aritmética de Pascal en un sistema mecánico capaz de restar, multiplicar, dividir y obtener raíces, por supuesto además de sumar.[10]

En 1804 el francés Joseph Marie Jacquard, construyo una máquina para tejer complicados diseños de telas; esta máquina se guiaba con tarjetas perforadas que contenían información del camino que debían seguir los hilos de la tela para lograr un diseño determinado. Jacquard se convirtió en el padre de las tarjetas perforadas.[11]

En Inglaterra en 1822 Charles Babbage diseño una máquina para el cálculo de funciones, capaz de actuar de diferente manera, según el programa que se le suministrara sobre datos introducidos en forma de fichas perforadas, esta no llego a ser fabricada por razones económicas y electrónicas de su época; poco después desarrollo su segunda máquina en 1833 denominada máquina analítica, se podía programar por medio de tarjetas perforadas, se basó en las ideas de Jacquard, también tenia un almacenamiento permanente de un número considerable de cifras el cual era de 1000 números de 50 cifras con 20 decimales de exactitud; Babbage no pudo ver realizado su invento ya que no había los suficientes componentes para la propia máquina, aunque no logró concretar su proyecto se le conoce como el padre da la informática.[12]

[10] Cfr. p.291.
[11] Cfr. p.292.
[12] Ídem.

Ada Augusta Byron, contemporánea de la época de Babbage, considerada la primera programadora de la historia, ya que ella desarrolló procedimientos para utilizar la máquina de Charles Babbage en la resolución de algunos problemas; la máquina de Babbage fue construida hasta el año de 1937, esto gracias a la ayuda de Ada, esto se refleja en que el lenguaje de programación de uso general para las computadoras u ordenadores se denomina ADA.[13]

En 1887, Herman Hollerith un estadístico que trabajaba para la oficina del censo de Estados Unidos de Norte América, concibió un sistema para el tratamiento de datos estadísticos llamado censadora, esta máquina al principio usaba tiras de papel con agujeros perforados de acuerdo a una clave, resulto poco práctica, así que desarrollo unas tarjetas de tamaño normal y el sistema finalmente uso tarjetas de tres por cinco pulgadas, con las esquinas cortadas, una prensa de alfileres, contadores electromagnéticos y una caja distribuidora; este invento procesaba 60 tarjetas por minuto, esta máquina logro hacer el censo poblacional en dos años cuando se hacia en diez; después del censo de 1890, hacia 1895, Hollerith, adaptó su equipo al uso de negocios incluyendo en su máquina la operación de sumar y construyendo un sistema de estadísticas de carga para líneas de ferrocarriles; Hollerith fundó en 1896 una compañía para explotar su invento, la Tabulating Machine Corporation (Compañía de Maquinas Tabuladoras), posteriormente se extendió el uso de máquinas Tabuladoras a otros campos de la industria y el comercio, se les llamó máquinas de registro unitario, utilizaban el mismo modelo de tarjetas perforadas de Hollerith; la empresa del inventor prosperó rápidamente y en el año de 1924 Thomas J. Watson adquiere la empresa y la convierte en la International Bussines Machines (Maquinas de Negocios Internacionales) mundialmente conocida como IBM, que aun hoy en día es una de las

[13] Ídem.

compañías más grandes en el mundo de las computadoras u ordenadores electrónicos.[14]

A principios del siglo XX, el ingeniero español Leonardo Torres Quevedo construyó una máquina automática, para jugar ajedrez; después presento un diseño de una máquina de calcular electrónicamente, pero no fue construida.[15]

Alan Turing matemático británico publicó un ensayo denominado Sobre números calculables, que establece las bases de la teoría matemática de la computación.[16]

En 1937, el profesor de la Universidad de Harvard, Howard Airen comenzó la construcción de una máquina de cálculo automático y electromagnético, por fin era la realización de la máquina de Babbage; el proyecto fue terminado en Harvard en 1944 con la ayuda de estudiantes graduados de su departamento e ingenieros de IBM, la maquina de Babbage no fue construida en su época por estar muy adelantado a su tiempo (1830) y no contaban con los materiales para poder realizarla.[17]

[14] Ídem.
[15] Ibidem. p.293.
[16] Ídem.
[17] Cfr. Sánchez Solana. Miguel Antonio. *Fundamentos* de *Informática*. sin/ed. Ed. Alfa-Omega Zama. México.1999.p.291.

1.2. DERECHO INFORMÁTICO.

1.2.1. CONCEPTO Y CLASIFICACIÓN.

El avance de la tecnología ha alcanzado todas las áreas del conocimiento humano, dentro la cual esta el Derecho, esto da lugar a una disciplina conocida como derecho informático: en la actualidad, la informática ha tocado todo quehacer humano, y cada vez se vuelve más compleja y por lo tanto el derecho protege estos recursos ya que se transformaron en herramientas de uso diario.

Julio Téllez Valdez define al derecho informático como "una rama de las ciencias jurídicas que contempla a la informática como instrumento y como objeto de estudio"[18].

El derecho informático se dice que es la relación que existe entre informática y el Derecho, regulando su creación, aplicación, estudio a través de normas jurídicas.

La clasificación del Derecho Informático obedece a dos vertientes fundamentales: la Informática jurídica y el Derecho de la informática, que más adelante se hablara de esto.[19]

[18] Cfr. Téllez, Valdez. Julio. *Informática Jurídica.* Ed. M.C. Graw Hill. México. 1997. p.13.
[19] Cfr. Téllez, Valdez. Julio. *Derecho Informático.* Ed. MC Graw Hill. México. 2004. p.21.

1.2.2. ANTECEDENTES.

En el año de 1949 con la obra de Norbert Wiener, en el capítulo IV llamado Derecho y de las Comunicaciones y menciona que influencia tiene la cibernética en el área jurídica, ésta se da a través de las comunicaciones.[20]

Lee Loevinger pública un artículo de 38 hojas en la revista Minnesota Law Review (Revista Legal de Minnesota) titulado The Next Step Forward (El Próximo Paso) que lo que sigue en el camino del progreso del hombre, debe ser de la transición de la Teoría General del Derecho hacia la Jurimetria, que se encarga de la investigación científica de los problemas jurídicos.[21]

1.3. INFORMÁTICA JURÍDICA.

1.3.1. CONCEPTO.

La Informática Jurídica nace como un instrumento al servicio del derecho es decir, con el avance de la tecnología hace que las computadoras se ocupen para cualquier manejo de la información.

Julio Téllez Valdez, describe a la Informática Jurídica como: “la técnica interdisciplinaria que tiene por objeto el estudio e investigación de los

[20] Ídem.
[21] Ídem.

conocimientos de la informática general, aplicables a la recuperación de información jurídica, así como la elaboración y aprovechamiento de los instrumentos de análisis y tratamiento de la información jurídica necesarios para lograr dicha recuperación"[22].

Otra definición es la da Emilio Suñé, y dice que es "la aplicación de los ordenadores electrónicos orientada la resolución de problemas jurídicos"[23].

Héctor Fix Fierro la entiende como "el conjunto de estudios e instrumentos derivados de la aplicación de la informática al Derecho, o más precisamente, a los procesos de creación, aplicación y conocimiento del Derecho"[24].

Para Enrique M. Falcón, define a la informática jurídica como:"el resultado del impacto de la computación en la ciencia del Derecho. En ella hay puntos de encuentro de distintas disciplinas; la documentación, la ciencia de la información, las matemáticas, la lógica, la lingüística y por supuesto el Derecho"[25].

Se dice que la Informática Jurídica es la ciencia del tratamiento y análisis de la información por medio de computadoras o dispositivos electrónicos aplicables al Derecho.

---

[22] Ibidem. p.26
[23] Ídem.
[24] Fix Fierro Héctor. *Informática y Documentación jurídica* Ed. UNAM. México. 1989:p. 56.
[25] Falcón M. Enrique *¿Qué es la Informática Jurídica? Del Ábaco al Derecho Informático.* Ed Abeledo Perrot. Buenos Aires.1992. p.90.

1.3.2. CLASIFICACIÓN.

La Informática Jurídica se divide en tres diversas ramas para su análisis u ordenación las cuales son: Informática Jurídica Documental, Informática Jurídica de Control y Gestión e Informática Jurídica Metadocumentaria o de Decisión.[26]

La Informática Jurídica Documental es el poder manejar y manipular información jurídica para facilitar su almacenamiento, clasificación y selección de ésta.

La segunda se dice que es la utilización de las computadoras en la organización y administración de los órganos encargados de crear y aplicar el Derecho. Es decir ayuda a resolver problemas cotidianos de Derecho, como tramites de expedientes judiciales, procedimiento legislativo, etc.

La Informática Jurídica Metadocumentaria o de Decisión tiene por objeto los estudios y aplicaciones que permitan a la computadora resolver por si misma problemas jurídicos a través de la simulación de procesos inteligentes o sirva de auxiliar al hacerlo.[27]

Desde nuestro particular de vista al parecer la Informática Jurídica es un espacio hecho para la elaboración teórica e instrumental de expertos en

[26] Cfr. Ríos, Estavillo José Juan. *Derecho Informático*. Ed. Instituto de Investigaciones Jurídicas UNAM. México. 1997. p.50.
[27] Ibidem. p.52.

computación, pero realmente sirve a cualquier persona que tenga nociones en computación y tenga una relación como, argumentación jurídica, análisis de sistemas normativos, almacenamiento de expedientes judiciales o simplemente con el mismo Derecho.

1.3.3. ANTECEDENTES.

En 1949 el jurista norteamericano Lee Lovinger planteo por primera vez la utilización de computadoras en el campo del Derecho en un artículo de la revista llamada Minnesota Law Review (Revista de Leyes de Minesota) llamado The Next Step Forward (El Siguiente paso Adelante); posteriormente en el año de 1963, Hans Baade edita la obra Jurimetrics: The methology of Legal Inquiry (Jurimetria: La Metodología de la información Legal), en la que especifica que para el desarrollo de esta materia se debían aplicar tres tipos de investigación:[28]

- En primer lugar, aplicar modelos lógicos a normas jurídicas establecidas según los criterios tradicionales;
- En segundo lugar, aplicar la computadora a la actividad jurídica y
- En tercero, llegar a prever futuras sentencias de los jueces

Las primeras investigaciones en el área de recuperación de documentos jurídicos, empezaron en los cincuentas; esto se logro gracias al esfuerzo del director del Health Law Center (Centro de Bienestar Legal) de la Universidad de Pittsburg llamado John Horta, él estaba convencido de la necesidad de

[28] Ídem.

encontrar los medios idóneos para el acceso a la informática legal; en 1959 este mismo Centro de Bienestar Legal, colocó los ordenamientos legales de Pennsylvania en cintas magnéticas; en 1960 en Washigton, D.C. se hizo la primera demostración de un sistema legal automatizado de búsqueda de información [29]

En Europa en los años de 1966 a 1969 utilizaron la computadora para hacer estadísticas judiciales, estudios de lógica formal aplicada al derecho, trabajos sobre normas jurídicas e investigaciones filosóficas del Derecho.[30]

Una siguiente incursión la hizo la Corporación de Investigación Automatizada de la Barra de Ohio (OBAR), en 1967 comenzaron a utilizar las computadoras para los abogados litigantes, la Barra de Ohio firmó un contrato en es mismo año con la Corporación de Datos de Dayton, Ohio. Los trabajos del sistema continuaron hasta que en 1970 a través de otra compañía se superó el sistema OBAR y en 1973 salió a la venta el sistema LEXIS como sistema de Informática Jurídica. [31]

En México, apenas en los años más recientes se ha despertado el interés por desarrollar sistemas de información jurídica, a pesar de que la computación tiene un desarrollo apreciable en el país y el problema del acceso a la información jurídica es real y apremiante.

[29] Cfr.Téllez Valdez Julio. *Derecho Informático*. Ed MC Graw Hill. México. 2004. p. 25.
[30] Ibidem. p.54
[31] Ibidem. P.27.

Entre los sistemas ya operativos pueden mencionarse:

- El Sistema UNAM-JURE, creado conjuntamente por el Instituto de Investigaciones Jurídicas y la actual Dirección de Servicios de Cómputo para la Administración, ambas dependencias de la UNAM y que se ha integrado al Sistema Nacional de Información Legislativa que coordina la Secretaría de Gobernación.
- El sistema del Centro de Informática Legislativa del Senado de la República (CILSEN), el cual opera tanto en el campo de la documentación como en el de la gestión parlamentaria.
- El Sistema de Información Legislativa de la Cámara de Diputados Federal.
- El sistema de la Suprema Corte de Justicia de la Nación, para la automatización de la Jurisprudencia y la gestión judicial.
- El sistema de la Procuraduría General de la República, destinado al control de las averiguaciones previas.
- El sistema del Tribunal Federal de Justicia Fiscal y Administrativa, sobre jurisprudencia fiscal.
- El sistema para la gestión y jurisprudencia de los Tribunales del Distrito Federal
- El sistema para la gestión de los tribunales del Estado de México.

Como parte del desarrollo de la informática jurídica en México debe hacerse notar, que numerosas oficinas de abogados y notarios se encuentran ya automatizadas y que, asimismo, empiezan a impartirse en instituciones públicas y privadas, cursos y seminarios sobre diversos aspectos de la relación entre informática y derecho.

1.4. DERECHO DE LA INFORMÁTICA.

1.4.1. CONCEPTO Y ANTECEDENTES.

Para Julio Téllez el Derecho de la Informática es "el conjunto de leyes, normas y principios aplicables a los hechos y actos derivados de la informática".[32]

Emilio Suñé la define como: "conjunto de normas reguladoras del objeto informática o de problemas directamente relacionados con la misma.[33]

Otro concepto lo proporciona Ríos Estavillo y señala que es: "el conjunto de normas jurídicas que regulan la creación, desarrollo, uso, aplicación de la informática o los problemas que se deriven de la misma en las que exista algún bien que eso deba ser tutelado jurídicamente por las propias normas"[34]

Los antecedentes del Derecho de la Informática los tenemos a finales de los años sesenta, se dieron inquietudes respecto del fenómeno informático que se suscitaba en esa época y después de diez años se necesitaba de un tratamiento especial a esta ciencia;[35]el Derecho de la Informática se divide en Política Informática y Legislación Informática.

---

[32] Ibidem. p. 21.
[33] Ríos Estavillo José Juan. *Derecho e Informática en México* .Ed. UNAM. México. 1997. p.73.
[34] Ídem.
[35] Cfr. Téllez Valdez Julio. *Derecho Informático.* Ed. MC. Graw Hill. México. 2004. p.21.

1.4.2. POLÍTICA INFORMÁTICA.

Prácticamente la Política Informática se refiere a los lineamientos o normas que regulan el Derecho de la Informática, de los cuales son:[36]

- Adecuado desarrollo de la industria de construcción de equipos de cómputo y de programación.
- Planeación, difusión y aplicación del fenómeno informático.
- Contratación gubernamental de bienes y servicios informáticos.
- Formulación de Normas y estándares en materia informática.
- Control de importaciones y exportaciones sobre equipos, accesorios y programas de computadoras.

1.4.3. LEGISLACIÓN INFORMÁTICA.

Se trata de la regulación de carácter jurídico preventivo y correctivo del uso inadecuado de la informática, es decir trata de reglamentar puntos específicos los cuales son:[37]

- Regulación de Bienes Informacionales: la información requiere de un tratamiento jurídico por su carácter económico.
- Protección de Datos Personales: Se refiere al atentado contra derechos fundamentales de las personas por el uso inadecuado de información privada.
- Regulación Jurídica de Internet: implica restringir información a través de sistemas de cómputo.

[36] Ibidem. pp.22-23.
[37] Ídem.

- Delitos Informáticos: sancionar los actos ilícitos en los que se contempla a las computadoras como instrumento para realizarlo.
- Contratos Informáticos: Es una categoría contractual derivada del uso de sistemas de computo.
- Comercio Electrónico: Es la forma de obtener bienes y servicios por vía del uso del Internet.

1.5. DELITOS INFORMÁTICOS.

1.5.1. CONCEPTO.

Para Téllez Valdez los Delitos Informáticos son: "actitudes contrarias a los intereses de las personas en que se tiene a las computadoras como instrumento o fin, o las conductas típicas, antijurídicas y culpables en que se tiene a las computadoras como instrumento o fin."[38]

Otro concepto de Delito Informático lo proporciona Ulrich Sieber y para él "comprende todas las lesiones dolosas e ilícitas del patrimonio relacionadas con datos procesados automáticamente"[39].

[38] Ibidem. p.163.
[39] Huerta M. Marcelo y Líbano M. Claudio. *Delitos Informáticos.* Ed. Jurídica ConoSur *Ltda*. Chile. 1998 p. 114.

Maria Cinta castillo Jiménez y Miguel Ramallo Romero lo definen como “toda acción dolosa que provoca un perjuicio a personas o entidades en cuya comisión intervienen dispositivos habitualmente utilizados en las actividades informáticas”[40].

Un concepto más completo es el de Marcelo Huerta M. y Claudio Líbano M. es “son todas aquellas acciones u omisiones típicas, antijurídicas y dolosas, tratase de hechos aislados o de una serie de ellos, cometidos contra personas naturales y jurídicas, realizadas en uso de un sistema de tratamiento de la información y destinadas a producir un perjuicio en la víctima a través de atentados a la sana técnica informática, lo cual, generalmente, producirá de manera colateral lesiones a distintos valores jurídicos, reportándose, muchas veces un beneficio ilícito en la gente, sea o no de carácter patrimonial, actué con o sin ánimo de lucro”[41].

La Organización para la Cooperación Económica y el Desarrollo define de manera extensa:”Cometerá delito informático la persona que maliciosamente use o entre a una base de datos, sistema de computadoras 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; también comete este tipo de delito al que maliciosamente y a sabiendas y sin autorización intercepta, interfiere, recibe, usa, altera, daña o destruye una computadora, un sistema o red de computadoras o los datos contenidos en la misma, en la base, sistema o red”.[42]

---

[40] Castillo Jiménez Maria Cinta; Ramallo Romero Miguel. *El Delito Informático*. Facultad de Derecho de Zaragoza Congreso sobre Derecho Informático. 22-24 junio. España. 1989. pp.564-581.
[41].Huerta M. Marcelo y Líbano M. Claudio. Op Cit. p.116.
[42] Ibidem p.117.

Se dice que Delitos Informáticos es cualquier acto cometido por persona física que cause un daño en su patrimonio, privacidad, intimidad, confidencialidad y derecho de propiedad a otra persona física o moral por medio de sistemas informáticos.

1.5.2. CLASIFICACIÓN.

Los Delitos Informáticos se clasifican según Ulrich Sieber en:[43]

- Delitos de Fraude mediante la manipulación de datos.
- Delitos de espionaje informático, piratería de software y sustracción de alta tecnología.
- Delitos de sabotaje informático.
- Delitos de sustracción de servicios.
- Delitos de acceso indebido.
- Delitos de fraude fiscal relacionados con en el uso de la computadora.

Aunque la clasificación de este catedrático alemán se acerca a entregar una cobertura amplia de estos hechos delictivos, el fraude fiscal ya esta tipificado en diversos códigos nacionales y protege otros valores.

[43] Huerta M. Marcelo y Líbano. M. Claudio. Op Cit. p.122.

Otra clasificación es la de Marcelo Huerta M. y Claudio Líbano M.[44] y clasifica como sigue:

- La manipulación indebida de datos a través de la utilización de un sistema de tratamiento de la información. Fraude Informático.
- Delitos de espionaje informático. Incluye formas de acceso no autorizado a sistemas informáticos.
- Delitos de sabotaje informático Incluye formas de destrucción y alteración de datos, así como los programas virus.
- Delitos de piratería de programas. Solo cuando se traduzca en la copia indebida de programas por medios informáticos.
- Delitos de Hacking en todas sus modalidades.

Las Naciones Unidas clasifican a los Delitos Informáticos en:[45]

Fraudes cometidos mediante manipulación de computadoras.

- Manipulación de datos de entrada: es la sustracción de datos, y lo puede cometer cualquier persona que tenga acceso a sistemas de procesamiento de datos.
- Manipulación de programas: Esto consiste en la modificación de programas ya existentes o insertar nuevos programas en la computadora, este delito lo va a cometer una persona que tenga conocimientos técnicos en informática, un ejemplo es el método conocido como Caballo de Troya que se basa en insertar instrucciones a la computadora de forma encubierta par que realice otra función.

[44] Ibidem. p.123.
[45] Cfr. Téllez Valdez Julio. Op Cit. pp.72-74.

- Manipulación de datos de salida: Se fija un objetivo el funcionamiento del sistema informático. Un ejemplo seria el de los cajeros automáticos, se clonan tarjetas de crédito a través de programas de computadora.
- Fraude efectuado por manipulación informática: Se aprovecha las repeticiones automáticas de los procesos de cómputo, un ejemplo es la transacción financiera de una cuenta a otra apenas imperceptibles también conocida como técnica de salami.

Falsificaciones informáticas.

- Como objeto: Cuando se alteran datos en los documentos almacenados en forma computarizada.
- Como instrumentos: Las computadoras pueden utilizarse para efectuar falsificaciones de documentos de uso común.

Daños o modificaciones de programas o datos computarizados.

Sabotaje informático: Es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con la intención de obstaculizar el funcionamiento normal del sistema; las técnicas que permiten esto son: virus, gusanos, bomba lógica o cronológica, etc.

Falsificaciones informáticas.

- Acceso no autorizado a sistemas y servicios: Puede ser cualquier motivo desde la simple curiosidad o los conocidos hakers.
- Piratas informáticos o Hakers: Este delito se realiza generalmente a distancia a través de la red de telecomunicación.

- Reproducción no autorizada de los programas de cómputo: esto no solo implica la reproducción sino el mismo tráfico a través de las redes de telecomunicaciones.

La clasificación hecha por las Naciones Unidas podría ser la más completa y por supuesto la mejor aceptada en varios países; pero, tiene inconvenientes, como la repetición en algunas clasificaciones de términos como piratas informáticos o hackers, o el delito de fraude informático en todas sus modalidades.

1.6. COMPUTADORAS.

1.6.1. CONCEPTO Y ESTRUCTURA.

La computadora es una máquina compuesta de elementos físicos electrónicos capaz de aceptar unos datos de entrada, realizar con ellos operaciones lógicas y aritméticas con gran velocidad y precisión y proporcionar los resultados por un medio de salida, todo ello sin la intervención de algún operador humano y bajo el control de un programa de instrucciones previamente almacenado en el propio dispositivo[46]; esto quiere decir que una calculadora no es una computadora porque requiere del control directo del usuario y solo realiza operaciones aritméticas.

[46] Cfr. Ureña López L. Alfonso. *Fundamentos de Informática*. Ed. Alfa-Omega. México.1999. p.2.

Otro concepto lo proporciona Téllez Valdez y es “máquina automatizada de propósito general, integrada por elementos de entrada, procesador central, dispositivo de almacenamiento y dispositivos de salida”[47].

Las computadoras tienen una estructura, es decir los elementos que la componen son:

Elementos de Entrada: Representan la forma de alimentación e información, por medio de instrucciones, programas y comandos realizada por el usuario, el dispositivo más común es el teclado o el ratón (mouse), otros dispositivos son un lápiz óptico, escáner, cámara Web, disquete, CD-ROM, etc.[48]

Dispositivos de Almacenamiento: Los sistemas informáticos pueden almacenar los datos tanto interna como externamente, la primera se hace por medio de chips de silicio llamados RAM. (Memoria de acceso aleatorio) y puede almacenar datos o instrucciones por un tiempo, es decir son como hojas de papel en los que se puede escribir, borrar y volver a utilizar; la otra parte lo conforma el ROM (memoria de solo lectura) y son los comandos, datos o programas que necesita la computadora para funcionar correctamente, éstos como, libros con palabras ya escritas, los dos, tanto RAM como ROM están enlazados al CPU a través de circuitos; las capacidades de almacenamiento de información internas llamada disco duro van desde 20 gigabytes(GB) hasta 250 gigabytes(GB); los sistemas de almacenamiento externos residen fuera de sistema informático y estos pueden ser: diskets o flopy disk inventado en los años setentas y estos solo tenían una capacidad de almacenamiento de

[47] Téllez Valdez Julio. Op.cit p.5.
[48] Cfr. Enciclopedia Encarta. Microsoft.2005.

información entre 100 y 500 KB, después fueron de 400 KB a 2.8 megabytes (MB) y los actuales d e 1.44 MB. El CD-ROM (Compact Disc-Read Only Memory), su capacidad de almacenamiento de información es de 640 MB a 1.2 GB, es decir solo se guarda información una vez y no se puede borrar o almacenar más, el CD-RW permite grabar miles de veces información y borrarla igualmente; el DVD-ROM este sistema permite almacenar 25 veces mas información que el CD-ROM, inclusive utilizarse por ambas caras y hasta dos capas de información por cara a diferencia que solo se puede usar una cara del CD-ROM este sistema permite almacenar audio y video, puede almacenar hasta 17 gigabytes (GB) de información; los dispositivos de tarjetas de memoria son otro tipo de sistema de almacenamiento muy utilizados en cámaras digitales, video cámaras digitales, PDA personal digital assistant (asistente digital personal) o teléfonos celulares, existen diversos dispositivos de este tipo entre los cuales destacan: Compact Flash (CF),Smart Media Card (SMC), Multimedia Card (MMC), Memory Stick (MS) y Secure Digital (SD) su capacidad de almacenamiento es desde 256KB hasta 512 MB; otro dispositivo son las memorias USB (Universal Serial Bus) su capacidad de almacenamiento de información es de 512 MB hasta 3.5 GB, y los llamados discos duros portátiles que tienen capacidad de almacenamiento de memoria desde 20 GB hasta 180 GB.[49]

Unidad Central de Proceso: Son una serie de chips que realizan cálculos aritméticos y lógicos, y que temporizan y controlan las operaciones de los demás elementos del sistema; en la actualidad su velocidad se mide en gigaherts. El CPU (Central Processing Unit por sus siglas en ingles) tiene cuatro secciones y son: una unidad aritmética/lógica; unos registros; una sección de control y un bus interno; la unidad aritmética/lógica proporciona al chip su capacidad de cálculo y permite la realización de operaciones aritméticas y lógicas; los registros son áreas de almacenamiento temporal que

[49] Ídem.

contienen datos, realizan un seguimiento de las instrucciones y conservan la ubicación y los resultados de dichas operaciones; la sección de control tiene tres tareas principales: temporiza y regula las operaciones de la totalidad del sistema informático; su decodificador de instrucciones lee las configuraciones de datos en un registro designado y las convierte en una actividad, como podría ser sumar o comparar, y su unidad interruptora indica en qué orden utilizará la CPU las operaciones individuales y regula la cantidad de tiempo de CPU que podrá consumir cada operación.[50]

El último segmento de un chip de CPU es su bus interno, una red de líneas de comunicación que conecta los elementos internos del procesador y que también lleva hacia los conectores externos que enlazan al procesador con los demás elementos del sistema informático.

Elementos de Salida: son lo medios en los que se recibe los resultados o manipulaciones de datos de la computadora y el más común es el monitor de la computadora que es VDU (Video Display Unit) que es como la pantalla de un televisor y actualmente de LCD (Liquid Cristal Displays), otros dispositivos son la impresora o el MODEM para conectarse a través de la red telefónica a Internet.[51]

Sistema Operativo: esta constituido por un programa de control principal almacenado de forma permanente en la memoria interpretando los comandos

[50] Ídem.
[51] Ídem.

del usuario que solicita como visualizar un archivo, copia de un dato o impresión del mismo, etc.[52]

Hardware: esta constituido por estructura física de la computadora, partes mecánicas, electromecánicas y electrónicas, es decir el monitor; CPU, teclado, etc.; las computadoras tienen casi siempre el mismo tipo de Hardware, pero algunos varían de acuerdo a su costo y tamaño como las computadoras portátiles o laptop o las supercomputadoras de universidades o departamentos de gobierno.

Software: este es la estructura lógica de las computadoras para realizar las actividades que se le ordena, es decir son las instrucciones que se le dan para realizar las operaciones con los datos; comúnmente se le conoce al software como programas y estos pueden estar almacenados en el propio hardware o pueden existir de manera independiente.

1.6.2. CLASIFICACIÓN.

Las computadoras se clasifican de acuerdo a las funciones que pueden realizar y sus aplicaciones:[53]

Computadoras Digitales: Pueden realizar dispositivos de cálculo que realiza valores discretos. Trabaja con números representándolo en valores, letras, cifras u otros símbolos, lo hace como un reloj digital que cuenta los

[52] Ídem.
[53] Del Pozo. Maria Luz. *Informática en Derecho.* Ed. Trillas. Madrid.1992.pp.28-35.

segundos y minutos para acumular horas y días, así la computadora cuenta los valores para alcanzar los resultados deseados, estas se subdividen en:

- Macrocomputadoras: Se caracteriza por tener una gran velocidad de proceso y almacenamiento de datos y producción de resultados, puede almacenar miles de archivos dentro de los cuales hay millones de datos, su costo es muy elevado, algunos ejemplos son las computadoras de sistemas de defensa como la del Pentágono en Washington Estados Unidos De Norteamérica o en Instituciones de Investigación científica.

- Minicomputadoras: Tienen una capacidad de proceso por debajo de la macrocomputadora al igual que su capacidad de almacenamiento, su costo es menor, por supuesto, pero no tanto como una computadora personal, éstas pueden estar en grandes empresas, hospitales de alto nivel, Universidades, laboratorios, etc.

- Microcomputadoras: Son las conocidas como computadoras personales o PC. (en ingles: personal computer), contiene las instrucciones o programas necesarios para realizar tareas diversas, están presentes en los hogares, oficinas, escuelas, etc. debido aun costo promedio no muy alto, hoy en día existen las denominadas computadoras portátiles o laptop, o las PDA personal digital Assistan (asistente digital personal).

Computadoras Analógicas: Es un dispositivo electrónico o hidráulico diseñado para manipular la entrada de datos por medio de magnitudes continuas, por ejemplo: niveles de tensión o presiones hidráulicas en lugar de numéricas. Un ejemplo común serian las bombas de gasolineras que convierte

el flujo de combustible en la cantidad en litros y precio de la cantidad de gasolina suministrada, otro ejemplo son las básculas de los supermercados o tiendas de abarrotes, que se les suministra el precio por unidad y automáticamente proporciona el peso y precio del producto adquirido.

Computadoras Híbridas: es la combinación de computadoras analógicas y digitales, un ejemplo seria en el diseño y fabricación de aviones, la computadora analógica simula el comportamiento de un avión no construido y la computadora digital alimenta de las condiciones atmosféricas y comportamiento del avión, para que se determine su comportamiento, seguridad y resistencia, antes de construirlo.

1.6.3. ANTECEDENTES DE LAS COMPUTADORAS.

Primera Generación.

La primera máquina que llevó a la realidad el sueño de Babbage fue la Mark I ocurrido en 1944 en la Universidad de Harvard con el apoyo de IBM realizado por Howard Aike, fue la primera computadora electrónicamente automática, era capaz de realizar secuencias de operaciones codificadas y la registra en papel perforado.[54]

La ENIAC Electronic Numerical Integrator and Calculator (Calculador e integrador numérico electrónico), es el primer sistema totalmente electrónico, surgió en 1945, se utilizó principalmente para resolver problemas de balística y

[54] Cfr. Huerta M. Marcelo y Líbano M. Claudio. Op.cit. p.5.

aeronáutica, fue construida por J. V. Atanasoff y C. Berry bajo la dirección del ingeniero eléctrico J. Presper Eckert y el físico Jonhn W. Mauchly.[55]

Entre 1948 y 1952 surge la EDVAC Electronic Discrete Variable Automatic, era capaz de hacer operaciones aritméticas y realizar algunas instrucciones. En 1951 surge la UNIVAC-I Universal Automatic Computer (Computadora automática universal), se caracteriza por permitir un almacenamiento de datos en forma secuencial y transfería de manera más rápida los mismos, esta fue diseñada por John W. Mauchly, es la primera computadora de serie puesta a la venta; surgen los modelos 650,701 y 702 de IBM; en 1951 se instala una UNIVAC-I en la Oficina del Censo de Estados Unidos y en 1954 la General Electric es la primera compañía privada en utilizar industrialmente la UNIVAC-I;[56] el uso fundamental durante esta primera generación de computadoras era la realización de aplicaciones en el campo científico y militar (resolución de ecuaciones lineales y diferenciales, tablas balísticas, etc.).

Segunda Generación.

La primera computadora con transistores fue la TRADIC Trasistorized Digital Computer (Computadora Digital Transistorizada) construida por los laboratorios Bell en 1954; en 1960 IBM puso a disposición su primera computadora con transistores el modelo IBM 7070; la compañía Sperry Rand obtiene también su primera computadora transistorizada la UNIVAC 1107.[57]

[55] Cfr. Ureña López L. Alfonso. *Fundamentos de Informática.* Ed. Alfa-Omega. México.1999.p.295.
[56] Ibidem. p 296.
[57] Ibidem. p.297.

En 1957 IBM desarrolla el sistema FORTRAN que es el primer lenguaje de programación de alto nivel, que permitía a los programadores escribir procedimientos sin tener que conocer el funcionamiento de la computadora, estaba orientado fundamentalmente a cálculos científicos; la primera versión fue mejorada Fortran II (1958); Fortran III (1959);Fortran IV (1970) y Fortran 77 (1977). Desde 1954 hasta 1964 surgen varios tipos de programas como ALGOL, COBOL, APT, JOVIAL, GPSS, SIMULA, JOSS y PL/I.[58]

Tercera Generación.

Entre 1963 y 1964 surge el BASIC Beguinners All-Purpose Symbolic Instruction Code (código simbólico de propósito general para la enseñanza de participantes), este lenguaje para computadoras era para la enseñanza, era un lenguaje interactivo; en 1979 Microsoft crea el primer sistema BASIC para Microcomputadoras; este sistema operativo mantenía un lazo entre el usuario y la computadora; los lenguajes de programación comienzan a ser más fáciles de aprender; en esta etapa surge la Teleinformática, (principios del Internet) sirve para acceder a otras computadoras utilizando redes telefónicas comunicándolas entre ciudades diferentes, solo para computadoras de gran tamaño.[59]

Cuarta Generación.

En 1970 los técnicos de INTEL Corporation consiguieron concentrar todos los componentes de un procesador en una pastilla de silicio con un tamaño aproximado de 1 cm., había nacido el microprocesador; ya no era necesario

[58] Cfr. Huerta M. Marcelo y Líbano M. Claudio. Op.cit. pp.5-8.
[59] Ibidem pp.9-11.

ocupar un gran espacio, sino que en un espacio pequeño cabía, teclado, monitor y procesador; en esta época se centran las investigaciones en las microcomputadoras; a principios de los años ochentas, éstas se interco-municaban para compartir recursos como impresora, programación, etc. [60]

En 1977 la empresa INTEL, desarrolla el microprocesador 8008, después crea el en 1974 modelo 8080: en 1975 se produjo las primera PC, el Altair, producido por la compañía MITS en Alburquerque, Nuevo México; en 1977 la compañía de computadoras Aplee produce la Aplee II, también aparece la TRS-80 de Radio Shack y la PET 2001, de Commodore; en agosto de 1981 IBM lanza sus computadora personal (PC), la cual tenia un teclado y una entrada para conectar la reproductora de audiocasetes, utilizaba como monitor el aparato de TV, a principios de 1983, Aplee produce LISA la primera computadora comercial con un sistema operativo grafico, esta ya incorpora el ratón (mouse), pero no tiene demasiada aceptación; en 1984 Aplee crea la computadora Macintosh despertando un gran interés, e IBM lanza el PC AT esta computadora utilizaba el procesador 80286 de INTEL, mucho más rápido que el anterior, estableció un nuevo estándar de PC.[61]

A finales de los años setentas aparecen las impresoras de margarita ya que anteriormente eran como una máquina de escribir conectadas a la computadora, posteriormente las térmicas, las de tinta, y hoy en día las de láser; se crean nuevos periféricos de entrada como: los lectores de códigos de barras, lectoras de tintas magnéticas (cheques), lectores ópticos, etc.[62]

[60] Ibidem. pp.11-13.
[61] Cfr. Ureña López L. Alfonso. Op Cit p.299.
[62] Cfr. Huerta M. Marcelo y Líbano M. Claudio. Op.cit. pp.12-13.

Quinta Generación.

A mediados de los ochentas surgieron las computadoras capaces de interactuar con el usuario, con gráficos, sonidos (multimedia) tienen una base de datos que les permite manejar grandes volúmenes de información, tratamiento de textos, es decir, como una máquina de escribir pero mejorada; procesamiento de gestión, como contabilidad, facturación, hoja de calculo; ideales para el hogar o la oficina; aquí surge la llamada IA Inteligencia Artificial, surge para que realice funciones intelectuales similares a las del hombre y lograr una comunicación hombre-máquina lo más natural posible, aunque esta ciencia tuvo sus primeros albores desde 1956.[63]

Las computadoras evolucionan de acuerdo a las necesidades de una sociedad que requiere mejores equipos de información en dispositivos más compactos. A finales de los ochentas surgieron las primeras computadoras portátiles (laptop) que son usadas como herramientas en oficinas, escuelas o institutos de investigación y por supuesto en el hogar ocupan poco espacio y son fáciles de transportar, al igual que una computadora personal (PC) tiene teclado y una pantalla, tiene la forma de una carpeta, cuenta con disco duro y entradas para disquete, CD-ROM y DVD-ROM así como otros dispositivos de almacenamiento de información, utilizan una batería recargable para sus funcionamiento o directamente conectadas a la corriente eléctrica; también en los ochentas nacieron las llamadas PDA personal digital assistant (asistente digital personal), la primera fue la llamad Newton de Aplee, era muy grande ,cara y difícil de maniobrar, pero no es hasta que la compañía PALM crea en 1996 su primera

[63] Ibidem. pp.14-15.

PDA llamada PALM PILOT era pequeña como para caber dentro de la bolsa del pantalón; estos sistemas permiten trasportar a cualquier lado información o datos por su tamaño de la palma de una mano y su pantalla táctil, es decir con una pluma sin tinta por medio de trazos en la pantalla se escribe, no tiene disco duro pero si las llamadas tarjetas de memoria para almacenar información, tiene capacidad para procesador de textos y hoja de cálculo, así como dispositivos internos de cámara y video cámara, música en formato MP3, utilizan una batería recargable o pilas alcalinas para poder funcionar, su costo es mucho menor a la de una computadora portátil, se pueden sincronizar con una (PC) es decir se trasladan los archivos de información a la computadora y se pueden guardar; estos sistemas informáticos utilizan los dispositivos Blueetoth e infrarrojo por medio de radiofrecuencia se pueden intercomunicar y obtener datos entre PDA, PC y computadoras portátiles (Laptop).[64]

El Internet es la interconexión de redes informáticas que permite comunicar una computadora con otra en cualquier parte del mundo por medio de una línea telefónica (LAN) o sistema inalámbrico (WLAN) de fibra óptica o enlaces por radiofrecuencia; este sistema funciona con redes interconectadas entre si por medio de una computadora denominada gateway (puerta); el IP (protocolo de Información) es el soporte lógico para controlar el sistema de Internet, este protocolo especifica como las getaway encamina la información de una computadora emisora a una receptora, otro protocolo denominado Protocolo de Control de Transmisión (TCP) esta comprueba si la información ha llegado a su destino y en caso contrario hace que la vuelva a enviar; este sistema proporciona información de cualquier tipo por medio del http que es protocolo de transferencia de hipertexto este protocolo lee e interpreta ficheros de texto

[64] http://www.entarate.unam.mx- 22-octubre 2005 11:30 hrs.

imágenes, video o sonidos; Internet también permite intercambiar mensajes de correo electrónico (e-mail), noticias, foros de debate, comercio electrónico y conversaciones en tiempo real (Chat, IRC, videoconferencia) entre otros servicios; la WWW (World Wide Web) también conocida como Web es una colección de ficheros de información en forma de textos, gráficos, sonidos y video, además de vínculos con otros ficheros estos ficheros son recuperados por un localizador universal de recursos (URL siglas en ingles) que especifica el protocolo de transferencia, la dirección de Internet y el nombre del fichero por ejemplo un URL podría ser http://www.unam.com.mx; la historia de Internet se remonta a finales de los años cincuenta donde el Departamento de Defensa estadounidense creó una red para mantener segura sus nodos así nació ARPA, más adelante surgió Arpanet era un Internet pero incipiente solo conectado a universidades, institutos de investigación en Norteamérica, esta red se creó en 1973; Arpanet dejo de existir en 1990; a finales de 1989, el informático británico Timothy Berners-Lee desarrolla la World Wide Web para la Organización Europea para la Investigación Nuclear, más conocida como CERN;su objetivo era crear una red que permitiese el intercambio de información entre los investigadores que participaban en proyectos vinculados a esta organización; el objetivo se logró utilizando archivos que contenían la información en forma de textos, gráficos, sonido y vídeos, además de vínculos con otros archivos;[65] en cuanto al sistema inalámbrico de Internet (WLAN) se remonta a los años 70, los orígenes de las redes de área local inalámbricas, WLAN (Wireless Local Area Network);fue en una fabrica suiza donde se obtuvieron los primeros resultados satisfactorios de comunicación inalámbrica dentro de una red local, desde entonces, las actividades hacia investigación y desarrollo de dispositivos que hacen posible las redes de esta naturaleza se han intensificado; utilizan ondas electromagnéticas para transportar información de un punto a otro sin necesidad de una conexión física; las ondas de radio frecuencia a menudo se refieren como portadoras de radio, debido a que su única función consiste en entregar la energía que conllevan al receptor remoto; los datos que se desean transmitir se superponen sobre la portadora de forma

[65] Cfr. Enciclopedia Encarta. Microsoft.2005.

tal que en el lado receptor puedan ser precisamente recuperados, este proceso es conocido como "modulación de la portadora", por la información que se desea transmitir; el punto de acceso o la antena asociada al punto de acceso usualmente se monta en un punto alto, sin embargo, puede colocarse en cualquier lugar práctico, siempre y cuando se obtenga la cobertura deseada; los usuarios acceden la WLAN a través de adaptadores inalámbricos, implementados en tarjetas PC para computadoras portátiles (Laptops), adaptadores ISA o PCI para computadoras de escritorio o mediante adaptadores totalmente integrados en asistentes personales digitales (PDA); el sistema llamado WIMAX Worldwide Interoperability for Microwave Access (de ahí el nombre corto WiMAX) es el sistema inalámbrico más nuevo, funciona de manera muy similar a la telefonía celular; el principal componente es una antena colocada en una torre con una cobertura de hasta 7500 kilómetros cuadrados; el segundo elemento es el receptor WiMAX, que puede ir desde una caja colocada en el techo de la casa, hasta algo tan pequeño como una tarjeta PCMCIA en una computadora portátil o PDA.[66]

Los teléfonos celulares denominados de tercera generación (3G) no solo se usan para hacer y recibir llamadas sino mandar mensajes cortos (SMC), mensajes multimedia (MMC) con imágenes y video, tomar fotografías y video grabar, reproducir archivos de música en formato MP3, pueden recibir y enviar correo electrónico (e-mail) y utilizar el Internet por medio de su micronavegador; integran infrarrojo y bluetooth así como ver programas de TV; y ahora tienen capacidades de una PDA es decir pueden trabajar con un

[66] http://www.entarate.unam.mx-22 enero 2006 16:15 hrs.

procesador de textos o una hoja de calculo y guardar archivos en su tarjetas de memoria.

CAPÍTULO SEGUNDO.
EL DELITO.

2.1. CONCEPTO.

Delito es para Jiménez de Asúa "la acción determinada por motivos individuales y antisociales que altera las condiciones de existencia y lesionan la moralidad de una sociedad en un momento determinado."[67]

Podría entenderse que delito seria el hecho del hombre, por que solo este puede cometer un delito, que infringe las relaciones fundamentales de la sociabilidad, prohibida por la ley, determinado por motivos antijurídicos y antisociales. El Artículo 7° del Código Penal Federal dice:

TITULO PRIMERO
REPONSABILIDAD PENAL
CAPITULO I
REGLAS GENERALES SOBRE DELITOS Y RESPONSABILIDAD

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

Existen numerosos conceptos acerca del Delito, ya sea en términos sociales y naturales, pero el que nos interesa es el jurídico, para lo cual para que exista el

[67] Jiménez de Asúa Luis. *Teoría del Delito* .Ed. Iure Editores. México. 2002. p.22.

delito es necesario que la voluntad humana se manifieste externamente en una acción o en la omisión de una acción. No se puede dejar de mencionar a la conducta que, aunque, se tratará por separado en este estudio acompaña al delito; la acción y la omisión deben ser típicos es decir que los describa la ley penal (tipicidad), es decir las leyes penales los individualizan en conductas punibles, pero el tipo solo es descriptivo ;otra característica del delito es que sea antijurídico, que se hallen en contradicción del derecho, para que no existan permisos o autorizaciones llamados causas de justificación, como legitima defensa, cumplimento de un deber, etc.; la última característica es que sea culpable, es decir que exista un reproche hacia el delito por esa conducta hecha, el sujeto que comete el delito debe tener la característica de ser imputable es decir la capacidad de comprender este acto delictivo.

El delito puede ser doloso y culposo, el primero tiene el sujeto el propósito y la intención de cometerlo y el segundo es un deber de cuidado o falta de atención o vigilancia que se tuvo en un actuar, en el dolo hay un elemento volitivo se quiere la conducta y el resultado y un elemento intelectual, y en la culpa solo hay predicibilidad y una conducta negligente, es decir que no presta la atención debida, pero estos conceptos los analizaremos más adelante.

2.2. TEORÍA DEL DELITO.

La teoría del delito es una parte del Derecho penal y estudia los elementos positivos y negativos del delito y como se manifiestan, los elementos positivos hacen posible la existencia de éste y los negativos hacen que no exista y su manifestación es como se presenta el mismo.

Esta rama del Derecho Penal es muy delicada y por eso se han formulado diversas teorías, entre las cuales destacan la Teoría Causalista y Finalista del Acción y Teoría Sociologista.

Teoría Causalista y Finalista de la Acción.

La acción es un aspecto del delito y para la teoría Causalista "es un comportamiento humano dependiente de la voluntad, que produce determinada consecuencia en el mundo exterior. Dicha consecuencia puede consistir en el puro movimiento corporal, o en movimientos corporales seguidos del resultado ocasionado por el mundo exterior."[68]

Esta teoría maneja la acción como una forma causal del resultado y no toma en cuenta las intenciones que lo orillaron a cometerlo. Los causalistas explican que hay un delito cuando el sujeto tiene voluntad de realizarlo y no toman en cuenta la finalidad que tenía este al hacerlo, es decir a la acción simplemente se le considera como un hacer voluntario pero no tiene realmente un porque si no solo se enfoca al resultado.

Para Zaffaroni la acción "es una inervación muscular, es decir un movimiento voluntario no reflejo pero en el que carece de importancia o se prescinde del fin a que esa voluntad se dirige".[69]

---

[68] Jescheck, Hans-Heinrich. *Tratado del Derecho Penal Parte General*, Vol. I, 3ra. Ed., Ed. Bosch, Barcelona. 1989. p.292.
[69] Zaffaroni, Eugenio Raúl. *Manual de Derecho Penal Parte General.* 2da ed. Ed. Cárdenas Editor y Distribuidor. México 1991. pp.369 y 370.

La teoría finalista dice “La acción no es solo un procesó casualmente dependiente de la voluntad, sino por su propia esencia, ejercicio de la actividad final. La finalidad obedece a la capacidad del hombre de prever, dentro de ciertos limites, las consecuencias de su comportamiento causal y de conducir el proceso, según un plan a la meta perseguida mediante la utilización de recursos”.[70]Para los finalistas la acción se realiza desde que el sujeto razona su objetivo, eligiendo los instrumentos para lograrlo, y finalmente realiza su objetivo manifestándolo externamente.

El concepto final de la acción no abarca el comportamiento humano en delitos penales por ejemplo los delitos cometidos por imprudencia, no se tiene la intención de cometerlos pero por una acción descuidada lo realiza. La teoría Causalista considera la acción como mecánica algo causal y la teoría Finalista determina el propósito del producto causal, en pocas palabras la voluntad dirigida en un sentido; Para los causalistas la voluntad debe aparecer en otro lugar de los elementos del delito y dicen que debería ser en el dolo que es una especie de culpabilidad.

La teoría Causalista no se puede aceptar ya que el sujeto piensa y medita su acción delictiva, no solamente se necesita realizar la acción, para haber un comportamiento humano encaminado a una dirección es necesario anticiparse al resultado, es decir no solo exteriorizarlo como un fenómeno natural o voluntario.

Teoría Psicologista y Normativista de la Culpabilidad.

La teoría Psicologista dice que la culpabilidad consiste en un nexo entre un sujeto y su conducta o resultado material según sea el caso. La culpa existe siempre y

[70] Ibidem. p.293.

cuando exista el nexo causal, pero en el caso de negligencia esta queda fuera del pensamiento porque es solamente falta de apreciación. Esta teoría no puede aceptarse ya que no solamente se necesita del dolo o la culpa para integrarla, necesita la imputabilidad entre otros elementos.

Por otro lado en la teoría normativa el dolo y la culpa son un mismo elemento, donde el dolo es una especie de culpabilidad es un motivo reprochable y la culpa es un elemento de imputabilidad. Para la corriente Normativa la culpabilidad es un juicio de reproche, es decir la reacción social o jurídica que se tiene por haber cometido un delito. La reprochabilidad puede existir solo cuando el sujeto se le exija una conducta distinta a la realizada, es decir pudo haberlo cometido el delito porque no lo hizo conforme a derecho en lugar que si lo hubiera hecho.

Teoría Sociologista del Delito.

Esta teoría maneja que el delito proviene de un fenómeno social y natural, es decir aquellas acciones que trascienden a terceros y no individualmente. Zaffaroni dice que “los autores que se alinean bajo este estandarte, comienzan a divergir, hasta que las misma teoría deja de ser tal para quedar reducida a escombros teóricos diversiformes que dan pie a estructuras del delito con injusto objetivo o con injusto complejo, con culpabilidad mixta o normativa, es decir que según las referencias del autor que toma la teoría debido a la nebulosidad de la

misma, adoptará la estructura del delito que compagina con la teoría finalista o la causalista".[71]

Siguiendo la misma línea se afirma que el delito de violación mediante acciones socialmente nocivas, de los sentimientos altruistas fundamentales de piedad y probidad, en la medida que son poseídos por una comunidad, en que aquella medida indispensable para la adaptación del individuo a la sociedad.[72]Dicen los sociologistas la acción será relevante en la medida que un individuo tenga efectos en su sociedad, también mencionan que no son acciones las múltiples actividades sociales de dos personas, tampoco hay una acción en una inactividad frente a una posibilidad de acción porque le falta al sujeto su capacidad de acción y por consiguiente excluyen todos los procesos psíquicos (sentimientos, actitudes, etc.).

Para los sociologistas no es esencial el hecho de que la acción produzca un cambio en el exterior, si no que haya una relación valorativa con su entorno social; Esta teoría contempla la acción como la simple producción de actuar separando el contenido de la voluntad; el derecho penal no puede aceptar un concepto de acción separado de la voluntad, se puede aceptar que el actuar sea un fenómeno social pero que tenga un sentido al realizarlo, es decir toda acción debe tener voluntad, que tengan un propósito su realización; no solo es necesario tener voluntad sino que esa misma voluntad este dirigida hacia un objetivo determinado.

[71] Zaffaroni. Eugenio. Raúl. *Manual de Derecho Penal Parte General*. 2da ed. Ed. Cárdenas Editor y Distribuidor, México. 1991. p.374.
[72] Cfr. López Betancourt. Eduardo. *Teoría del Delito*. 7ma ed. Ed. Porrúa. Buenos Aires. Argentina.1992. p.21.

2.3 PRESUPUESTOS DEL DELITO.

2.3.1 SUJETO ACTIVO.

En épocas pasadas se llego a considerar que los animales y objetos sin vida podían cometer delitos; Por supuesto se sabe que para delinquir se necesita voluntad y conciencia, algo que solo le concierne al hombre, por lo tanto solo él puede realizar una conducta delictuosa y castigada por las leyes penales, ya sea que lo realice por si solo como autor material e intelectual o auxiliado por otros.

Atendiendo a lo mencionado, sólo las personas pueden ser responsables de la comisión de delitos, en razón a esto se han creado diversas teorías, como la formas de peligrosidad en los individuos y los mismos delitos. Una teoría es la del médico llamado Cesar Lombroso, el cual se baso en investigaciones en establecimientos penitenciarios y mencionaba en sus estudios que existía el delincuente nato el cual era una persona con anomalías somáticas y psíquicas tendiente a convertirse en un delincuente, aun viviendo en condiciones favorables para su desarrollo, esta teoría es del tipo sociologista anteriormente mencionada; el sujeto activo es la persona que realiza u omite un actuar en un delito.

El artículo 22 del Nuevo Código Penal para el Distrito Federal menciona las personas responsables del delito:

I. Los que lo realicen por si (Autor Material); es quien realiza el delito lo ejecuta directamente y puede ser tanto de acción como de omisión, siempre es una conducta típica.

II. Los que lo realicen conjuntamente (Coautor Material); se le considera al que en unión de otros autores, ejecutan el delito haciendo conductas descritas en el Código Penal, cada coautor material es responsable de su propio acto, cada uno tiene su objetivo de común acuerdo previo, no se puede presentar la coautoría en delitos imprudenciales, ya que no hay intención de cometerlos, solo serían participes, si cabe la omisión en la coautoría.

III. Los que lo lleven a cabo sirviéndose de otro como instrumento (Autor mediato); hace uso de otra persona para cometer el delito, puede ser un individuo lo más cercano posible incluyendo un inimputable como un menor de edad o con trastornos mentales.

IV. Los que determinen dolosamente al autor cometerlo (Autor intelectual); realiza acciones encaminadas a realizar el delito puede ayudar al autor material instruyéndolo o participando directamente en la ejecución del mismo.

V. Los que dolosamente presten ayuda o auxilien a otro para su comisión (Asociación delictuosa);es cuando dos o más sujetos en unión actúan para cometer un delito y este no solo debe ser ocasionalmente sino permanente como los secuestradores, falsificadores, ladrones de bancos, actualmente estas asociaciones se reúnen para cometer el delito y luego se disuelven.

VI Los que con posterioridad a su ejecución auxilien al delincuente, en cumplimiento de una promesa anterior al delito(Encubridor); es o son los que ocultan a los sujetos del delito o los instrumentos del mismo, saben con anterioridad que se cometerá un delito y pueden ser también encubridores cuando disfrutan de las ganancias del mismo.

El sujeto activo es la persona que realiza la conducta típica antijurídica que menciona el Código Penal con expresiones como “al que” “el responsable” o “al que”, etc., describiendo al individuo.

Cuando en ocasiones el tipo penal exige determinadas características del sujeto, se originan los llamados delitos especiales, es decir el tipo exige determinada calidad del sujeto activo para ser autor del delito y poder integrar el mismo.

La participación de los sujetos que cometen un delito, se les nombra de diferente manera, como la coparticipación; existen diversas formas de intervención y a cada una se les da un tratamiento especial, esto depende en el modo en que cada sujeto haya participado en el delito

2.3.2. SUJETO PASIVO.

Eduardo López Betancourt menciona que es sobre quien recaen todos los actos realizados en el ilícito, es la persona que sufre directamente la acción delictiva, es decir el titular del derecho dañado o puesto en peligro[73].

Wiarco señala “es el titular del bien jurídico tutelado y es la persona física o moral incluyendo el Estado que sufre directamente los efectos de la conducta delictiva; es sobre quien recae material o jurídicamente la acción u omisión, ejecutado por el sujeto activo”[74]

[73] López Betancourt Eduardo. *Teoría del Delito*.7ma ed. Ed. Porrúa. México. 1999 p 52-53.
[74] Wiarco Arrellano. Alberto Octavio *Curso de Derecho Penal*. 2da ed. Ed.Porrua. México. 2001. p.472.

La persona es la que tiene el mayor número de bienes jurídicos tutelados, protegiéndolo toda su vida el Derecho Penal, es decir un ser es protegido desde que es viable en el seno materno hasta su muerte. En el caso de un cadáver los sujetos pasivos serian los familiares por ser ellos los titulares del bien jurídico protegido; las personas jurídicas colectivas también pueden ser sujetos pasivos en la realización de un delito, el mismo Estado puede serlo o asociaciones sociales; en el proceso penal ordinario se le denomina ofendido al sujeto pasivo, e igualmente a sus sucesores al ser este privado de la vida o que tenga una incapacidad. El artículo 20 de la Constitución Política de los Estados Unidos Mexicanos en su apartado B menciona las garantías que tiene el ofendido en un proceso penal cuando es victima de un delito.

2.3.3. OBJETO MATERIAL.

Es sobre lo que debe recaer la ejecución del delito, objeto material del delito puede ser tanto una persona como una cosa; si es una persona física, ésta deviene con ello sujeto pasivo de la acción delictuosa, según acontece en incontables tipos de delito: homicidio, lesiones, privación ilegal de libertad, amenazas, atentados al pudor, violación, etc. Si es una cosa, puede la acción delictiva consistir en crearla o alterarla, como en la falsificación de monedas y de documentos; en destruirla, como en el delito de daño en propiedad ajena; en desplazarla de la esfera de tutela de otra persona, como en el robo, etc.[75]

[75] Cfr. López Betancourt Eduardo. Op.Cit. p. 53.

Por lo que hace al objeto material, la formulación que antecede afirma que la descripción legal respectiva tiene por tal de donde se infiere que no constituyen objeto material, en sentido jurídico, las cosas materiales con que se cometió el delito, o constituyen su producido, o son huellas de su perpetración, pues ellas conciernen al episodio delictivo concreto y no a su abstracta previsión legal.

El objeto material pertenece al mundo fáctico y por lo tanto es corporal y puede ser una persona como una cosa, en resumen el objeto material es toda persona o cosa que forme parte del tipo descrito por la ley; el objeto material se puede identificar, y seria comprensible que no solo es sobre quien recae la conducta sino también aquello a quién se dirige la conducta.

2.3.4. OBJETO JURÍDICO.

Es el bien o derecho protegido por las leyes penales, es decir el bien jurídicamente tutelado, algunos ejemplos serian la vida o la libertad sexual entre otros; Asúa dice que "es la ley, la norma, el derecho que ha sido violado, el bien o interés jurídicamente protegido."[76]

Objeto jurídico del delito, se conviene en que éste es el bien jurídico penalmente protegido que el delito ofende: en el homicidio, la vida; en las lesiones, la integridad corporal el cohecho la incorruptibilidad de los funcionarios

[76] Jiménez de Asúa Luis. *Teoría del Delito.* Ed. Iure Editores. México. 2002. p.75.

públicos, etc. Un bien puede ser tanto una persona, como una cosa, como una relación entre personas y una entre personas y cosas, como una idea, como un sentimiento, etc. Entre esos bienes hay algunos que, por ser vitales para la colectividad y el individuo, reciben protección jurídica por su significación social y a los cuales el derecho acuerda su especial tutela erigiendo en tipos delictivos algunas formas especialmente ominosas de atentar contra ellos; en cuanto, pues, objetos de interés jurídico vienen a constituir el objeto jurídico que se halla tras cada delito.

El bien jurídico es un valioso instrumento de interpretación del alcance y límites de cada tipo, al extremo de que ha llegado a tenérsele como norma directriz en ese dominio, para la labor de interpretación de la ley; además, en la parte especial de «CP» sirve como criterio clasificatorio de los tipos en grupos y subgrupos; aporta, en fin, criterios para determinar, entre otras materias, el área en que procede la legítima defensa, en que se valida el consentimiento del ofendido y en que puede haber lugar al delito continuado.[77]

El objeto jurídico es un bien o interés del sujeto pasivo, este mismo esta ligado con el objeto material pues todo delito, en cuando lesiona un interés determinado, individual o colectivo, tiene un objeto peculiar, es decir es la norma penal impuesta por el Estado y transgredida por el delincuente.

Se puede decir que el objeto jurídico esta constituido por bienes jurídicos, en cuya lesión no sólo se ve el quebranto de un interés particular, sino a la vez, la

[77] Cfr. Diccionario Jurídico. Desarrollo Jurídico. Microsoft. México.2000.

ofensa a un interés público con la violación del deber de respetar las normas de cultura cívica reconocidas por el Estado.

El objeto jurídico es de daño o de peligro; el primero se da cuando se destruye totalmente el bien jurídico tutelado, hay un deterioró, le quita o disminuya su valor y puede recaer en las personas o en las cosas, el Derecho penal solo protege el daño cuando vulnere un derecho protegido jurídicamente, un ejemplo seria el homicidio que protegería la vida y éste seria el daño causado; el segundo es de peligro, este ocasiona una lesión en el bien jurídico protegido, el cual no lo destruye totalmente sino como su nombre lo indica compone un peligro, un ejemplo de este tipo de objeto jurídico es el delito de violación ocasionando un peligro que es el normal desarrollo psicosexual.

2.4. LA CONDUCTA.

2.4.1. CONCEPTO.

Lo define Betancourt como “el comportamiento humano voluntario, positivo o negativo, encaminado a un propósito.”[78]Es decir solo los seres humanos pueden tener conductas positivas y negativas y son voluntarias por ser decisiones libres del sujeto y tienen un fin; otra definición de conducta nos la proporciona Jiménez de Asúa y dice “es la manifestación de la voluntad que mediante una acción produce un cambio en el mundo exterior, o que por no hacer lo que se espera deja inerte ese mundo externo, cuya mutación se aguarda.”[79]

[78] López Betancourt. Eduardo. *Teoría del Delito.*7ma ed. Ed. Porrúa. México. 1999. p.83.
[79] Jiménez de Asúa Luis. Op.cit. p. 90.

La conducta debe contener tres elementos para que pueda darse y son: Manifestación de la voluntad, resultado y nexo causal; la manifestación de la voluntad es la actividad externa del hombre con plena conciencia y por lo cual se establecen las causas, esta debe ser libre, espontánea y conciente. Se puede señalar que la manifestación de la voluntad es la parte final de un proceso mental combinado con un motivo; el resultado seria el acto exteriorizado obteniendo una modificación en el entorno social al realizar una conducta delictiva; por último el nexo causal que es la relación entre esa conducta de voluntad propia y el resultado; la conducta puede ser positiva cuando consiste en un hacer; y omisiva o negativa cuando es un no hacer.

2.4.2. DELITO DE ACCIÓN.

Cuello Calon menciona “consiste en un movimiento corpóreo voluntario encaminado a la producción de un resultado, consiste en la modificación del mundo exterior o en peligro de que se produzca”.[80]

Otra definición de conducta de acción nos la da Castellanos Tena “es todo hecho humano voluntario, todo movimiento voluntario del organismo humano capaz de modificar el mundo exterior o de poner en peligro dicha modificación.”[81] La acción consiste en una actividad corporal, externa y el derecho se ocupa sólo de estos actos, en virtud de que los actos puramente, espirituales, los pensamientos, las ideas o simples intenciones, no son sancionados penalmente

[80] Cuello Calón Eugenio. Op Cit. 1990. p. 148.
[81] Castellanos Tena Fernando. *Lineamientos Elementales de Derecho Penal*. ed.41. Ed. Porrúa. México. 2000. p. 152.

por estar fuera del derecho positivo; la conducta de acción es una activad voluntaria realizada por un sujeto, teniendo dos elementos el primero el movimiento y el otro es la voluntad propia.

La conducta de acción se integra por un movimiento voluntario descrito en el tipo legal; en estos delitos siempre se viola siempre una norma prohibitiva. Se menciona que el Derecho no crea un conducta humana, "la ley no crea la conducta porque la describa o individualice: la conducta es tal, sin que la circunstancia de que un tipo penal la describa afecte en nada, su ser conducta humana."[82]

2.4.3. DELITO DE OMISIÓN.

Porte Petit señala que la omisión consiste "es el no hacer, voluntario o involuntario (culpa), violando una norma preceptiva y produciendo un resultado típico."[83]

La omisión es una forma negativa de la acción, y radica en un abstenerse de obrar, simplemente de obrar, en dejar de hacer lo que se debe ejecutar. Dentro de la omisión hay dos clases la omisión simple u omisión propia y la comisión por omisión u omisión impropia; la primera consiste en dejar de ejecutar algo, es decir no se realiza el movimiento corporal esperado, se viola una norma dispositiva; al

[82] Zaffaroni. Eugenio Raúl. Op Cit. p.43.
[83] Porte Petit. Candaudp. Celestino. *Apuntamientos de la Parte General del Derecho Penal.* Ed. Porrúa. México. 1985. p.305.

igual que en los delitos de acción puede lesionar bienes jurídicamente tutelados por el derecho o solo ponerlos en peligro; en los delitos de omisión la conducta es inactiva, es la manifestación de la voluntad exteriorizada pasivamente en una inactividad; para que esta omisión interese al Derecho Penal debe existir el deber jurídico de hacer algo.

2.4.4. DELITO DE COMISIÓN POR OMISIÓN.

Los delitos de comisión por omisión u omisión impropia, el sujeto viola una norma prohibitiva, omitiendo realizar una conducta que evitaría la producción del resultado dañoso.

Existe una omisión impropia cuando se produce un resultado típico y material, por un no hacer, doloso o culposo violando una norma preceptiva y norma prohibitiva; en la conducta de omisión simple se obtiene el tipo con la falta de una actividad jurídicamente ordenada, no requiere de un resultado material, en la comisión por omisión, es necesario un resultado material, una mutación en el mundo exterior mediante no hacer lo que el derecho ordena; la omisión simple tiene un resultado jurídico y la conducta de comisión por omisión tiene resultado jurídico y material.[84]

[84] Cfr. López Betancourt Eduardo. Op Cit. p. 55.

2.5. AUSENCIA DE CONDUCTA.

La Ausencia de Conducta es el elemento negativo de la conducta, abarca la ausencia de acción o de omisión de la misma, en la realización de un delito.

El Nuevo Código Penal para el Distrito Federal lo tipifica en las causas de exclusión del delito en el artículo 29 fracción I:

TITULO SEGUNDO
EL DELITO
CAPITULO V
CAUSAS DE EXCLUSIÓN DEL DELITO

Artículo 29.- (Causas de exclusión). El delito se excluye cuando:
I.- (Ausencia de conducta).La actividad o la inactividad se realice sin intervención de la voluntad del agente.

La doctrina hace referencia que se presenta por: Vis Absoluta o fuerza superior irresistible, Vis mayor o fuerza mayor, movimientos reflejos, sueño, hipnotismo y sonambulismo.

2.5.1. VIS ABSOLUTA.

Lópes Betancourt dice: “consiste en que una fuerza humana exterior irresistible se ejerce contra la voluntad de alguien, quien en apariencia comete la conducta

delictiva; no se puede constituir una conducta delictiva cuando no se presenta la voluntad del agente".[85]

En presencia de la fuerza física irresistible, el sujeto productor de la última condición en el proceso material de la causalidad contribuye al resultado con su movimiento corporal, o con su inactividad, pero no con su voluntad; actúa involuntariamente, impulsado por una fuerza exterior de carácter físico procedente de otro; cuya superioridad manifiesta no le es posible resistir. La fuerza física irresistible (Vis absoluta), implica, por consiguiente, la ausencia del coeficiente psíquico (voluntad), en la actividad o inactividad, de forma tal que la manifestación meramente física de la conducta no puede integrar por si una acción o una omisión jurídicamente relevantes aquel que actúa o deja de actuar se convierte en simple instrumento de una voluntad ajena, expresada a través de una fuerza física respecto de la cual el constreñido no ha podido materialmente oponerse.

La ausencia de conducta, en la fuerza física irresistible, resulta más evidente si tenemos en cuenta la desaparición del nexo psicológico entre el agente y el resultado; pero además falta igualmente la relación psíquica entre el sujeto y su propia conducta, que precisamente por este motivo ni siquiera llega a nacer.

No hay punibilidad a consecuencia de la falta de culpabilidad; pero la falta de ésta a su vez emana de la ausencia de conducta (en el sentido material y en el de la relevancia jurídica); ausencia de conducta que origina inexistencia del hecho y, consecuentemente inexistencia del delito; en definitiva: al faltar la conducta no se

[85] López Betancourt Eduardo. Op Cit. p 87.

configura el elemento objetivo y congruente no existe antijuricidad formal, en consecuencia no hay culpabilidad, y en última instancia tampoco hay punibilidad.

La fuerza física irresistible tiene como características de acuerdo al Diccionario Jurídico:[86]

Respecto del sujeto medio o constreñido: 1) un hecho inevitable; 2) una fuerza física, humana, irresistible; 3) un resultado no atribuible al sujeto medio, 4) consustancialidad objetiva, y 5) un efecto jurídico, precisamente la falta de conducta.

2.5.2. VIS MAYOR.

La vis mayor es la fuerza que proviene de la naturaleza, es cuando el sujeto realiza una acción en sentido amplio (acción u omisión) coaccionado por una fuerza irresistible de la naturaleza.[87]

Es un acontecimiento que no se puede prever ni resistir, la diferencia entre la vis absoluta, y la vis mayor es que esta es una aprehensión de carácter físico de procedencia natural o meta-humana, que impide al sujeto que la recibe conducir su voluntad con relación al resultado que se produce, aun cuando pueda preverse no es factible superarse o vencerse; es un acontecimiento extraño a la voluntad del individuo que sucede alrededor de su esfera social y del cual no pueden surgir

[86] Diccionario Jurídico. Microsoft. 2002.
[87] Eduardo López Betancourt. Op Cit. p. 108.

consecuencias jurídicas ya que no hay voluntad propia del individuo debido a que fue provocado por la fuerza de la naturaleza.

2.5.3. MOVIMIENTOS REFLEJOS.

Son aquellos que obedecen a estímulos no percibidos por la conciencia, por transmisión nerviosa a un centro neuronal y de este a un nervio periférico. Como el sujetó esta impedido para controlarlos, se considera que no existe la conducta responsable y voluntaria; en caso de poder controlarlos a volunta habría un delito.[88]

Los movimientos reflejos, son los actos involuntarios que realiza el cuerpo humano como respuesta a estímulos específicos percibidos por el cerebro; un ejemplo seria el cierre de los parpados cuando algo toca el ojo.

2.5.4. SUEÑO.

Eduardo López Betancourt menciona “el sueño es el descanso regular y periódico de los órganos sensoriales y del movimiento corporal, acompañado de relajación de los músculos y disminución de varias funciones del cuerpo; en este acto no se da la voluntad, solo existirá la responsabilidad cuando se le haya impuesto al sujeto el estado de vigilia como obligación.”[89]

---

[88] Diccionario Jurídico. Microsoft.2002.
[89] López Betancourt Eduardo. Op Cit. p.109.

2.5.5 HIPNOTISMO.

Es un procedimiento para producir el llamado sueño magnético, por fascinación, influjo personal o por aparatos personales.[90]

Cuando el sujetó se hipnotiza con su consentimiento con fines delictuosos, en este caso el sujeto si es responsable, por que el sujeto se colocó intencionalmente en ese estado para cometer el delito; en el caso que se hipnotice el sujeto sin consentimiento y realice una conducta o hechos punibles por la ley penal, aquí el sujeto no seria responsable.

En el caso que se hipnotice al sujeto con su consentimiento, pero sin una intención delictuosa, el sujeto también es responsable del delito, pero sería culposo.

Realmente la hipnosis como tal no se puede aceptar, ya que no se puede suponer que una persona se mantenga en un estado semiinconsciente para realizar actos ajenos a su propia voluntad, ya sea que lo permita o sea forzado a hacerlo; la medicina y la psiquiatría la utilizan como sistema de relajación muscular, fijación ocular, etc. también puede ser utilizada para relajación o concentración de la propia respiración cuando esta es autoinducida. La mayoría de las personas que se someten a este tipo de estado de inconciencia oscila en un veinte por ciento; este estado puede ir desde un trance leve casi despierto hasta un estado casi de sonambulismo.

[90] Cfr. López Betancourt Eduardo. Op Cit. p. 121.

2.5.6. SONAMBULISMO.

Es el estado psíquico inconsciente, mediante el cual la persona que padece sueño anormal tiene cierta aptitud para poder levantarse, andar, hablar y ejecutar otros actos, sin que al despertar recuerde lo ocurrido.[91]

Cuando un sujeto se encuentra en este estado, y comete un delito la conducta que hace no es voluntaria, salvo que el mismo sujeto se aproveche de ese estado previendo el resultado y cometa un delito, pero solo será culposo; los sonámbulos realizan generalmente búsqueda de objetos perdidos que reflejan estados de tensión experimentadas durante las horas de vigilia del sueño; esta conducta sucede más ha menudo en los adolescentes que en los adultos.

2.6. TIPICIDAD.

La tipicidad es la adecuación de la conducta al tipo penal. Para Jiménez de Asúa la tipicidad es "la exigida correspondiente entre el hecho real y la imagen rectora en la ley en cada especie de infracción."[92]

La tipicidad es uno de los elementos esenciales del delito cuya ausencia impide su configuración, habida cuenta que nuestra Constitución Política de los Estados Unidos Mexicanos, en su artículo catorce párrafo tercero, establece en forma expresa:

---

[91] Enciclopedia Encarta. Microsoft.2005.
[92] López Betancourt Eduardo. Op Cit. p.110.

CAPITULO I

DE LAS GARANTIAS INDIVIDUALES.

Art. 14. .....

.....

En los juicios del orden criminal queda prohibido imponer, por simple analogía y aun por mayoría de razón, pena alguna que no esté decretada por un ley exactamente aplicable al delito de que se trata.

Es decir no hay delito sin tipicidad; la tipicidad no debe confundirse con el tipo, ya que éste solo es la creación legislativa, es la descripción de una conducta prohibida realizada por una norma jurídico-penal que realiza el Estado y la tipicidad es la adecuación a esa conducta descrita en la norma legal.

La Suprema Corte de Justicia de la Nación, ha establecido que para que una conducta humana sea punible conforme a derecho positivo, es preciso que la actividad desplegada por el sujeto activo, se subsuma en un tipo legal, esto es, que la acción sea típica, antijurídica y culpable, y que no concurra en la tal consumación exterior del acto injusto, una causa de justificación o excluyente de culpabilidad; puede una conducta humana ser típica porque la manifestación de voluntad o la modificación del mundo exterior, es decir, la producción del resultado lesivo, enmarque dentro de la definición de un tipo penal, como puede ocurrir por ejemplo, tratándose del homicidio o fraude, pero si se demuestra que el occiso fue privado de la vida, por el sujeto activo, cuando este era objeto de una agresión injusta, real, grave, desaparece la antijuridicidad del acto incriminado y consecuentemente al concurrir la causa justificadora de la acción, resulta no culpable, o si, tratándose del segundo de los delitos no satisfacen los

presupuestos de tipicidad al integrarse sus elementos constitutivos" (semanario judicial de la Federación, CXVII:p. 371.)

Cortes Ibarra dice que "Tipicidad es la adecuación exacta y plena de la conducta al tipo. Afirmamos que la conducta es típica cuando se superpone o encuadra exactamente a la prevista; la tipicidad exige, para su conformación, un agotamiento exhaustivo de la conducta en concreto a la descripción abstracta e indeterminada de la ley."[93]

Por más inmoral o antisocial que se considere cualquier conducta, si no se encuentra en un tipo penal, no será un delito; el tipo es solo una descripción de una conducta delictiva y la tipicidad es la averiguación que sobre una conducta se efectúa para saber si presenta las características que el legislador describió en ese tipo, es decir es el resultado afirmativo de esta averiguación o juicio.

Octavio Arellano Wiarco clasifica al tipo de la siguiente manera[94]:

- Normales y Anormales: si las palabras empleadas se refieren a situaciones puramente objetivas, se estará en presencia de un tipo normal. Si es necesario establecer una valoración, ya sea cultural o jurídica, el tipo será anormal.

- Fundamentales o básicos: Son cuando el tipo tiene plena independencia, es decir son los delitos esénciales consagrados en ley como el robo o el homicidio y a su alrededor están los delito que necesitan del tipo básico.

[93] Cortés Ibarra Miguel Ángel. Op Cit. p.227.
[94] Wiarco Orellano Alberto Octavio. *Curso de Derecho Penal*.2da.ed. Ed.Porrua. México. 2001.p 228.

- Especiales: Son los formados por el tipo básico y se agregan elementos que los distinguen.

- Complementados: Estos se integran con el tipo fundamental y unas circunstancias que lo atenúan o agravan, un ejemplo sería el homicidio calificado, solo existe cuando hay alevosía, premeditación y ventaja o se comete en riña.

- Autónomos o Independientes: Son los que tienen vida propia, no necesitan de otro tipo para poder existir, un ejemplo es el robo simple, estos mismos también son básicos o fundamentales.

- Subordinado: Dependen para su existencia de otro tipo, un ejemplo el homicidio en riña.

- De formación casuística: Son aquellos que el legislador no describe una modalidad única, sino varias formas de ejecutar el ilícito.

- De formación amplia: Evita señalar caso por caso se describe una hipótesis única donde caben todos lo modos de ejecución, la conducta se puede realizar de diversa manera ejemplo el homicidio.

- De peligro: En este tipo de delitos se protege el bien jurídico y el riesgo que corran estos.

- De daño o Lesión: Es la destrucción del bien jurídico protegido por la ley como el homicidio destruye la vida.

2.7. ATIPICIDAD.

La atipicidad es la falta total o parcial de adecuación de la conducta al tipo penal, es el aspecto negativo de la tipicidad; hay que diferenciar la atipicidad de la falta de tipo, la atipicidad se da cuando existe el tipo, pero la conducta no embona dentro de éste y la ausencia de tipo, cuándo el legislador no describe la conducta en la Ley penal, es decir no existe.

Habrá entonces atipicidad cuando la conducta no satisfaga lo descrito por la ley, por no completar los requisitos que el tipo menciona. El fundamento se encuentra en el artículo 29 fracción II del Nuevo Código Penal del Distrito Federal y dice:

TITULO SEGUNDO
EL DELITO
CAPITULO V
CAUSAS DE EXCLUSIÓN DEL DELITO

Artículo 29.- (Causas de exclusión). El delito se excluye cuando:
.....
II.- (Atipicidad). Falte alguno de los elementos que integran la descripción legal del delito de que se trate.

La falta de tipo es que el hecho o conducta no aparecen en la ley, no existe el tipo, no se puede decir que una conducta es atípica porque no se encuadra a un tipo inexistente.

Las causas de atipicidad según Luis Jiménez de Asúa son las siguientes:[95]

A) Ausencia del presupuesto de conducta o del hecho.

b) Ausencia de la calidad del sujeto activo exigido en el tipo.

c) Ausencia de la calidad del sujeto pasivo exigido en el tipo.

d) Ausencia del objeto jurídico.

e) Ausencia del objeto material.

f) Ausencia de las modalidades de la conducta: referencias especiales, temporales y medios empleados.

g). Ausencia del elemento normativo.

h) Ausencia del elemento subjetivo del injusto.

2.8. ANTIJURIDICIDAD.

Eduardo López Betancourt dice La antijuridicidad, es cuando la conducta del ser humano es delictiva y contraviene las normas penales, es antijurídica.[96]

Jiménez de Asúa dice antijuridicidad "es lo contrario al Derecho. Por tanto, no basta que el hecho encaje descriptivamente en el tipo que la ley ha previsto sino que necesita que sea antijurídico, contrario a derecho."[97]

La antijuridicidad es choque de la conducta con el orden jurídico y el orden normativo; esta nace del juicio valorativo de la oposición existente entre la

[95] Jiménez de Asúa Luis. *Teoría del Delito*. Ed. Iure Editores y Distribuidores. México. 2002. p.946.
[96] Eduardo López Betancourt. Op Cit. p. 149.
[97] Jiménez de Asúa Luis. Ob.cit .p.958.

conducta humana y norma penal, recayendo el juicio solo en las acciones realizadas; la antijuridicidad se da cuando no solo se encuadre el tipo penal, además debe tener una conducta antijurídica que no este protegida con una causa de justificación que expresa la ley penal.

La antijuridicidad de acuerdo a Eduardo López Betancourt se divide en formal y material, la primera habla que una conducta se le considera delito cuando infringe una norma estatal, un mandato o prohibición del orden jurídico y la segunda cuando el sujeto es considerado peligroso para la sociedad; la antijuridicidad formal nace cuando la conducta encuadre en el tipo penal y l a material cuando la conducta contraviene valores sociales o culturales que protege la norma.

Recapitulando: se dice que la antijuridicidad es el estado querido por derecho y la inconformidad de un estado de hecho, lesionando no solo un deber jurídico sino también un bien o interés que el derecho protege, no solo violando la obligación jurídica sino además la norma jurídica. Se necesitan dos requisitos para darse la antijuricidad; el primero la adecuación de la conducta al tipo penal y el otro cuando no se encuentre la conducta en una causa de exclusión de lo injusto o de alguna causa de licitud.

2.9. CAUSAS DE JUSTIFICACIÓN.

Eduardo López Betancourt dice: “la conducta aparentemente es delictuosa, falta la antijuridicidad, se esta en el caso de una causa de justificación por no haber delito, el sujeto actuó de tal forma que no vulneró una norma penal; son

aquellas condiciones que se tienen para excluir la antijuridicidad de una conducta típica".[98]

En las cusas de justificación el sujeto actúa de forma normal ya que su conducta no es delictiva por estar ajustada al derecho, actúa de forma justa no lesionando ningún bien jurídico; una definición la proporciona Porte Petit y dice "la conducta o hechos realizados no son contra derecho sino conforme al derecho y esta conformidad puede provenir de la ley penal o del cualquier otro ordenamiento jurídico público o privado;"[99]en resumen se puede definir las causas de justificación como las condiciones que excluyen la antijuridicidad de una conducta que puede estar en un tipo legal, es decir serían los actos u omisiones que revisten aspecto de un delito, pero falta el carácter de ser antijurídico, de ser contrarios a derecho.

Las causas de justificación de acuerdo a legislación penal son:

- Legitima Defensa.
- Estado de necesidad.
- Ejercicio de un derecho.
- Cumplimiento de un deber.
- Consentimiento del titular del bien jurídico afectado.

LEGITIMA DEFENSA.

EL artículo 29 fracción IV del Nuevo Código Penal para el Distrito Federal describe:

[98] López Betancourt Eduardo. Op Cit. p152.
[99] Porte Petit. Celestino. ob.cit. p.491.

TITULO SEGUNDO

EL DELITO

CAPITULO V

CAUSAS DE EXCLUSIÓN DEL DELITO

Artículo 29.- (Causas de exclusión). El delito se excluye cuando:

.....

IV.- se repele una agresión real, actual o inminente y sin derecho en defensa de bienes jurídicos propios o ajenos, siempre que exista necesidad de la defensa empleada y no medie provocación dolosa suficiente e inmediata por parte del agredido o de su de defensor.

Eduardo López Betancourt menciona que quien se defiende legítimamente obra conforme a derecho, aunque su actuar corresponda aun delito descrito en una norma; esté actuar no solo es lícito para el derecho penal sino también para las otras ramas del derecho; el bien jurídico puede ser cualquiera como: la vida, la propiedad, la libertad, etc.

Los elementos de la definición legal son:

a) Repeler: Esto es evitar, impedir que una agresión que realizamos se rechace.

b) Agresión: Es todo acto que lesiona o pone en peligro un bien jurídicamente protegido de otro.

c) Real: Es decir que sea cierto, no inventado o imaginado.

d) Actual o Inminente: Debe ser en el mismo instante que ocurre la agresión esa repulsa, inminente que este a punto de ocurrir, que se pueda desencadenar en cualquier momento.

e) Sin derecho: La agresión no debe tener derecho, sino, no se justifica la defensa.

f) Necesidad de defensa: Es decir que la repulsa sea en proporción del daño que se pretende hacer, no debe ser exagerada.

g) Sin mediar provocación suficiente dolosa e inmediata: El ofendido no debe provocar la agresión, y el tercero no debe haber dado causa a ello.

ESTADO DE NECESIDAD.

En sentido concreto se entiende como la necesidad de salvaguardar los intereses protegidos por el derecho de un peligro actual o inminente, agrediendo otros bienes protegidos cuando no queda otra opción; es decir se preserva el bien amenazado atacando otro bien también protegido por las leyes.[100]

El artículo 29 fracción V del Nuevo Código en cita contempla es estado de necesidad y dice:

TITULO SEGUNDO
EL DELITO
CAPITULO V
CAUSAS DE EXCLUSIÓN DEL DELITO

Artículo 29.- (Causas de exclusión). El delito se excluye cuando:
.....
V.- (Estado de necesidad). Se obre por la necesidad de salvaguardar un bien jurídico propio o ajeno, de un peligro real, actual o inminente, no ocasionado dolosamente por el sujeto, lesionando

[100] Diccionario Jurídico. Microsoft.2002.

> otro bien de menor o igual valor que el salvaguardado, siempre que el peligro no sea evitable por otros medios y el agente no tuviere el deber jurídico de afrontarlo.

Las partes de este concepto son:

A) Peligro: Debe existir una situación de peligro hacia un bien jurídico.

B) Real; actual o Inminente: El daño debe ser tangible no inventado, que sea en el momento o próximo a suceder.

C) El peligro no debe haber sido ocasionado con ánimo doloso por el sujeto, esto quiere decir que el sujeto no lo haya ocasionado ese peligro.

D) Que no exista otro medio practicable par evitar el peligro: No debe existir otro medio para poder salvaguardar el bien jurídico o menos perjudicial, más que el empleado, de lo contrario anularía la causa de justificación.

F) Que el agente no tenga el deber jurídico de afrontar el peligro: El sujeto no debe tener la obligación de hacerlo, sino se estaría hablando de otra causa de justificación.

CUMPLIMIENTO DE UN DEBER O EJERCICIO DE UN DERECHO.

El cumplimiento de un deber, es: cuando se tiene la facultad de obrar en forma legítima por medio de una ley o norma reconocida jurídicamente, siempre y cuando el actuar sea positivo.[101]

[101] Diccionario Jurídico. Microsoft. 2002.

El ejercicio de un derecho, significa el actuar de un sujeto en forma permitida pero no obligatoria, empleando el medio de forma racional, el cual este regulado por una norma jurídica o de otra especie.

El artículo 29 fracción VI del Nuevo Código Penal para el Distrito Federal lo describe de la siguiente forma:

TITULO SEGUNDO
EL DELITO
CAPITULO V
CAUSAS DE EXCLUSIÓN DEL DELITO

Artículo 29.- (Causas de exclusión). El delito se excluye cuando:
.....

VI.- (Cumplimiento de un deber o ejercicio de un derecho). La acción o la omisión se realice en cumplimiento de un deber jurídico o en ejercicio de un derecho, siempre que exista necesidad racional de la conducta empleada para cumplirlo o ejercerlo.

CONSENTIMIENTO DEL TITULAR DEL BIEN JURIDICO.

El artículo 29 fracción III del Código citado menciona esta cusa de justificación y dice:

TITULO SEGUNDO
EL DELITO
CAPITULO V
CAUSAS DE EXCLUSIÓN DEL DELITO

> Artículo 29.- (Causas de exclusión). El delito se excluye cuando:
> .....
> III.- (Consentimiento del titular). Se actué con el consentimiento del titular del bien jurídico afectado, o del legitimado legalmente para otorgarlo, siempre y cuando se cumplan los siguientes requisitos:
>
> a) Que se trate de un bien jurídico disponible;
> b) Que el titular del bien jurídico, o quien este legitimado para consentir, tenga la capacidad jurídica para disponer libremente del bien; y
> c) Que el consentimiento sea expreso o tácito y no medie algún vicio del consentimiento.
>
> Se presume que hay consentimiento, cuando el hecho se realiza en circunstancias tales que permitan suponer fundadamente que, de haberse consultado al titular del bien o quien esté legitimado para consentir, éstos hubiesen otorgado el consentimiento.

2.10. IMPUTABILIDAD.

Octavio Arellano Wiarco dice que la imputabilidad es la capacidad que tiene una persona para atribuirle la responsabilidad de sus actos, es la aptitud del sujeto que por su desarrollo físico y psíquico, tiene el deber de respetar la ley, y que traduzca esa aptitud en acciones u omisiones voluntarias.

Imputabilidad es la capacidad de querer y entender; querer es aceptar o realizar algo concientemente y voluntariamente y entender es: tener la capacidad mental con la edad adecuada.[102]

[102] López Betancourt Eduardo. Op Cit. p.80.

El Diccionario Jurídico Mexicano define a la imputabilidad como “la capacidad, condicionada por la madurez y salud mentales, de comprender el carácter antijurídico de la propia acción u omisión y de determinarse de acuerdo a esa comprensión.”[103]

La capacidad de querer, es la libre voluntad, es exteriorizar un deseo, es la facultad de autodeterminarse, determinar con libertad los diversos motivos que impulsan a realizar una conducta, el sujeto tiene motivos para querer una cosa o la contraria, pero su voluntad queda libre para determinarse en un sentido o en otro.

La capacidad de entender, es el discernimiento, el conocimiento exacto entre licitud o ilicitud, y este solo se da cuando se tiene la madures física e intelectual, así como gozar de salud psíquico-mental, el sujeto tendrá cierta comprensión de sus actos generando la conciencia propia, el cual distinguirá entre un hacer o no hacer; es necesario que se tenga la capacidad de entender y no solo la de querer una conducta para que sea imputable un sujeto, y entre al elemento de la culpabilidad; el sujeto debe tener estos elementos para ser imputable y en el mismo sujeto esta la facultad para preservar el orden jurídico y la paz social.

2.11. INIMPUTABILIDAD.

La inimputabilidad es lo contrario a la imputabilidad, es el aspecto negativo, es la incapacidad de querer y entender la conducta. El Código Penal menciona en su artículo 29 fracción VII:

[103] *Diccionario Jurídico Mexicano.* Ed. Porrúa. México. 1985. p 51.

TITULO SEGUNDO

EL DELITO

CAPITULO V

CAUSAS DE EXCLUSIÓN DEL DELITO

Artículo 29.- (Causas de exclusión). El delito se excluye cuando:

.....

VII.- (Inimputabilidad y acción libre en su causa). Al momento de realizar el hecho típico, el agente no tenga la capacidad de comprender el carácter ilícito de aquél o de conducirse de acuerdo con esa comprensión, en virtud de padecer trastorno mental o desarrollo intelectual retardado, a no ser que el sujeto hubiese provocado su trastorno mental para en ese estado cometer el hecho, en cuyo caso responderá por el resultado típico producido en tal situación.

Jiménez de Asúa señala "son causas de inimputabilidad la falta de desarrollo y salud de la mente, así como lo trastornos pasajeros de las facultades mentales que privan o perturban en el sujeto la facultad de conocer el deber, esto es, aquellas causas en las que si bien el hecho es típico y antijurídico, no se encuentra el agente en condiciones de que se le pueda atribuir el acto que perpetró."[104]

Los casos de inimputabilidad son los siguientes:

- Trastorno Mental
- Desarrollo mental retardado.

[104] Jiménez de Asúa Luis. *Principios de Derecho Penal, La Ley y el Delito.* ed 3ra. Ed. Sudamericana, Buenos Aires. 1990. p.339.

- Miedo Grave.
- Minoría de edad.

Trastorno Mental.

Es cualquier alteración o mal funcionamiento en las facultades psíquicas, siempre que impidan al sujeto comprender el carácter ilícito del hecho, o conducirse acorde a esa comprensión; estos trastornos pueden ser patológicos o por ingestión de alguna sustancia nociva; el trastorno mental puede ser transitorio o permanente, el transitorio es una perturbación mental temporal de grado leve no orgánico, como lo sería una fobia más concreto claustrofobia (temor a lugares cerrados), el trastorno mental permanente es la perturbación mental perpetua originada generalmente por algún trastorno orgánico, que también puede ser físico, en este caso el ejemplo seria la esquizofrenia, que se caracteriza por agudas perturbaciones del pensamiento, la percepción y la emoción que afecta las relaciones con los demás individuos.

Desarrollo Intelectual Retardado.

Es el proceso tardío de inteligencia provocando la incapacidad de querer y entender.

Miedo Grave.

Es aquella circunstancia interna subjetiva en que el individuo se encuentra marginado por la misma, para actuar razonadamente, es una situación subjetiva que lo obliga actuar de manera distinta, esto derivado de circunstancias especiales

del mundo subjetivo de cada individuo, actuando de manera diversa al cotidiano; el miedo grave procede de procesos psicológicos.

Minoría de Edad.

En el derecho penal mexicano se considera que los menores de 18 años son inimputables, ya que carecen de madures, y capacidad de querer y entender lo negativo del delito; la Ley para el Tratamiento de menores Infractores para el Distrito Federal, describe que los menores de 18 años de edad son susceptibles de ser corregidos; faltando la capacidad de saber que lo que hace esta mal y por lo tanto no tiene el elemento de culpabilidad, entonces el menor de edad no comete delitos sino infracciones a la Ley, pero estas infracciones por supuesto también tienen sus sanciones

2.12. CULPABILIDAD.

Eduardo Mezger menciona la culpabilidad se puede decir que es el conjunto de presupuestos de la pena que fundamentan frente al autor la reprochabilidad personal de la acción antijurídica; se reprocha el comportamiento antijurídico en base a la libertad, el fin o alcance conocido o conocible.[105]

Zaffaroni dice: “la culpabilidad es la reprochabilidad de un injusto a un autor, la que sólo es posible cuando revela que el autor ha aprobado con una disposición

[105] Mezger Eduardo. *Derecho Penal Parte General*. Ed. Cárdenas. México. 1985. p. 189.

interna a la norma violada, disposición que es fundamento de culpabilidad."[106]Entonces se estaría hablando de que culpabilidad es la responsabilidad del autor por el acto antijurídico; en síntesis es el reproche que se le hace al autor de un acto punible ligado con un nexo causal, que con ese comportamiento se le pudo exigir que actuara conforme a las normas.

De acuerdo a la doctrina las formas de culpabilidad son dos dolo y culpa:

2.12.1. DOLO.

Actúa dolosamente el que conoce la circunstancia del hecho y la significación de su acción y ha admitido en su voluntad el resultado.

López Betancourt dice "dolo consiste en el conocimiento de la realización de las circunstancias que pertenecen al tipo, y voluntad o aceptación de la realización del mismo."[107]

Para que exista el dolo debe haber tres circunstancias, que el sujeto haya tenido la posibilidad de conocer la existencia de un deber, que conociendo ese deber produciría con su actuar una violación a ese deber y que previó y quiso los medios para realizarlo, es decir un elemento volitivo y un elemento intelectual el primero se refiere a la voluntad de ejecutar el acto y el segundo a la manifestación del acto con plena conciencia.

---

[106] Zaffaroni Eugenio Raúl. *Tratado de Derecho Penal Parte General*. tomo. IV. Ed. Cárdenas Editor y Distribuidor. México. 1988. p.12.
[107] López Betancourt. Eduardo. Op Cit. pp.218 y 219.

El artículo 18 del Nuevo Código Penal para el Distrito Federal segundo párrafo describe:

TITULO SEGUNDO

EL DELITO

CAPÍTULO I FORMAS DE COMISIÓN

.....

Obra dolosamente, el que conociendo los elementos objetivos del hecho típico de que se trate, o previendo como posible el resultado típico, quiere o acepta su realización.

El dolo se clasifica según Luis Jiménez de Asúa en:

A) En cuanto a su nacimiento:
- Inicial o precedente.
- Subsiguiente o sucesivo.

B) En cuanto a su extensión:
- Determinado.
- Indeterminado.

C) En cuanto a la modalidad de su dirección:
- Directo.
- Eventual.
- De consecuencias necesarias.

D) en cuanto a su intensidad:
- Genérico.
- Especifico.

E) En cuanto a su duración:
- De ímpetu.
- Simple
- De propósito.

F) En cuanto a su contenido:
- De daño.
- De peligro
- De daño con resultado de peligro.
- De peligro con resultado de daño.

Dolo inicial: Se presenta en el momento de realizar el hecho o conducta cuando se quiere violar la norma.

Dolo subsiguiente: Es cuando en un principio el actuar del sujeto es lícito, surgiendo posteriormente en él la voluntad antijurídica de realizar un hecho delictuoso.

Dolo determinado: Cuando la intención de actuar se dirige concretamente a un hecho delictivo.

Dolo Indeterminado: Cuando la intención del sujeto se encamina hacia varios resultados delictivos.

Dolo directo: Se quiere la conducta y el resultado. Es decir se quiere la conducta cuando el delito es formal y se quiere el resultado cuando el delito es material.

Dolo eventual: Existe una representación del resultado, pero no hay voluntariedad del mismo, porque no se quiere el resultado, sino se acepta en caso de que se produzca.

Dolo de consecuencias necesarias: Es cuando queriendo el resultado, se prevé como seguro otro resultado derivado de la misma conducta.

Dolo genérico: Se configura cuando el sujeto quiere el hecho o conducta tipificados como delito.

Dolo especifico: Requiere por mandato de las normas o leyes, una actuación del sujeto con un fin especial.

Dolo de ímpetu: Hay una simple deliberación, el sujeto persiste en querer el evento criminal pero carece de la frialdad de ánimo.

Dolo simple: Es cuando el sujeto activo del delito, lleva la idea de realizar la conducta ilícita, prepara todos los medios necesarios para realización del acto antijurídico para la obtención del resultado esperado.

Dolo de propósito: Se integra por la premeditación, la frialdad del cálculo y la perseverancia de querer el evento delictuoso, a instancia del tiempo transcurrido entre la determinación y la actuación.

Dolo de daño: Se configura cuando el sujeto encamina su propósito a un hecho delictuoso tendiente a destruir o disminuir un bien jurídico.

Dolo de peligro: Es cuando el sujeto quiere y prevé un hecho que solo causa un peligro por ejemplo el abandono de personas.

Dolo de daño con resultado de peligro: La intención se dirige a producir el daño, pero la ley, con fines de tutela pública, supone el momento consumativo anterior a la realización del daño.

Dolo de peligro con resultado de daño: Se da cuando el sujeto quiere la producción del peligro y sólo la penalidad esta condicionada a la verificación del evento dañoso.

2.12.2. CULPA.

La culpa se conforma cuando el sujeto que realizó un hecho del cual resultó la ofensa a la ley, no quiso ni previó la consecuencia, sino que sólo previó y quiso el antecedente[108]; se puede decir que la culpa se configura cuando el sujeto no previó lo que pudo y debió prever, o cuando habiéndolo previsto, no realiza lo necesario para evitar el hecho mediante una conducta diversa a la que causo el resultado.

Los elementos de la culpa son:[109]

- Voluntariedad del acto. La conducta debe quererse se omisiva o comisiva.
- Resultado dañoso tipificado en la Ley. Debe estar catalogado como delito.
- La ausencia de dolo. Es decir no hay intención delictiva, o si se presenta espera que no se produzca.
- La previsión o falta de previsión del resultado.
- La relación causal directa entre el acto inicial y el resultado. Es cuando existe un enlace entre el proceso psicológico del sujeto y el resultado lesivo, por no haber obrado con previsión.

La doctrina clasifica a la culpa en: culpa conciente o con representación e inconciente o sin representación.

---

[108]

[109] Cfr. Wiarco Arellano. Alberto Octavio. *Curso de Derecho Penal*. Ed. Porrúa. México. 2001. p. 315.

Culpa Conciente o Con Representación: Es cuando el sujeto de su acto se originen consecuencias perjudiciales pero no las toma en cuenta confiándose en que no se produzcan; la culpa con representación existe cuando se prevé el resultado como posible y se tiene la esperanza de que no suceda.

Culpa Inconciente o Sin Representación: Es una negligencia en el obrar del sujeto, pero no en contraste estricto con la norma o las leyes, sino en contraste a su proyección social; la culpa sin representación existe cuando no se previó el resultado por descuido y se tenia la obligación de preverlo por ser de naturaleza previsible y evitable.

El Nuevo Código Penal para el Distrito Federal describe el concepto de culpa en el artículo 18 párrafo tercero:

TITULO SEGUNDO

EL DELITO

CAPÍTULO I FORMAS DE COMISIÓN

.....

Obra culposamente el que produce el resultado típico, que no previó siendo previsible o previo confiando en que no se produciría, en virtud de la violación de un deber de cuidado que objetivamente era necesario observar.

2.13. INCULPABILIDAD.

Eduardo López Betancourt menciona la inculpabilidad opera cuando falte alguno de los elementos esenciales de la culpabilidad, ya sea el conocimiento o la voluntad; tampoco es culpable una conducta si falta alguno de los otros elementos del delito o la imputabilidad del sujeto, porque si el delito se integra con un todo, sólo existirá mediante las partes que crean su esencia.[110]

Cualquier excluyente de responsabilidad elimina los elementos del delito causando la inculpabilidad, también habrá inculpabilidad siempre que por error o ignorancia falte tal conocimiento y siempre que la voluntad no sea libre y espontánea.

Las causas de la inculpabilidad de acuerdo a la Legislación son:

- Error o Ignorancia.
- No exigibilidad de otra conducta.

El Error.

Eduardo López Betancourt dice el error es la falsa o equivocada idea de la realidad, ya sea que radique en un objeto o situación, dando un

[110] Cfr. López Betancourt. Eduardo. Op Cit. p. 235-236.

conocimiento incorrecto. La ignorancia es el desconocimiento total de la realidad o ausencia del conocimiento.[111]

El error es el conocimiento falso sobre los elementos requeridos para la definición legal del delito o sobre el carácter prohibido de la conducta en que este consiste.

El error se divide en: error de derecho, error de hecho, este a su vez se clasifica en error accidental y esencial, y el accidental se subdividen en error en la persona, en el golpe y en el delito.

Error de derecho: Es cuando un sujeto en la realización de un hecho delictivo alega ignorancia o error en la ley.

Error de hecho: Este tipo de error se divide en error esencial y error accidental. El primero es el que recae sobre un extremo básico del delito, impidiendo al sujeto conocer, advertir la realización del hecho realizado con el formulado en un precepto de la norma penal, el sujeto realiza una conducta antijurídica creyendo que es jurídica, desconoce la antijuridicidad.

El error accidental se subdivide en:

[111] Ibidem. p. 237.

Error en el golpe: es cuando el sujeto provoca un delito equivocadamente menor o mayor al propuesto originalmente.

Error en la persona: se da debido a una errónea representación, ya que el sujeto destina su fin hacia otra persona creyendo que es otra equivocadamente.

Error en el delito: es cuando el sujeto piensa que esta en un supuesto delito determinado y se encuentra en otro.

El artículo 29 fracción VIII del Nuevo Código Penal para el Distrito Federal describe:

TITULO SEGUNDO
EL DELITO
CAPITULO V
CAUSAS DE EXCLUSIÓN DEL DELITO

Artículo 29.- (Causas de exclusión). El delito se excluye cuando:

.....

VIII.- (Error de tipo y error de prohibición). Se realice la acción o omisión bajo un error invencible, respecto de :

a) Alguno de los elementos objetivos que integran la descripción legal del delito de que se trate; o
b) La licitud de la conducta, ya sea porque el sujeto desconozca la existencia de la ley o el alcance de la misma o porque crea que está justificada su conducta.

La No Exigibilidad de Otra Conducta.

Esta conducta sucede cuando a un sujeto no se le puede considerar culpable, dadas las circunstancias que se le presentan, no se le puede exigir otra conducta a la realizada; es decir el sujeto tiene plena conciencia y determinación en su actuar pero una situación hace que se exima de la culpabilidad. Se podría entender la no exigibilidad de otra conducta a la realización de un hecho tipificado penalmente, obedece a una situación especial, apremiante, que hace excusable ese comportamiento.

El articulo 29 fracción IX de la ley ya citada habla de la no exigibilidad de otra conducta:

TITULO SEGUNDO
EL DELITO
CAPITULO V
CAUSAS DE EXCLUSIÓN DEL DELITO

Artículo 29.- (Causas de exclusión). El delito se excluye cuando:

.....

IX.- (Inexigibilidad de otra conducta). En atención a las circunstancias que concurren en la realización de una conducta ilícita, no sea racionalmente exigible al sujeto una conducta diversa a la que realizó, en virtud de no haberse podido conducirse conforme a derecho.

CAPÍTULO TERCERO.
RÉGIMEN JURÍDICO.

3.1. ORGANISMOS INTERNACIONALES.

Los sistemas informáticos en si mismos constituyen un fuerte producto económico y sus obligaciones y derechos que producen en la relación emisor y receptor o entre posesión del objeto y su autor, esto requiere de un régimen jurídico aplicable a casos concretos.

Las computadoras permiten un manejo rápido y eficiente de enormes volúmenes de información, siendo así, pueden constituir esta en datos personales y utilizarlos en cualquier momento, durante más de treinta años se han recopilado numerosos archivos de información de carácter confidencial como filiación, domicilio, estado civil, raza, religión, ingresos, cuentas bancarias, etc. Estos datos son recopilados en registros civiles, médicos, académicos, deportivos, administrativos, fiscales, laborales y otros más, esto hace que se pueda disponer de éstos en cualquier momento.

CONVENIO DE ESTRASBURGO.

El veintiocho de enero de 1981, se realiza un acuerdo internacional para la Protección de las Personas respecto al Tratamiento Automatizado de Datos de Carácter personal, mejor conocido como convenio de Estrasburgo, inicialmente

fueron ocho países los que lo iniciaron: Austria, Alemania, Dinamarca, España, Francia, Luxemburgo, Suecia y Turquía. Más adelante fueron agregándose varias Naciones y todo aquel país que se interesara; esta integrado por siete capítulos distribuidos en 27 artículos relativos a objetivos, definiciones, ámbitos de aplicación, obligaciones de las partes, derechos, excepciones, sanciones, autoridades y consignas relativas a la protección de datos personales y de datos transfronterizos.

Los países que hasta la fecha han firmado y entrado en vigor son: Alemania firmado el 28 de enero de1981 y entrado en vigor el 1 de enero de 1985; Austria firmado el 28 de enero de 1981 y entró en vigor el 1 de julio de 1988; Bélgica firmado el 7 de mayo de 1982 y entró en vigor el 1 de septiembre de 1993; Bulgaria firmado el 2 de agosto de 1998; Chipre firmado el 27 de julio de 1986; Dinamarca firmado el 28 de enero de 1981 en vigor 1 de febrero de 1990, España firmado el 28 de enero de 1982 en vigor el 1 de octubre de 1985; Estonia firmado el 24 de enero del 2000; Eslovaquia firmado el 14 de abril del 2000 en vigor el 1 de enero del 2001; Eslovenia firmado el 23 de noviembre de 1993 en vigor el 1 de septiembre de 1994; Finlandia firmado el 10 de de abril de 1991 en vigor el 1 de abril de 1992; Francia firmado el 28 de enero de 1981 en vigor el 1 de octubre de 1985; Grecia firmado el 17 de febrero de 1983 en vigor el 1 de diciembre de 1995; Holanda firmado el 21 de enero de 1988 en vigor el 1 de diciembre de 1993; Hungría firmado el 13 de mayo de 1993 en vigor el 1 de febrero de 1998; Irlanda firmado el 18 de diciembre de 1986 en vigor el 1 de agosto de 1990; Islandia firmado el 27 de septiembre de 1982 en vigor el 1 de julio de 1991; Italia firmado el 2 de febrero de 1983 en vigor el 1 de julio de 1997; Letonia firmado el 31 de octubre del 2000; Lituania firmado el 11 de febrero del 2000; Luxemburgo firmado el 28 de enero de 1981 en vigor el 1 de junio de 1988; Moldavia firmado el 4 de mayo de 1998; Noruega firmado el 13 de marzo de 1981 en vigor el 1 de octubre de 1985; Portugal firmado el 14 de mayo de 1981 en vigor el 1 de enero de 1994; Reino Unido

firmado el 14 de mayo de 1981 ratificado el 25 de agosto de 1987; República Checa firmado el 8 de septiembre del 2000; Rumania firmado el 18 de marzo de 1997; Suecia firmado el 28 de enero de 1981 en vigor desde 1982; Suiza firmado el 2 de octubre de 1997 en vigor el 1 de febrero de 1998.[112]

La Organización para la Cooperación del Desarrollo Económico, firmó directrices reguladoras de la Protección de la Vida Privada y los Flujos Trasfronterizos de datos de carácter personal, del 23 de septiembre de 1980. La Organización de las Naciones Unidas, firmó unas líneas directivas para la regulación de los archivos informatizados de Datos de carácter Personal en 1989.

Las organizaciones interesadas en el tema son: centro de Cooperaciones Trasnacionales de las Naciones Unidas (UNCTC), enfocada a resolver el problema de tarifas y régimen fiscal aplicable a la información; la Organización Mundial de la Propiedad Intelectual (OMPI), interesada en la propiedad de la información y el registro de nombres dominio; la Organización Mundial del Comercio (OMC), se interesa en el régimen fiscal aplicable y el Banco Mundial en cuanto a lo relativo a privacidad y confidencialidad de los datos entre otras organizaciones.

[112] Cfr. Valdez Téllez Julio. *Derecho Informático*. 3era ed. Ed. Trillas. México, 2004. Pág. 114.

CONVENIO SAFE-HARVOR (PUERTO SEGURO)

La Unión Europea firmó este convenio a principios del año 2000, el acuerdo entre administraciones de los Estados Unidos de Norteamérica y la Unión Europea, éste consistía que las empresas estadounidenses se unieran al programa Safe Harvor para la protección de datos de los europeos para que los Estados Unidos no los utilicen.

3.2. PAÍSES QUE TIENEN LEGISLACIÓN.

ALEMANIA.

El 21 de enero de 1977, se crea la Ley Federal para la Protección contra el Empleo Abusivo de Datos de Identificación Personal, esta ley se firmó el 28 de enero de 1981 y entró en vigor hasta 1985. Se modificó el 20 de diciembre de 1990 por la Ley de Protección de Datos (Bundes Datenschutzegsetz) y se volvió a reformar el 14 de septiembre de 1994. Estas normas reglamentarias en materia tributaria, identificación personal, registros de población, seguridad social, archivos policíacos, etc. El encargado de velar su cumplimiento es un Juez Federal. En 1986 se crea la Ley contra la Criminalidad Económica, contemplando los delitos de: espionaje de datos, fraude informático, alteración de datos y sabotaje informático. El Estado alemán de Hesse tiene un organismo propio supervisor llamado Data Inspektion Board D.I.B (Consejo de Inspección de Datos) desde 1970.

ARGENTINA.

En 1985 una comisión de juristas convocada por la Subsecretaria de Informática y Desarrollo expidió ciertas normas sobre el software y el derecho de autor, junto con estas normas se integró un proyecto de ley para regular la difusión de software y la informática, esta contemplaba los derechos del titular de un programa de computación y su uso. En esos años hubo también, un proyecto de ley para la protección de datos personales y se enfocaba a las libertades privadas y públicas de los archivos de sistemas informáticos y serían sancionados por omisiones especiales dotadas de autonomía. No fue hasta el 2 de noviembre del 2000 se crea la Ley de Protección de Datos Personales, el 30 de junio del 2003 la unión Europea publicó en su Diario Oficial que Argentina proporciona un nivel de protección adecuada para los datos personales. Con esto la Unión Europea permite el libre tránsito de datos personales hacia Argentina, esto se logró por los votos aprobatorios de las autoridades de protección de datos europeos, así como, los Estados miembros y el Parlamento Europeo. Este país latinoamericano es el único hasta la fecha en contar con la aprobación de la Unión Europea en materia de protección de datos.

AUSTRIA.

La Ley Federal sobre Protección de Datos de 18 de octubre de 1978, se modificó en 1986.

El 22 de diciembre de 1987 se promulga la Ley de reforma al Código Penal, en el artículo 148 y sanciona a los que causen un perjuicio patrimonial al elaborar un programa; por introducir, cancelar o alterar datos o actuar sobre el curso del procesamiento de datos. También contempla sanciones a los que aprovechándose de la profesión de especialistas en sistemas informáticos cometen estos hechos.

ESTADOS UNIDOS DE NORTEAMÉRICA.

Este país con su Acta de Privacidad (Privasy Act) del 31 de diciembre de 1974, elaborada para proteger la vida privada, encargada a los tribunales federales y éstos órganos jurisdiccionales lo sancionarían de forma penal.

En 1986 se crea el acta de Fraude y Abuso Computacional y en 1994 se adoptó la Acta Federal de Abuso computacional, sustituyendo la anteriormente mencionada. Esta Acta elimina argumentos técnicos de qué es y qué no es un virus, así como prohíbe la transmisión de un programa, información, códigos o comandos que causen daños a la computadora, sistemas informáticos, a las redes, información, datos o programas, esta Ley protege de la transmisión de virus informáticos. Esta Ley no define a los virus, sino describe el acto dando cabida conforme avancen los sistemas informáticos con el uso de la tecnología a que se sancionen los ataques informáticos.

Esta Acta sanciona de diferente manera a los que crean virus informáticos de manera intencional, castigándolos hasta con 10 años de prisión federal y

una multa y los que cometen el delito de manera imprudencial, se sancionarán con prisión de un año y una multa. En materia de fraudes electrónicos y otros actos dolosos realizados con acceso a sistemas informáticos, se sanciona con prisión y multa a la persona que defraude a otra utilizando una computadora o red informática.

ESPAÑA.

La ley Orgánica para la Regulación de Transmisión de Datos de 1992, cumplió su cometido hasta la abrogación por parte de la Ley Orgánica de Protección de Datos de Carácter Personal del 13 de diciembre de 1999.

El Nuevo Código Penal de España en su articulo 264-2, establece que se aplicara prisión de tres años y multa al que destruya, altere, inutilice o dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos. Este Código sanciona los delitos de manera muy detallada como son: la violación de secretos, espionaje y divulgación, y aplica pena de prisión y multa y se agrava cuando el delito se comete de manera dolosa y/o es cometido por servidores públicos, se sanciona con su inhabilitación. En materia de fraude electrónico en el articuló 248 solo describe el delito cuando es cometido con ánimo de lucro utilizando algún sistema informático, pero no detalla las penas a seguir en la comisión de este.

FRANCIA.

En 6 de enero de 1978 se crea la Ley 78-17 relativa a la Informática, Archivos y Libertades. En enero de 1988 se dicta al Ley relativa al fraude

informático, la cual sanciona con prisión de dos meses a los dos años de prisión y multas de diez mil a cien mil francos por la intromisión fraudulenta que modifique o suprima datos el articulo 462-2 sanciona a la persona que tenga acceso al sistema informático como al que permanezca en él y aumenta la pena si de ese acceso hay una modificación o supresión de datos contenidos en el sistema o se altere el funcionamiento de éste. El artículo 462.3 sanciona al que cometa de manera intencional el delito vulnerando o alterando los derechos de terceros que haya impedido o alterado el funcionamiento de un sistema de procesamiento de datos.

GRAN BRETAÑA.

En 1991 debido a un caso de hacking, (Piratería Informática) comenzó a regir en este país la Computer Misuse Act (Ley de Abusos Informáticos). Con esta ley las personas que alteraran datos informáticos o que no lo logran serian puestos en prisión hasta de cinco años o multa.

Esta Ley tiene una parte especial que especifica la modificación de datos sin autorización, también incluye a los virus en esta categoría, cuando se suelta un virus en un sistema informático las penas de prisión van desde un mes a cinco años dependiendo del daño causado. El 12 de julio de 1988 se crea en el Reino Unido la Ley Sobre Protección de Datos, se modificó esta Ley de acuerdo a la Unión europea el 16 de julio de 1998 y en el año 2000 se crea la Ley sobre Acceso a la Información.

HOLANDA.

El 28 de diciembre de 1988 se crea la Ley sobre protección de Datos, esta Ley fue complementada por la Ley de Archivo Policíaco del 21 de junio de 1990.

En marzo de 1993 entró en vigor la Ley de Delitos Informáticos la cual penaliza el hacking (piratería informatica) y el preacking (uso de servicios de telecomunicaciones evitando su pago total o parcialmente), por medio de esta ley el acto de alterar datos informáticos, es penado hasta con cinco años de prisión o multa. En el caso de los virus informáticos son penados de distinta forma, si fueron puestos por error o liberados dolosamente, en el primer caso la pena solo alcanza el mes de prisión; en el caso de que fueron liberados dolosamente la pena puede llegar hasta los cuatros años de prisión.

Como se observa, algunos países tienen legislación a nivel federal y algunos de manera particular en sus ciudades de esos mismos países, y ya desde hace varios años pusieron atención en estos delitos informáticos que vulneran su economía y sociedad, inclusive crearon leyes específicas para dar protección a los datos que se almacenan en sistemas informáticos. En el caso de América latina no sólo Argentina tiene una ley especifica para la protección de datos personales; también Chile tiene la Ley para la Protección de la Vida privada con fecha de 1999 y Paraguay con su Ley de Protección de Datos del 28 de diciembre del 2001; aunque realmente son relativamente nuevas es un gran avance en la prevención de estos delitos informáticos. En el continente asiático Hong Kong tiene su Ley de Protección de Datos de 1990 y el Ordenamiento sobre Protección de Datos de 1995 y Japón la Ley sobre Protección de Datos

Personales Informatizados del Sector Publico de 1988 y en el sector Privado de mayo del 2001.

3.3. LEGISLACIÓN EN MEXICO.

3.3.1. CÓDIGO PENAL FEDERAL.

En el año de 1999, el ejecutivo federal a cargo del Dr. Ernesto Zedillo Ponce de León emprendió una Cruzada Nacional contra el Crimen y la delincuencia, como parte del Programa Nacional de Seguridad Publica, con esto se pretendía que el Honorable Congreso de la Unión, se involucrará más en la creación del marco normativo para contar con mejores leyes contra la delincuencia. Con estos antecedentes, el Honorable Congreso de la Unión revisó varios artículos del Código Penal Federal entre los cuales destacaron, robo en todas sus modalidades y la incorporación de nuevos tipos penales como: falsificación de documentos y placas para vehículos automotores, sustracción indebida de hidrocarburos y sus derivados, entre otros; se propone la creación de figuras delictivas que utilizan la tecnología informática, el cohecho a servidores públicos extranjeros.

El uso de la tecnología en todas las áreas de la sociedad facilita el desarrollo nacional, pero aunado a esto también surgieron nuevas conductas antisociales, utilizando sistemas informáticos para poder delinquir; presentándose incluso conductas que los sistemas informáticos son el objeto o fin en si mismo del delito. Con esto el Honorable Congreso de la Unión presento su iniciativa de adición de una nueva figura delictiva conocida doctrinalmente como delitos

informáticos, dentro de los cuales se encuentran: el acceso no autorizado a computadoras o sistemas informáticos, la destrucción o alteración de información, el sabotaje por computadora, la intercepción de correo electrónico, el fraude electrónico y la transferencia ilícita de fondos. El congreso dentro de su iniciativa mencionaba que países como: Alemania y Francia, ya tenían legislación específica como se mencionó algunos estados de la República también ya contaban en sus códigos penales con figuras delictivas en torno a este delito como: Tabasco, Morelos, etc. El 17 de mayo de 1999 se publicó en el Diario Oficial de la Federación la adición del nuevo tipo penal relativo a delitos informáticos y que hasta la fecha sigue vigente:

TITULO NOVENO

REVELACIÓN DE SECRETOS Y ACCESO ILÍCITO A SISTEMAS Y EQUIPOS DE INFORMÁTICA

CAPÍTULO II

ACCESO A SISTEMAS Y EQUIPOS DE INFORMÁTICA

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

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

Articulo 211.Bis 2.- Al que sin autorización modifique, destruya o provoque pérdida de la información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán uno a cuatro años de prisión y de doscientos a seiscientos días multa.

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

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 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 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 que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrá de seis meses a cuatro años de prisión y de cien seiscientos días multa.

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

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 seiscientos días multa.

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

Las penas previstas ene este artículo se incrementaran en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instuciones 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 capítulo se aumentarán hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno.

Como se puede apreciar el bien jurídico que tutela este tipo penal es la privacidad y la integridad de la información, la penalidad aumenta cuando esas conductas son cometidas en perjuicio del Estado y el sistema financiero utilizando computadoras o sistemas informáticos. Desde los primeros artículos se menciona que "...protegidos por un mecanismo de seguridad..." es decir necesariamente para que el tipo se de, el sistema informático debe tener un mecanismo de seguridad, aunque no todos los sistemas lo tienen como puede ser una computadora personal, laptop (computadora portátil) o una P.D.A. (agenda digital personal) que son herramientas de uso cotidiano o inclusive un teléfono celular con una tarjeta de memoria.

El precepto no define a que se refiere con sistema o equipo de informática, tampoco menciona que se entiende por mecanismo de seguridad. En la iniciativa presentada por el Honorable Congreso de la Unión se menciona otros delitos informáticos que no fueron contemplados para estar en el tipo penal descrito como: la intercepción de correo electrónico (e-mail), que hoy en día es de uso común tanto para particulares, como empresas.

El delito informático que contempla el Código Penal Federal es determinado unisubjetivo, es decir un solo individuo realice la conducta descrita "al que estando autorizado...y "al que sin autorización...". Con esto habrá sujeto activo. En el aspecto subjetivo el sujeto activo realiza la conducta queriendo y conociendo el resultado, es decir no admite la culpa solo admite la comisión del delito de manera dolosa. El tipo penal descrito fue un gran avance en materia de combate a los delitos informáticos, pero se le dio mayor énfasis a la

protección del Estado y al sistema financiero ya que cuando se elaboro se pensó en el daño económico y de seguridad nacional que tenían que proteger

3.3.2. CÓDIGO PENAL PARA EL ESTADO DE MORELOS.

El Código Penal del Estado de Morelos fue promulgado el primero de octubre de 1945, desde entonces ha recibido diversas modificaciones, pero no ha modificado sus lineamientos fundamentales propios de la época en que fue elaborado. Hoy hace medio siglo de ese Código ha evolucionado, este en particular al igual que los demás códigos de los Estados y la legislación federal han sido trasformados de acuerdo a su tiempo y la vida social, por eso era necesario contar con un ordenamiento penal congruente con las con las necesidades del medio y los adelantos del derecho.

Es de suma importancia la tipificación y penalización de la conducta o su contraparte en el caso que se requiera, éste Estado ampara la libertad del hombre creando condiciones adecuadas de justicia y desarrollo; la incriminación debe reducirse a lo estrictamente indispensable y la consecuencia jurídica del delito debe respetar con mayor escrúpulo la dignidad del ser humano, todo este fundamento filosófico, ético y político de la ley penal debe quedar puntualmente traducido en las normas correspondientes y en la aplicación jurídica.

La redacción del Código Penal del Estado de Morelos es acorde con los avances de la ciencia jurídica penal, pero esta exenta de formulaciones doctrinales innecesarias o de afiliaciones filosóficas que se pueden perdonar,

este texto debe ser bien comprendido y aplicado por quienes tienen a su cargo esta misión, así como todos los morelenses destinatarios de las normas jurídicas, esto es lo que en parte en su iniciativa de reformas describía este Código.

El Capitulo Sexto Titulo Primero del Código Penal en cita tipifica en su artículo 150 la violación a la intimidad personal y familiar. Este artículo sanciona a quien utiliza medios de diversa naturaleza para escuchar, observar, trasmitir, grabar o reproducir la imagen o el sonido. Con esto se pretende salir al paso a ciertas conductas cometidas por particulares o agentes de autoridad, que afecten seriamente la intimidad personal y se valen de medios que la tecnología pone al alcance de los autores, estas conductas solo pueden sustraerse a la sanción cuando resulten amparadas por una excluyente del delito.

A continuación se transcribirá el artículo 150 del Código penal para el Estado de Morelos:

TITULO SEXTO
DELITOS CONTRA LA INTIMIDAD PERSONAL O FAMILIAR
CAPÍTULO I
VIOLACIÓN DE LA INTIMIDAD PERSONAL

Articulo 150.- Se impondrá de seis meses a cuatro años de prisión, a quien sin consentimiento de otro o sin autorización judicial, en su caso, y para conocer asuntos relacionados con la intimidad de aquel:

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

II. Reproduzca dichos documentos u objetos o

III. Utilice medios técnicos para escuchar, observar, trasmitir, grabar o reproducir la imagen o el sonido.

3.3.3. CÓDIGO PENAL PARA EL ESTADO DE TABASCO.

La publicación de la adición al Código Penal del Estado de Tabasco, correspondiente al delito de violación a la intimidad personal es de los más recientes en el país siendo del 22 de febrero de 1997, este articulo podría encuadrarse en los delitos informáticos

A continuación se transcribe este artículo:

TITULO SEPTIMO
DELITOS CONTRA LA INTIMIDAD PERSONAL
CAPÍTULO UNICO VIOLACIÓN DE LA INTIMIDAD PERSOANL

Articulo 150.- Se impondrá de seis meses a cinco años de prisión, a quien sin consentimiento de otro o sin autorización judicial, en su caso, y para conocer:

I. Se apodere de documentos u objetos de cualquier clase;
II. Reproduzca dichos documentos u objetos o
III. Utilice medios técnicos para escuchar, observar, trasmitir, grabar o reproducir la imagen o el sonido.

Los dos Códigos penales anteriores otorgan protección con fundamento a el derecho a la intimidad, la única diferencia radica es que el Código Penal del estado de Tabasco impone la prisión hasta por cinco años, solo un año más que el Código penal del estado de Morelos.

Su protección es muy limitada solo protege la intimidad de las personas, siendo que la información contenida en sistemas informáticos, es el verdadero bien jurídico tutelado en el caso del delito que estamos tratando. En los dos casos el delito es de carácter unisubjetivo, ya que solo se necesita un individuo para que realice la conducta descrita "...a quien sin consentimiento de otro...".
En el caso del aspecto subjetivo solo admite el dolo, conoce y quiere el resultado, no puede haber delito culposo.

3.3.4. CÓDIGO PENAL PARA EL ESTADO DE SINALOA.

EL Código Penal para el Estado de Sinaloa adiciono para su protección los delitos informáticos, poniéndolo en el Titulo Décimo Delitos contra el Patrimonio, publicado el 28 de octubre de 1992,a continuación se transcribe el articulo:

TITULO DECIMO DELITOS CONTRA EL PATRIMONIO
CAPÍTULO V DELITO INFORMATICO

Articulo 217.- Comete el 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 del delito informático se le impondrá una pena de seis meses a dos años de prisión y de noventa a trescientos días multa.

El artículo citado enuncia el delito informático tipificado en delitos patrimoniales, desde su colocación se esta limitando, ya que el delito informático no solo protege el patrimonio de las personas como se ha mencionado, su colocación se debe a su naturaleza de los derechos que se trasgreden con el actuar del individuo, el delito informático vulnera también la intimidad y sobre todo la información.

Este delito que enuncia el artículo es unisubjetivo, solo basta que un individuo lleve a cabo la conducta como describe "…la persona…" y "…al que cometa…". En el aspecto subjetivo, el individuo debe conocer y aceptar su resultado, es decir no admite la culpa, solo puede existir el dolo en su actuar.

En su fracción primera, se menciona la conducta de usar o entrar a una base de datos o sistema de computadoras, pero no delimita que se entiende por diseñar, ejecutar o alterar esquemas o artificios, entendiéndose diseñar hacer diagramas para la realización de un programa informático, y artificio seria la decodificación de señales de telecomunicaciones. En esta misma fracción, también se menciona el fraude, que se hace con medios o soportes informáticos, usándose como instrumento para obtener el dinero, y no se

emplean como fin en si mismo, como un delito informático propiamente dicho, por lo tanto la única diferencia, según este tipo penal de obtener un lucro indebido entre fraude y delito informático, es el empleo de sistemas de computadoras. Actualmente el Nuevo Código Penal para el Distrito Federal tipifica el fraude electrónico en el artículo 231 fracción XIV.

En la fracción segunda, establece que el sujeto en su actuar no hay un propósito especifico, solo basta que realice la conducta, sin importar la causa de su realización, la cual la lleve a cabo a través del empleo de sistemas o red de computadoras.

El delito no menciona quien es sujeto activo y el sujeto pasivo, ya que el actor también puede ser el titular del sistema de computadoras, o bien quien haga uso de este. La tentativa tampoco se señala, estos aspectos son de suma importancia en materia penal y no fueron considerados en su elaboración.

3.3.5. CÓDIGO PENAL PARA EL ESTADO DE NUEVO LEÓN.

Este Código hace mención en el artículo 365 fracción IV, lo que seria un robo informático, esta adición se publico el 26 de febrero de 1990

TITULO DECIMO NOVENO

DELITOS EN RELACIÓN CON EL PATRIMONIO

CAPÍTULO I ROBO

Articulo 365.- Se equipara al robo, y se castigará como tal:……..

.....

IV. El apoderamiento material de los documentos que contengan datos de computadoras, o el aprovechamiento o utilización de dichos datos, sin derecho y sin consentimiento de la persona que legalmente pueda disponer de los mismos.

Este artículo menciona al robo como fin utilizando computadoras, es decir el bien tutelado es el patrimonio. Este delito es unisubjetivo, cualquier persona puede cometerlo, basta que el sujeto activo se apodere de los documentos o aproveche o utilice esos datos sin consentimiento de su titular, se limita a un robo simple, tampoco hace mención que tipo de información se puede sustraer. La utilización de la información contenida en estos sistemas no solo puede sustraerse por un sujeto que no tenga derecho al mismo. sino también por su propio titular del sistema informático y esto sucede por estar a su alcance, este artículo limita esta conducta.

TITULO VIGESIMO SEGUNDO

DE LOS DELITOS POR MEDIOS ELECTRÓNICOS

Artículo 427.- A quien indebidamente accese a un sistema de tratamiento o de transmisión automatizado de datos, se le impondrá de dos meses a dos años de prisión y multa de doscientos a cien cuotas.

Artículo 428.- A quien indebidamente suprima o modifique datos contenidos en el sistema, o altere el funcionamiento del sistema de tratamiento o de transmisión automatizado de datos, se le impondrá de dos a ocho años de prisión y multa de trescientos a mil quinientas cuotas.

Artículo 429.- A quien indebidamente afecte o falsee el funcionamiento de un

> sistema de tratamiento o de transmisión automatizada de datos, se les impondrá de dos a ocho años de prisión y multa de trescientos a dos mil cuotas.

En los artículos anteriores se adecua más a lo que es un delito informático, si bien esta tipificado como delitos por medios electrónicos, el bien jurídico protegido son los datos o información contenida en los sistemas informáticos, se habla de un delito unisubjetivo en el caso de los tres artículos, ya que solo se necesita de un individuo para realizar la conducta como lo describe “a quien indebidamente…”. Estos artículos tampoco delimitan al sujeto activo ni el sujeto pasivo porque tampoco mencionan si el mismo titular del sistema informático puede indebidamente sustraer la información.

Nuestro país ha tenido grandes avances en materia de legislación en cuanto a la protección de sistemas informáticos incluso más que otros países de Latinoamérica, aunque realmente se basan más en la protección a la privacidad como es el caso de algunos códigos penales de los Estados de la Republica.

CAPÍTULO CUARTO.
NECESIDAD DE CREAR UN TIPO PENAL EN EL DISTRITO FEDERAL QUE REGULE EL ACCESO A SISTEMAS INFORMÁTICOS.

4.1. SEGURIDAD INFORMÁTICA.

En el presente capítulo que nos ocupa se hablará del acceso ilícito a sistemas informáticos, esto quiere decir que un sujeto de manera no autorizado tenga acceso a un sistema informático, esto es que esta en pleno conocimiento de que su conducta es contraria a derecho, ya que sabiendo que no tiene libre acceso a la información accese a ella; el supuesto se da también cuando se cuenta con autorización hasta cierto limite, pero el sujeto viola un deber jurídico de no hacer, ya que en el uso de esa autorización, realiza la conducta aún cuando le es permitido ingresar a los sistemas informáticos que contienen archivos diversos, de las dos formas se puede ingresar directamente o a través de Intranet o Internet.

La seguridad informática: Es el conjunto de 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 los 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 de la computadora o sistema informático, manteniendo la información, y los sistemas bajo llave o retirando de las mesas los documentos sensibles, sin embargo, impedir los delitos informáticos exige también métodos más complejos.

En un sistema de los denominados “tolerante a fallos” dos o más computadoras funcionan a la vez de manera redundante, por lo que si una parte del sistema falla el resto asume el control.

Los virus informáticos son programas, generalmente destructivos, que se introducen en una computadora (al leer un disco o acceder a una red informática), y pueden provocar pérdida de la información (programas y datos) almacenada en el disco duro. Existen programas antivirus que los reconocen y son capaces de “inmunizar” o eliminar el virus del sistema. La continua aparición de nuevos tipos de virus hace necesario mantener en el ordenador la versión más actualizada posible del programa antivirus.

Para evitar problemas en caso de apagón eléctrico existen las denominadas UPS (acrónimo de Uninterrupted Power Supply), baterías que permiten mantener el sistema informático en funcionamiento, por lo menos el tiempo necesario para apagarlo sin pérdida de datos, sin embargo, la única forma de garantizar la integridad física de los datos es mediante copias de seguridad; algunas aplicaciones ya las realizan de forma automática, otras se pueden configurar para que hagan copia de seguridad cada cierto intervalo de tiempo, con el fin de que se guarde el trabajo realizado en el mismo.

El mayor problema que tienen que resolver las técnicas de seguridad informática es el acceso a datos no autorizado. En un sistema seguro de alguna forma por así decirlo, el usuario, antes de realizar cualquier operación, se tiene que identificar mediante una clave de acceso o el denominado “pasword”. Las claves de acceso son secuencias confidenciales de caracteres que permiten que sólo los usuarios que las conozcan puedan acceder a una computadora o cualquier otro sistema informático. Para ser eficaces, las claves de acceso deben resultar difíciles de adivinar, las claves responden a una palabra real. Además, para aumentar la seguridad, los sistemas informáticos suelen limitar el número de intentos de introducir la clave; esto es un sistema muy utilizado pero no es realmente eficaz ni mucho menos seguro para restringir el acceso a sistemas informáticos, ya que simplemente utilizamos nombres comunes o números familiares que son fácilmente descifrables para cualquier otro sujeto que tenga contacto de relación social o de trabajo con nosotros.

Las tarjetas de contraseña son tarjetas de plástico, que no fácilmente pueden ser manipuladas; están dotadas de un microprocesador que almacena una clave de acceso que cambia frecuentemente de forma automática. Cuando se entra en una computadora mediante una tarjeta de acceso, la computadora lee la clave de la tarjeta y otra clave introducida por el usuario, y las compara respectivamente con una clave idéntica a la de la tarjeta (que la computadora genera automáticamente), y con la clave de acceso del usuario que está almacenada en una lista confidencial. En sistemas de alta seguridad las claves y las tarjetas de acceso se ven reforzadas por mecanismos biométricos basados en características personales únicas, como: las huellas dactilares, los capilares de la retina, las secreciones de la piel, el ácido desoxirribonucleico (ADN), las variaciones de la voz o los ritmos de tecleado; estos sistemas son empleado en los llamados edificios inteligentes o en oficinas corporativas para poder tener acceso a sistemas operativos como Mac OS, UNIX y Windows-NT que permiten

restringir el acceso a recursos del sistema (ficheros, programas, etc.) de acuerdo con este tipo de identificación.

Los hackers son usuarios muy avanzados que por su elevado nivel de conocimientos técnicos son capaces de superar determinadas medidas de protección. Internet, con sus grandes facilidades de conectividad, permite a un usuario experto intentar de forma anónima, y a veces conseguir el acceso remoto a una máquina conectada. Los ataques ahora son más complejos, han cambiado de trinchera y se modernizan con el tiempo, paralelamente al desarrollo cultural y tecnológico. En materia informática, nuestras sociedades están amenazadas no solamente por atentados cibernéticos desde sitios remotos, infiltraciones de crackers o hackers sino, también, por intrusiones deliberadas a sistemas de redes locales usando lo último en tecnología, inclusive la inalámbrica en movimiento llamada War Driving, esta es una actividad ilícita, aunque no regulada, encaminada a descubrir los puntos vulnerables para tener acceso a las redes inalámbricas de instituciones y organizaciones, de cualquier tipo y tamaño: esto sucede cuando una persona transita con una computadora personal y una antena, así, al estar en movimiento o caminando, captan la señal, logran el acceso y realizan las transacciones u operaciones deseadas o sólo entran y comprueban las vulnerabilidades. Es decir, el comportamiento e impacto de los intrusos ha evolucionado de manera muy significativa, antes de los accesos de banda ancha se usaban los módems, se marcaba el número telefónico para tener acceso a las computadoras, como redes de cómputo este se llama War Dialing. Las redes corporativas o computadoras con datos confidenciales no suelen estar conectadas a Internet; en el caso de que sea imprescindible esta conexión se utilizan los llamados cortafuegos, un ordenador, situado entre las computadoras de una red corporativa e Internet. El cortafuegos, impide a los usuarios no autorizados acceder a los

ordenadores de una red, y garantiza que la información recibida de una fuente externa no contenga virus.

Unas computadoras especiales denominadas servidores de seguridad proporcionan conexiones seguras entre las computadoras conectadas en red y los sistemas externos como: instalaciones de almacenamiento de datos o de impresión. Estos ordenadores de seguridad emplean el cifrado en el proceso de diálogo inicial, en el comienzo del mismo para proteger la confidencialidad es el cifrado. La información puede cifrarse y descifrarse empleando ecuaciones matemáticas y un código secreto denominado clave; generalmente se emplean dos claves, una para codificar la información y otra para descodificarla. La clave que codifica la información, llamada clave privada, sólo es conocida por el emisor, la clave que descodifica los datos, llamada clave pública, puede ser conocida por varios receptores; ambas claves se modifican periódicamente, lo que complica todavía más el acceso no autorizado y hace muy difícil descodificar o falsificar la información cifrada. Estas técnicas son imprescindibles si se pretende transmitir información confidencial a través de un medio no seguro como puede ser Internet.

4.2. VIRUS INFORMÁTICOS.

Cuando escuchamos la palabra virus es sinónimo de alguna enfermedad, es decir, que nos afecta en algo, nuestros sistemas informáticos o computadoras también sufren daños o ataques provocados por virus; al oír esta palabra o que

se esta propagando algún virus informático empezamos a tratar de buscar una solución para que nuestros sistemas no se vean alterados.

Un virus es un pequeño programa informático, creado con instrucciones precisas para provocar daños o alteraciones en documentos, mensajes de correo electrónico o áreas del software o hardware de un sistema informático, una base de datos, archivos, etc. Otra definición sería: "programa de ordenador. que se reproduce a si mismo e interfiere con el hardware de una computadora o con su sistema operativo (software que controla una computadora)".[113]

Se les denomina virus en analogía a los seres biológicos, pues son pequeños, se auto reproducen e infectan a cientos o miles de entes receptores desde una fuente de emisión o transmisión, que a la vez se convierte en receptor. 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, la computadora debe cargar el virus desde la memoria de ésta y seguir sus instrucciones; estas instrucciones se conocen como carga activa del virus, la carga activa puede trastornar o modificar archivos de datos, presentar un determinado mensaje o provocar fallos en el sistema operativo.

Existen otros programas informáticos nocivos, similares a los virus, pero que no cumplen ambos requisitos de reproducirse y eludir su detección; estos programas se dividen en tres categorías: caballos de Troya, bombas lógicas y gusanos. Un caballo de Troya aparenta ser algo interesante e inocuo; por ejemplo: un juego, pero, cuando se ejecuta puede tener efectos dañinos. Una bomba lógica, libera su carga activa cuando se cumple una condición

[113]Enciclopedia Encarta 2005.Microsoft Corporation.

determinada, como, cuando se alcanza una fecha u hora determinada, o cuando se teclea una combinación de letras. Un gusano se limita a reproducirse, pero puede ocupar memoria de la computadora y hacer que sus procesos vayan más lentos.

HISTORIA DE LOS VIRUS INFORMATICOS.

En el año 1939, el matemático estadounidense de origen húngaro John Von Neumann escribió un artículo exponiendo su “Teoría y organización de autómatas complejos,” realizada en el Instituto de Estudios Avanzados de Princenton en Nueva Jersey, donde demostraba la posibilidad de desarrollar pequeños programas que pudiesen tomar el control de otros de similar estructura. Hacia 1949 en los laboratorios Bell Computer, subsidiaria de A&T, tres jóvenes programadores Robert Thomas Morris, Douglas Mcllory y Victor Vysottsky, crearon un juego al que denominaron: Core Wars, inspirados en la teoría de John Von Neumann. El juego consistía en que cada uno de los dos jugadores escribiera un programa llamado organismo, cuyo hábitat fuera la memoria de la computadora, a partir de una señal, cada programa intentaba forzar al otro a efectuar una instrucción, ganando el primero que lo consiguiera; al término del juego, se borraba de la memoria todo rastro de la batalla, pues eran actividades severamente sancionada debido al gran riesgo que implicaba el dejar a un organismo suelto, que pudiera acabar con las aplicaciones al día siguiente. Así nacieron programas destinados a dañar recursos computacionales.

En agosto de 1981, IBM introduce al mercado su primera computadora personal (PC), sin embargo, la prisa con la cual se puso a la venta la IBM PC, impidió que se le equipara de un buen sistema operativo, y como resultado de esa improvisación, todas las versiones del llamado PC-DOS y posteriormente del MS-DOS fueron totalmente vulnerables a los virus.

En el año de 1983, el ingeniero eléctrico estadounidense Fred Cohen, acuñó el término virus para describir un programa informático que se reproduce así mismo. En 1986, se propagaron intencionalmente con fines maliciosos los primeros virus: “Brain, Bouncing Ball y Marihuana,” que fueron las primeras especies virales significativas de difusión masiva. En 1987, el virus “Brain” ya se había extendido por todo el mundo. En 1985 aparecieron los primeros caballos de Troya, que es un método para insertar otras funciones de manera encubierta en una computadora, esto se disfrazaba como programa de mejora de gráficos llamado EGABTR, y un juego de nombre NUKE-LA. En 1988 aparecieron dos nuevos virus: Stone el primer virus de sector de arranque inicial y el primer gusano de Internet, que cruzó Estados Unidos de un día a otro a través de una red informática. Por su parte, durante 1989, el virus de origen búlgaro Dark Avenger, se propagó por toda Europa y Estados Unidos, haciéndose famoso por su ingeniosa programación y rápida técnica de infección y propagación, y en 1990 apareció el primer virus polimorfo. Con el avance informático, el desarrollo tecnológico, y el uso generalizado de Internet a mediados de los noventas, el mundo cibernético tuvo un medio ideal para la inmediata y masiva replicación de los gusanos y virus de diversos niveles de peligrosidad, los cuales, cada día son más sofisticados. El correo electrónico (e-mail) es el medio más común, mediante archivos adjuntos que se activan una vez que se abre el mensaje o se ejecutan aplicaciones o se cargan documentos que lo acompañan.

¿COMO SE PRODUCEN LAS INFECCIONES?

Los virus informáticos se difunden, cuando las instrucciones o código ejecutable que hacen funcionar los programas pasan de una computadora a otra. Una vez que un virus está activado, puede reproducirse copiándose en disket o CD-ROM, en el disco duro, en programas informáticos legítimos o a través de redes informáticas, estas infecciones son mucho más frecuentes en los PC que en sistemas profesionales de grandes computadoras, porque los programas de los PC se intercambian fundamentalmente a través de diskets, CD-ROM o de redes informáticas no reguladas.

Los virus funcionan, se reproducen y liberan sus cargas activas sólo cuando se ejecutan; por eso, si una computadora está simplemente conectada a una red informática infectada o se limita a cargar un programa infectado, no se infectará necesariamente. Normalmente, un usuario no ejecuta conscientemente un código informático potencialmente nocivo; sin embargo, los virus engañan frecuentemente al sistema operativo de la computadora o al usuario informático, para que ejecute el programa viral.

Algunos virus tienen la capacidad de adherirse a programas legítimos; esta adhesión puede producirse cuando se crea, abre o modifica el programa legítimo; cuando se ejecuta dicho programa ocurre lo mismo con el virus. Los virus también pueden residir en las partes del disco duro, disket o CD-ROM, que cargan y ejecutan el sistema operativo cuando se arranca el ordenador, por lo

que dichos virus se ejecutan automáticamente. En las redes informáticas, algunos virus se ocultan en el software que permite al usuario conectarse al sistema.

Una variante de los virus, es que estos intrusos informáticos secuestran los archivos para que los usuarios paguen una cierta cuota monetaria, y pueden incluso crear su propio punto de acceso inalámbrico en un hotsspot por medio de redes inalámbricas o Wi-Fi. Cuando se enciende una computadora y se quiere ver los estados de cuenta de una tarjeta de crédito o débito, pero al dar "click" se recibe un advertencia que el archivo esta incriptado y se necesita una clave por cierta cantidad, al incriptar la información, este virus se autodestruye para evitar ser detectado,; como en un secuestro no se tiene la seguridad de que se pueda desencriptar la información, los expertos en informática llaman a esta modalidad rasonware (programa de rescate). Otra modalidad de los virus es el ataque a servidores de nombre dominio, es decir, se teclea la página de Internet, pero se direcciona a otro sitio donde será usada su información, por ejemplo, cuando se entra a la página de nuestro banco y dejamos nuestra información.

ESPECIES DE VIRUS.

Existen seis categorías de virus: parásitos, del sector de arranque inicial, multipartitos, acompañantes de vínculo, y de fichero de datos. Los virus

parásitos infectan ficheros ejecutables o programas de la computadora, no modifican el contenido del programa huésped, pero se adhieren al huésped de tal forma que el código del virus se ejecuta en primer lugar, estos virus pueden ser de acción directa o residentes; un virus de acción directa selecciona uno o más programas para infectar cada vez que se ejecuta; un virus residente se oculta en la memoria de la computadora e infecta un programa determinado cuando se ejecuta dicho programa. Los virus del sector de arranque inicial residen en la primera parte del disco duro, disket o CD-ROM, conocida como sector de arranque inicial, y sustituyen los programas que almacenan información sobre el contenido del disco o los programas que arrancan la computadora; estos virus suelen difundirse mediante el intercambio físico de disket o CD-ROM Los virus multipartitos combinan las capacidades de los virus parásitos y de sector de arranque inicial, y pueden infectar tanto ficheros como sectores de arranque inicial.

Los virus acompañantes no modifican los ficheros, sino que crean un nuevo programa con el mismo nombre que un programa legítimo y engañan al sistema operativo para que lo ejecute. Los virus de vínculo modifican la forma en que el sistema operativo encuentra los programas, y lo engañan para que ejecute primero el virus y luego el programa deseado; un virus de vínculo puede infectar todo un directorio (sección) de una computadora, y cualquier programa ejecutable al que se acceda en dicho directorio desencadena el virus. Otros virus infectan programas que contienen lenguajes de macros potentes (lenguajes de programación que permiten al usuario crear nuevas características y herramientas) que pueden abrir, manipular y cerrar ficheros de datos; estos virus, llamados virus de ficheros de datos, están escritos en

lenguajes de macros y se ejecutan automáticamente cuando se abre el programa legítimo, son independientes de la máquina y del sistema operativo.

PREVENCIÓN Y DETECCIÓN DE VIRUS.

Los usuarios, pueden prepararse frente a una infección viral, creando regularmente copias de seguridad del software original legítimo y de los ficheros de datos, para poder recuperar el sistema informático en caso necesario; puede copiarse en un disket o CD-ROM el software del sistema operativo y proteger el disco contra escritura, para que ningún virus pueda sobreescribir el disco. Las infecciones virales se pueden prevenir obteniendo los programas de fuentes legítimas, empleando una computadora en cuarentena para probar los nuevos programas y protegiendo contra escritura los diskets y CD-ROM siempre que sea posible.

Para detectar la presencia de un virus se pueden emplear varios tipos de programas antivirus; los programas de rastreo pueden reconocer las características del código informático de un virus, y buscar estas características en los ficheros de la computadora, como los nuevos virus tienen que ser analizados cuando aparecen, los programas de rastreo deben ser actualizados periódicamente para resultar eficaces. Algunos programas de rastreo buscan características habituales de los programas virales; suelen ser menos fiables.

Los únicos programas que detectan todos los virus son los de comprobación de suma, que emplean cálculos matemáticos para comparar el estado de los programas ejecutables, antes y después de ejecutarse, si la suma de comprobación no cambia, el sistema no está infectado. Los programas de comprobación de suma, sin embargo, sólo pueden detectar una infección después de que se produzca.

Los programas de vigilancia detectan actividades potencialmente nocivas, como la sobreescritura de ficheros informáticos o el formateo del disco duro de la computadora. Los programas caparazones de integridad establecen capas por las que debe pasar cualquier orden de ejecución de un programa, dentro del caparazón de integridad se efectúa automáticamente una comprobación de suma, y si se detectan programas infectados no se permite que se ejecuten.

Una vez detectada una infección viral, ésta puede contenerse aislando inmediatamente los ordenadores de la red, deteniendo el intercambio de ficheros y empleando sólo discos protegidos contra escritura, para, que un sistema informático se recupere de una infección viral, primero hay que eliminar el virus; algunos programas antivirus intentan eliminar los virus detectados, pero a veces los resultados no son satisfactorios; se obtienen resultados más fiables, desconectando la computadora infectada, arrancándola de nuevo desde un disket o CD-ROM protegido contra escritura, borrando los ficheros infectados y sustituyéndolos por copias de seguridad de ficheros legítimos, y borrando los virus que pueda haber en el sector de arranque inicial.

Los creadores de virus, cuentan con sus propias estrategias para escapar de los programas antivirus, por ejemplo, los virus polimorfos, que efectúan variaciones de si mismos para evitar ser detectados por los programas de rastreo de virus, otros se ocultan en el sistema operativo y simulan los resultados de un sistema que no esta infectado; los virus llamados infectores rápidos, no necesitan ejecutarse, basta con que se abran e infecten la computadora; los infectores lentos que infectan los archivos solo cuando se modifican; los infectores escasos que hacen, por ejemplo, que un programa de cada diez se infecte; esto hace cada vez se más difícil detectar un virus.

Los usuarios que utilizan frecuentemente el correo electrónico y reciben información, no toda es segura, ya que reciben spam (correo basura), mensajes fraudulentos, virus, spyware, etc.

Para combatir estos problemas, no basta con actualizar de vez en cuando un simple programa antivirus, se necesitan acciones preventivas más efectivas por parte del usuario.

Algunas recomendaciones para evitar ser víctima de virus o hackers son:

- Mantener actualizado el sistema operativo y el navegador de Internet ya que los ataques utilizan sus vulnerabilidades.
- Tratar de no hacer transacciones o banca en línea en un hotspot. y menos si nunca se ha conectado a uno.
- Evitar sitios que ofrezcan almacenamiento virtual, la información podría estar vigilada por hackers.

- No enviar ni recibir archivos por mensajería instantánea, ya que pudieron ser interceptados y contaminados con información maliciosa.
- Instalar y mantener actualizado soluciones de antivirus, firewall y detector de intrusos.

Diariamente se trasmiten en el mundo millones de correos electrónicos pero la mayor parte de esos mensajes son: spam, contienen virus o algún elemento malicioso. Por este motivo la compañía Iron Port México, ofrece la emisión de alertas en tiempo real contra epidemias virales mediante una red de monitoreo, que analiza los patrones de comportamiento del flujo de correo electrónico. El único requisito es inscribirse en su página de Internet www.ironport.com/outbreack_alerts; luego se recibe gratuitamente desde el Centro de Operaciones Contra Amenazas (Treat Operation Center), su tiempo de anticipación es de 13.6 horas en promedio, teniendo una ventaja de 50 horas para ciertos virus polifórmicos, difícil de identificar con un antivirus tradicional; con esto los usuarios, al llegar a su computadora un correo electrónico (e-mail) lo identifica el sistema como sospechoso éste evite abrirlo y contaminarse, también recibe el nombre del virus su variante, así como su patrón o historial relevante detectada.

4.3. SEGURIDAD PARA MENORES.

La asociación Mexicana de Internet (AMIPCI), registra en el 2005, la cifra de 19 millones de mexicanos usuarios de esta tecnología, de los cuales 47% oscila entre los 13 y 24 años, y 42% corresponde a jóvenes adultos con edades entre

25 y 45 años, mientras que el porcentaje restante pertenece a edades superiores a los 46 años.

Aún, sin tener un dato estadístico preciso que refleje el porcentaje del mercado que utiliza Internet menor a los 13 años, pero que, con seguridad lo consulta, resulta de singular importancia las cifras antes señaladas por la AMIPCI, donde se refleja la enorme penetración con respecto al uso de esta herramienta entre los menores de edad, que, sin llevar un control adecuado por parte de los padres o responsables de los niños, podría volverse un producto nocivo para la salud mental y física de ellos.

Como en la vida real, los peligros a los que se enfrentan los menores de edad, al navegar en la Web son muchos y muy variados: pornografía, pedofilia, venta de droga, cuestiones racistas y de comportamientos que pueden manipular de manera negativa la conducta del niño. La ventaja que tienen los padres en cuanto a este tipo de tecnología, es que se puede programar al equipo de cómputo sobre que páginas abrir, cuáles sitios son seguros y cuáles representan un peligro para el niño.

La empresa de seguridad Symantec, refleja en un estudio reciente, realizado a más de cinco mil niños italianos, cuyas edades oscilan entre los 8 y 13 años, que el 27% de ellos no son supervisados en sus visitas a páginas Web, 34% de ellos nunca han recibido algún consejo por parte de los padres sobre lo que deben y no deben hacer, o ver cuando naveguen en Internet; y la mayoría

utilizan con frecuencia algunos servicios como salas de chat, videoconferencia, grupos de noticias, entre otros; para comunicarse en la Web con extraños.

Cabe señalar que en este estudio, la mayoría de profesores encuestados no están seguros acerca de la forma de abordar el tema de Internet; sin embargo, creen que se debe mejorar de alguna forma el método de enseñanza, para desarrollar las destrezas en las nuevas tecnologías, aunque el estudio no se realizó en nuestro país, refleja la vulnerabilidad a que están expuesto los niños y jóvenes, al usar esta herramienta tan cotidiana que les facilita el contacto con fuentes de información de manera rápida.

RECOMENDACIONES.

Hay varias empresas de seguridad a nivel nacional e internacional, públicas y privadas, que abarcan el tema de la seguridad infantil en la Web con seriedad y aún más, con prontitud y mucho cuidado. No está por demás decir que la población infantil está muy protegida actualmente, con leyes y penas sumamente estrictas y severas, pero que, sin la debida información por parte de los padres o tutores del menor, estas medidas no llegarán a ser efectivas y eficaces.

Ante el cúmulo de opciones que se manejan en la misma Internet; podemos señalar dos tipos principales de recomendaciones, las de índole personal y las del campo tecnológico.

A) Personales.

Como resultado de una coordinación directa entre diversas instituciones mexicanas, entre ellas, la AMIPCI, PROFECO, Policía cibernética–PFP; se han emitido una serie de recomendaciones para hacer del Internet un espacio seguro, para la diversión y el conocimiento del menor.

Algunas recomendaciones básicas que estos organismos proporcionan son:

- Instalar la computadora en un lugar visible, evitando lo más que se pueda las recámaras o habitaciones aisladas; con ello se podrá tener una supervisión más accesible acerca de los contenidos que los jóvenes estén visitando en Internet.
- Advertirles que no deben confiar en las personas que conozcan en chats, e-mails, entre otros, así como a negarse a proporcionar datos o fotos personales o familiares.
- Navegue algún tiempo con sus hijos en la red, mostrando interés por los temas que le gusten, así como por las personas con las que se comunica; de ser posible, trabaje en conjunto con los padres de los amigos de sus hijos para ofrecer un ambiente de navegación seguro.
- Proteja sus contraseñas y cree nombres genéricos. Asegúrese de que sus menores no tengan alias que revelen su información personal, incluyendo su nombre completo, edad, género, etc.

- Señáleles los peligros que pueden tener al llenar cuestionarios que se encuentren en Internet, sin su permiso y supervisión.
- Enseñe a sus pequeños a nunca revelar la contraseña de Internet a ninguna persona, incluso si esta persona dice trabajar para alguna compañía proveedora de este servicio.
- Fije y establezca los tiempos y horarios para acceder a la red.
- Evite proporcionar a sus hijos los números de tarjetas de crédito, débito o de cuentas bancarias que maneje.
- Procure enseñarles a no aceptar dinero o favores de extraños.

B) Tecnológicas.

Esta parte se refiere al software especializado que se debe habilitar para evitar algún mal al estar navegando en Internet. Hay algunos programas que se especializan en la protección de menores, y algunos proveedores de Internet ya lo incluyen en su paquete de instalación.

Otros, por ejemplo, son de empresas privadas de seguridad en Internet que lo distribuyen como cualquier otro software, de ahí que se puedan comprar en línea o en una tienda ordinaria especializada en equipos de cómputo. Hay algunos más que se pueden bajar de manera gratuita en la red.

El software con mayor demanda en este tipo de temas es conocido como un “filtro”. Este programa bloquea los accesos a sitios que contienen determinadas

palabras o imágenes, y permiten la entrada a otros lugares previamente determinados por los padres o el proveedor de servicio.

Las funciones son tan variadas como los productos. Hay algunos filtros que pueden limitar el tiempo al navegar por la red, monitorear constantemente los sitios visitados, así como los chats o e-mails del usuario. En otras modalidades, hay filtros que bloquean el intercambio de archivos, juegos, chats, foros, y hay unos más que únicamente permiten el acceso a canales especializados sólo para niños, como en el caso de American On Line.

Es indispensable contemplar que todas estas medidas nunca sustituirán la presencia y comunicación que debe existir entre los padres e hijos para entender y resolver los problemas y circunstancias que puedan encontrarse en la red. La verdadera importancia de estas recomendaciones es apoyar la exploración segura del Internet para futuras generaciones.

4.4. CLARA (COOPERACIÓN LATINOAMERICANA DE REDES AVANZADAS)

La falta de administradores capacitados en seguridad, además de una inadecuada configuración de sistemas y redes y la ausencia de políticas de seguridad, ha provocado que exista poca o nula seguridad en redes o sistemas informáticos en América Latina.

La Red CLARA: (Cooperación Latinoamericana de Redes Avanzadas), este sistema interconecta comunidades académicas y de investigación en 19 países de América Latina, que comprende universidades, escuelas de educación superior, centros de tecnología, laboratorios, institutos y centros de investigación.

La misión fundamental de CLARA, es la de promover una cultura de seguridad en sistema y redes informáticas en la región de Latinoamérica y el Caribe, esto es trabajar para la creación de un Grupo de Trabajo en Seguridad (GTS).que cuente con la participación de los CSIRT Computer Security Incident Responce, con el objetivo de fomentar acciones con la colaboración de redes y sistemas académicas involucradas.

Este grupo de trabajo en seguridad, es coordinado por la UNAM a través de DGSC/UNAM-CERT Departamento de Seguridad en Cómputo y Equipo de Respuesta a Incidentes de Seguridad, es capaz de reaccionar a la red de miembros CLARA en la discusión de aspectos importantes como: la comunicación y colaboración segura, que incluyen, autenticación, identificación, privacidad, etc. Así como en actividades relacionadas con la detección e intervención en incidentes de seguridad.

Los objetivos de la red CLARA son:

- Establecer una estructura de seguridad en cómputo en cada uno de los países afiliados.

- Promover el surgimiento de nuevos CERTs en la región, y coordinar el entrenamiento de sus grupos.
- Proveer un foro de discusión para el intercambio de experiencias y conocimientos.
- Facilitar la correlación e intercambio de información relativa a incidentes de seguridad en la región.
- Promover la respuesta coordinada y oportuna a incidentes de seguridad.
- Tener una visión sistémica de los incidentes de seguridad en América Latina.
- Establecer servicios piloto para la comunidad de CERTs en América Latina.
- Elaborar mejores prácticas en el área de seguridad.
- Colaborar con otras iniciativas regionales similares en el mundo.

La participación en este Grupo de Trabajo está abierta para los representantes de todas las redes, miembros de CLARA y las respectivas organizaciones usuarias; de igual forma, la incorporación de terceros en dicha labor es posible por lo que se analizará de manera particular.

Para el periodo 2005-2006, el plan de acción de este Grupo de Trabajo, coordinado en México por el DSC/UNAM-CERT de la DGSCA-UNAM y en Brasil por el CASI/RNP, comprende el estudio de la situación de seguridad en América Latina, un análisis del estado de los CERTs en el área, fomentar la educación y entrenamiento en seguridad, la creación del acervo digital de “Buenas prácticas”, además de la coordinación de reuniones y seminarios donde se estudie a profundidad este fenómeno.

Entre los proyectos de colaboración de los CERTs de América Latina, destaca el concurso “Reto Forense” puesto que permite desarrollar y enriquecer diversas habilidades en la aplicación de procedimientos y técnicas para determinar intrusiones en un sistema de cómputo.

En el área de educación y entrenamiento, el curso “FIRST/TRANSITS” (Training of Network Security Incident Team Staff), dirigido a los responsables de seguridad en cómputo de las instituciones de educación superior del país y realizado por vez primera en la Ciudad de México en el marco del Congreso de Seguridad en Cómputo, tuvo como objetivo crear conciencia en los responsables de la seguridad en cómputo de las instituciones de educación superior, en cuanto a la conformación de equipos de respuesta a incidentes de seguridad, además de propiciar entre ellos el intercambio de ideas, propuestas y soluciones, con miras a la conformación de grupos de seguridad.

PAÍSES MIEMBROS.

Argentina, Costa Rica, Guatemala, Perú, Brasil, Cuba, México, República Dominicana, Bolivia, Ecuador, Nicaragua, Uruguay, Colombia, el Salvador, Panamá, Venezuela, Chile, Honduras y Paraguay.

4.5. UNAM-CERT.

HSTORIA.

En la medida que crece y se diversifica el uso de sistemas informáticos, se incrementan también los riesgos de que los equipos de cómputo y dispositivos electrónicos, conectados o no a Internet, sean vulnerables a ataques e incidentes que ponen en peligro la integridad de la información que en ellos se procesa, almacena o transfiere; de ahí la importancia fundamental de contar con programas preventivos, estrategias correctivas, planes de emergencia y respuestas inmediatas para proteger los equipos y sistemas; así como salvaguardar información y datos, en una sociedad que, cada día, basa más sus dinámicas y procesos en sistemas de cómputo y redes; la seguridad debe pasar de ser una responsabilidad importante a ser una prioridad para los gobiernos, las instituciones y empresas, así como para las personas, es decir, se requiere de una política clara e integral de seguridad en cómputo.

En este marco, desde hace diez años, la Universidad Nacional Autónoma de México (UNAM), a través de la Dirección General de Servicios de Cómputo Académico (DGSCA), ha impulsado diversas acciones para promover, por un lado, una cultura de seguridad y, por otro, la integración de grupos de trabajo altamente especializados que den respuesta a sistemas que han sido víctimas de ataques.

Las actividades requeridas para poder mantener un buen nivel de seguridad en los equipos aumentaron conforme el uso de la nueva tecnología se expandió. pronto se recibió información de problemas de seguridad en la UNAM

y en el resto del mundo, dada la importancia y naturaleza de estos problemas, surgió la idea de formar un área para la salvaguarda de los equipos.

En agosto de 1994, en la DGSCA se formó el Equipo de Seguridad en Cómputo (ESC) con el objetivo de difundir información sobre seguridad en cómputo, así como crear y difundir políticas en la materia. En 1995, el Departamento de Supercómputo, también constituye un Área de Seguridad en Cómputo (ASC), cuya labor consistía en mantener la seguridad de los equipos de supercómputo, realizando actividades encaminadas a promover la cultura de seguridad en cómputo.

A partir de 1999, el ASC toma mayor importancia debido a que se desempeñaba tanto al interior de la DGSCA como en entidades de la UNAM.

El desarrollo cambiante del nuevo siglo y la evolución de las tecnologías de la información, hicieron del campo de la seguridad en cómputo un área de primer orden, por lo que la DGSCA se propuso convertir al Área de Seguridad en Cómputo en un organismo que cubriera las exigencias de la vida moderna del cómputo, tanto dentro de la UNAM, como en el país, constituyéndose en el 2000 en el Departamento de Seguridad en Cómputo (DSC). Desde su conformación, el DSC ha realizado labores de difusión, capacitación, asesoría y atención de incidentes dentro y fuera de la UNAM.

Después de ocho años de trabajo e investigación, y luego de cubrir los exigentes requisitos técnicos, académicos y administrativos, establecidos por el Forum Incident Response Security Team (FIRST), www.first.org, organismo rector a nivel mundial con sede en Chicago, Estados Unidos, la DGSCA funda en el año dos mil uno UNAM-CERT y con ello se crea, en nuestro país, el primer equipo de respuesta a incidentes con reconocimiento internacional, y con respaldo del System Administration Networking Security, entidad que trabaja de cerca con el F.B.I.

ACTIVIDADES DE UNAM-CERT.

La UNAM-CERT son un equipo de especialistas en seguridad en cómputo que atiende a instituciones de cualquier tipo, que han sido víctimas de algún ataque tanto en sus sistemas de cómputo como en sus sitios de Internet; pública periódicamente información actualizada sobre alertas y vulnerabilidades, implantación de políticas, elabora análisis de riesgos, y realiza investigación dentro de esta área para contribuir a hacer, cada día, más seguros los sistemas y las redes.

Una tarea particular de este organismo académico, consiste en la realización de programas de divulgación y capacitación en seguridad en cómputo, por lo que realiza los seminarios Grupo de Administración y Seguridad en Unix (GASU) y Admin-UNAM, participa desde 1993 en la celebración mundial del Día Internacional de Seguridad en Cómputo (DISC) y anualmente realiza un congreso internacional altamente especializado.

El UNAM-CERT es el único organismo oficial reconocido en México en materia de seguridad por diversas agrupaciones de los Estados Unidos. Anualmente atiende más de 1,000 incidentes en instituciones educativas públicas y privadas, así como gubernamentales de los tres niveles de gobierno y empresas, emite más de 50 boletines y notas de seguridad y más de 800 alertas; y entre sus principales funciones también se encuentran informar, catalogar, clasificar y analizar oportunamente los problemas relacionados con la seguridad en cómputo; así como regular, controlar estándares y facilitar la difusión de normas para que los laboratorios, centros de investigación, instituciones bancarias y financieras, empresas y organizaciones las adopten en su beneficio; también trabaja en línea y ofrece un foro abierto en donde concurren diferentes instituciones, escuelas y universidades para obtener información, asesorías y herramientas especializadas.

UNAM-CERT es un organismo universitario y sin fines de lucro, único en su tipo en América Latina y el Caribe, pues sólo hay dos más, uno en Brasil y el otro en Perú, el primero pertenece a la policía brasileña y el segundo opera con un enfoque comercial, en tanto pertenece a la compañía transnacional ATT.

Contar con un CERT en México, y particularmente situado en la UNAM, implica contar con respaldo internacional sobre las prácticas de seguridad en cómputo sugeridas, las leyes en Internet y sus amenazas, disponibilidad de información para detectar la información más crítica en una empresa, salvaguardar la información, ahorro de tiempo en el manejo de incidentes en diferentes sitios y países, y compartir experiencias con CSIRTs de otros países. Todo ello se traduce en formas directas de prevenir incidentes y solucionarlos.

Asimismo, ofrece oportunidades seguras en las distintas variaciones del e-commerce, Business to business (B2B), Business to consumer (B2C) y Business to goverment (B2G), para que cuenten con información provista al CERT de México de los organismos internacionales que proveen las regulaciones especiales, los avances en materia de legislación informática; información relevante de seguridad en cómputo; respuestas a incidentes; soluciones de seguridad en cómputo; consultorías y asesorías; auditorias locales y remotas; evaluación de seguridad local; auditoria y reconfiguración de firewalls y ruteadores; evaluación de seguridad en servicios de red; servicios de exploración de líneas telefónicas y evaluación de bases de datos, etcétera.

4.6. LA POLICÍA CIBERNÉTICA Y DC MÉXICO.

4.6.1. POLICÍA CIBERNÉTICA.

La Policía Federal Preventiva (P.F.P), desarrolló en México la primera Unidad de Policía Cibernética, esto por la creciente ola de delitos informáticos entre los cuales destacan: pornografía infantil, prostitución, fraude e intrusión, utilizando sistemas informáticos. Esta Policía, además de las acciones preventivas en materia de delitos cometidos en Internet, y usando medios informáticos, cuenta con un área específica en materia de prevención y atención de denuncias de delitos contra menores, como los que hay en países desarrollados. Los crímenes cometidos en agravio de menores, a través de una computadora y otros medios, han tenido un gran incremento en México, como en otros países debido al desarrollo tecnológico y la oportunidad que les brinda el uso de Internet, éste es utilizado por organizaciones criminales de pedófilos

que promueven y trasmiten pornografía infantil, también lo utilizan bandas internacionales de prostitución, utilizando medios informáticos como promoción y reclutamiento.

Otro tipo de delitos que se han incrementado de manera considerable son el fraude cibernético, la piratería de software, la intrusión a sistemas de cómputo, el hackeo, la venta de armas y drogas por Internet y ciberterrorismo; las cuales son amenazas para la sociedad.

ACTIVIDADES.

- Identificación y desarticulación de organizaciones dedicadas al robo, lenocinio, tráfico y corrupción de menores, así como a la elaboración, distribución y promoción de pornografía infantil, por cualquier medio.
- Análisis y desarrollo de investigaciones de campo sobre actividades de organizaciones locales e internacionales de pedofília, así como redes de prostitución infantil.
- Localización y puesta a disposición ante Agentes del Ministerio Público a personas dedicadas a cometer delitos utilizando computadoras.
- Realización de operaciones anti-hacker, utilizando Internet como detector de delincuentes, que cometen fraudes, intrusiones y organizan sus actividades en la red.
- Integrar un equipo especializado en delitos cibernéticos, a fin de hacer este medio electrónico un lugar seguro para el intercambio de información.
- Realizar patrullajes en la red a fin de localizar sitios que hayan podido ser vulnerados.

- Acciones de operación con autoridades locales, federales e internacionales.

Esta corporación tiene conocimiento de la existencia de cuatro millones de sitios Web que explotan la pornografía, 60 % son lucrativos, es decir, el sitio exige el pago del servicio por medio de tarjeta de crédito del usuario, el 40 % restante es el intercambio de fotos y videos persona a persona. Se estima que quinientos sitios Web son creados diariamente asegura la P.F.P.

En relación con el fraude electrónico, otro ilícito con alto índice de incidencia, la PFP ha documentado una serie de patrones que son resultado de sus extensos patrullajes en la red. La P.F.P., asegura que los delincuentes actúan entre las 12 del día y las tres de la tarde para subir las ofertas; utilizan cuentas bancarias donde realizan sus depósitos las víctimas, la mayoría de ellas se encuentran en un rango entre los 18 y 30 años, además de que los usuarios afectados son primordialmente hombres. En el mapa geográfico, el mayor número de delitos se localizan en los estados de Jalisco, Estado de México, Morelos, Yucatán, Sonora y Sinaloa.

El robo o alteración de información, sabotaje, pedofília, tráfico de menores, fraude, clonación de señales satelitales, de tarjetas de crédito y el ciberterrorismo; son actividades consideradas por las autoridades de los tres niveles (federal, estatal y municipal), como una muestra de estos ilícitos, los

cuales día con día muestran un incremento en nuestro país, expandiéndose de manera considerablemente rápida.

Uno de los problemas de los delitos informáticos que se mencionan, es la persecución que tiene que ver con la rapidez que ofrece la publicación electrónica para quitar y poner información de cualquier tipo y formato en la red informática Internet.

4.6.2. DC MÉXICO (DELITOS CIBERNÉTICOS MÉXICO)

Se crea el grupo DC México (Delitos Cibernéticos México), para combatir los delitos cibernéticos en México y proporcionar las condiciones de seguridad para el desarrollo integral de la red Internet, este grupo corre a cargo de la Secretaria Técnica de la P.F.P.

El objetivo de DC México, es garantizar la seguridad y la capacidad para combatir ilícitos provocados por la acción humana en Internet mediante el uso de sistemas de cómputo.

INTEGRANTES.

- Entidades del Poder Ejecutivo Federal, integrantes del gabinete de Seguridad Nacional.
- El poder Legislativo Federal a través de las comisiones de Comercio; Seguridad, Equidad y Género, Población Vulnerable y Derechos Humanos, de la Cámara de Diputados y Senadores.

- Gobiernos Estatales: Distrito Federal, Jalisco, Baja California y Coahuila.
- Universidades y Centros de Educación Superior.
- Empresas privadas vinculadas con seguridad en sistemas en cómputo, asociaciones nacionales e internacionales.
- Organizaciones civiles comprometidas con la seguridad en Internet y de comercio electrónico.
- Proveedores de servicios de Internet en México.

ACTIVIDADES.

Es un cuerpo colegiado, que concentra la información necesaria para la identificación, monitoreo, rastreo y localización de todas aquéllas manifestaciones delictivas tanto en el territorio nacional como fuera de él.

A su vez, DC México tiene varias divisiones que ejecutan distintas funciones, entre ellas se encuentran el subgrupo de contingencias informáticas, el subgrupo de capacitación y el subgrupo de gobierno.

DC México, 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, donde se afecten los 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. A través de la

Secretaria Técnica de la P.F.P.; DC México, representa a nuestro país en el grupo internacional de respuesta inmediata denominado “24X7”.

DC México trabaja conjuntamente con el servicio de aduanas de los Estados Unidos, además de que establece vínculos cercanos con el Servicio Secreto y la Brigada Tecnológica de España

4.7. ANÁLISIS JURÍDICO SOBRE EL DELITO QUE SE PRETENDE ANEXAR AL NUEVO CÓDIGO PENAL PARA EL DISTRITO FEDERAL.

PRESUPUESTOS DEL DELITO.

SUJETO ACTIVO.

Este delito conforme al número de sujetos que intervienen en su comisión es unisubjetivo, ya que solo se necesita de una persona para cometer el delito, aunque puede ser plurisubjetivo, dos o más personas. En este caso no es necesario que el sujeto requiera de elevados conocimientos técnicos, sino que se trata de comportamientos capaces de ser desarrollados por cualquier individuo, minimamente introducido en el manejo de computadoras o sistemas informáticos, así como por aquellos que tengan avanzados conocimientos técnicos.

El artículo en su fracción I nos describe “al que sin autorización…”, es decir cualquier persona no importa sexo, edad, condición social, cultural o económica pueda producir la conducta descrita.

En la fracción II expresa “al que estando autorizado…,” es decir para que la conducta se realice es necesario que el sujeto activo cuente con autorización del titular del sistema informático, y a través de esa autorización tener acceso al sistema o equipo de informática, esta puede ser tacita o expresa que se deriva de su profesión o empleo.

En la fracción IV describe “que tenga la calidad de encargado o responsable de sistemas informáticos…”, en este caso tiene cierta calidad, que es que el sujeto tenga bajo su resguardo sistemas informáticos. En la fracción IV párrafo segundo “cuando se realicen las conductas descritas en las fracciones I a III con fines lucrativos…”, es decir que se obtenga un beneficio económico con la realización de este delito.

SUJETO PASIVO.

Los titulares de los bienes serian cualquier persona física o moral que posea información de carácter personal, familiar o cualquier otro tipo ya sea pública o privada que este dentro de su sistema informático.

En la fracción IV párrafo segundo describe: “se afecte con la obtención de la información de carácter personal a un menor de edad o persona con alguna discapacidad…”, se entiende por menor de edad al sujeto menor de 18 años, al no tener la suficiente madures para comprender el hecho delictivo. Se entenderá como discapacidad: la disminución o impedimento para la realización de una actividad, generada por una deficiencia, pérdida o anormalidad de una estructura o función psicológica, fisiológica o anatómica de un ser humano.

OBJETO MATERIAL.

Es el objeto sobre quien recae la ejecución del delito, en este caso es la información contenida en sistemas informáticos que se puedan modificar, destruir o copiar, en este caso, sino existe información, es imposible llevar acabo la conducta delictiva descrita en el tipo penal.

OBJETO JURÍDICO.

Es el bien jurídico tutelado, en este caso se puede decir que no solo se tutela la intimidad de las personas o la protección de la información personal, sino también protege en materia de seguridad pública.

En este caso el bien jurídicamente tutelado es la información, ya que esta abarca la pública como la privada, y en esta conducta ilícita lo que se vulnera es la información contenida en sistemas informáticos.

En las conductas descritas en el tipo penal, el objeto jurídico es de daño ya que hay una modificación, destrucción, o pérdida de la información contenida en los sistemas informáticos.

CONDUCTA DE ACCIÓN.

El tipo penal que se propone se anexe, describe las conductas de utilizar, destruir, apoderar, perder o modificar información de carácter personal o familiar, de negocios o cualquier otra pública o privada.

Se entiende como apoderarse: tomar posesión de algo; utilizar: saber o entender y sacar provecho de lo obtenido; por modificar: alterar algo, es decir hacerlo de manera distinta a como era originalmente.

Las conductas anteriores descritas implican una acción, ya que el sujeto activo necesita un movimiento corpóreo para apoderase, destruir, modificar perder, utilizar la información, primero, necesita encender la computadora o sistema informático y realizar las conductas descritas en el tipo penal; .por lo tanto se llega a la conclusión, que la conducta es de acción ya que se requiere de la voluntad, y no puede ser de omisión. La conducta de acción requiere de

movimientos corporales exteriores que sean voluntarios, que realice el sujeto para acceder a los sistemas informáticos en sus diversas formas de comisión.

El elemento normativo “sin autorización” el sujeto que realiza la conducta tiene pleno conocimiento de que su actuar es contrario a la ley.

El sujeto puede actuar de distinta manera, una de las cuales es directamente introducirse en el sistema informático y se apodera, modifica, destruye o pierda información del sujeto pasivo, utilizando el teclado o insertando virus que produzcan daños en el software, que puede ser inmediato o en el transcurso de un lapso de tiempo, mediante el uso de de sistemas electrónicos de activación, que pueden modificar, destruir o perder información en un sistema informático.

Otra forma de actuar es a distancia mediante el uso de una computadora o sistema informático conectado a Internet, y se introduzca destruyendo modificando, apoderando o perdiendo información en la computadora o en el sistema informático del sujeto pasivo, al igual en la parte de copiar puede hacerse directamente o a distancia.

En la fracción III menciona “difundir o ceder”, también son conductas de acción ya que requieren movimientos corpóreos para realizar estas conductas, se entiende difundir como trasmitir por cualquier medio la información que se

obtiene. En la fracción IV segundó párrafo del tipo penal, se refiere a “afecte” esto es producir un daño al obtener la información de carácter personal.

AUSENCIA DE CONDUCTA.

Éste como se mencionó en el Capítulo Tercero es el aspecto negativo de la conducta ya sea de acción o de omisión y la tipifica el Nuevo Código Penal para el Distrito Federal en el articulo 29 fracción I (Ausencia de Conducta), en este caso ninguno se acepta ni vis mayor, vis absoluta, sueño sonambulismo, movimientos reflejos o hipnotismo, ya que no es atribuible un actuar de un sujeto que se introduzca a un sistema informático por alguna de estas causas de ausencia de conducta.

DELITO INSTANTÁNEO.

Es un delito instantáneo ya que se consuma en el momento en que se modifica, destruya, utilice o pierda la información contenida en los sistemas informáticos, sin embargo también puede darse el delito permanente ya que los efectos de la conducta se pueden prolongar en el tiempo que ocurra la modificación, destrucción, modificación o pérdida y esta pueda recuperarse.

TIPICIDAD.

En el Capitulo tercero se menciono que la tipicidad es la adecuación de la conducta al tipo penal, es decir el tipo es la creación legislativa se describe en una norma jurídico-penal y la tipicidad es esa adecuación a la conducta .En el caso del tipo que se propone se anexe al Nuevo Código Penal la conducta debe adecuarse a alguno de los supuestos, el tipo que nos ocupa es fundamental por tener plena independencia, es de formación causistica por que se puede ejecutar de diversas formas y seria anormal por necesitar una valoración jurídica que seria: “al que sin autorización” y “al que estando autorizado” describe el tipo.

ATIPÍCIDAD.

Es el aspecto negativo de la Tipicidad, sería la falta total o parcial de adecuación de la conducta al tipo penal, el tipo existe pero la conducta no embona dentro de este., siendo las causas de atipicidad:

a) Ausencia del presupuesto de conducta o del hecho: en este caso la conducta no se adecuaría al tipo propuesto.

b) Ausencia de calidad del sujeto activo: En la fracción IV del tipo en propuesta exige cierta calidad y es “tenga la calidad de encargado o responsable de sistemas informáticos…”

c) Ausencia del sujeto Pasivo: la fracción IV describe ”…afecte con la obtención de la información de carácter personal a un menor de edad o persona con alguna discapacidad…”

d) Ausencia del objeto jurídico: en este caso en el tipo que se propone seria la seguridad de la información personal y la seguridad de la información pública.

e) Ausencia del objeto material: sino existe información contenida en sistemas informáticos abría atipicidad.

ANTIJURIDICIDAD.

La conducta debe ser contraria a una norma jurídica y no estar en algún supuesto de alguna causa de justificación, es decir no solo debe la conducta encuadrar en el tipo penal también vulnerar un bien que este protegido por el derecho, en el caso de la propuesta el bien protegido es la información y seria antijurídica el tener un acceso ilícito a esta información; destruyendo, copiando o modificando en perjuicio de un tercero.

CAUSAS DE JUSTIFICACIÓN.

En este caso ni la legítima defensa, el estado de necesidad, ni el consentimiento del titular del bien jurídico se aceptarían, solo en el caso del

cumplimiento de un deber o ejercicio de un derecho es decir que existiera una norma que justificará su actuar,

IMPUTABILIDAD.

Anteriormente ya analizamos la imputabilidad, es decir que para que un sujeto realice la conducta y sea de modificar, destruir o perder información; se declare penalmente responsable es necesario que sea imputable al momento de cometer el delito, debe conocer y comprender el hecho delictivo que comete con su actuar.

INIMPUTABILIDAD.

En este caso, en particular de este delito la inimputabilidad se puede dar en la minoría de edad, ya que no se requiere un amplio conocimiento en materia informática para realizar las conductas descritas en el caso del trastorno mental y desarrollo mental retardado, no se puede dar ya que sus capacidades intelectuales y motrices están disminuidas.

CULPABILIDAD.

La culpabilidad se divide en dolo y culpa como ya se trato anteriormente este tema, en este caso el delito es de dolo ya que necesariamente el sujeto que tenga cierto conocimiento de utilizar un sistema informático quiere y acepta su resultado, no puede darse la culpa porque puede prever su actuar, sabe de antemano el resultado que se obtendrá.

INCULPABILIDAD.

La inculpabilidad se da cuando falte el conocimiento o la voluntad, al igual existiría inculpabilidad cuando hay error o ignorancia y la no exigibilidad de otra conducta según la legislación.

En el caso del error se tendría una equivocada idea al realizar la conducta suponiendo que es correcta; en la ignorancia seria el desconocimiento de la norma lo cual seria el tipo penal que se propone.

La no exigibilidad de otra conducta seria el caso de que el sujeto tiene plena conciencia de su actuar y su determinación por supuesto de que esta tipificado pero una situación hace que se exima de la culpabilidad.

PROPUESTA PARA CREAR UN TIPO PENAL QUE REGULE EL ACCESO A SISTEMAS INFORMÁTICOS EN EL DISTRITO FEDERAL.

El cual quedará de la siguiente manera:

TÍTULO DÉCIMO TERCERO

DELITOS INFORMÁTICOS

CAPÍTULO ÚNICO ACCESO ILÍCITO A SISTEMAS INFORMÁTICOS

Artículo 212 . Se le impondrá prisión de uno a tres años y de cien a doscientos días de multa al que:

I.- Sin estar autorizado utilice, modifique, destruya, pierda o copie en perjuicio de un tercero información de carácter personal, familiar trabajo, profesión, negocios o de cualquier otro tipo que se halle contenida en sistemas informáticos públicos o privados.

II.- Estando autorizado utilice, modifique, destruya, pierda o copie en perjuicio de un tercero información de carácter personal, familiar trabajo, profesión, negocios o de cualquier otro tipo que se halle contenida en sistemas informáticos públicos o privados.

III.- Con conocimiento de su origen delictivo sin haber participado en

la obtención de la información contenida en sistemas informáticos difunda o ceda a terceros los datos, hechos, imágenes o video.

IV.- Tenga la calidad de encargado o responsable de sistemas Informáticos públicos o privados incurra en las conductas descritas de las fracciones anteriores.

Cuando se realicen las conductas descritas anteriores con fines lucrativos o se afecte con la obtención de la información de carácter personal a un menor de edad o persona con alguna discapacidad se duplicará la pena de prisión y multa de doscientos a cuatrocientos días. En el caso de ser servidor público se le impondrá además destitución e inhabilitación de seis meses a tres años para desempeñar otro empleo cargo o comisión públicos.

C O N C L U S I O N E S.

PRIMERA.- La informática vino a resolver la concurrencia del esfuerzo humano y lograr que la producción, reproducción y almacenamiento de un documento se hiciera de manera electrónica o automáticamente.

SEGUNDA.- Los sistemas informáticos siguen su desarrollo creando la llamada sociedad de la información, a través del uso continuo de la tecnología de la información para difundir el conocimiento.

TERCERA.- El Derecho Informático considerado como instrumento derivado de la Informática Jurídica para estudiar e investigar la informática en general y su aprovechamiento de la información jurídica en conjunto con el Derecho de la Informática para regular su uso, aplicación y desarrollo.

CUARTA.- Los avances en Legislación en nuestro país son buenos, pero se requiere una ley en particular para regular los sistemas informáticos.

QUINTA.- En los llamados delitos informáticos el objeto jurídico a salvaguardar en el caso concreto, acceso ilícito a sistemas informáticos no es la intimidad o privacidad, es la información misma contenida en estos sistemas.

SEXTA.- La Doctrina Clásica sanciona las conductas penales ya existentes, los delitos informáticos requieren de un mayor análisis para su debida sanción, ya

que los mismos avances tecnológicos hacen inadecuados los medios ordinarios utilizados.

SÉPTIMA.- Que el personal como son: Ministerios Públicos, Jueces, peritos estén capacitados en materia de delitos informáticos para su mismo estudio e investigación, proporcionándole los recursos cognoscitivos para su eficaz desarrollo, así como la coadyuvancía de ingenieros en informática, ingenieros en computación o técnicos especialistas.

OCTAVA.- El sujeto que puede cometer un delito informático puede ser cualquier persona con el mínimo de instrucción en computación, ya que estos sistemas están al alcance de casi cualquier sujeto tenga o no sistema informático propio.

NOVENA.- El acceso a sistemas informáticos puede hacerse de manera directa o a través de la red Internet, inclusive de tecnología inalámbrica siendo vulnerables el sector privado como el sector público.

DÉCIMA.- Los menores de edad están expuestos a ser usados como medio para obtener información privada por medio de Internet, debe proliferar la seguridad particular en los hogares.

DÉCIMA PRIMERA.- Los organismos creados para combatir estos ilícitos son: la Policía Cibernética y DC México (Delitos Cibernéticos México), de gran relevancia para combatir estas nuevas conductas, seria justo que en cada estado de la República se tuvieran organismos similares para la debida vigilancia de estos delitos y proporcionar una persecución más eficaz aunada a lo que ya es.

DÉCIMA SEGUNDA.- Es de suma importancia crear un tipo penal para el Distrito Federal, y así garantizar la seguridad de la información contenida en sistemas informáticos tanto públicos como privados, ya que éste esta dentro de las principales entidades en que se cometen más delitos informáticos.

DÉCIMA TERCERA.- Con esto se resuelve la hipótesis planteada al principio de la investigación y sí es necesaria la creación de un tipo penal en el Distrito Federal que regule el acceso a sistemas informáticos, tal cual debe de considerarse que el acceso a sistemas informáticos esta permitido hasta cierto limite, ya sea en archivos públicos o privados, el acceso no autorizado a sistemas informáticos o estando autorizado haga mal uso de este, es el que debe estar regulado jurídicamente es decir el acceso ilícito.

BIBLIOGRAFIA.

- ALCALDE. Penuelas, Manuel. INFORMÁTICA BÁSICA. 2da ed. Ed. M. C. Graw Hill. México. 1994.

- AZPICUETA. Hermillo, Tomas. DERECHO INFORMÁTICO. sin/ed. Ed. Abelero-Perrot. Buenos Aires. Argentina. 1989.

- BEEKMAN. G. COMPUTACIÓN E INFORMÁTICA HOY. sin/ed. Ed. Addison-Wesley. México. 1995.

- BEER. Stafford. CIBERNETICA Y ADMINSTRACIÓN. sin/ed. Ed. Nacional. México. 1995.

- BIESA. A, Rafael. INFORMÁTICA Y DERECHO. sin/ed. Ed. Ediciones de palma. Buenos Aires. Argentina. 1988.

- BARRIOSO. Ruiz, Carlos. INTERACCIÓN DEL DERECHO Y LA INFORMÁTICA. sin/ed. Ed. Dy Kinson. Madrid. España. 1996.

- CASTELLANOS. Tena. Fernando. LINEAMIENTOS ELEMENTALES DE DERECHO PENAL. 4ta ed. Ed. Porrúa. México. 2000.

- CAMPOLI. Andrés, Gabriel. DERECHO PENAL INFORMÁTICO EN MÉXICO. sin/ed. Ed. Instituto Nacional de Ciencias Penales. México. 1995

- CORTES. Ibarra. Ángel. DERECHO PENAL PARTE GENERAL. 5ta ed. Ed. Cárdenas. México. 2001.

- CORREA. Carlos. DERECHO INFORMÁTICO. sin/ed. Ed. De palma. Buenos Aires Argentina. 1989.

- CUELLO Calon. Eugenio. DERECHO PENAL PARTE GENERAL. 12va ed. Ed. Porrúa. México. 1990.

- DEL POZO. Contreras, Maria Luz. INFORMÁTICA EN DERECHO. sin/ed. Ed. Trillas. Madrid. España. 1992.

- DÍAZ. Barriga, Jesús. INTRODUCCIÓN A LA COMPUTACIÓN. sin/ed. Ed. UNAM. México. 1995.

- FIX. Fierro, Héctor. INFORMÁTICA Y DOCUMENTACIÓN JURÍDICA. sin/ed. Ed. Facultad de Derecho. UNAM. México. 1990.

- HUERTA. M. Marcelo. y LIBANO M. Claudio. DELITOS INFORMÁTICOS. 2da ed. Ed. Jurídica Cono Sur Ltda. Chile. 1998.

- JIMENEZ De Asúa. Luis. PRINCIPIOS DE DERECHO PENAL LA LEY Y EL DELITTO. 3era ed. Ed. Sudamericana. México. 1990.

- JIMENEZ De Asúa. Luis. TEORIA DEL DELITO. sin/ed. Ed. Iure Editores y Distribuidores. México. 2002.

- LÓPEZ, Betancourt, Eduardo. TEORÍA DEL DELITO. 7ma ed. Ed. Porrúa. México. 1999.

- PIERRE. Conso. INFORMÁTICA Y GESTIÓN. sin/ed. Ed. Técnicos Asociados. Buenos Aires. Argentina. 1992.

- PORTE Petit Candaup. Celestino. APUNTAMIENTOS DE LA PARTE GENERAL DEL DERECHO PENAL. Ed. Porrúa. México. 1985.

- PRASE. Peris, Antoni. LA INFORMÁTICA Y EL ABOGADO. sin/ed. Ed. Abeledo Perrot. Buenos Aires. Argentina. 1992.

-RÍOS. Estavillo. José Juan. DRECHO INFORMÁTICO. 1era ed. Ed. Instituto de Investigaciones Jurídicas. UNAM. México. México. 1995.

- RÍOS. Estavillo, José Juan. DERECHO E INFORMÁTICA EN MÉXICO. 1era ed. Ed. Instituto de Investigaciones Jurídicas. UNAM. México. 1997.

- SÁNCHEZ. Solana, Miguel Antonio. FUNDAMENTOS DE INFORMÁTICA. sin/ed. Ed. Alfa Omega- Zama. México. 1999.

-TÉLLEZ. Váldez, Julio. DERECHO INFORMÁTICO. 3ed. Ed. M.C. Graw Hill. México. 2004.

- TÉLLEZ. Valdez, Julio. LA PROTECCIÓN JURÍDICA DE LOS PROGRAMAS DE COMPUTACIÓN. sin/ed. Ed. Trilllas. México. 1992.

- UREÑA. López. Alfonso. FUNDAMENTOS DE INFORMÁTICA. Sin/ed. Ed Alfa-Omega. México.1999.

- WIARCO. Arellano. Alberto Octavio. CURSO DE DERECHO PENAL. 2da ed. Ed. Porrúa. México.2001.

- Witker. José. TÉCNICAS DE INVESTIGACIÓN JURÍDICA. sin/ed. Ed. M.C. Graw Hill. México. 1992.

- ZAFFARONI. Eugenio. Raúl. MANUAL DE DERECHO PENAL PARTE GENERAL. 2da ed. Ed. Cardenas. México 1991.

LEGISLACIÓN.

- Constitution Política de los Estados Unidos Mexicanos. Ed. Costa-Amic. México. 2006.
- Código Penal Federal. Agenda Penal del D. F. Ed. Isef. México.2005.
- Nuevo Código Penal Para el Distrito Federal. Agenda Penal del D. F. Ed. Isef. México.2005.
- Código Penal del Estado de Morelos. Ed. Sista. México. 2005.
- Código Penal del Estado de Tabasco. Ed. Sista. México. 2005.
- Código Penal del Estado de Sinaloa. Ed. Sista. México. 2005.
- Código Penal del Estado de Nuevo León. Ed. Sista. México. 2005.

OTRAS FUENTES.

- Diccionario Jurídico. Microsoft.2001.

- Enciclopedia Encarta. Microsoft. 2005.

- http://www.apple.com/firewire
- http://www.asesoriainformatica.com/definiciones.htm
- http://www.bibliotecadgsa.unam.mx/cuproductosboletines/msq/00007htm
- http://www.enterate.unam.mx
- http://www.compaq.com.mx
- http://www.informaticainformatica24.com.art
- http://www.palm.com
- http://www.pda.thoshiba.com
- http://www.ssp.gob.mx/aplication?pageid=pcibertnet
- http://www.symantec.com.mx/region/mx/homecomputing/library/
am_s_curt.html.
- http://www.unamcert.unam.mx

G L O S A R I O

ARPANET: En informática, una red formada por unos 60.000 computadoras en la década de 1960, desarrollada por la Advanced Research Projects Agency (ARPA) del Departamento de Defensa de Estados Unidos, que posteriormente surgió Internet.

BANDA ANCHA: Característica de cualquier red que permite la conexión de varias redes en un único cable. Para evitar las interferencias en la información manejada en cada red, se utilizan diferentes frecuencias para cada una de ellas. La banda ancha hace referencia también a una gran velocidad de transmisión.

BLUETOOTH: Reemplaza la conexión alámbrica en distancias entre los 10 y 100 metros mediante un enlace de radiofrecuencias, alcanzando velocidades del rango de 1Mbps. Es una tecnología desarrollada por Ericsson en 1994, que hace factible la conectividad inalámbrica entre dispositivos a corta distancia, éstos pueden llegar a formar redes con diversos equipos de comunicación: computadoras móviles, radiolocalizadores, teléfonos celulares, PDAs, la transferencia de archivos entre dispositivos móviles, la comunicación de voz con dispositivos manos libres, la conectividad de equipos periféricos como teclados, impresoras, monitores, etc.; y el control de electrodomésticos como refrigeradores y hornos de microondas, así como productos comerciales que abarcan áreas como audio y video, dispositivos periféricos, dispositivos médicos, equipo de oficina aparatos de medición y juegos, entre otros.

CABLE MODEM: Programa que se queda residente en un sistema y que ha sido desarrollado para obtener algún tipo de información y enviarla a una dirección IP específica.

CABALLO DE TROYA: Programa que se queda residente en un sistema y que ha sido desarrollado para obtener algún tipo de información y enviarla a una dirección IP específica.

CACHÉ: En Internet, es el espacio de almacenamiento temporal que emplea el navegador para almacenar los archivos (textos e imágenes) que recibe de Internet. Cuando se vuelve a visitar una página, el navegador obtiene los archivos desde el caché en lugar de obtenerlos de la localidad remota donde originalmente los encontró. Se habla del caché de disco cuando los datos se guardan en el disco duro y de caché de memoria cuando se almacenan en la RAM de la computadora.

CAMARA DIGITAL: Cámara de video que graba imágenes en forma digital. A diferencia de las tradicionales cámaras analógicas que convierten las intensidades de luz en señales infinitamente variables, las cámaras digitales convierten las intensidades de luz en números discretos.
La cámara digital descompone la imagen de la figura en un número fijo de pixeles (puntos), verifica la intensidad de luz de cada pixel y la convierte en un número. En una cámara digital de color, se crean tres números, que representan la cantidad de rojo, verde y azul en cada píxel.

CDMA: (Code didivison Multiple Access). Acceso Múltiple de División de Código. Norma de transmisión de datos a través de teléfonos inalámbricos.

CD: Compact Disc. [Disco Compacto]. Medio de almacenamiento óptico de 12 cm. de diámetro. Los datos se leen por medio de un pequeño láser y se utiliza para guardar información en formato digital. Un disco compacto puede almacenar 650 MB de información o 74 minutos de música. Cuando el CD contiene datos informáticos se llama, genéricamente CD-ROM. Cuando se trata de discos de audio, se suele denominar CD-A (CD-Audio).

CD-R: Disco compacto que se puede grabar. Se conoce también como CD-WORM (Compact Disc Write Once Read Many), [Disco compacto-Grabar una vez, leer muchas]. Se vende sin grabar y admite una grabación. Los discos CD-R tienen un color verde, azul o dorado por la parte inferior que es consecuencia del material del que está hecho el sustrato que se graba. El proceso de grabación se basa en la aplicación de calor (por medio del láser), que da como resultado la fusión de pequeñas zonas del sustrato lo que provoca cambios en la reflectividad de la superficie del disco. Estas variaciones permiten al láser de lectura detectar las zonas grabadas y, por tanto, leer los datos grabados.

CD-ROM: Disco compacto que contiene datos informáticos.

CD-RW: Compact Disc ReWritable. [Disco Compacto Regrabable]. Disco que se puede grabar y borrar. El proceso de grabación y borrado de las pistas se diferencia del que se produce en un CD-R en que no se funde el sustrato, sino que éste cambia de estado. Estos cambios modifican la reflectividad de la superficie, aunque en menor medida que en un CD-R, por lo que estos discos no se pueden leer en todas las unidades de CD-ROM o CD-Audio.

CERT: Computer Emergency Response Team (Equipo de respuesta para emergencias informáticas) Grupo de personas que se dedican a monitorear la

seguridad informática, para alertar de peligros potenciales o bugs (gusanos). El CERT fue creado por DARPA en Noviembre de 1988 como respuesta a las carencias mostradas durante el incidente del gusano ("worm") de Internet. Los objetivos del CERT son trabajar junto a la comunidad Internet para facilitar su respuesta a problemas de seguridad informática que afecten a los sistemas centrales de Internet, dar pasos proactivos para elevar la conciencia colectiva sobre temas de seguridad informática y llevar a cabo tareas de investigación que tengan como finalidad mejorar la seguridad de los sistemas existentes. Los productos y servicios del CERT incluyen asistencia técnica 24 horas al día para responder a incidencias sobre seguridad informática, asistencia sobre vulnerabilidad de productos, documentos técnicos y cursos de formación. Adicionalmente, el CERT mantiene numerosas listas de correo (incluyendo una sobre Avisos CERT) y ofrece un servidor de FTP anónimo, en cert.org, donde se archivan documentos y herramientas sobre temas de seguridad informática.

CHAT: [Charla]. Se trata de una comunicación en tiempo real sobre Internet o un servicio on line. A diferencia del correo electrónico, en el que tras enviar un mensaje hay que esperar la respuesta, el chat implica a dos o más personas escribiendo comentarios en un área de forma similar a una conversación hablada. Cuando se escribe algo, aparece en la pantalla del resto de los usuarios en tiempo real (al menos, en teoría). Los canales de conversación se encuentran en grandes redes mundiales a las que se accede por medio de pequeños programas de software creados para el Internet Relay Chat.

CIBERESPACIO: (Cyberspace). Se usa para describir la totalidad de los recursos informáticos disponibles a través de las redes de cómputo, particularmente de Internet.

CIBERCAFE O CAFÉ INTERNET: Espacio donde, además de beber y comer, los clientes pueden usar computadoras para acceder a Internet.

COOKIES: [Galletas]. Archivos que contienen información respecto a los visitantes de un sitio. Esta información la toma el servidor o la proporciona el usuario en su primera visita al servidor. El servidor registra esta información un archivo de texto y la guarda en el disco duro del usuario. Al regresar al sitio, el servidor busca la galleta y la utiliza para reconocer al usuario o al equipo.

CRAKER: Persona que sin derecho se introduce a un sistema informático con el fin de destruir o copiar información valiosa, realiza transacciones ilícitas e impide el correcto funcionamiento de una computadora, este es un termino derivado de hacker acuñado por ellos mismos. Persona que desprotege programas y los modifica para obtener determinados privilegios.

CRIPTOGRAFIA: Técnica que trata del enmascaramiento de la comunicación de modo que sólo resulte inteligible para la persona que posee la clave, o método para averiguar el significado oculto, mediante el criptoanálisis de un texto aparentemente incoherente. En su sentido más amplio, la criptografía abarca el uso de mensajes encubiertos, códigos, algoritmos matemáticos para la trasformación de la información en un lado y la realización inversa en el otro.

E-MAIL (CORREO ELECTRÓNICO): sistema de envío y recepción de correo mediante el uso de un ordenador o computadora u otro dispositivo electrónico, de manera que se utilice una red de área local (LAN), Internet o conexiones inalámbricas para su transmisión y recepción. Un mensaje de correo electrónico puede constar tanto de texto escrito como de imágenes, archivos de datos o

mensajes de voz y otros elementos multimedia digitalizados, como animaciones o vídeo.

ENCRIPTACIÓN: Proceso de cifrar la información para proteger su uso o visualización no autorizado durante el proceso de transmisión o cuando se guarda en algún medio transportable.

FIBRA OPTICA: Sistema de transmisión que utiliza fibra de vidrio como conductor de frecuencias de luz visible o infrarrojas. Este tipo de transmisión tiene la ventaja de que no se pierde casi energía pese a la distancia (la señal no se debilita) y que no le afectan las posibles interferencias electromagnéticas que sí afectan a la tecnología de cable de cobre clásica.

FIREWALL: mecanismo de seguridad y protección. Se utiliza para impedir el acceso a una red.

FIREWIRE: Bus serial desarrollado por Apple y Texas Instruments que permite la conexión de 63 dispositivos a velocidades que van de 100 a 400 Mbits/seg. Pueden conectarse hasta 1022 buses FireWare suministrando una enorme capacidad. Se prevé como un reemplazo para puertos seriales, paralelos y SCSI. También denominado IEEE 1394 o iLink. Se trata de un puerto externo de alta velocidad utilizado para conectar ordenadores y periféricos. Utilizar este sistema es bastante costoso, por eso sólo se usa para periféricos que requieran una velocidad alta para funcionar correctamente (como es el caso de las cámaras digitales). Para otros dispositivos externos (ratón, teclado) resulta más económico el puerto USB, aunque permite velocidades inferiores.

GIGA: Prefijo que significa mil millones. Con frecuencia se refiere al valor preciso 1073741824, puesto que las especificaciones del computador por lo general están en números binarios.

GIGABYTE: Mil millones de bytes. También GB, Gbyte y G-byte.

GUSANO: Programa informático que se reproduce así mismo copiándose una y otra vez de sistema en sistema y que usa recursos de los sistemas atacados.

HACK: La palabra Hack viene de hachar, derribar, se refiere al golpe seco que debían dar los operarios de la máquina que se usaba en el MIT para realizar operaciones matemáticas, máquinas que cuando se bloqueaban requerían el famoso golpe seco, "quien no haya golpeado una pc que tire la primera piedra", por consiguiente hackers eran los que hacían las veces de hack, o sea los que golpeaban, por consiguiente ellos mismos se llamaron hackers, he ahí el origen de la palabra hacker, no pirata informático.

HACKER: Usuario de ordenadores especializado en penetrar en las bases de datos de sistemas informáticos estatales con el Fin de obtener información secreta. En la actualidad, el término se identifica con el de delincuente informático, e incluye a los cibernautas que realizan operaciones delictivas a través de las redes de ordenadores existentes. Tradicionalmente se considera Hacker al aficionado a la informática cuya afición es buscar defectos y puertas traseras para entrar en los sistemas. Para los especialistas, la definición correcta sería: experto que puede conseguir da un sistema informático cosas que sus creadores no imaginan. Un Master en programación capaz de pensar y hacer cosas como si fuera "magia". Se dice que el termino de Hacker nació por los programadores de Massachusetts Institute of Technology que en los años

sesentas se llamaron a si mismos Hackers, para hacer mención de que podían hacer programas mejores y mas eficientes, o que hacían cosas que nadie había podido hacer.

HIPERTEXTO: Describe un tipo de funcionalidad de exploración en línea interactiva. Los vínculos (direcciones URL) incrustados en palabras o frases permiten al usuario escoger un texto concreto para que se muestre inmediatamente la información relacionada y el material multimedia asociado.

HTTP (Hipertex trasnfer protocol): [Protocolo de transferencia de hipertexto]. Es un conjunto de estándares que permite a los usuarios de la Web intercambiar información. Es el método que se utiliza para transferir documentos desde el sistema donde se almacenan las páginas hasta los usuarios individuales.

IMPRESORA DE TINTA: También se conoce por su definición en inglés (ink-jet). Este tipo de impresoras funcionan mediante una serie de inyectores que proyectan gotas diminutas de tinta, de manera que la acumulación de gotas permite la formación de letras, imágenes, etc. Esta clase de impresoras se ha impuesto por ofrecer una alta calidad de impresión a un precio aceptable.

IMPRESORA LASER: La tecnología láser es, en la actualidad, la que ofrece mayor calidad de impresión, aunque a un precio más elevado que el de las otras tecnologías. Resultan muy veloces y silenciosas. Funcionan mediante la combinación de un tambor fotosensible al que se adhieren partículas de tóner que luego son transferidas al papel, de igual forma a como funcionan las fotocopiadoras.

INFORMÁTICA: Conjunto de conocimientos y herramientas científicas, técnicas y tecnológicas que se encarga del tratamiento racional y estructurado de la información por medios automáticos electrónicos digitales.

INFRARROJO: Emisión de energía en forma de ondas electromagnéticas en la zona del espectro situada inmediatamente después de la zona roja de la radiación visible. Requiere de una comunicación lineal entre transmisor y receptor, lo que hace imprescindible la línea de vista para su efectiva transmisión. Las frecuencias de la banda del infrarrojo no permiten la penetración a través de paredes, dándole una importante ventaja a la radiofrecuencia que opera Bluetooth.

INTELIGENCIA ARTIFICIAL (IA): Ciencia que investiga la posibilidad de que una computadora simule el proceso de razonamiento humano. Pretende también que la computadora sea capaz de modificar su programación en función de su experiencia y que «aprenda».

INTERNET: [inter=internacional, net=red]. Red mundial que conecta entre sí a computadoras del mundo mediante el protocolo IP y proporciona diversos servicios de intercambio de información. En su primera etapa la conexión de las computadoras fue a través de la red telefónica existente. Actualmente existen conexiones por medio de fibra óptica y vía inalámbrica. Esta compuesto, por tantos, por un conjuntos de redes locales conectadas entre si por medio de un ordenador llamado GATEWAY que se encuentra en cada red. La información que se debe mandar aun ordenador remoto es etiquetada con la dirección computarizada de dicho ordenador esta dirección puede tener diferentes formatos. Una vez que la información ha sido etiquetada, esta sale de la red

donde se ha creado a través de la puerta (GATEWAY). A partir de ahí va siendo encaminada de puerta a puerta hasta llegar a la red local, donde figura la computadora de destino.

INTRANET: [Red interna]. Red que utiliza los protocolos de Internet pero que es de uso interno, por ejemplo, la red corporativa de una empresa. Puede exponer parcialmente información al exterior vía Internet. La mayoría de las Intranets están configuradas de forma que sus usuarios puedan tener acceso a Internet sin permitir que los usuarios de Internet tengan acceso a los equipos de la Intranet.

IP ADRESS: Dirección IP. Matrícula que identifica a una computadora de la red. A las computadoras personales se les asigna una IP adress para que naveguen por la red, que es HTTP: (Hiper Text Transfer Protocol). Protocolo de transferencia de HiperTexto. Es el protocolo de Internet que permite que los exploradores del WWW recuperen información de los servidores. Cambia en cada sesión de acceso a Internet.

IRC INTERNET RELAY CHAT: [Canal de Chat de Internet]. Es un sistema que permite las conversaciones de texto en tiempo real entre varios participantes y utilizando la Internet. Los usuarios se conectan a un grupo y después entran en uno de los muchos canales de conversación, comunicándose entre ellos por medio de una pantalla de texto. Participar en una conversación IRC implica la conexión a Internet, acceso a una red dedicada a IRC y un software cliente. Este último es el encargado de enviar y recibir los mensajes.

ISP INTERNET SERVICE PROVIDER: [Proveedor de Servicios Internet]. Organización o empresa que establece la conexión entre los usuarios e Internet.

Generalmente, los ISP ofrecen servicios de conexión, correo electrónico, hospedaje de páginas Web y el software de navegación por la Web; el ISP ofrece un número de teléfono, por lo general local, para que los usuarios se conecten a su servidor y puedan acceder a la Red mundial.

LAN: (Local Area Network) El término LAN define la conexión física y lógica de computadoras en un entorno generalmente de oficina. Se comparten recursos como acceder a una misma impresora y permite el intercambio de información entre computadoras.

MEGABYTE: MB. 1.024 Kilobytes (KB).

MENSAJERÍA ELECTRÓNICA: Sistema de intercambio de mensajes sin soporte papel, es decir, de computadora a computadora. Puede operarse en cualquiera de los sistemas de red de comunicaciones, respetando determinados protocolos.

MÓDEM: Es un dispositivo que se conecta a la computadora y que permite intercambiar datos con otras computadoras a través de la línea telefónica.

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.

ROUTER O RUTEADOR: [Encaminador]. Dispositivo que une entre sí dos redes, de forma que la información que no va dirigida a la otra red, no pasa a ella.

SITIO WEB: Es un conjunto de páginas web afines, normalmente gestionadas por un único usuario, por ejemplo: asesoriainformatica.net.

SPAM: Correo electrónico no solicitado y enviado repetidamente. Es una forma de ataque a un usuario o servidor, basada en la saturación del servidor de correo y de las conexiones a Internet.

VIDEOCONFERENCIA: Conferencia mantenida mediante imágenes y sonidos transmitidos por una red de comunicaciones.

WAN (WIDE AREA NETWORK): Red de Área Extensa.

WAP (WIRELESS ACCESS PROTOCOL): [Protocolo de acceso inalámbrico]. Especificación que permite la comunicación en red a través de un medio inalámbrico.

WEB: Por éste término se suele conocer a WWW (World Wide Web), creado por el Centro Europeo de Investigación Nuclear como un sistema de intercambio de información y que Internet ha estandarizado.

WEBCAM: Cámara conectada a una página web a través de la cual los visitantes pueden ver imágenes normalmente en directo.

WWW (WORLD WIDE WEB): [Red Mundial]. Telaraña o malla mundial. Sistema de información con mecanismos de hipertexto. Los usuarios pueden crear, editar y visualizar documentos de hipertexto. Sistema de información global desarrollado en 1990 por Robert Cailliau y Tim Berners.

WI-FI (WIRELESS FIDELITY) La expresión Wi-Fi se utiliza como denominación genérica para los productos que incorporan cualquier variante de la tecnología inalámbrica 802.11, que permite la creación de redes de trabajo sin cables (conocidas como WLAN, Wireless Local Area Netwoks).

WLAN (WIRELEES LOCAL AREA NETWOKS): Redes sin hilos. Las redes sin cables permiten compartir periféricos y acceso a Internet.