VNIVERSIDAD NACIONAL AVFNOMA DE MEXICO

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO.

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES.

"CAMPUS ARAGÓN".

"ARGUMENTOS PARA ADICIONAR LOS DELITOS INFORMÁTICOS EN MATERIA DE VÍAS DE COMUNICACIÓN Y CORRESPONDENCIA DEL CÓDIGO PENAL PARA EL D.F."

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

LICENCIADO EN DERECHO

P R E S E N T A:

ISRAEL SIMÓN PÉREZ

ASESOR: MTRA. MA. GRACIELA LEÓN LÓPEZ.

SAN JUAN DE ARAGÓN, ESTADO DE MÉXICO. **2003.**

UNAM

A TODA LA GENTE QUE NO TUVO LA SUERTE
DE ESTUDIAR CON NOSOTROS.
SI UN DIA TOCAS LAS PUERTAS DE LA UNAM
Y NO TE ABREN, NO TE PREOCUPES Y VUELVE
A INTENTARLO Y SI NO TE VUELVEN A ABRIR
NO TE PREOCUPES , LO MAS IMPORTANTE ES QUE
NO TE LAS CIERRES TU MISMO .
PORQUE LA UNIVERSIDAD NO SOLO ES UNA ESCUELA
ES EL ORGULLO DE NUESTRO PAÍS.

ASESOR

GRACIAS POR EL TIEMPO DEDICADO
Y POR ENSEÑARME QUE EL CONOCIMIENTO
SIRVE CUANDO PUEDES TRANSMITIRLO A OTROS,
SIN CAER EN EL EGOÍSMO DE GUARDARLO
SOLO PARA TI MISMO.
QUE ANTES QUE CUALQUIER COSA,
LA SENCILLEZ Y LA HUMILDAD
SON ASPECTOS IMPORTANTES DEL SER HUMANO.

JUAN CARLOS LÓPEZ NORIEGA

PUEDO DECIR QUE MI VIDA ESTA DIVIDA EN
DOS PARTES , ANTES DE J .C Y DESPUÉS DE J.C.
JUAN CARLOS LÓPEZ NORIEGA GRACIAS
POR DARME LA CONFIANZA DE ENTRAR TRES VECES
A UN QUIRÓFANO CON LA SEGURIDAD
DE QUE SALDRÍA VIVO POR MODIFICAR MI VIDA
QUE DIA CON DIA TRATO DE VOLVER A CONSTRUIR
DESPUÉS DE 18 AÑOS DE TRISTEZAS.

MAESTROS

PARTE DEL ÉXITO DE LA UNIVERSIDAD SON LOS ALUMNOS
PERO ESTOS NO EXISTIRÍAN SIN SUS CONOCIMIENTOS
Y EXPERIENCIAS.
PORQUE PESE A QUIEN LE PESE SEGUIMOS SIENDO
LA MÁXIMA CASA DE ESTUDIOS DE LATINOAMÉRICA
GRACIAS A USTEDES.

AMIGOS

A TODOS AQUELLAS PERSONAS QUE ME CONSIDERAN
SU AMIGO Y QUE FORMAN PARTE DE MI VIDA,
DE QUIENES SIEMPRE RECIBO UN SALUDO CARIÑOSO
AUN CUANDO HE DEJADO DE VERLOS
POR MUCHO TIEMPO.
NO ES NECESARIO NOMBRARLOS PORQUE
LOS RECUERDOS NOS SEGUIRÁN UNIENDO.

MATTY

JAMÁS IMAGINARIAS TODAS LAS EMOCIONES
QUE ME HACES SENTIR CON SOLO MIRARME,
BASTARON SOLO UNOS MINUTOS PARA SABER
QUE ERAS ESPECIAL Y QUE NUNCA TE OLVIDARÍA.
NADIE SABE QUE NOS DEPARA EL DESTINO,
PERO ESPERO TENER LA OPORTUNIDAD
DE COMPARTIRLO CONTIGO.

HERMANOS

ESPERO QUE UN DIA PUEDAN SENTIR ESTA SENSACIÓN
Y DISFRUTAR ESTE MOMENTO .
DICEN QUE NO HAY QUE LLEGAR PRIMERO,
PERO HAY QUE SABER LLEGAR.
Y ESPERO QUE ESTA SEA SOLO UNA META DE MUCHAS
QUE TRACEN EN SU VIDA .

PADRE

CON EL TIEMPO APRENDÍ A RECOGER
LO BUENO Y LO MALO DE TI,
TRATO DE NO COMETER LOS MISMOS ERRORES
QUE TU COMETISTE Y ESPERO QUE MI HIJO
NO REPITA LOS MÍOS .
GRACIAS POR SER MI ESCUELA DE LA VIDA
Y SEGUIR APRENDIENDO DE TI DIA CON DIA.

MADRE

PERDÓN POR TODOS LOS DESVELOS,
PERDÓN POR TODOS LOS MALOS MOMENTOS,
PERDÓN POR TODO EL DOLOR QUE TE HE CAUSADO,
ESTA ES MI FORMA DE SECAR SOLO UNA
DE TUS LAGRIMAS Y DARTE LAS GRACIAS
POR SEGUIR JUNTO A MI .
TE QUIERO.

DIOS

POCA GENTE ENTENDERÍA UNA AMISTAD COMO LA NUESTRA,
SIEMPRE HEMOS TENIDO CONFLICTOS MUY FUERTES
POR PROBLEMAS QUE TUVIMOS DEL PASADO,
AFORTUNADAMENTE SEGUIMOS UNIDOS.
SOLO TU CONOCES LA HISTORIA DE CADA UNO DE NOSOTROS
Y AUNQUE SIGO PREGUNTÁNDOME ¿POR QUE YO?
HOY ME DISTE LA PRIMERA RESPUESTA SIN
NI SIQUIERA MOVER LOS LABIOS.
GRACIAS POR SEGUIR SIENDO LA ESPERANZA DE MILLONES
Y POR DEJARME TOCAR POR ALGUNOS SEGUNDOS EL CIELO
EN LA TIERRA.

I N D I C E

CAPÍTULO II . DELITOS INFORMÁTICOS.

CAPÍTULO III. LEGISLACIÓN INTERNACIONAL Y NACIONAL SOBRE DELITOS INFORMÁTICOS

CAPÍTULO IV. ARGUMENTOS PARA ADICIONAR LOS DELITOS INFORMÁTICOS EN MATERIA DE VÍAS DE COMUNICACIÓN Y CORRESPONDENCIA DEL CÓDIGO PENAL PARA EL DF.

INTRODUCCION

Desde tiempos muy remotos el hombre aun no articulaba palabras pero ya desarrollaba conductas que afectaban a otros hombres por ejemplo , el apoderamiento ilegitimo del animal cazado, la violencia física ejercida contra una mujer etc. De ahi la necesidad de regular tales conductas y señalar tales castigos, para lograr el orden y la convivencia pacifica .

La finalidad de empezar con una breve reseña histórica sobre el Derecho universal y posteriormente enfocarnos a nuestro país es principalmente para todas aquellas personas que puedan leer este trabajo, tengan una noción del acontecer mundial y de las principales caracteristicas y leyes que en la antigüedad hicieron lo que hoy conocemos como nuestro Derecho Penal,que al hablar de el derecho y sus fuentes no solo se remonte al Derecho Romano, pues existen otras civilizaciones que realizaron aportaciones importantes que poco a poco fueron enriqueciendo a el Derecho penal y sin duda alguna los elementos del delito formaran parte importante de la investigación para poder deducir que conductas con la ayuda de la tecnología informática pueden ser ilícitas.

Por otra parte, el hombre al verse en la necesidad de cuantificar sus pertenencias, animales, objetos de caza, pieles, etcétera, ha tenido que procesar datos, limitándose en un principio al número de sus dedos, después a cuentas de granos y objetos similares,

posteriormente, inventó sistemas numéricos que le permitieron realizar sus operaciones con mayor confiabilidad y rapidez.

Al paso de los siglos inventando el ábaco, las tablas de logaritmos (1614), la regla de cálculo (1630), las tarjetas perforadoras (1804) hasta la creación de la computadora en (1937) conocida como "MARK", la cual en pocos años ha sufrido una transformación tan rápida, convirtiéndose en la herramienta más importante en la sociedad actual.

Una de las ciencias que mas importancia a tenido a nivel mundial, es la INFORMATICA que se a convertido en la tecnología del presente siglo, palabra formada por la asociación de los términos Infor-mación y auto-matica, Es el conjunto de métodos y mecanismos que tienen como objetivo el tratamiento racional y automático de la información, generando una nueva etapa en el desarrollo científico además de propiciar una nueva Revolución Industrial trascendiendo con mayor importancia que la que se suscito en el siglo XIX , en la que sorpresivamente la maquina de vapor desplaza al músculo del hombre y del animal .

Los equipos informáticos han abierto una nueva era en las técnicas de automatización, han permitido mejorar los sistemas modernos de comunicación y sin lugar a dudas la informática es hoy una forma de poder social pero también pone al descubierto actos lícitos e ilícitos en donde es necesario el derecho para regularlos.

Los sistemas informáticos pueden proporcionar datos e informaciones sobre miles de personas, físicas y morales, en aspectos tan fundamentales para el normal desarrollo y funcionamiento de diversas actividades como bancarias, financieras, tributarias, provisionales y de identificación de las personas, y si a ello se agrega que existen bancos de datos, empresas o entidades dedicadas a proporcionar, si se desea, cualquier información, sea de carácter personal o sobre materias de las más diversas disciplinas a un Estado o particulares, se comprenderá que están en juego o podrían llegar a estarlo de modo dramático, algunos valores colectivos y los consiguientes bienes jurídicos que el ordenamiento jurídico debe proteger.

En la actualidad la informatización se ha implantado en casi todos los países. Tanto en la organización y administración de empresas y administraciones públicas como en la investigación científica, en la producción industrial o en el estudio e incluso en el ocio, el uso de la informática es en ocasiones indispensable y hasta conveniente. Sin embargo, junto a las incuestionables ventajas que presenta comienzan a surgir algunas facetas negativas, como por ejemplo, lo que ya se conoce como criminalidad informática.

Estamos frente a la posibilidad real de que individuos o grupos sin escrúpulos, con aspiraciones de obtener el poder que la información puede conferirles, la utilicen para satisfacer sus propios intereses, a expensas de las libertades individuales y en detrimento de las personas. Así mismo, la amenaza futura será directamente proporcional a los adelantos de las tecnologías informáticas.

No son los grandes sistemas de información los que afectan la vida privada, sino la manipulación o el consentimiento de ello por parte de individuos poco conscientes e irresponsables de los datos que dichos sistemas contienen.

El espectacular desarrollo de la tecnología informática ha abierto las puertas a nuevas posibilidades de delincuencia antes impensables. La manipulación fraudulenta de los ordenadores con ánimo de lucro, la destrucción de programas o datos y el acceso y la utilización indebida de la información que puede afectar la esfera de la privacidad, son algunos de los procedimientos relacionados con el procesamiento electrónico de datos mediante los cuales es posible obtener grandes beneficios económicos o causar importantes daños materiales o morales.

Pero con los delitos informáticos la cuantía de los perjuicios ocasionados es a menudo infinitamente superior a la que es usual en la delincuencia tradicional, sino que también son mucho más elevadas las posibilidades de que no lleguen a descubrirse. Se trata de una delincuencia de especialistas capaces muchas veces de borrar toda huella de los hechos.

En este sentido, la informática puede ser el objeto del ataque o el medio para cometer otros delitos reúne unas características que la convierten en un medio idóneo para la comisión de muy distintas modalidades delictivas, en especial de carácter patrimonial (estafas, apropiaciones indebidas, fraudes, etc.).

La idoneidad proviene, básicamente, de la gran cantidad de datos que se acumulan, con la consiguiente facilidad de acceso a ellos y la relativamente fácil manipulación de estos.

El estudio de los distintos métodos de destrucción y/o violación del hardware y el software es necesario en orden para determinar cuál será la dirección que deberá seguir la protección jurídica de los sistemas informáticos, ya que sólo conociendo el mecanismo de estos métodos es posible encontrar las similitudes y diferencias que existen entre ellos.

Los sistemas de computadoras ofrecen oportunidades nuevas y sumamente complicadas de infringir la ley, y han creado la posibilidad de cometer delitos de tipo tradicional en formas no tradicionales.

En los últimos tiempos, ha sido evidente que la sociedad ha utilizado de manera benéfica los avances derivados de la tecnología en diversas actividades, sin embargo, es necesario que se atiendan y regulen las consecuencias del uso indebido de las computadoras y los sistemas informáticos en general.

Durante la etapa de investigación se encontró que no existe un consenso en cuanto al concepto de delito informático, y que estudiosos del tema lo han definido desde diferentes puntos de vista como son el criminógeno, formal, típico y atípico, etc., dando lugar a que la denominación de esta conducta haya sufrido diferentes interpretaciones.

Los llamados delitos informáticos no son cometidos por la computadora, sino que es el hombre quien los comete con ayuda de aquélla. En ese entendido, el presente trabajo se dirige al análisis de las posibles medidas preventivas, ya sean de carácter administrativo o penal deben ser tomadas en cuenta para evitar que la comisión de este tipo de infracciones o delitos, alcance en México los niveles de peligrosidad que se han registrado en otros países.

La protección de los sistemas informáticos puede abordarse tanto desde una perspectiva penal como de una perspectiva civil o comercial, e incluso de derecho administrativo. Estas distintas medidas de protección no tienen porque ser excluyentes unas de otras, sino que, por el contrario, éstas deben estar estrechamente vinculadas.

Por eso, dadas las características de esta problemática, sólo a través de una protección global, desde los distintos sectores del ordenamiento jurídico, es posible alcanzar una cierta eficacia en la defensa de los ataques a los sistemas informáticos.

A nivel internacional un grupo de expertos, invitados por la Organización de Cooperación y Desarrollo Económico (O.C.D.E.) a Paris, Francia, en mayo de 1983,
Definió a el término delitos relacionados con las computadoras como "cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático de datos y/o transmisiones de datos".

La amplitud de este concepto es ventajosa, puesto que permite el uso de las mismas hipótesis de trabajo para toda clase de estudios penales, criminólogos, económicos, preventivos o legales.

Esta era de las aplicaciones de la informática no sólo tiene un lado ventajoso, también plantea problemas de significativa importancia para el funcionamiento y la seguridad de los sistemas informáticos en los negocios, la administración, la defensa nacional y la sociedad.

Debido a esta vinculación, el aumento del nivel de los delitos relacionados con los sistemas informáticos registrados en la última década en los Estados Unidos, Europa Occidental, Australia y Japón, representa una amenaza para la economía de un país y también para la sociedad en su conjunto. En este ámbito internacional la Organización de Naciones Unidas reconoce distintos tipos de delitos informáticos.

Se Analizo la regulación que han tenido en la legislación mexicana las conductas ilícitas relacionadas con la informática. Para ello se estudian los antecedentes que han tenido las regulaciones vigentes en esta materia: Acuerdos celebrados como Tratado de Libre Comercio de América del norte (T.L.C.) relacionada con las convenciones de la O.C.D.E.

México solo cuenta con 2 estados que tipifican los delitos Informáticos, pero existen otras conductas ilícitas que se realizan y quedan impunes, de las cuales ni siquiera se tiene conocimiento,

mucho menos estadísticas, pero están ahí, y casi nunca nos enteramos, como cuando se nos pierde un correo que estaba guardado en la computadora, la base de datos de nomina que fue alterada, las llamadas que jamás realizamos al extranjero y que nuestra compañía telefónica nos cobra en nuestro recibo telefónico o el exceso de llamadas locales en ambos casos sin ninguna explicación y que tenemos que pagar, pequeñas cantidades de uno a cuatro pesos de tu cuenta bancaria que evidentemente no le das la importancia , que le podría dar un banco, si tomamos en cuenta que tiene una cartera de 900 000 clientes.

Es increíble que a través de Internet por medio de una computadora y un teléfono puedas planear un secuestro o puedas obtener todo el Software y música de todos tus artistas favoritos "gratis" sin pagar toda la infraestructura de los derechos de autor .

La Asamblea Legislativa del Distrito Federal debe realizar un estudio detallado para legislar los Delitos informáticos ya que hasta el momento en Aguascalientes y en Sinaloa solo se han enfocado a defender los Delitos contra el Patrimonio, pero existen otros supuestos que también necesitan ser protegidos por el Código Penal del Distrito Federal por ejemplo los Delitos contra la Seguridad y el Normal Funcionamiento de las Vías de Comunicación y de los Medios de Transporte.

En nuestro país ya que existen diversas legislaciones desde la Constitución hasta un Instituto Nacional de Estadística ,Geografía e

Informática pero desgraciadamente su contenido no se ha actualizado , en donde las nuevas tecnologías no son mencionadas.

Para finalizar se incluyen algunos argumentos para anexar los delitos informáticos pero en materia de Vías de Comunicación ya que aun cuando parece que este capitulo solo se refiere a caminos y puentes, la investigación nos llevara a ver que tiene mucha mas relación con este capitulo del Código Penal, que con cualquier otro, por el simple hecho de hablar de "comunicación" de forma generalizada y ante las nuevas formas de cometer delitos considero que es ideal para adicionar los delitos informáticos en materia de vías de comunicación y correspondencia para el Código Penal del Distrito Federal.

CAPITULO I. DERECHO PENAL

1.1 ANTECEDENTES DEL DERECHO PENAL UNIVERSAL

No se puede concebir una sociedad cualquiera sin la existencia de un orden jurídico, las sociedades en su evolución crean el orden jurídico que consideran adecuado para lograr sus fines u objetivos y ese orden se traduce en leyes que permitan conocer a sus destinatarios , sus derechos y obligaciones , ya sean los encargados de aplicarlas o bien se trate de aquellos que deban cumplirlas .

El surgimiento del derecho penal obedece a la necesidad de regular el comportamiento del hombre en sociedad. El crimen nace con el hombre, cuando todavía no existía un orden jurídico o una sociedad organizada el delito se manifiesta en su mas rudimentaria forma al inferirle daño a bienes ajenos .

Para conocer el principio verdadero de las primeras ideas penales no nos sirve la dialéctica jurídica tenemos que valernos de la historia ; por esta conocemos las primeras sociedades humanas y los primeros pueblos.

Ya lo dijo Aristóteles que el hombre es un ser sociable (zoón politikón),en el hombre como en el animal , un obrar que satisface sus necesidades se hace costumbre, la costumbre automatizada y esta a su vez se hace instinto .

En el reino de los instintos en la humanidad primitiva, la aproximación produjo no obstante choques y pugnas que predominaron con el dominio del mas fuerte , inteligente o astuto, por ultimo los intereses generales, creando formulas de derecho , de paz jurídica para regular los intereses de todos y hacer posible la convivencia social de unos a otros , y como la función crea al órgano , así las penas fueron creando el Derecho Penal .

Las penas primitivas fueron primero la reacción natural de cada uno contra la lesión en sus bienes , vida e integridad corporal y después reaccionaron contra la trasgresión de la normas de convivencia comunes , castigando al que hubiera atentado contra los intereses de cada uno , de aquí el carácter social de la venganza .

Los periodos de la evolución por las que ha pasado el Derecho Penal son los siguientes:

El Periodo de la Venganza, significa que el hombre ante una agresión recibida obtiene la satisfacción mediante un acto violento En esta fase cabe distinguir tres subfases :venganza privada , divina y publica .

La Venganza privada se le conoce como venganza de sangre y consiste en que el ofendido se hace justicia por propia mano, el afectado ocasiona a su ofensor un daño igual al recibido, esta fase se identifica como la ley del talion.

La Venganza divina es un castigo impuesto a quien causa un daño en virtud de creencias divinas, de modo que a veces se entremezclan rituales mágicos , el castigo es impuesto por representantes de diferentes deidades .

La Venganza pública aun se trata de un acto de venganza pero ejercida por un representante del poder publico y se traslada la ejecución justiciera a quien representa los intereses de la comunidad.

El Periodo Humanitario; aparece en el siglo XIX caracterizada por la revolución filosófica denominada Iluminismo que fue promovida por ideas renovadoras que influyeron en la humanización de los sistemas punitivos en donde Cesar Bonessana, Marquez de Becaria en su libro se combate las crueles e infames penas que se ejecutaban reprueba la aplicación de suplicios y tormentos, pugna por la prescripción de la pena de muerte sostiene que los delitos deben de estar claramente establecidos por las leyes y solo los jueces pueden declarar su violación , las penas deben ser publicas y prontas proporcionadas al delito y nunca atroces y admitió la protección del delincuente mediante el respeto de especificas garantías procesales.

"Para que una pena logre su efecto , basta con que el mal de la misma exceda del bien que nace del delito y en este exceso de mal debe de tenerse en cuenta la inhabilidad de la pena y la perdida del bien que produciria el delito . Los hombres se gobiernan por la acción repetida de los males que conocen y no por la de los que ignoran...A medida que los suplicios se hacen mas crueles el espíritu

de los hombres , que al modo de los líquidos se pone siempre al nivel con los objetos que le circundan , estos espíritus pues , se irán endureciendo ."[1]

El Periodo Cientifico ha provocado una profunda transformación del Derecho penal , la aparición de las llamadas ciencias penales (Antropología Criminal , Sociología Criminal, Endocrinología Criminal etc.), han influido notablemente en la concepción del delito, delincuente y pena.

El delincuente al realizar su conducta ilícita externa su personalidad antisocial .La pena es la nueva orientación se considera en su fundamental noción finalista persigue la prevención general de la criminalidad y es el medio o conducto por medio del cual el Estado procura la corrección o resocialización del delincuente previniendo en lo futuro actos delictivos.

A través de historia sobresalen civilizaciones que nos permiten comprobar los periodos de evolución del Derecho Penal.

1.1.1 BABILONIA .

La mayoría de los códigos orientales que tenían vigente en las antiguas civilizaciones , involucraban un sentido religioso a diferencia

[1] BONESANA ,Cesar , MARQUEZ DE BECARIA. **TRATADO DE LOS DELITOS Y LAS PENAS** . Editorial Cajica ,Puebla 1965, pp.151-153.

del código de hammurabi el cual adopto fielmente la ley del talión y dio reconocimiento a los delitos dolosos y culposos . Su importancia según el maestro Ignacio Villalobos *"Radica en el derecho de familia, y por ello, como por otras consideraciones históricas supone que es una compilación de las sabias y antiquísimas reglas de los sumerios , adaptada a su época de acuerdo con los fines de unificación que animaron todo el gobierno de hammurabi."*[2]

A este código lo sitúan aproximadamente 2250 a de C y 2300 a.de C. Esculpido en un bloque de diorita en caracteres cuneiformes el código fue descifrado y traducido por el alemán Winckler; de donde se puede afirma que regula la venganza para evitar que esta se extralimite.

Distingue los delitos voluntarios de los causados por negligencia y los hechos debidos a caso fortuito , reconoce el atenuante de arrebato y obcecación, incluso en caso de riña ,hace distinción entre Derecho patrimonial y publico, sus garantias procesales y regula la imputabilidad etc.

Este código es considerado el cuerpo de leyes mas antiguo del cual se tiene conocimiento , y por tanto , resulta esencial la información que en el se contiene , a fin de tener el criterio de lo fundamental del Derecho Penal para la humanidad .

---

[2] VILLALOBOS, Ignacio. **DERECHO PENAL MEXICANO**. Editorial Porrúa ,México ,1994. p. 104.

1.1.2 CHINA

Constituye una de las civilizaciones mas antiguas y su organización jurídico penal data desde el año 2205 a de C. , época en la que estuvo vigente el Código de Hia . Se tienen noticias de que hubo anteriormente en el periodo del emperador Seinu un libro denominado de Las Cinco Penas , cuya característica esencial era la ley del talión , la cual sigue el principio citado " Ojo por ojo diente por diente"; y es la facultad que se ejerce en contra del causante de un daño de recibir un castigo en proporción del cometido .

En el primitivo derecho de china, contenido en el libro de las Cinco Penas , en tiempos del mítico emperador Seinu predomina la venganza y el talión y cuando este no era aplicable se recurría a formas de talión simbólico ; así, al ladrón se le amputaban las piernas , porque en chino una misma palabra significa "ladrón" y "huir" .La pena de muerte se imponía en publico , con el fin de escarmiento y purificación y se ejecutaba por decapitación , horca y descuartizamiento y entierro en vida . Las otras clases de pena eran rutilantes o de marca ; esta ultima para los delitos de menos gravedad.

"En 1783 A de C se tuvo conocimiento, con posterioridad, de la existencia de los Códigos de Chang y de Chou de 1052 a. de C. La característica predominante en todos estos códigos es la crueldad, la pena de muerte , la amputación de órganos , la tortura y en

general los medios intimidantes y ejemplares común denominador del Derecho Penal Chino ."[3]

1.1.3 EGIPTO

El Derecho Penal egipcio es pionero en materia de disposiciones; hay noticias de estas desde 2700 a. de C. Época de la quinta dinastía donde aparecen los jueces de carrera, una organización parecida a la actual Suprema Corte de Justicia , un procedimiento escrito, además de archivos judiciales.

Los atentados contra los faraones , la complicidad en estos atentados , la desobediencia de las ordenes reales , las ofensas del faraón y sus familiares , el perjurio y el homicidio , eran estimados delitos de esa divinidad. Se aplicaba el talión simbólico: al espía se le cortaba la lengua; al estuprador, los genitales y a la mujer adultera la nariz. Como otras penas para otros delitos existían los trabajos públicos o en las minas , así como la esclavitud.

Jiménez de Asúa indica que "Su derecho esta impregnado del espíritu religioso: el delito era ofensa a los dioses , y las penas mas crueles se imponía por los sacerdotes como delegación divina y para aplicar a la divinidad, el signo de justicia era un pluma de Avestruz. , "[4]

[3] LÓPEZ BETANCOURT, Eduardo. **HISTORIA DEL DERECHO PENAL**. 5ta Ed., Editorial Porrua, México 2001 p.6.
[4] JIMENES DE AZUA , Luis. **TRATADO DE DERECHO PENAL**. 3a Ed.,Editorial Losada, Buenos Aires, Argentina 1964, tomo I, p. 270.

El Derecho Penal Egipcio , en general, estuvo influido por un profundo sentimiento religioso ya que el delito era una ofensa a los dioses y los encargados de aplicar las penas se justificaban en nombre de la divinidad.

1.1.4 GRECIA.

En la antigua Grecia se distinguen tres grandes periodos :

I.- Periodo legendario. Corresponde inclusive, a la época de las leyendas de Grecia predomina la venganza privada. El concepto de delito tuvo su origen en el destino, pero también la venganza inexorablemente era un acto del propio destino. Se crean los institutos de venganza.

II.- Periodo religioso. Se caracteriza por que el Estado al dictar las penas, lo hace como delegado del dios Júpiter. El que cometía un delito debía purificarse mediante el cumplimiento de una pena.

III.-Periodo histórico. Se distingue en la medida que el Derecho Penal se sustenta en las bases morales. La responsabilidad adquiere así un carácter individual . Una pena terrible era la expulsión de la comunidad (atimia) , cuando se decretaba, cualquiera podía matar al expulsado y decomisarle sus bienes .

En esparta descuella un gran legislador, quien promulgo leyes de muy avanzada envergadura : Licurgo quien vive durante el siglo VII

a. de C. hizo castigar el celibato y la piedad para el esclavo, mientras declaraba impune el robo ejecutado diestramente por los adolescentes.

Atenas también fue cuna de notables creadores de leyes : Primero Dracon distinguió entre delitos públicos y privados señalando un progreso que Roma habría de recoger , también en el siglo VII a. de C. en Catania sancionaron la venganza privada. No obstante ser considerado el delito como imposición fatal del destino (ananke).

Los filósofos penetraron hasta el fin científico de la pena anticipándose a la moderna penología ; "*platón sentó que si el delito es una enfermedad , la pena es una medicina del alma ;y Aristóteles que el dolor inflingido por la pena debe ser tal que sea contrario en su grado máximo a la voluptuosidad deseada, con lo que se anticipó al correccionalismo.*"[5]

1.1.5 ISRAEL

La legislación de Moisés data del siglo XVI antes de la era vulgar, y encuentro sustentación en el Pentateuco ,los primeros cinco libros de Biblia, donde recogen los preceptos religiosos, morales y jurídicos promulgados en un periodo de 40 años .

[5] CARRANCA Y TRUJILLO, Raúl, CARRANCA Y RIVAS, Raúl. **DERECHO PENAL MEXICANO**, 21ª ed., Editorial Porrúa , México. 2001,pp 96 y 97

Éxodo ,Levítico y Deuteronomio principalmente contienen las normas de carácter penal, y no fue sino hasta la integración del tamul que dicha legislación empezó a aminorar el rigor que la caracterizaba , la ley penal hebrea tiene importante peculiaridad que consiste en una absoluta igualdad ya que no toma en consideración la clase social , el estatus político o la religión. Tanto la legislación mosaica como la posterior a esta se caracterizan por la atenuación general de las penas .

En el Derecho hebreo la venganza personal constituyó un derecho, y la venganza de sangre, un deber. Las penas se clasificaban en aflictivas y pecuniarias. La pena de muerte se admitió en la ley de Moisés, aunque con ciertas limitaciones.

Fue muy superior a leyes en cuanto a los sentimientos humanitarios de esa época. Considerada una legislación primitiva a partir de la época del segundo templo se produjo un notable cambio principalmente en cuanto el sentido que se dio a los conceptos de crimen y castigo incluyendo la antigua ley del talión que se le fijo a un valor pecuniario.

La ley judía , esta íntimamente emparentada con la babilónica ,en cuanto a las normas procesales , instituidas por todos los códigos de la tierra , la Biblia establecía las reglas que suelen ser comunes a todas las legislaciones que el crimen sea debidamente comprobado , que existan testigos oculares y que estos reúnan determinadas condiciones de honestidad e imparcialidad ; que el

delito haya sido cometido ; que el culpable haya sabido conscientemente que cometía un hecho punido por la ley.

1.1.6 ROMA

En la Roma antigua, pena significaba tanto como composición .En las XII tablas (siglo V a de C.) Se ven consagradas la venganza privada , el talión y la composición y posteriormente se distinguió entre delicta publica y privada; según pudieran ser los delitos perseguidos en interés del Estado y por sus funcionarios o en interés del ofendido y por estos diferenciándose la disciplina domestica , común y militar .

En la época clásica las instituciones Justineanas , los Digestos , los Códigos y las Novelas desarrollaron abundante material penal no inferior en sabiduría jurídica plasmada en realismo positivo, a la justicia civil .

Se distinguen cuatro principales periodos en esta importante civilización, cuna del Derecho Occidental.

I.- Anterior a la fundación de Roma (siglo IX a de C.) la pena tiene carácter de expiación religiosa ; la venganza privada es obligatoria para quienes forman parte de la familia y de la gens. El pater familias ejercía el derecho de matar a los miembros de su familia se carecía de un sistema procesal ; y se depositaba en tres

principales personajes la facultad de imponer sanciones : El pater familias , el jefe militar y un Magistrado que actuaba siempre de manera discrecional , basándose en el arbitrio .

II.- Fundación de Roma (753 -509 a de C.) . Es el periodo de monarquía en el que subsiste el carácter sagrado de la pena, aparecen los delitos públicos, entre ellos el parricidio y el incesto .

III.- La Republica. Aquí surgen importantes disposiciones jurídicas , como la ley de las XII Tablas, en las tablas VII y XII se analizan todo lo referente a los delitos , sobresalen los señalamientos siguientes : se precisan cuales son los delitos privados , se afirma el principio de la Ley del Talión y aparece la composición como medio para evitar la venganza privada que consiste en comprar la venganza entre los particulares se mantienen los delitos públicos posteriormente prevalecerían las disposiciones dictadas por los gracos y las contenidas en las leyes de coronelía y julia , donde en otras innovaciones se prescriben la disminución de los delitos privados y el incremento de los públicos . La pena se vuelve intimidatoria. Se atenúan las penas y al final de la República se suspende la pena de muerte .

IV.- El Imperio Se crea tribunales de justicia penal Se implanta nuevamente la pena de muerte pero reservándose solo al parricidio y hasta Adriano se aplica también a otros delitos . Se establecen nuevos castigos en lo concerniente al trabajo en las minas y el de trabajos forzados. la pena adquiere una función

manejan nuevos conceptos jurídico penales como la provocación , la preterintensión . Se considera una obra jurídica notable la de Justiniano.

El Derecho Penal romano no alcanzo los impresionantes niveles del derecho civil, la importancia del Derecho Penal romano lo constituye:

a) La afirmación del carácter publico y social del Derecho Penal no obstante la diferencia siempre entre delitos privados y públicos. Pues la ilicitud privada no se equiparaba a una acción civil daba lugar a una verdadera pena .

b) El amplio desarrollo alcanzado por la doctrina de la imputabilidad, de la culpabilidad y de las causas que la excluyen especialmente el error .

c) El elemento subjetivo se encuentra claramente diferenciado , aun por la clase de pena que correspondía al dolo y la culpa , pues mientras al hecho doloso seguía la poenitio , al culpable se le aplicaba la castigatio que tenia fin sobre todo intimidante, era aplicado a menores y personas colectivas .

d) La teoría penal no alcanzo tampoco a la aplicación del principio de reserva , prohibición de la analogía .

"Del viejo tronco romano parten muchos de los principios que luego habían de recoger las escuelas Clásica y Positiva . Así , sobre

el Derecho Romano se encuentran muchas de las palabras que hay son universalmente reconocidas delictum, poena, carcer ,crimen, supplitium ,injura dammun, fuertum."[6]

1.1.7 ESPAÑA

Durante la Edad Media, el derecho en España atravesó por un largo periodo indefinible en cuanto a las tendencias que lo regían. En el siglo XIII España adopta el Derecho Romano.

Las siete partidas escritas en magnifico castellano son un documento maravilloso que en su partida VII da una definición de Delito , de la Pena y sobre todo de las circunstancias y entre ellas las que ahora denominamos causas de justificación.

En 1567 , surge la nueva recopilación que regiría la legislación activa para las colonias conquistadas en América y en 1805 se elabora la Novísima Recopilación . Entre los preceptos penales mas destacados de la historia española consideramos el Ordenamiento de Alcalá, las Ordenanzas Reales de Castilla , las Leyes de Toro, la Nueva Recopilación , y la Novísima Recopilación.

Para facilitar el estudio de la historia Española existen cinco periodos que resaltan por su importancia según el maestro López Betancourt

---

[6] Idem.

en su obra intitulada Historia del Derecho Penal cita al jurista hispano Luis Jiménez de Asúa junto con la siguiente clasificación.

"I.- Época Primitiva y Romana.

II.- Periodo Visigótico.

III.-Periodo de la reconquista que a su vez se expone , conforme a estos apartados ;

a) El derecho penal en el periodo de los fueros;

b) Legislación Alfonsina (la Recepción);

c) Derecho Territorial Castellano;

d) Derechos regionales.

IV.-Derecho penal de los musulmanes españoles .

V.- Ordenamientos y recopilaciones."[7]

La legislación feudal en España es muy numerosa e importante mas que la de cualquier otro país en Europa durante esa época.

1.- Siglos IX a XIV. Carta -pueblos y fueros municipales ; fueron instrumentos de privilegios , los cuales actuaban en favor de los titulares , mediante ellos se dispensaba diversidad de beneficios y en cierta forma se les trataba con favorable parcialidad .

2.-Fuero Viejo de Castilla este fue uno de los que mas destaco, también conocido como fuero de fazañas y albedríos en razón que le reconocían valor al derecho consuetudinario . En este documento jurídico se regularizo la composición pecuniaria para los delitos de sangre bajo el nombre de enmienda o caloña.

[7] LOPEZ BETANCOURT,Eduardo. Op.cit., p.15

3.- Fuero Real con sus suplementos , leyes para los adelantados mayores y leyes nuevas con los escritos de juristas privados que lo ilustran, llamados Leyes del Estilo y Especulo ; es una de las grandes obras legislativas de Alfonso IX , de León y XIX de castilla conocido como Alfonso "El Sabio" sirvió a todos los lugares que carecían de disposiciones jurídicas escritas .

Al Fuero Real también se le conoció como los nombres del Fueros de las Leyes , Fuero de Libro , Libro de los Consejos de castilla que en su contenido abarca a los derechos civil, penal , procesal y político ; varias disposiciones se encontraron señaladas en el Fuero de Juzgo y sirvió de base para las siete partidas .

El Fuero Real se divide en cuatro libros y en el cuarto se encuentra contemplado el Derecho Penal y sus principales características son:

a) Se disminuye la aplicación de la pena de muerte .
b) Las penas que impone son crueles y llegan a suscitar el horror de la sociedad.
c) Sostiene la no retroactividad de la ley .
d) Concede a todo hombre el derecho de acusar a cualquier otro, dándose así la acusación pública popular .
e) Distingue el procedimiento civil privado del procedimiento penal público y paralelamente a ellos se establece el de oficio.
f) El adulterio es considerado como delito público y los adúlteros son entregados al marido apara que disponga de ellos .

4.-Las siete partidas ; Forman parte de la obra jurídica mas importante de Alfonso "El sabio", Originalmente se le denomino Libro de las Leyes que hizo el Rey don Alfonso con ellas se pretendió la unidad de la legislación y la consolidación del poder real la partida VII trata lo concerniente al Derecho Penal y sus características fueron las siguientes:

a) El establecimiento del sistema acusatorio mediante la forma escrita.
b) Exigir en los delitos privados la querella del ofendido.
c) Se permita la acusación de los muertos en los delitos de traición y herejía .
d) La acusación podía probarse de tres maneras : por testigos; por pesquisas y por lid ; seguida de un duelo judicial o juicio de Dios , el acusador retaba a su contraparte .Si el acusado ganaba se le consideraba alevoso , si perdía era traidor y por lo tanto condenado a morir y a privarlo de todos sus bienes.
e) La prevaricación del abogado se equipara al fraude.
f) Se permitía el homicidio del adulterio solo si era sorprendido infraganti.
g) Los tormentos se encontraban restringidos y su aplicación dependía por mandato de un Juez.
h) La pena contiene tres principios; expiatorio, intimidatorio y ejemplar.

5.-Ordenamiento de Alcalá ;Se componen de 32 títulos divididos en 126 leyes , Los primeros 15 títulos se refieren al enjuiciamiento.

Muchas de sus disposiciones fueron conformadas posteriormente en diversas leyes entre ellas las ordenanzas Reales de Castilla. La Nueva y La Novenisima Recopilación.

6.-En 1485. Ordenanzas Reales de castilla .Son la compilación de leyes que no estuvieron comprendidas en el fuero juzgo y las Partidas. Se dividen en Ocho Libros que conforman 115 títulos y 11666 leyes y se deben al jurisconsulto Alfonso Díaz Montalvo del Consejo Real R I libro VIII contiene todo lo relativo al castigo y a los delitos y sobre todo varios aspectos del derecho procesal .

En 1770 empezaron a reunirse para un código penal y en 1822 se promulgo el primero, en 1869 se expidió una ley fijando las bases para organizar el sistema penitenciario Establecida la Republica el 14 de abril de 1931 se elimino el Código de la dictadura y sin tiempo para una nueva elaboración se restableció desde luego la vigencia del anterior de 1870 pero en 1932 se aprobaron 32 bases para la reforma del viejo ordenamiento conforme a las cuales se publico la nueva ley que debia regir desde el 1de noviembre de 1932 .

Derecho Canonico.

También durante la Edad Media prevaleció el Derecho Canónico con influencia de los derechos romano y germánico donde se distinguen tres tipos de delitos .

-Los Eclesiásticos atentaban contra el poder de la divinidad,
-Los Seculares constituían la regla general ,

-Los Mixtos transgredían tanto contra el poder divino como contra el humano.

A pesar de esta división , y que a los ilícitos eclesiásticos se les denominaba pecados y a los seculares delitos , la realidad es que se utilizaban indistintamente y había una absoluta confusión del poder público con el eclesiástico en donde la iglesia católica toma la justicia por su cuenta , conocido como la inquisición.

1.2 EVOLUCION DEL DERECHO PENAL EN MEXICO.

La realidad es que todo lo acontecido antes de la llegada de los españoles se tienen escasas noticias fidedignas , lamentablemente la mayor parte de los documentos como los pergaminos códices y otros vestigios que nos hablaban de las culturas prehispánicas fueron destruidos por los propios españoles , Fraile Bartolomé de las Casas relata que en la zona de Yucatán , donde floreció la cultura maya la quema de papiros y códices se hizo de tal magnitud que las lenguas de fuego se veían a varias leguas de distancia .

Se ha dicho que en lo penal la historia de México comienza con la conquista pues todo lo anterior , protohistoria y prehistoria , esta por descubrir todavía o tal vez los pueblos indígenas nada tenían en materia penal lo que parece imposible , o si lo tenían nada les quedo después de la conquista ; fue borrado y suplantado por la legislación colonial tan rica .

La influencia del rudimentario Derecho Indio en la génesis del pueblo Mexicano es difícil la comprobación, los mexicanos aun el indio de raza pura , estamos totalmente desprendidos de toda idea jurídica propiamente indígena es decir ; que tenga su raíz y su origen en los usos y costumbres precortesianos .

A pesar de la escasa información que debido a su gravedad y rigidez en materia penal , mantenían una apacible y ordenada vida

social, los actos considerados por ellos como delitos graves, consistieron en : abuso de confianza , embriaguez, alcahuetería, adulterio, asalto, calumnia judicial, daño en propiedad ajena, aborto, estupro, encubrimiento, falso testimonio, falsificación de medidas, hechicería ,homicidio ,incesto , pederastia , peculado, mal versión de fondos , riña ,robo sedición y traición .

El Derecho represivo de esta época se caracterizaba por ser drástico ; de ahí que la mayoría de estos actos delictuosos se castigaban con la pena de muerte (mediante decapitación, lapidación y descuartizamiento), el destierro , la cárcel ,los azotes y la mutilación .

1.2.1 EPOCA PRECORTESIANA

Los Aztecas.

A la llegada de los españoles, este pueblo se erigía como el mas poderoso y el territorio dominado por él era muy extenso, comprendía los estados ahora conocidos como : Veracruz, Oaxaca, Guerrero, Puebla ,Tlaxcala , Hidalgo ,México y el Distrito federal.

Gozaban de un régimen de gobierno sustentado en la participación ciudadana , se constituyo en una confederación de tribus dirigida por un jefe militar y por un jefe político y su forma de gobierno se dividía en poder ejecutivo, judicial y religioso .

El Poder Judicial se confería a los jueces a quienes se les envestía con la personalidad de funcionarios públicos. Los aztecas fraccionaron la ciudad de Tenochtitlan en calpullis o barrios y con ellos se constituyo la unidad étnica y jurídica mas trascendental de dicho pueblo donde existía un tribunal o casa de justicia , donde se dirimían los problemas legales ; para juzgar a una persona se seguían determinadas reglas .

En materia penal , los aztecas se esforzaron en dividir a los delitos tomando en cuenta el bien jurídicamente tutelado por ejemplo dentro de los delitos contra la vida y la integridad corporal se comprendía las lesiones y el homicidio , en lo relativo al patrimonio incluían al robo , el fraude y el daño en propiedad ajena .

"Aplicaban penas como lapidación, azotes, pena de muerte , la cárcel era poco común y generalmente servia por pocos periodos . La pena capital se aplicaba por ahorcamiento a garrotazos o quemándolos ; todo dependía de la gravedad del delito ."[8]

Practicaban una moral propia , diferente a la nuestra ; por ello se consideraban delitos ,muchos actos que en la actualidad han sido superados tales como la embriaguez ,la cual inclusive llegaba a castigarse con la pena de muerte ; el celestinaje (alcahuetear en materia de amores) o al mentir podía ser pena de muerte .

---

[8] Ibid. p. 22

En general podemos concluir que existe una gran coincidencia entre el derecho penal azteca y el actual Derecho mexicano.

"Los aztecas conocieron la distinción entre delitos dolosos y culposos las circunstancias atenuantes y agravantes de la pena, las excluyentes de responsabilidad , la acumulación de sanciones la reincidencia el indulto y la amnistía."[9]

Los Mayas.

Su cultura Florecía fundamentalmente en al península de Yucatán extendiéndose por Chiapas y en buena parte de América Central , y se organizaron en una Confederación llamada Nuevo Imperio Maya formada por las tribus asentadas en Uxmal, Chichen Itza y Mayapan.

El pueblo era religioso, profesaba la misma tesis dual de los aztecas, contaba con dos gobernantes uno de carácter político (Canek) y otro de carácter religioso (Kinkanek) y tenían que consultar decisiones importantes a un consejo el cual se conformaba con los principales de cada tribu o grupo étnico .

El Derecho Penal maya tendía precisamente a proteger el orden social imperante, la función represora la mantenía el Estado, se castigaba basándose en los resultados y no en la intención ,los jueces eran funcionarios públicos con amplio arbitrio los delitos mas

[9] CASTELLANOS TENA, Fernando .**LINEAMIENTOS ELEMENTALES DE DERECHO PENAL**.19a ed Editorial Porrua, México 1984.p. 43.

graves fueron el homicidio, el adulterio ,el robo , el incendio, la traición a la patria, la injuria y difamación .

Dentro de las sanciones se encuentra la muerte , una especie de esclavitud la infamación y la indemnización , la cárcel la utilizaban solo por los delitos - in fraganti cuando era delito de robo operaba una excusa absolutoria si era la primera vez y si era reincidente se le marcaba la cara.

Los Purepechas.

Este grupo étnico habitó esencialmente los ahora estados de Michoacán , Guanajuato , Colima y parte de Jalisco , Guerrero, Querétaro, México se les conoce equivocadamente como tarascos que en la lengua purepecha significa "amante de tu hija" siendo un pueblo religioso es profundamente moralista originando que se identifique mas con el Derecho .

En materia penal los purepechas llegan a aplicar sanciones , con extrema crueldad, perseguían con mayor dureza , los delitos de homicidio , traición a la patria y el adulterio cometido con una de las esposas del calzontzin o jefe militar , se aplicaba generalmente la pena de muerte se les enterraba vivos hasta la cabeza para ser devorados por aves de rapiña atados de pies y manos.

Las principales penas eran la pena capital, la confiscación, la demolición de la casa, el destierro, el arresto en la propia habitación

y en casos de excepción la encarcelación. El adulterio se castigaba con la muerte y si el esposo la encontraba infraganti la podía golpear pero no matar puesto que la venganza privada estaba prohibida, por la comisión de un primer delito que no fuera grave se concedía el indulto , Hechiceros y brujos eran castigados con la muerte.

1.2.2 EPOCA COLONIAL.

El 13 de agosto de 1521 , Fecha de la caída de Tenochtitlan se inicia propiamente la época colonial , prolongándose por tres siglos, el dominio español sobre las tierras conquistadas se vuelve absoluto y en ocasiones desalmado ,la llegada de los españoles se ven reducidos para dar paso a la creación por un lado, de un estado unitario y por el otro, de aborígenes o indios sin importar sus esenciales y evidentes diferencias; por ejemplo entre un maya y un azteca ya que mantenían su independencia y personalidad propia .

Precisamente luego de la caída de Tenochtitlan se creó el Virreinato de la Nueva España, institución que formaba parte del estado monárquico español , aplicándose tres tipos de leyes:

I.- Las destinadas a todo el territorio español.
II.- Las dirigidas solo a las colonias de ultramar.
III.- Las exclusivas de la Nueva España .

A los aborígenes se les permitió aplicar el derecho de sus antepasados cuando no se opusiera al español. Esto en realidad fue una utopía en la práctica ya que se marginaba de manera evidente a los nativos y la de los mestizos que día con día se acrecentaban más.

"La colonia represento el transplante de las instituciones jurídicas españolas a territorio americano .La ley 2.Titulo. I , Libro .II de las leyes de Indias dispuso que en todo lo que no estuviese decidido ni declarado ... por las leyes de esta recopilación o por cedulas, provisiones u ordenanzas dadas y no revocadas para las indias se guarden las leyes de nuestro Reino de Castilla conforme a las del Toro."[10]

Principales leyes Españolas vigentes durante la Colonia.

a) La recopilación de Leyes de Indias de 1681. En esta legislación se incorpora la orden expedida por Carlos V , el 6 de agosto de 1555 , mediante el cual las leyes de los indios que no pugnaran las disposiciones españolas , mantenían su vigencia . Las leyes indias fueron las fuentes mas sobresalientes de la legislación colonial con ellas se origina el derecho indiano .

b) Las leyes de castilla principalmente reconocían el valor del derecho consuetudinario.

---

[10] CARRANCA Y TRUJILLO, Raúl, CARRANCA Y RIVAS, Raúl Op.cit .p.116.

c) El Fuero Real eran cuatro libros en donde el cuarto hace referencia al Derecho Penal en donde incluyen la disminución de la pena de muerte, la no retroactividad ,crueldad en las penas, división del proceso civil privado y el proceso penal publico etc.

d) Las partidas consolidación del poder real lo mas importante para nosotros es la VII partida ; porque contiene el sistema acusatorio escrito , la querella del ofendido en delitos privados , la acusación se prueba por testigos por pesquisas o por duelo judicial o juicio de dios permitía el homicidio del adultero .

e) Las ordenanzas Reales son una compilación de leyes que no estuvieron comprendidas en el fuero juzgo y las partidas.

Las audiencias eran cuerpos colegiados , integrados por personas llamados oidores , designados por el rey . Tenían facultades judiciales y administrativas , fungían como tribunales de apelación y además eran órganos consultivos del virrey, en especial para revisar y aprobar las ordenanzas que se daban alas poblaciones.

Durante el siglo XVIII se incrementan en la nueva España diversos Tribunales especializados como el Tribunal de la Acordada encargado principalmente de perseguir y castigar a los salteadores de caminos, el Real Tribunal de minería que conocía de contiendas surgidas entre mineros,Así mismo con y con anterioridad a éste se creó la Casa de Contratación de Sevilla cuya finalidad era la contratación del comercio de las colonias.

Por ultimo el Consejo de las Indias, el cual ejercía funciones judiciales en los negocios de carácter civil y penal .

Se establecieron diversos tribunales eclesiásticos de lo cual podemos deducir:

-Durante tres siglos de dominación española se dio un transplante de las instituciones jurídicas peninsulares.
-Algunas disposiciones jurídico penales fueron propias para la Nueva España.
-El abuso , la arbitrariedad y en general la injusticia , fueron los signos característicos de esa época en perjuicio de los aborígenes, a quienes en especial en materia penal se les imponía crueles penas .

1.2.3 MEXICO INDEPENDIENTE

México logra su independencia política en 1821 , después de una lucha interna y desgastante que duro 11 años .Durante los primeros años fueron gobernados por el derecho español vigente ,es decir la mismas disposiciones de la época colonial .

El 12 de enero de 1822 se designo una comisión para elaborar el Código Criminal de la incipiente nación integrada por Ignacio Espinosa , Antonio Gama , Andrés Quintana Roo y Carlos García de Bustamante .

Gracias a la intervención y perseverancia de este ultimo personaje quien realmente lo elaboró y leyó en el seno del Congreso Constituyente , Mexicano dando como resultado el primer proyecto de Código Penal .

En 1835 el Estado de Veracruz aprobó el primer Código penal Vigente debido a los trabajos de una comisión integrada por Bernardo Couto , Manuel Fernández Leal, José Julián Tornel y Antonio Manuel Solorio , y Porte PETIT nos dice que esta dividido en tres partes : La primera parte "Las Penas y Delitos en General" ;la Parte segunda llamada "Delitos contra la Sociedad" y al tercera se refiere contra "Los Delitos Contra los Particulares".

Durante el Imperio de Maximiliano de Habsburgo entro en vigor el Código Penal Francés , pero formo una comisión formada por Teodosio Lares , Urbano Fonseca y Juan b. Herrera para elaborar un proyecto propio que nunca llego a tener una vigencia debido a la caída del Imperio .

En 1861 , Benito Juárez ,Presidente de la República , ordenó el restablecimiento de una Comisión para formular un proyecto de Código Penal la cual fue presidida por Antonio Martínez de Castro.

Su trabajo concluyo en 1868 y para 1971 se aprobó esta nueva ley, básicamente influenciada por el Código Español de 1870 por su orientación en favor de la escuela clásica del derecho Penal .

1.2.4 MEXICO DESPUES DE LA REVOLUCION.

Los ideales de la Revolución Mexicana se plasmaron y proyectaron en todas las actividades del país particularmente en el campo legislativo sobre todo a partir de la Constitución Política Mexicana de 1917 .

El Derecho Penal Mexicano no podía quedar a la zaga del cambio político del país y dados los primeros años del triunfo del movimiento armado se manifestaron muchas inquietudes.

En 1925 Plutarco Elías Calles designo una comisión para redactar un Código para el Distrito y territorios federales formada por Ignacio Ramírez Arriaga , Antonio Ramos Pedrosa, Enrique Gudiño, Manuel Ramos Estrada y José Almaraz conocido también como Código de Almaraz llegando a ser ley positiva en 1929 el 15 de diciembre fue un Código para los delitos es decir que las contravenciones no se abarcan en su texto y constaba de 1228 artículos y otros cinco transitorios .

El licenciado Emilio Portes Gil Presidente en turno designo una nueva comisión por Antonio Teja Zabre , Ernesto Garza, Luis Garrido, José Ángel Ceniceros , José López Lara.

Formularon el proyecto que dio vida al Código Penal del Distrito Federal en materia del fuero común y de toda la República en materia Federal promulgado el 13 de agosto de 1931 promulgado

por el Presidente Pascual Ortiz Rubio y entro en vigor el 17 de Septiembre del mismo año desde entonces tantas reformas han suscitado confusiones y hasta criterios contradictorios .

Por decreto del 29 de abril de 1999 entro en vigor El Código Penal para el Distrito Federal quedándose el de 1931 en consecuencia como Código Penal Federal.

En Sesión del pleno de la Asamblea Legislativa , verificada el dia 30 de abril se aprobó por unanimidad de votos de los C.C. Diputados presentes, en lo general y en lo particular el Proyecto de *"Decreto del Nuevo Código Penal para el Distrito Federal"*[11]

1.2.5 CONCEPCION ACTUAL DEL DERECHO PENAL EN MEXICO.

Si el hombre ha de vivir en sociedad para su conservación y desarrollo, es claro que en esa sociedad, organizada con tales fines, ha de tener posibilidad de hacer todo aquello que sea medio adecuado para llenar sus propias necesidades, hallándose obligado a respetar el ejercicio de iguales facultades en los demás y aun a contribuir con su esfuerzo para la satisfacción de las exigencias colectivas, constituyéndose así el orden jurídico por el conjunto de normas que regulan y hacen posible y benéfica la vida en común.

---

[11] **Gaceta Oficial del Distrito Federal** 16 de julio de2002.

El Derecho Penal en sentido subjetivo, es el atributo de la soberanía por el cual a todo Estado corresponde reprimir los delitos por medio de las penas; en tanto que objetivamente se forma por el conjunto de normas y de disposiciones que reglamentan el ejercicio de ese atributo: el Estado, como organización política de la Sociedad, tiene como fines primordiales la creación y el mantenimiento del orden jurídico; por tanto, su esencia misma supone el uso de los medios adecuados para tal fin.

El autor Orellana Wiarco nos comenta en su obra intitulada Curso de Derecho penal .*"El derecho penal es el conjunto de normas de derecho público que estudia los delitos las penas y medidas de seguridad aplicables a quienes realicen las conductas previstas como delitos con el fin de proteger los bienes jurídicos fundamentales de la sociedad y de los individuos."*[12]

Para el maestro **Miguel Ángel Cortes Ibarra** define *"El Derecho Penal, rama del Derecho General, encuentra su justificación en la finalidad del Estado que tiende a preservar el orden social de la necesidad de salvaguardar bienes de carácter preponderantemente social y proteger elevados intereses personales, ha surgido el Derecho Penal que mediante la amenaza y aplicación efectiva de las penas tutela tales bienes."*[13]

---

[12] ORELLANA WIARCO,Octavio Alberto. **CURSO DE DERECHO PENAL.** Editorial Porrua . México 1999 .p 5.
[13] IBARRA CORTÉS, Miguel Angel.Op.cit, p.1.

El Derecho Penal es de carácter Publico desde el momento que sus normas aspiran a proteger intereses vinculados con la colectividad, es Finalista porque al proteger esos valores persiguen como fin general precisamente el logro de la convivencia humana , es Valorativo por tutelar bienes fundamentales para la vida social .es Regulador Externo del hombre al manifestarse materialmente en la realización de la conducta, es sancionatorio cuando violan alguna norma y castigan la trasgresión de la misma.

Conceptos Generales del Derecho Penal.

Derecho Penal Objetivo .

Lo constituye el conjunto de normas jurídicas que definen las penas y medidas de seguridad , es el cúmulo de disposiciones jurídicas dictadas por el Estado y constan en el cuerpo legal punitivo.

Derecho Penal Subjetivo.

Es la facultad del Estado de imponer penas es derecho de castigar (ius poniendo),al Estado que es soberano le corresponde la función punitiva por eso fija las sanciones y las aplica.

Derecho Penal Sustantivo .

Conjunto de normas jurídico penales relativas al delito, penas o medidas de seguridad, es el objeto de estudio del Derecho Penal .

Derecho Penal Adjetivo .

Es el complemento necesario del derecho sustantivo ,se trata del conjunto de normas que se ocupan de señalar la forma de aplicar las normas jurídico penales en los casos concretos , se llama mas comúnmente Derecho procesal.

1.3 EL DELITO EN MEXICO.

La palabra "delito", deriva de expresiones romanas delicto o delictum, supino del verbo delinquí , delinquere que significa desviarse , resbalar abandonar, abandono de una ley Abandonar el buen camino.

La Definición legal del Delito se encuentra en el artículo 15 del Código Penal para el Distrito Federal que a la letra dice , **El delito sólo puede ser realizado por acción o por omisión.**

"El delito a lo largo de los tiempos , ha sido entendido como una valoración jurídica objetiva y subjetiva la cual encuentra sus precisos fundamentos en las relaciones necesarias surgidas entre el hecho humano contrario al orden ético social y su estimación legislativa."[14]

1.3.1 SUJETO .

Sujeto Activo.

Es primera persona física que comete el delito, se llama también, delincuente, agente o criminal. Esta última noción se maneja desde el punto de vista de la criminología .

[14] PAVÓN VASCONCELOS, Francisco. MANUAL DE DERECHO PENAL MEXICANO. Editorial Porrua, México 2002, p. 187

El sujeto activo será siempre una persona física, independientemente del sexo, edad (la minoría de edad que da lugar a la inimputabilidad) nacionalidad y otras características. Cada tipo (Descripción legal de un delito) señala las calidades o caracteres especiales que se requieren para ser un sujeto activo.

Nunca la persona moral o jurídica , podrá ser sujeto activo de algún delito cabe mencionar que en ocasiones aparentemente es la institución la que comete un ilícito pero siempre habrá sido una persona física la que ideó actuó y en todo caso , ejecutó el delito .

El fundamento jurídico lo podemos encontrar en el Código Penal para el Distrito Federal, Articulo 22. (Formas de autoría y participación).

Son responsables del delito, quienes:
I.- Lo realicen por sí;
II.- Lo realicen conjuntamente con otro u otros autores;
III.-Lo lleven a cabo sirviéndose de otro como instrumento;
IV.-Determinen dolosamente al autor a cometerlo;
V . -Dolosamente presten ayuda o auxilio al autor para su comisión; y
VI.-Con posterioridad a su ejecución auxilien, al autor en cumplimiento de una promesa anterior al delito.

Quienes únicamente intervengan en la planeación o preparación del delito, así como quienes determinen a otro o le presten ayuda o auxilio, sólo responderán si el hecho antijurídico del autor alcanza al menos el grado de tentativa del delito que se quiso cometer.

La instigación y la complicidad a que se refieren las fracciones IV y V, respectivamente, sólo son admisibles en los delitos dolosos. Para las hipótesis previstas en las fracciones V y VI se impondrá la punibilidad dispuesta por el artículo 81 de este Código.

Sujeto Pasivo.
Sujeto pasivo es la persona física, moral sobre quién recae el daño o peligro causado por la conducta del Delincuente. Por lo general se le denomina también víctima u ofendido en cuyo caso una persona jurídica puede ser sujeto pasivo de un delito .

Sujeto Pasivo de la Conducta: Es la persona que de manera directa reciente la acción por parte del sujeto activo .
Sujeto Pasivo del Delito: Es el titular del bien jurídico tutelado que resulta afectado.

1.3.2 OBJETO

El objeto del delito se subdivide en Objeto Material y Objeto Jurídico. *"En la doctrina se distingue entre el objeto jurídico que es el bien jurídico tutelado a través de la ley penal mediante la amenaza de sanción , puede decirse que no hay sin objeto jurídico por ser este su esencia y por otra el objeto material que es la persona o cosa dañada o que sufre peligro derivado de la conducta delictiva."*[15]

---

[15].Ibid.,p 189

Objeto Jurídico.

Es el interés jurídicamente tutelado por la ley .El Derecho Penal en cada figura típica (delito) tutela determinados bienes que considera dignos de ser protegidos. al derecho le interesa tutelar o salvaguardar la libertad de las personas ; así el legislador crea los delitos de secuestro , homicidio aborto con lo cual pretende proteger la vida humana . Todo delito tiene un bien jurídicamente protegido, recuérdese que justamente en razón de este criterio , el Código Penal clasifica los delitos en orden al objeto jurídico (bien jurídicamente tutelado).

Objeto Material.

Es la persona o cosa sobre la cual recae directamente el daño causado por el delito cometido .

Cuando se trata de una persona esta se identifica con el sujeto pasivo de modo que en una misma figura coincide el sujeto pasivo y el objeto material ,por tanto la persona puede ser física o jurídica por ejemplo ;el homicidio ,lesiones y difamación . En estos delitos, el objeto material que es la persona afectada .coincide con el sujeto pasivo del delito .

Cuando el daño recae directamente en una cosa el objeto material será la cosa afectada. Así, según la disposición penal puede tratarse de un bien mueble o inmueble , derechos , etc. por ejemplo en el robo la cosa mueble ajena es el objeto material en el despojo lo son el inmueble , las aguas o los derechos reales y en el daño en

propiedad ajena lo son el inmueble , los muebles indistintamente.

El cuadro No. 1 muestra dos ejemplos para poder diferenciar entre el objeto jurídico y el objeto material.

DELITO	OBJETO MATERIAL	OBJETO JURIDICO
Homicidio	Persona física	La vida
Robo	Cosa mueble ajena	El patrimonio

Cuadro No . 1

1.3.3 FORMAS DE MANIFESTACION.

En este tema , se analizaran las formas en que puede ocurrir el delito es decir ; los casos en los cuales surgen varios resultados típicos , de manera que se presenta el problema de determinar si se produjeron varios delitos o si uno absorbe a otros .

En la práctica, dicho aspecto es muy importante por que de su conocimiento adecuado se podrá resolver cuando un delito subsiste solo aisladamente y cuando hay acumulación o absorción. También se estudiará la vida o desarrollo del delito.

Concurso:
El concurso es el modo en que puede aparecer el delito en relación con la conducta y el resultado.

En principio una conducta produce un solo resultado pero hay dos casos en los cuales se presentan dos figuras que hacen ubicarse en el concurso de delitos :

Concurso ideal o formal ,ocurre cuando con una sola conducta se producen varios resultados típicos delitos en cuyo caso se dice que existe unidad de acción y pluralidad de resultados .

CONCURSO IDEAL O FORMAL

	LESIONES
UNA CONDUCTA	HOMICIDIOS
	DAÑO EN PROPIEDAD

Cuadro No. 2

Concurso real o material. se presenta cuando con varias conductas se producen diversos resultados. Aquí existe pluralidad de conductas y pluralidad de resultados.

CONCURSO REAL O MATERIAL

PRIMERA CONDUCTA	DAÑO EN PROPIEDAD AJENA
SEGUNDA CONDUCTA	ROBO
TERCERA CONDUCTA	LESIONES

Cuadro No.3

Su fundamento legal lo encontramos en el Código Penal vigente para el Distrito Federal que a la letra dice:

Articulo 28. (Concurso ideal y real de delito). Hay concurso ideal, cuando con una sola acción o una sola omisión se cometen varios delitos.

Hay concurso real, cuando con pluralidad de acciones u omisiones se cometen varios delitos.

No hay concurso cuando las conductas constituyan un delito continuado.

En caso de concurso de delitos se estará a lo dispuesto en el artículo 79 de este Código.

Articulo 79 .(Aplicación de la sanción en el caso de concurso de Delitos)En caso de concurso Ideal se impondrán las sanciones correspondientes al delito que merezca la mayor penalidad , las cuales podrán aumentarse hasta en una mitad mas del máximo de duración de las penas correspondientes de los delitos restantes ,si las sanciones aplicables son de la misma naturaleza podrán imponerse las penas correspondientes a los restantes delitos .En ningún caso podrán exceder de las máximos señalados en el Titulo Tercero del Libro Primero de este Código.

En caso de concurso real se impondrá la pena del delito que merezca la mayor , la cual podrá aumentarse con las penas que la ley contempla para cada uno de los delitos restantes sin que exceda del máximo señalado en el articulo 33 de este Código,no menor de tres meses ni mayor de cincuenta años .

Desarrollo del Delito (Iter Criminis).

El delito tiene un desarrollo , la fase interna que comprende la idea criminal ,la deliberación que consiste en el rechazo o aceptación y por ultimo la decisión de delinquir , y otra externa en donde la manifestación de delinquir no es castigada, la preparación son los actos que realiza el sujeto con el propósito de delinquir que por si mismos pueden constituir un delito por ultimo la ejecución actos que dan origen propiamente al delito.

La Tentativa es un grado de ejecución que queda incompleta por causas no propias al agente y toda vez que denota la intención delictuosa, se castiga y al respecto se ha establecido en el Código Penal vigente para el Distrito Federal.

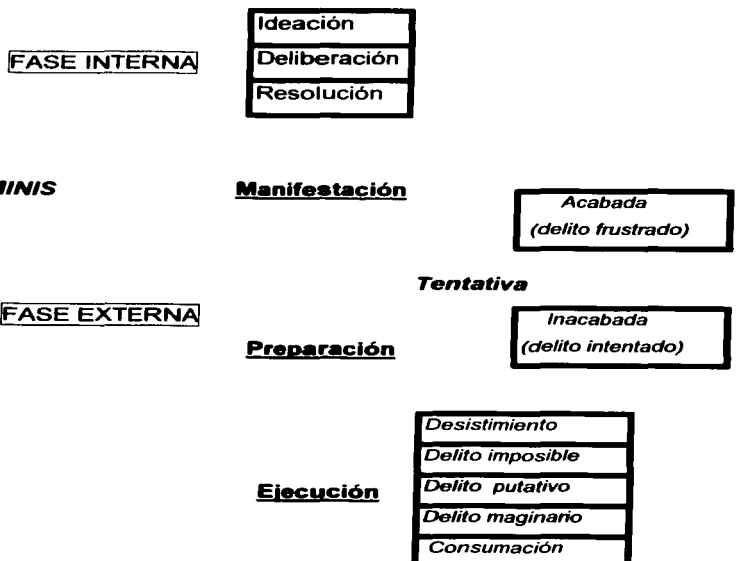
Articulo 20 (Tentativa punible). Existe tentativa punible, cuando la resolución de cometer un delito se exterioriza realizando, en parte o totalmente, los actos ejecutivos que deberían producir el resultado, u omitiendo los que deberían evitarlo, si por causas ajenas a la voluntad del sujeto activo no se llega a la consumación, pero se pone en peligro el bien jurídico tutelado.

No todos los delitos admiten la posibilidad de integrar la tentativa existen otras figuras que se relacionan con el tema :

Articulo 21 (Desistimiento y arrepentimiento). Si el sujeto desiste espontáneamente de la ejecución o impide la consumación del delito,

no se le impondrá pena o medida de seguridad alguna por lo que a éste se refiere, a no ser que los actos ejecutados constituyan por sí mismos algún delito diferente, en cuyo caso se le impondrá la pena o medida señalada para éste.

DESARROLLO DEL DELITO



CUADRO No 4

1.3.4 ELEMENTOS DEL DELITO.

Los diferentes estudiosos del tema no han llegado aun acuerdo sobre los elementos del delito pues para unos este es indivisible, (Corriente unitaria) y para otros , se constituye por varios elementos (Corriente atomizadora).

Raúl Carranca y Trujillo son solo dos de varios autores que concuerdan con el numero de elementos del delito y lo define como *"el acto o típicamente antijurídica ,culpable ,sometido a veces a condiciones objetivas de penalidad , imputable a un hombre y sometido a una sanción penal ."*[16]

Fernando Castellanos considera que la imputabilidad es un presupuesto de la culpabilidad , la punibilidad es considerada como componente de la norma mientras que las condiciones objetivas de punibilidad no son elemento esencial del delito puesto que son exigidas por el legislador y solo la conducta, la tipicidad, la antijuricidad y la culpabilidad con imputabilidad como presupuesto necesario son elementos esenciales del delito .

El cuadro No. 5 nos muestra los 7 elementos de la teoría heptatomica. *"La teoría Heptatomica sostiene la existencia de siete elementos conducta o hecho, tipicidad, antijuricidad, imputabilidad, culpabilidad, punibilidad y condiciones objetivas de punibilidad."*[17]

[16] CARRANCA Y TRUJILLO, Raúl,Op.cit.15ª ed, p223.
[17] GARCÍA RAMÍREZ, Sergio .DERECHO PENAL .Editorial Mc Graw Hill .México1998 p59

ELEMENTOS DEL DELITO

Positivos	Negativos
a) Conducta	a)Ausencia de conducta.
b) Tipicidad	b)Ausencia de tipo o atipicidad.
c) Antijuricidad	c)Causas de justificación.
d) Imputabilidad	d)Inimputabilidad.
e) Culpabilidad	e)Inculpabilidad
f) Punibilidad	f) Excusas absolutorias
g) Condicionalidad objetiva	g) Falta de condiciones objetivas

Cuadro No. 5

La Conducta.

La conducta es el primer elemento básico del delito, y se define como el comportamiento humano voluntario, positivo o negativo, encaminado a un propósito delictuoso. Lo que significa que sólo los seres humanos pueden cometer conductas positivas o negativas, ya sea una actividad o inactividad respectivamente. Es voluntario dicho comportamiento porque es decisión libre del sujeto y es encaminado a un propósito porque tiene una finalidad al realizarse la acción u omisión. La conducta puede ser de acción o de omisión y esta última se subdivide en omisión simple y comisión por omisión.

La conducta tiene tres elementos:

1) Un acto positivo o negativo (acción u omisión)

2) Un resultado.

3) Una relación de causalidad entre el acto y el resultado

La palabra acción proviene de la voz latina "actio" que significa movimiento.
El acto, es el comportamiento humano positivo o negativo que produce un resultado. Positivo será una acción, que consiste en una actividad, en un hacer; mientras la omisión es una inactividad, es cuando la ley espera una conducta de un individuo y éste deja de hacerla.

El Delito de Acción es aquella actividad que realiza el sujeto, produciendo consecuencias en el mundo jurídico, en dicha acción debe de darse un movimiento por parte del sujeto, de esta manera, la conducta de acción tiene cuatro elementos:
a) voluntad
b) actividad
b) Resultado;
c) Nexo de causalidad

Cuando se comete un delito de acción se esta haciendo lo prohibido , es decir , lo que la ley ordena que no se haga por lo tanto , se viola una ley prohibitiva aqui el sujeto activo quiere que suceda un resultado por lo tanto encamina su acción a que este se produzca , de esto se desprende los elementos de la acción

El Delito de omisión es la inactividad voluntaria cuando existe el deber jurídico de obrar.

La omisión tiene cuatro elementos:
a) Manifestación de la voluntad
b) Una conducta pasiva.(inactividad)
c) Deber jurídico de obrar
d) Resultado típico jurídico

Estos delitos se clasifican en:

Delitos de Omisión simple o propios consisten en hacer lo que no se puede hacer , imprudencialmente con lo cual se produce un delito aunque no haya un resultado de modo que se infringe una norma preceptiva (portación de arma prohibida).

Delitos de Comisión por Omisión o impropios, es un no hacer imprudencialmente cuya abstención produce un resultado material y se infringe una norma preceptiva y otra prohibitiva , (abandono de la obligación de alimentar a los hijos con la que se causa la muerte de estos).

Su fundamento lo encontramos en el Código Penal Vigente.
Articulo 16 (Omisión impropia o comisión por omisión). En los delitos de resultado material será atribuible el resultado típico producido a quien omita impedirlo, si éste tenia el deber jurídico de evitarlo, si:

I . Es garante del bien jurídico;
II . De acuerdo con las circunstancias podía evitarlo; y

III . Su inactividad es, en su eficacia, equivalente a la actividad prohibida en el tipo.

Es garante del bien jurídico el que:
a). Aceptó efectivamente su custodia;
b). Voluntariamente formaba parte de una comunidad que afronta peligros de la naturaleza;
c). Con una actividad precedente, culposa o fortuita, generó el peligro para el bien jurídico;
d). Se halla en una efectiva y concreta posición de custodia de la vida, la salud o integridad corporal de algún miembro de su familia o de su pupilo.

"Hay diversas clasificaciones del delito en orden a la conducta otra clasificación relevante puntualizada en la reforma de 1983 , distingue entre el delito instantáneo , permanente o continuo y continuado . Esta distinción tiene efectos en diversos campos: aplicación de la ley mexicana, competencia territorial imposición de la pena prescripción ."[18]

Articulo 17 del Código Penal del Distrito Federal (Delito instantáneo, permanente o continuo y continuado). El delito, atendiendo a su momento de consumación, puede ser:
I. Instantáneo: cuando la consumación se agota en el mismo momento en que se han realizado todos los elementos de la descripción legal;

[18] Ibid . p. 59

II. Permanente o continuo: cuando se viola el mismo precepto legal, y la consumación se prolonga en el tiempo; y
III. Continuado: cuando con unidad de propósito delictivo, pluralidad de conductas e identidad de sujeto pasivo, se concretan los elementos de un mismo tipo penal.

La Ausencia de Conducta.

Cuando la conducta no existe da lugar a la inexistencia del delito y estos podrian ser supuestos.

Vis Absoluta: Es quien comete un delito forzado físicamente a ello, no es su conducta la que impera ,sino de quien lo ha obligado, convirtiéndose así en un instrumento de quien emplea la vis absoluta por lo tanto aquí opera la hipótesis "nullum crime sine actione."

Vis mayor: Aunque esta no se encuentra contemplado contemplada en la legislación penal, si se comete un delito bajo estas circunstancias , quien lo realiza no tuvo deseo de hacerlo es decir falto la voluntad elemento necesario de la conducta humana , sino que fue empujado por fuerza de la naturaleza.

Movimientos. Reflejos : Estos son movimientos corporales involuntarios , o sea que el hombre no puede controlar pero en caso de esto sea factible , existiría la voluntad del sujeto y , por lo tanto, conducta , elemento esencial del delito.

Ahora bien, el aspecto negativo de la conducta es la ausencia de conducta, la cual abarca la ausencia de acción o de omisión de la misma, en la realización de un ilícito. Nuestra legislación Mexicana, en el artículo 29 del Código Penal vigente, en su fracción primera, determina como causa de exclusión del delito cuando : "La actividad o la inactividad se realice sin intervención de la voluntad del agente".

La Tipicidad.

La tipicidad es la adecuación de la conducta al tipo penal. La acción típica es sólo aquella que se acomoda a la descripción objetiva, aunque saturada a veces de referencia a elementos normativos y subjetivos del injusto de una conducta que generalmente se reputa delictuosa, por violar, en la generalidad de los casos, un precepto, una norma, penalmente protegida.

El tipo es la descripción legal de un delito o bien la abstracción plasmada en la ley de la figura delictiva suele hablarse indistintamente de tipo , figura típica ,ilícito penal conducta típica y cualquier otra idea similar .

Se debe tener cuidado de no confundir la tipicidad con tipo, la primera se refiere a la conducta, y el segundo pertenece a la ley, a la descripción o hipótesis plasmada por el legislador sobre un hecho ilícito, es la fórmula legal a la que se debe adecuar la conducta para la existencia de un delito.

La tipicidad se encuentra fundamentada en el artículo 14 Constitucional, párrafo tercero, que a la letra dice: "En los juicios de orden criminal, queda prohibido imponer, por simple analogía y aún por mayoría de razón, pena alguna que no esté decretada por una ley exactamente aplicable al delito de que se trata"

Y en el articulo 2 del Código Penal Vigente (Principio de tipicidad y prohibición de la aplicación retroactiva, analógica y por mayoría de razón). No podrá imponerse pena o medida de seguridad, si no se acredita la existencia de los elementos de la descripción legal del delito de que se trate. Queda prohibida la aplicación retroactiva, analógica o por mayoría de razón, de la ley penal en perjuicio de persona alguna.

La ley penal sólo tendrá efecto retroactivo si favorece al inculpado, cualquiera que sea la etapa del procedimiento, incluyendo la ejecución de la sanción. En caso de duda, se aplicará la ley más favorable.
La tipicidad se encuentra apoyada en el sistema jurídico mexicano por diversos principios supremos que constituyen una garantía de legalidad como lo muestra el cuadro No. 6

Nullum crimens inelege	no hay delito sin ley
Nullum crimen sine tipo	no hay delito sin tipo
Nullum poena sien tipo	no hay pena sin tipo
Nulla poena sine crimen	no hay pena sin delito
Nulla poena sine lege	no hay pena sin ley

Cuadro No.6

Aspecto Negativo: Atipicidad.

"El aspecto negativo de la tipicidad es la ***atipicidad*** *es la no adecuación de la conducta al tipo penal por lo cual da lugar a la no existencia del delito la conducta del agente no se adecua al tipo por faltar algunos de los requisitos o elementos que el tipo exige y que puede ser respecto de los medios de ejecución , el objeto material , las peculiaridades del sujeto pasivo o activo."*[19]

La atipicidad es la falta de alguno de los elementos que integran la descripción legal del delito de que se trate su fundamento lo encontramos en el articulo 29 Fracción II del Código Penal Vigente.

Es importante diferenciar la atipicidad de la falta de tipo, siendo que en el segundo caso, no existe descripción de la conducta o hecho, en la norma penal .

La Antijuricidad.

La antijurídica o ilicitud significa contradicción entre el comportamiento y la norma es decir "disvalor" de la conducta frente a la cultura en medio y una época determinados.
Existe , pues , una cultura con sus componentes éticos - que exige cierta conducta , la valora como plausible y rechaza otra la califica de ilícita , injusta ,delictiva.

[19] Amuchategui Requena, Irma.**PRIMER Y SEGUNDO CURSO DE DERECHO PENAL.** Editorial Harla, México1994, p.64.

La antijurídica la podemos considerar como un elemento positivo del delito, es decir, cuando una conducta es antijurídica, es considerada como delito. Para que la conducta de un ser humano sea delictiva, debe contravenir las normas penales, es decir, ha de ser antijurídica.
El Código Penal para el Distrito Federal en su artículo 4 menciona el Principio del bien jurídico y de la antijuridicidad material. Para que la acción o la omisión sean consideradas delictivas, se requiere que lesionen o pongan en peligro, sin causa justa, al bien jurídico tutelado por la ley penal.

La antijurídica es lo contrario a Derecho, por lo tanto, no basta que la conducta encuadre en el tipo penal, se necesita que esta conducta sea antijurídica, considerando como tal, a toda aquella definida por la ley, no protegida por causas de justificación, establecidas de manera expresa en la misma.

Causas de Justificación.

El aspecto negativo de la antijuricidad lo constituye las causas de justificación que son las razones o circunstancias que el legislador considero para anular la antijuricidad de la conducta típica realizada al considerarla licita jurídica o justificativa.

La causa de justificación, es cuando es un hecho presumiblemente delictuoso si falta el elemento de antijuricidad, podemos decir: no hay delito, por la existencia de una causa de justificación, es decir, el individuo ha actuado en determinada forma sin el ánimo de transgredir

las normas penales, Así, si un hombre ha matado a otro, en defensa de su vida injustamente atacada, estará en una causa de justificación, excluyéndose la antijurídica en la conducta del homicida.

La Legislación Mexicana en el Código Penal para el Distrito Federal contempla las siguientes:

Articulo .- 29 (Causas de exclusión). El delito se excluye cuando:
I.- .....
II.- .....
III.(Consentimiento del Titular). Se actúe con el consentimiento del titular del bien jurídico afectado, o del legitimado legalmente para otorgarlo, siempre y cuando se cumplan los siguientes requisitos:
Que se trate de un bien jurídico disponible;
Que el titular del bien jurídico, o quien esté legitimado para consentir, tenga la capacidad jurídica para disponer libremente del bien; y
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 a quien esté legitimado para consentir, éstos hubiesen otorgado el consentimiento.

IV. (Legítima Defensa). Se repela 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 defensor.

Se presume que existe legítima defensa, salvo prueba en contrario, cuando se cause un daño a quien por cualquier medio trate de penetrar o penetre, sin derecho, al lugar en que habite de forma temporal o permanente el que se defiende, al de su familia o al de cualquier persona respecto de las que el agente tenga la obligación de defender, a sus dependencias o al sitio donde se encuentren bienes propios o ajenos respecto de los que exista la misma obligación.

Igual presunción existirá cuando el daño se cause a un intruso al momento de sorprenderlo en alguno de los lugares antes citados en circunstancias tales que revelen la posibilidad de una agresión.

Carranca y Trujillo define a la legitima defensa como *"la repulsa de una agresión antijurídica y actual por el atacado o por terceras personas contra el agresor sin traspasar la medida necesaria para la protección."*[20]

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, siempre que el peligro no sea evitable por otros medios y el agente no tuviere el deber jurídico de afrontarlo;

---

[20] CARRANCA Y TRUJILLO, Raul Op.cit.,p.531

VI. (Cumplimiento de un Deber o Ejercicio de un Derecho). La acción o la omisión se realicen 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;

VII.- .....
VIII.- .....
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 conducir conforme a derecho.
Las causas de exclusión del delito se resolverán de oficio, en cualquier estado del proceso.

Imputabilidad.

La imputabilidad es la capacidad de querer y entender, en el campo del Derecho Penal. Querer es estar en condiciones de aceptar o realizar algo voluntariamente y entender es tener la capacidad mental y la edad biológica para desplegar esa decisión.

"Es la posibilidad condicionada por la salud mental y por el desarrollo del autor para obrar según el justo reconocimiento del deber existente podemos entender que es la capacidad de entender y de querer en el campo del derecho."[21]

[21] CASTELLANOS TENA. Fernando , Op. cit.,p.218.

Inimputabilidad.

El aspecto negativo de la imputabilidad es la inimputabilidad, consistente en la incapacidad de querer y entender en el mundo del Derecho. Son 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.

Concretamente pude decirse que las causas de inimputabilidad son las siguientes:
-Trastorno Mental.
-Desarrollo Intelectual Retardado.
-Miedo Grave .
-Minoría de Edad.

El Código Penal para el Distrito Federal en su artículo 29 señala:
I.- .....
II.- .....
III.- .....
IV.- .....
V.- .....
VI.- .....
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.
Cuando la capacidad a que se refiere el párrafo anterior se encuentre considerablemente disminuida, se estará a lo dispuesto en el artículo 65 de este Código. (Tratamiento para inimputables disminuidos).

Culpabilidad

La culpabilidad es el elemento subjetivo del delito y el eslabón que asocia lo material del acontecimiento típico y antijurídico con la subjetividad del autor de la conducta.

El Código Penal Vigente para el Distrito Federal a la letra dice:

Articulo 5 (Principio de culpabilidad). No podrá aplicarse pena alguna, si la acción o la omisión no han sido realizadas culpablemente. La medida de la pena estará en relación directa con el grado de culpabilidad del sujeto respecto del hecho cometido, así como de la gravedad de éste.

Igualmente se requerirá la acreditación de la culpabilidad del sujeto para la aplicación de una medida de seguridad, si ésta se impone accesoriamente a la pena, y su duración estará en relación directa con el grado de aquélla. Para la imposición de las otras medidas penales será necesaria la existencia, al menos, de un hecho antijurídico, siempre que de acuerdo con las condiciones personales del autor,

hubiera necesidad de su aplicación en atención a los fines de prevención del delito que con aquéllas pudieran alcanzarse.

Grados y tipos de culpabilidad.

Dolo y culpa.
Articulo 18 Código Penal del Distrito Federal. (Dolo y Culpa). Las acciones u omisiones delictivas solamente pueden realizarse dolosa o culposamente.

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.

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

Dolo.
"El dolo consiste en causar intencionalmente el resultado típico con conocimiento y conciencia de la antijuridica del hecho. La doctrina le llama delito intencional o doloso, los elementos del dolo son dos, ético que consiste en saber que se infringe la norma y la voluntad de realizar la conducta antijuridica"[22]

[22] AMUCHATEGUI REQUENA ,Irma G .Op. cit . p.83.

El dolo fundamentalmente sera directo, indirecto o eventual, genérico especifico e indeterminado.

Directo.

El sujeto activo tiene intención de causar un daño determinado y lo hace, de manera que existe identidad entre la intención y el resultado típico por ejemplo. El agente desea violar y lo hace.

Indirecto o eventual.

El sujeto desea un resultado típico a sabiendas de que hay posibilidades de que surjan otros diferentes, por ejemplo, alguien quiere lesionar a un comensal determinado para lo cual coloca una sustancia venenosa en la sal de mesa al saber que podrían salir lesionados otros sujetos.

Genérico.

Es la intención de causar un daño o afectación o sea la voluntad consciente encaminada a producir el delito.

Específico.

Es la intención de causar un daño con una especialidad que la voluntad que la propia norma exige en cada caso de modo que deberá ser objeto de prueba.

Indeterminado.

Consiste en la intención de delinquir de manera imprescindible, sin que el agente desee causar un delito determinado por ejemplo, colocar una bomba para protestar el sujeto sabe que causara uno o

mas daños , pero no tiene la intención de infringir uno en especial.
El dolo es un proceso psicológico que se traduce en la intención de querer un resultado típico.

Culpa
La culpa es el segundo grado de culpabilidad y ocurre cuando se causa un resultado típico sin intención de producirlo .
Obra culposamente el que produce el resultado típico, que no previó siendo previsible o previó confiando en que no se produciría, en virtud de la violación de un deber de cuidado que objetivamente era necesario observar.

El Lic. Tena Castellanos defina la culpabilidad como el "*nexo intelectual y emocional que liga al sujeto con su acto*"[23]

Inculpabilidad

La inculpabilidad es la ausencia de culpabilidad significa la falta de reprobabilidad ante el derecho penal por faltar la voluntad o el conocimiento del hecho .esto tiene una relación con la imputabilida; así no puede ser culpable de un delito quien no es imputable.

Las causas de inculpabilidad son las circunstancias que anulan la voluntad o el conocimiento a saber.
El Error el conocimiento deformado o Falsa concepción de la realidad.

---

[23] CASTELLANOS TENA ,Fernando. Op. cit. P.234.

a)Error esencial de hecho invencible existe cuando no hay culpabilidad Este error constituye una causa de inculpabilidad.

b) Eximentes putativas

Son los casos en que el agente cree ciertamente por error esencial de hecho que esta amparado por una circunstancia justificativa. porque se trata de un comportamiento ilícito. Como la legitima defensa, el estado de necesidad cumplimiento de un deber, ejercicio de un derecho u obediencia jerarquiza en todos los caso de forma putativa putativo.

c) No Exigibilidad de Otra Conducta

"Es común que entender que el sacrificio de un bien de menor jerarquía en aras de otro superior implica exclusión de licitud, Si la colisión ocurre entre bienes de igual jerarquía quien sacrifica el ajeno se ampara en una causa de inculpabilidad."[24]

d) Caso Fortuito

No hay delito cuando es causado por mera fortuna sin la intención ni imprudencia alguna , ejecutando un hecho ilícito con todas las precauciones debidas , no hay delito cuando el resultado típico se produce por caso fortuito.

El mero accidente puede provenir de fuerzas de la naturaleza o de fuerzas circunstanciales del hombre.

---

[24] GARCÍA RAMÍREZ, Sergio. Op.cit. p.71.

La Punibilidad

La Punibilidad es un elemento secundario del delito, que consiste en el merecimiento de una pena, en función o por razón de la comisión de un delito; dichas penas se encuentran señaladas en nuestro Código Penal.

Pena es la restricción o privación de derechos que se impone al autor de un delito. Implica un castigo para el delincuente y una protección para la sociedad.

El maestro Cuello Calón, considera que la punibilidad no es más que un elemento de la tipicidad, pues el hecho de estar la acción conminada con una pena, constituye un elemento del tipo delictivo.

Por su parte Ignacio Villalobos, tampoco considera a la punibilidad como elemento del delito, ya que el concepto de éste no concuerda con el de la norma jurídica.

Una acción o una abstención humana son penadas cuando se les califica de delictuosas, pero no adquieren este carácter porque se les sancione penalmente.

Las conductas se revisten de delictuosidad por su pugna con aquellas exigencias establecidas por el Estado para la creación y conservación del orden y por ejecutarse culpablemente. Mas no se pueden tildar como delitos por ser punibles.

Variación de la Pena.
Existen tres variantes que modifican la penalidad arbitrio judicial, margen señalado por la ley en cada norma que establece una pena al considerar que esta tiene un margen de acuerdo con un mínimo y máximo y el juez podrá imponer la mas justa artículo .Para ello tendrá en cuenta lo establecido en los artículos 71 y 72 del Código Penal Vigente.

Circunstancias Atenuantes o Privilegiadas.
Son las consideraciones que tiene el legislador para determinados casos , la pena correspondiente a un delito se puedan disminuir .

Circunstancias Agravantes.
Son las consideraciones del legislador contenidas en la ley para modificar la pena y agravarla por ejemplo homicidio con premeditación alevosía y ventaja o traición.

Dichas variantes obedecen a las circunstancias o factores que la propia ley tiene en cuenta para variar la pena , con lo cual trata que la pena se ajuste al caso concreto de acuerdo con sus circunstancias especiales y de modo que la pena sea mas justa .

Excusas absolutorias

El Aspecto Negativo de la punibilidad se llama excusa absolutoria lo que significa que un acto típico , antijurídico , imputable a un autor

y culpable, no se asocie pena alguna por razones de utilidad pública.

Las excusas absolutorias son circunstancias específicamente señaladas en la ley y por las cuales no se sanciona al agente. Así como la punibilidad no es considerada por muchos autores de elementos del delito, así tampoco la imputabilidad como se mencionó en el capítulo anterior.

" En estado de necesidad: robo famelico , aborto terapéutico.
** Por temibilidad mínima: robo por arrepentimiento poca peligrosidad.*
** Por ejercicio de un derecho: aborto producto de una violación*
**Por imprudencia: aborto por imprudencia de la mujer embarazada*
**Por no exigibilidad de otra conducta: encubrimiento de parientes*
**Por innecesariedad de la pena: cuando el sujeto activo sufrió consecuencias graves que hacen irracional la pena"*[25]

Condiciones Objetivas de Punibilidad .

La condicionalidad objetiva esta constituida por requisitos que la ley señala eventualmente para que se pueda perseguir el delito algunos autores dicen que son requisitos de procedibilidad o perseguibilidad mientras que para otros son simples circunstancias o hechos adicionales o exigibles .

[25] Amuchategui Requena, Irma G. Op.cit. p.92

Jiménez de Asúa "*afirma que son Condiciones Objetivas de Punibilidad son presupuestos procesales a los que a menudo se subordinan la persecución de ciertas figuras del delito .*"[26]
En realidad las condiciones objetivas son elementos del tipo a veces tienen que ver con la intencionalidad del sujeto , otras con aspectos referentes a la perseguibilidad.

Para que ala circunstancia atenuante contemplada en el Art. 310 del Código Penal vigente opere en beneficio del cónyuge ofendido por infidelidad conyugal se requiere que el no haya contribuido a la corrupción de su cónyuge

Falta de Condicionalidad Objetiva.

La ausencia objetiva de punibilidad , la carencia de ellas hace que el delito no se castigue.

[26] Jiménez de Asua, Luis. Op.cit. p .425

CAPITULO II. DELITOS INFORMATICOS

2.1 ANTECEDENTES DE LA INFORMATICA

Las tecnologías de la información, actualmente son elementos fundamentales para la superación y desarrollo de un país. Por eso, los países desarrollados basan su crecimiento en la aplicación y la programación estratégica de las herramientas computacionales y han definido políticas que los inducirán a su permanencia mundial de los próximos años.

Ante el nuevo entorno económico mundial los países emergentes están obligados a preparar profesionales en áreas de la informática y las telecomunicaciones, capaces de enfrentar los retos que se tienen hoy en día. Así mismo, la presencia de la computación en los sectores productivos es un factor determinante para su funcionamiento.

En tal sentido, las instituciones educativas deberán aportar a la sociedad recursos humanos que formen la estructura sólida en informática, acorde con los países del primer mundo, sobre la que crecerá la economía nacional.

La Informática es tan popular que es muy difícil que una empresa adquiera una ventaja competitiva por tener computadoras potentes o una red más extensa. La ventaja competitiva se logra con el uso eficiente de la tecnología, optimizando la gestión de la empresa.

Es una ciencia.
El concepto de información es muy reciente y además sumamente sencillo. Fue desarrollado en la década de los 40's por el matemático norteamericano Claude Shannon, para referirse a todo aquello que está presente en un mensaje o señal cuando se establece un proceso de comunicación entre un emisor y un receptor.

Así, cuando dos personas hablan, intercambian información; cuando ves una película, recibes información; es más, al probar una galleta tu sentido del gusto recaba información sobre el sabor y la consistencia del bocado. La información puede entonces encontrarse y enviarse en muchas formas, a condición de que quien la reciba pueda interpretarla.

Procesar información implica el almacenamiento, la organización y, muy importante, la transmisión de la misma. Para ello, en la informática intervienen varias tecnologías; en términos generales, podemos decir que son dos sus pilares: la computación y la comunicación.

Es decir, en lo que hoy conocemos como informática confluyen muchas de las técnicas y de las máquinas que el hombre ha desarrollado a lo largo de la historia para apoyar y potenciar sus capacidades de memoria, de pensamiento y de comunicación

El origen de las máquinas de calcular está dado por El Ábaco Chino, éste era una tablilla dividida en columnas en la cual la primera,

contando desde la derecha, correspondía a las unidades, la siguiente a la de las decenas, y así sucesivamente. A través de movimientos se podía realizar operaciones de adición y sustracción.

Otro de los hechos importantes en la evolución de la informática lo situamos en el siglo XVII, donde el científico francés Blas Pascual inventó una máquina calculadora. Ésta sólo servía para hacer sumas y restas, pero este dispositivo sirvió como base para que el alemán Leibnitz, en el siglo XVIII, desarrollara una máquina que, además de realizar operaciones de adición y sustracción, podía efectuar operaciones de producto y cociente.

Jacquard fue el primero en emplear tarjetas perforadas para almacenar la información sobre el dibujo del tejido y además controlar la máquina de tejer de Jaquard presentada en 1801 supuso gran éxito comercial y un gran avance en la industria textil.

Ya en el siglo XIX se comercializaron las primeras máquinas de calcular. En este siglo el matemático inglés Babbage desarrolló lo que se llamó "Máquina Analítica", la cual podía realizar cualquier operación matemática. Además disponía de una memoria que podía almacenar 1000 números de 50 cifras y hasta podía usar funciones auxiliares, sin embargo seguía teniendo la limitación de ser mecánica.

Otro inventor digno de mención es Herman Hollerith. A los 19 años. en 1879 fue contratado como asistente en las oficinas del censo norteamericano que por aquel entonces se disponía a realizar el

recuento de la población para el censo de 1880. Este tardó 7 años y medio en completarse manualmente.

El sistema inventado por Hollerith utilizaba tarjetas perforadas en las que mediante agujeros se representaba el sexo la edad raza etc.
Ante las posibilidades comerciales de su máquina Hollerith dejó las oficinas del censo en 1896 para fundar su propia Compañía la Tabulating Machine Company.

En 1900 había desarrollado una máquina que podía clasificar 300 tarjetas por minuto una perforadora de tarjetas y una máquina de cómputo semiautomática.

En 1924 Hollerith fusionó su compañía con otras dos para formar la Internacional Bussines Machines hoy mundialmente conocida como IBM .

En el primer tercio del siglo XX, con el desarrollo de la electrónica, se empiezan a solucionar los problemas técnicos que acarreaban estas máquinas, reemplazándose los sistemas de engranaje y varillas por impulsos eléctricos, estableciéndose que cuando hay un paso de corriente eléctrica será representado con un "1" y cuando no haya un paso de corriente eléctrica se representaría con un "0" .

Con el desarrollo de la segunda guerra mundial se construye el primer ordenador, el cual fue llamado Mark I y su funcionamiento se basaba en interruptores mecánicos.

"En 1951 son desarrollados el Univac I y el Univac II con memoria de núcleos magnéticos lo que le haría claramente superior a su antecesor pero por diversos problemas esta máquina no vio la luz hasta 1957 fecha en la que había perdido su liderazgo en el mercado frente al 705 de IBM."[27]
(se puede decir que es el punto de partida; en el surgimiento de los verdaderos ordenadores, que serán de acceso común a la gente).

Generaciones:

1ra.- Generación: se desarrolla entre 1940 y 1952. Es la época de los ordenadores que funcionaban a válvulas y el uso era exclusivo para el ámbito científico/militar. Para poder programarlos había que modificar directamente los valores de los circuitos de las máquinas.

2da.- Generación: va desde 1952 a 1964. Ésta surge cuando se sustituye la válvula por el transistor. En esta generación aparecen los primeros ordenadores comerciales, los cuales ya tenían una programación previa que serían los sistemas operativos. Éstos interpretaban instrucciones en lenguaje de programación (Cobol, Fortran), de esta manera, el programador escribía sus programas en esos lenguajes y el ordenador era capaz de traducirlo al lenguaje máquina además de la reducción del tamaño por los transistores que son mucho mas péquenos que los tubos de vacío.

---

[27] DE LA CALLE, Eduardo. **INTRODUCCIÓN A LA INFORMÁTICA**. Editorial Iberoamericana. España 1993. pp 28,29.

3ra.- Generación: se dio entre 1964 y 1971. Es la generación en la cual se comienzan a utilizar los circuitos integrados; Estos elementos son unas plaquitas de silicio llamadas chips sobre cuya superficie se depositan por medios especiales unas impurezas que hacen las funciones de diversos componentes electrónicos.

Así pues un puñado de transistores y otros componentes se integran ahora en una plaquita de silicio. Aparentemente esto no tiene nada de especial salvo por un detalle; un circuito integrado con varios centenares de componentes integrados tiene el tamaño de una moneda. esto permitió por un lado abaratar costos y por el otro aumentar la capacidad de procesamiento

4ta.- Generación: se desarrolla entre los años 1971 y 1981. Esta fase de evolución se caracterizó por la integración de los componentes electrónicos, y esto dio lugar a la aparición del microprocesador, que es la integración de todos los elementos básicos del ordenador en un sólo circuito integrado.

Aparecen innumerables lenguajes de programación. Las capacidades de memoria empiezan a ser enormemente grandes. En esta etapa cobran gran auge los mini computadoras. Estos son maquinas con un procesador de 16 bits una memoria de entre 16 32 KB y un precio de unos pocos millones.

5ta.- Generación: va desde 1981 hasta nuestros días (aunque ciertos expertos consideran finalizada esta generación con la aparición de los

procesadores Pentium, consideraremos que aun no ha finalizado) Esta quinta generación se caracteriza por el surtimiento de la PC, tal como se la conoce actualmente

Se caracteriza por una serie de tendencias y avances en todos los campos de la informática como son:

"Avances en inteligencia artificial, lenguajes de quinta generación o natural, Interconexión entre todo tipo de computadora y equipos informáticos mediante redes de transmisión (redes integradas) Integración de datos imágenes y voz (entornos-multimedia), existencia y de dos tipos de maquinas supercomputadoras de altísima velocidad y computadoras de funciones inteligentes."[28]

2.2 DESARROLLO MUNDIAL EN INTERNET

Desde los tiempos más remotos el ser humano ha buscado la mejor forma de comunicarse con otros de su misma especie, aun cuando éstos se encuentren en lugares lejanos. La historia de la comunicación está marcada por los adelantos tecnológicos de cada época y lugar.

En un principio, la comunicación que se establecía con otros pueblos lejanos era mediante la voz, viajeros que recorrían grandes distancias con la finalidad de llevar y traer mensajes e información. Con la

[28] UREÑA LÓPEZ ,L Alfonso. **FUNDAMENTOS DE INFORMÁTICA** . Editorial Alfa Homega, Madrid 1999, p 300

aparición de la escritura se inicia una nueva era, sin embargo los mensajes seguían siendo enviados de igual manera, era un proceso lento y difícil.

"Técnicamente se puede definir Internet de la siguiente forma en una red formada por la interconexión cooperativa de redes de ordenadores , Internet es una red de redes y deriva de las palabras inglesas interconexión y network esto es interconexión y red .Lo que da como resultado que Internet sea miles de interconexiones conectadas entre si."[29]

Con el inicio de la era tecnológica, se dispuso de un medio con el cual fue posible establecer una comunicación a distancia y casi instantánea por medio de códigos y claves de sonido: el telégrafo; posteriormente la comunicación humana se vio beneficiada con la invención del teléfono permitiendo el uso de la voz, más adelante vino la radio, la televisión y con ello las computadoras.

Estos grandes inventos son la base de los adelantos tecnológicos que disfrutamos hoy en día en cuanto a comunicación, desde el envío y recepción de un fax hasta la comunicación instantánea en cualquier lugar del mundo por medio de Internet.

Internet es hoy en día una infraestructura informática extendida ampliamente, su influencia alcanza no sólo al campo técnico de las

[29] LOZADA PEREA, Carlos. **INTERNET LIBRO DEL NAVEGANTE** .Editorial Ra –Ma , Madrid 2000, p. 5

comunicaciones entre computadoras (redes), también a toda la sociedad en la medida en que su empleo se incrementa cada vez más para llevar a cabo procesos como el comercio electrónico, la adquisición de información y la interacción entre la comunidad o comunidades remotas.

La Unión Soviética había lanzado el satélite Sputnick en 1957 se estaban en plena guerra fría y los Estados Unidos querían estar a la cabeza de la tecnología militar .El Departamento de la Defensa de los Estados Unidos considero que la red telefonica era demasiado frágil y mas para una guerra nuclear y es por ello que en :

Los Años sesenta.
La Agencia de Proyectos de Investigación Avanzada (**ARPA**) se inició en el Departamento de Defensa de los Estados Unidos en los últimos años de la década de los cincuenta para investigar los campos de ciencia y tecnología militar.

Paralelamente, entre 1962 y 1964 la **RAND** Corporation publicó artículos escritos por Paul Baran sobre 'Redes de Comunicación Distribuidas".

El objetivo de la propuesta era plantear una red que tuviera la máxima resistencia ante cualquier ataque enemigo. Se suponía que una red de comunicaciones, por si misma, no es fiable debido a que parte de ella podría ser destruida durante un ataque bélico.

Por lo tanto, cada nodo debería mantener la misma importancia que los demás para garantizar que no pudiera ser un punto critico que pudiera dejar la red inactiva o fuera de servicio.

Raran promovió el uso de redes de conmutación de paquetes de datos (Packet Switching Networks) que permitiesen que la información transmitida se dividiese en paquetes del mismo tamaño e importancia y se transmitieran a través de los nodos en los cuales se encontrara la ruta más eficiente para que al llegar a su destino se reagruparan en el orden que tenían previamente.

Los paquetes de información no necesitaban tener ninguna información sobre el ordenador de destino -salvo su dirección- ni sobre el medio de transmisión de la red. La utilidad fundamental de esta idea seria que cada paquete de información encontraría su propio camino independientemente de otros paquetes que constituirían parte del mismo mensaje.

Al llegar al punto de destino. Todos los pequeños paquetes de información serían reagrupados en el orden correcto, el orden en que se encontraban antes de ser separados.

En 1968 el Laboratorio Físico Nacional en Inglaterra estableció la primera red de prueba basada en estos principios. En el mismo año, el primer diseño basado en estos principios de envío de paquetes de información, realizado por Lawrence Roberts, fue presentado en la ARPA. La red se llamó ARPANET.

Al año siguiente, el Departamento de Defensa dio el visto bueno para comenzar la investigación en ARPANET.

A partir de ese momento se puso en marcha un proyecto aún mayor y mas ambicioso en los Estados Unidos e inicio la transformación de la red militar para darle un uso científico en 1969 se instalo en la Universidad de los Ángeles el primer súper ordenador con el fin de construir una red que funcionase según las especificaciones propuestas por la RAND corporation .[30]

Pronto le siguieron otros tres nodos: la Universidad de California en Santa Bárbara, el Instituto de Investigación de Stanford y la Universidad de Utah. Estos sitios constituyeron la red original de cuatro nodos de ARPANET. Los cuatro sitios podían transferir datos en ellos en líneas de alta velocidad para compartir recursos informáticos

En 1969 apareció el primer RFC (Request For Comment). Los RFC's, documentos emitidos Periódicamente, se han convertido en su conjunto en las normas y estándares de Internet. Literalmente, una solicitud para comentario", en su origen eran preguntas formuladas por estudiantes que no sabían qué acción tomar ante la falta de normativas. Es la respuesta a dicha pregunta o la iniciativa de tomar un camino particular ante la falta de orientación. lo que convierte la RFC en norma.

---

[30] LACHERBAUER ,Ingo. **TODO SOBRE INTERNET** . Editorial Boixareu , España 2000, p. 194.

Los años setenta.

El comienzo de la década de los setenta vio el crecimiento de la popularidad del correo electrónico sobre redes de almacenamiento y envío. En 1971, ARPANET había crecido hasta 15 nodos con 23 ordenadores hosts (centrales).

En este momento, los hosts de ARPANET comienzan a utilizar un protocolo de control de redes, pero todavía falta la estandarización. Además, había muy diferentes tipos de hosts, por lo que el progreso en desarrollar los diferentes tipos de interfaces era muy lento.

Para el año de 1971, se contaba con 11 nodos más, y en el año siguiente ya había un total de 40.En ese año se tiene registrado el primer mensaje enviado y recibido por correo electrónico de Ray Tomlinson, pero fue hasta el segundo mensaje de prueba cuando se estableció que todos los mensajes que se enviaran deberían emplear el signo @.

En 1972 Larry Roberts de DARPA decidió que el proyecto necesitaba un empujón. Organizó la presentación de ARPANET en la Conferencia Internacional sobre Comunicaciones por Ordenador.

A partir de esta conferencia, se formó un grupo de trabajo internacional para investigar sobre los protocolos de comunicación que permitirían a ordenadores conectados a la red, comunicarse de una manera transparente a través de la transmisión de paquetes de información.

También en 1972 Bolt, Beranek v Newman (BBN) produjeron una aplicación de correo electrónico que funcionaba en redes distribuidas como ARPANET. El programa fue un gran éxito que permitió a los investigadores coordinarse v colaborar en sus proyectos de investigación y desarrollar las comunicaciones personales.

Las primeras conexiones internacionales se establecieron en la Universidad College London, en Inglaterra. y en el Royal Radar Establishment, en Noruega. junto con los ahora 37 nodos en EE. UU. La expansión en ARPANET era muy fácil debido a su estructura descentralizada.

"En 1974 se estableció el Transmission Control Protocol (TCP), creado por Vinton Cerf y Bob Kahn que luego fue desarrollado hasta convenirse en el Transmission Control Protocol/Internet Protocol (TCP/IP). TCP convierte los mensajes en pequeños paquetes de información que viajan por la red de forma separada hasta llegar a su destino donde vuelven a reagruparse. IP maneja el direccionamiento de los envíos de datos, asegurando que los paquetes de información separados se encaminan por vías separadas a través de diversos nódulos, e incluso a través de múltiples redes con arquitecturas distintas." [31]

En julio de 1975 ARPANET fue transferido por DARPA a la Agencia de Comunicaciones de Defensa.

[31] FREZZE T. Hill. **COMPUTACIÓN BÁSICA.** Editorial M.I.G., Buenos Aires 1994 , pp. 303- 304

El crecimiento de ARPANET hizo necesario algunos órganos de gestión: el Internet Configuration Control Board fue formado por ARPA en 1979. Más tarde se transformó en el Internet Activities Board y en la actualidad es el Internet Architecture Board of the Internet Society.

Los años ochenta.
ARPANET en sí mismo permaneció estrechamente controlado por el Departamentol de Defensa, hasta 1983 cuando su parte estrictamente militar se segmento convirtiéndose en MILNET.

La "European Unix Network" (EuNet), conectado a ARPANET, se creó en 1982 para proporcionar servicios de correo electrónico y servicios Usenet a diversas organizaciones usuarias en los Países Bajos, Dinamarca, Suecia e Inglaterra.

En 1984 el número de servidores conectados a la red había ya superado los 1000. Dado que el software de TCP/IP era de dominio público y la tecnología básica de Internet (como ya se denominaba esta red internacional extendida) era algo anárquica debido a su naturaleza, era difícil evitar que cualquier persona en disposición del necesario hardware (normalmente en universidades o grandes empresas tecnológicas) se conectase a la red desde múltiples sitios.

En 1986, la National Science Foundation (NSF) de EE.UU. inició el desarrollo de NSFNET que se diseñó originalmente para conectar cinco superordenadores. Su interconexión con Internet requería unas líneas de muy alta velocidad.

Esto aceleró el desarrollo tecnológico de INTERNET y brindó a los usuarios mejores infraestructuras de telecomunicaciones. Otras agencias de la Administración norteamericana entraron en Internet, con sus inmensos recursos informáticas y de comunicaciones: NASA y el Departamento de Energía.

Un acontecimiento muy importante era que los proveedores comerciales de telecomunicaciones en EE. UU. y Europa empezaron a ofrecer servicios comerciales de transporte de señales y acceso.
En 1 987 el número de servidores conectados a Internet superaba ya los 10.000.

El día 1 de noviembre de 1988 Internet fue "infectada" con un virus de tipo "gusano". Hasta el 10% de todos los servidores conectados fueron afectados.

El acontecimiento subrayó la falta de adecuados mecanismos de seguridad en Internet, por lo cual DARPA formó el Computer Emergency Reponse Team (CERT), un equipo de reacción rápida que mantiene datos sobre todas las incidencias en red y sobre las principales amenazas.

En 1989 el número de servidores conectados a Internet alcanza ya los 100.000. En este mismo año, se inauguró también la primera conexión de un sistema de correo electrónico comercial a Internet (MCI y Compuserve). Una nueva época estaba a punto de empezar, la de la explotación comercial de Internet.

Los años noventa .
ARPANET como entidad se extinguió en 1989/90, habiendo sobrepasado con mucho los objetivos y metas que tenía en su origen. Los usuarios de la red apenas lo notaron, ya que las funciones de ARPANET no solamente continuaron, sino que mejoraron notablemente a través de nuevos órganos más representativos de la utilización actual de la red.

En 1990 redes de diversos países como España, Argentina, Austria, Brasil, Chile, Irlanda, Suiza y Corea del Sur se conectaron también a NSFNET.

En 1991 se retiraron las restricciones de NFS al uso comercial de INTERNET. Ese mismo año también se Conectaron más países a la NSFNET incluyendo: Croacia, Hong Kong, República Checa, Sudáfrica, Singapur, Hungría, Polonia, Portugal, Taiwan y Túnez.

En 1992 el número de servidores conectados a INTERNET sobrepasaba la cifra de un millón de servidores. En ese año, la Sociedad de INTERNET (ISOC) se formó para promocionar el intercambio global de información. La Internet Architecture Board (IAB) fue reorganizada para llegar a formar parte del ISOC.

Como acontecimiento clave en la historia reciente de Internet, también en 1992 se desarrolló la World Wide Web en el Laboratorio Europeo de Física en Suiza. Esta tecnología provocó un drástico cambio en la apariencia. en el sentido y en el uso de INTERNET.

En 1993 el número de servidores INTERNET sobrepasa los 2.000.000. También NSF patrocina la formación de una nueva organización, ínterNIC, creada para proporcionar servicios de registro en Internet y bases de datos de direcciones.

El conocido navegador WWW 'Mosaic" se desarrolló en el National Center for Supercomputing.

"*En 1993 se funda Netscape, compañía que lanza al mercado un navegador con el cual Internet pasa de una fase escrita a una gráfica, lo que ayudó a popularizar esta tecnología. Más adelante surgieron otros navegadores en el mercado como el Explorer de Microsoft.. A partir de entonces, el crecimiento de Internet ha sido impresionante, en enero de 1993 tan sólo había 100 sitios WWW, para enero de 1996 ya existían 90 mil. Todo este crecimiento ha sido propiciado por los fines comerciales que persiguen la mayoría de las empresas que lo forman, de esta manera entramos a la nueva era comercial de Internet.*"[32]

El número de servidores de Internet alcanza los 3.800.000 en 1994. Las primeras tiendas Internet empiezan a aparecer junto con "emisores" de radio on-line. El conflicto potencial entre los internautas tradicionales y los nuevos usuarios se manifestó con el tumulto que causó un gabinete legal americano que introdujo publicidad en Internet.

[32] http://www.interware.com.mx/tecnologia/tecnologia/iwetecnologia_historia_internet. 24/01/03

En 1997, se piensa que algo fallaba, si no aparece la publicidad en una página Web. En 1995 había más de 5 millones de servidores conectados a Internet. La espina dorsal de NSFNET empezaba a ser sustituido por proveedores comerciales interconectados.

Hoy en día Internet está formada, no solamente de restos de la ARPANET original, sino que también incluye redes como la Academia Australiana de Investigación de redes (AARNET), la NASA Science Internet (NSI), la Red Académica de Investigación Suiza (SWITCH), por no mencionar las miles de redes de mayor o menor tamaño de tipo educativo y de investigación.

La velocidad de crecimiento de Internet en los primeros años de la década de los noventa ha sido espectacular: se podría decir casi salvaje. Se extiende casi a la misma velocidad que los ordenadores personales en los años ochenta.

La Administración norteamericana sigue apoyando en gran medida a la comunidad de Internet, debido, sin duda, a que ésta era en su origen un programa de investigación respaldado federalmente, y ha llegado a ser una parte importante de la infraestructura de investigación académica e industrial estadounidense.

Internet en México

"*La historia del Internet en México empieza en el año de 1989 con la conexión del Instituto Tecnológico y de Estudios Superiores de Monterrey, en el Campus Monterrey, ITESM hacia la Universidad de*

Texas en San Antonio (UTSA), específicamente a la escuela de Medicina. Una Línea privada analógica de 4 hilos a 9600 bits por segundo fue el enlace."[33]

La Universidad Nacional Autónoma de México accedió a Internet por medio de una conexión vía satélite de 56 Kbps con el Centro Nacional de Investigación Atmosférica de Boulder, Colorado, siendo éste el segundo nodo de Internet en México.

Después se interconectaron ambas universidades mexicanas usando líneas privadas analógicas de 9600 bps, velocidad suficiente para proveer correo electrónico, transferencia de archivos y acceso remoto.

Poco a poco se fueron incorporando a Internet otras instituciones educativas mexicanas como son: Universidad de Chapingo en el Estado de México, el Centro de Investigación de Química Aplicada de Saltillo, el Laboratorio Nacional de Informática Avanzada de Jalapa, Veracruz, los cuales se conectaban al ITESEM para salir a Internet.

Para este entonces, en México ya existía un organismo llamado RED-MEX, formado por la academia y dirigida por una organización civil, donde se discutían las políticas, estatutos y procedimientos que habrían de regir y dirigir el camino del control de la red de comunicación de datos de México. Tiempo más tarde, surgió otro organismo denominado MEXNET que reunía representantes legales

[31] http://www.banderas.com.mx/hist__de_internet.htm 02/02/03

de cada institución, el cual incluía a varias universidades de distintos lugares del país. Dicha organización, en 1992, establece una salida de 56 kbps al Backbone de Internet.

En 1993 la CONACyT se conecta a Internet mediante un enlace satelital al NCAR (Centro Nacional de Investigación Atmosférica) al igual que el ITAM, la UAM, en ese mismo año, se establece como el primer NAP (Network Access Point), al intercambiar tráfico entre dos diferentes redes.

A finales de este año en México ya se contaba con distintas redes: MEXnet, Red UNAM, Red ITESEM, RUTyC (desaparece el mismo año), BAJAnet, Red total CONACyT y SIRACyT. Fue en 1994, con la fundación de la Red Tecnológica Nacional (RTN), integrada por MEXnet y CONACyt, que se generó un enlace a 2 Mbps (E1).

En el mismo año, Internet se abre en el ámbito comercial en México, con lo cual se inicia una nueva era de desarrollo para nuestro país que beneficia a todas las personas, empresas o instituciones que deciden participar en el proyecto desde sus inicios, ya que hasta entonces sólo instituciones educativas y de investigación tenían acceso a la súper carretera de la información.

A fines de1995 se crea el Centro de Información de Redes de México (NIC-México) el cual se encargó de la coordinación y administración de los recursos de Internet asignados al país, como son la administración y delegación de los nombres de dominio bajo ".mx".

En 1996, se registran cerca de 17 enlaces contratados con Telmex para uso privado, asimismo se consolidan los principales ISP (proveedores de servicios de Internet) en el país, de los casi ya 100 ubicados a lo largo y ancho del territorio nacional.

Para el año de 1997 existen más de 150 ISP's, ubicados en los principales centros urbanos: Ciudad De México, Guadalajara, Monterrey, Chihuahua, Tijuana, Puebla, Laredo, Saltillo, Oaxaca, entre otros.

Actualmente, Internet es utilizado tanto por instituciones educativas y gubernamentales, empresas privadas y personas de todo el mundo, entre quienes se llevan a cabo intercambios constantes de información dando origen a la llamada globalización de la comunicación.

Hasta el día de hoy, gracias a Internet, se puede recibir información al instante de cualquier parte del mundo, agilizando y facilitando de esta forma el proceso comunicativo a distancia. Superando los obstáculos de la comunicación

2.3 CONCEPTO CARACTERISTICAS Y CLASIFICACION DE DELITOS INFORMATICOS.

Mucho se habla de los beneficios que los medios de comunicación y el uso de la Informática han aportado a la sociedad actual, pero el

objetivo de nuestro trabajo será analizar la otra cara de la moneda, o sea, las conductas delictivas que puede generar el gran avance tecnológico, sobre todo en el campo de la informática.

El desarrollo tan amplio de las tecnologías informáticas ofrece un aspecto negativo: ha abierto la puerta a conductas antisociales y delictivas que se manifiestan de formas que hasta ahora no era posible imaginar.

Los sistemas de computadoras ofrecen oportunidades nuevas y sumamente complicadas de infringir la ley, y han creado la posibilidad de cometer delitos de tipo tradicional en formas no tradicionales.

En los últimos tiempos, ha sido evidente que la sociedad ha utilizado de manera benéfica los avances derivados de la tecnología en diversas actividades; sin embargo, es necesario que se atiendan y regulen las cada vez más frecuentes consecuencias del uso indebido de las computadoras y los sistemas informáticos en general.

"La difusión de la informática da origen a nuevas formas delictivas que utilizan los sistemas informáticos como medio de comisión o bien en parte o en todo como su objeto, Si bien la difusión de informática en la América latina no ha dado dimensión mayor a este problema mayor previsible que su importancia crecerá a medida que aquella progrese"[34]

[34] CORREA, CARLOS María. **INFORMÁTICA Y DERECHO**. Editorial Depalma ,Buenos Aires 1987, p.23.

Para la comisión de dicha conducta antisocial, encontraremos a uno o varios sujetos activos como también pasivos, los cuales tienen características propias.

El Sujeto Activo, posee ciertas características que no presentan el denominador común de los delincuentes, esto es, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados.

Aún cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos, es decir, el sujeto activo del delito es una persona de cierto status socioeconómico, su comisión no puede explicarse por pobreza ni por mala habitación, ni por carencia de recreación, ni por baja educación, ni por poca inteligencia, ni por inestabilidad emocional, pues son personas listas, decididas y motivadas, dispuestas a aceptar un reto tecnológico.

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

Muchos de los delitos son descubiertos causísticamente por el desconocimiento del modus operandi de los sujetos activos.

Dado lo anterior, ha sido imposible conocer la verdadera magnitud de los "delitos informáticos", ya que la mayor parte de los delitos no son descubiertos o no son denunciados a las autoridades responsables y si a esto se suma la falta de leyes que protejan a las víctimas de estos delitos; la falta de preparación por parte de las autoridades para comprender, investigar y aplicar el tratamiento jurídico adecuado a esta problemática.

El temor por parte de las empresas de denunciar este tipo de ilícitos por el desprestigio que esto pudiera ocasionar a su empresa y las consecuentes pérdidas económicas, entre otras más, trae como consecuencia que las estadísticas sobre este tipo de conductas se mantenga bajo la llamada "cifra oculta o cifra negra."

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

Sin embargo, debe destacarse que el uso de las técnicas informáticas ha creado nuevas posibilidades del uso indebido de las computadoras lo que ha propiciado a su vez la necesidad de regulación por parte del derecho.

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

Concepto.

María de la Luz Lima dice que el "delito Electrónico" "*en un sentido amplio es cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en un sentido estricto, el delito informático, es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin.*"[35]

Por lo que se refiere a las definiciones que se han intentado dar en México, cabe destacar que Julio Téllez Valdés señala que no es labor fácil dar un concepto sobre delitos informáticos, en razón de que su misma denominación alude a una situación muy especial.

Ya que para hablar de "delitos" en el sentido de acciones típicas es decir tipificadas o contempladas en textos jurídicos penales, se requiere que la expresión "delitos informáticos" esté consignada en los códigos penales, lo cual en nuestro país, al igual que en otros muchos no ha sido objeto de tipificación aún.

[35] LIMA DE LA LUZ, María. **"DELITOS ELECTRÓNICOS"**. Academia Mexicana de Ciencias Penales. Ed. Porrúa, No. 1-6. Año I.. Enero-Junio. México1984, pp.99,100.

Pero la investigación da como resultado que el estado de Sinaloa si tipifica al delito informático en su Código Penal Vigente como delito contra el patrimonio.

El autor mexicano Julio Téllez Valdés señala que los delitos informáticos son *"actitudes ilícitas en que se tienen a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin (concepto típico)."*[36]

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

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

Lógicamente este concepto no abarca las infracciones administrativas que constituyen la generalidad de las conductas ilícitas presentes en México debido a que la legislación se refiere a derecho de autor y

---

[36] TÉLLEZ , VALDÉS Julio. **DERECHO INFORMÁTICO**. Editorial. Mc Graw Hill, 2ª Edición. México 1996, pp.103,104.

propiedad intelectual sin embargo, deberá tenerse presente que la propuesta final de este trabajo tiene por objeto la regulación penal de aquellas actitudes antijurídicas que estimamos más graves como último recurso para evitar su impunidad.

Características.

Según el Maestro Téllez Valdés, este tipo de acciones presentan las siguientes características principales:

a) Son conductas criminogenas de cuello blanco (white collar crime), en tanto que sólo un determinado número de personas con ciertos conocimientos (en este caso técnicos) pueden llegar a cometerlas

b) Son acciones ocupacionales, en cuanto a que muchas veces se realizan cuando el sujeto se halla trabajando

c) Son acciones de oportunidad, ya que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.

d) Provocan serias pérdidas económicas, ya que casi siempre producen "beneficios" de más de cinco cifras a aquellos que las realizan.

e) Ofrecen posibilidades de tiempo y espacio, ya que en milésimas de segundo y sin presencia física pueden llegar a consumarse.

f) Son muchos los casos y pocas las denuncias, y todo ello debido a la misma falta de regulación por parte del Derecho.

g) Son muy sofisticados y relativamente frecuentes en el ámbito militar.

h) Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.

i)En su mayoría son imprudenciales y no necesariamente se cometen con intención.

j)Ofrecen facilidades para su comisión a los menores de edad.

k) Tienden a proliferar cada vez más, por lo que requieren una urgente regulación.

l) Por el momento siguen siendo ilícitos impunes de manera manifiesta ante la ley.

Clasificación

Asimismo, este autor clasifica a estos delitos, de acuerdo a dos criterios:

1) Como instrumento o medio.
En esta categoría se encuentran las conductas criminales que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito, por ejemplo:

a).- Falsificación de documentos vía computarizada (tarjetas de crédito, cheques, etc.).
b).- Variación de los activos y pasivos en la situación contable de las empresas .
c).- Planeamiento y simulación de delitos convencionales (robo, homicidio, fraude , etc.).
d).- Lectura, sustracción o copiado de información confidencial modificación de datos tanto en la entrada como en la salida.
e).- Aprovechamiento indebido o violación de un código para penetrar a un sistema introduciendo instrucciones inapropiadas.
f).- Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa.
g).- Uso no autorizado de programas de computo.
h).- Introducción de instrucciones que provocan "interrupciones" en la lógica interna de los programas.
i) .- Alteración en el funcionamiento de los sistemas, a través de los virus informáticos.

j).- Obtención de información residual impresa en papel luego de la ejecución de trabajos.
k).- Acceso a áreas informatizadas forma no autorizada.
l).-Intervención en las líneas de comunicación de datos o teleproceso.

2) Como fin u objetivo
En esta categoría, se enmarcan las conductas criminales que van dirigidas contra las computadoras, accesorios o programas como entidad física, como por ejemplo:

a).- Programación de instrucciones que producen un bloqueo total al sistema.
b).- Destrucción de programas por cualquier método.
c).- Daño a la memoria.
d).-Atentado físico contra la máquina o sus accesorios.
e).- Sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centro neurálgicos computarizados.
f).- Secuestro de soportes magnéticos entre los que figure información valiosa con fines de chantaje (pago de rescate, etc.).

La Red de Internet permite dar soporte para la comisión de otro tipo de delitos como podrían ser los siguientes:

a).-Espionaje: Acceso no autorizado a sistemas informáticos gubernamentales y de grandes empresas e interceptación de correos electrónicos.

b).-Terrorismo: Mensajes anónimos aprovechados por grupos terroristas para remitirse consignas y planes de actuación a nivel internacional.
c).-Narcotráfico: Transmisión de fórmulas para la fabricación de estupefacientes, para el blanqueo de dinero y para la coordinación de entregas y recogidas.

El autor Julio B. J. Maier cita en su obra Delitos No Convencionales al Lic. Ulrico Sieber quien nos da la siguiente clasificación:

"Delitos Informáticos de carácter Económico en donde por medio del sistema informático como herramienta o tomando al sistema informático como objeto de la acción disvaliosa se produce un perjuicio patrimonial.
Delitos Informáticos contra la Privacidad mediante la divulgación indebida de datos contenida en sistemas informáticos ."[37]

María de la Luz Lima, presenta una clasificación, de lo que ella llama "*delitos electrónicos*", diciendo que existen tres categorías, a saber:

"1.- *Los que utilizan la tecnología electrónica como método para,*
-Falsificar tarjetas de crédito
-Defraudar a una compañía
-Fraudes con técnica salami que consiste en extraer pequeñas cantidades de dinero de miles de cuentas bancarias

[37] MAIER , Julio B . **DELITOS NO CONVENCIONALES** .Editores del Puerto. Buenos Aires 1994, p 227

-Adquisición de bienes materiales modificando inventarios archivados
-Falsificación de cintas magnéticas
-Reproducción no autorizada de películas

2.- Los que utilizan la tecnología electrónica como medio o símbolo para Interceptar teléfonos con transistores , beepers, radios , bugs, se usa mucho para el espionaje industrial , el sabotaje político.
-Lectura de información confidencial para bloquear la capacidad operativa de la víctima y cometer sabotaje industrial.
-Lectura de ficheros judiciales para extorsionar y chantajear.

3.- Los que utilizan la tecnología electrónica como fin.
-Destrucción de un programa.
-Dañar una memoria.
-Quemar la computadora".[38]

2.4 DELITOS QUE SE PUEDE TRASLADAR AL CIBERESPACIO.

El ciberespacio es un mundo virtual en el que los defectos, miserias y malos hábitos del ser humano se reproducen con la misma fidelidad que las virtudes. El efecto de aldea global generado por el entramado de redes y la proliferación de nodos en todo el planeta ayudan a la difusión inmediata de los mensajes y permite el acceso a cualquier información introducida en la red.

---

[38] LIMA DE LA LUZ, María. Ibid. pp.100,101

A las reconocidas ventajas que ello supone se unen las distorsiones y los malos usos que pueden tener lugar en el sistema y que confirman una vez más que el mal no está en el medio utilizado sino en la persona que lo utiliza.

Actualmente se está produciendo un intenso debate respecto a la necesidad de prevenir y sancionar estos malos usos en la red de redes Internet y el objetivo de este trabajo es localizar las distorsiones más habituales que se producen y resumir los argumentos que se han dado a favor de una legislación que regule el uso de la red y los criterios contrarios a esa regulación tomando como base la legislación nacional e internacional.

Fraude Informático.

Solo está limitado por la imaginación del autor, su capacidad técnica y las medidas de seguridad de la instalación.

Se pueden clasificar en cuatro grupos:

1.- Intervención en los datos de entrada al sistema;

2.- Incorporación de modificaciones no autorizadas en los programas;

3.- Modificación fraudulenta de la información almacenada en el sistema.

4.- Intervención en la líneas de transmisión de datos.

Acceso No Autorizado.

El uso ilegítimo de passwords y la entrada en un sistema informático sin la autorización del propietario debe quedar tipificado como un delito, puesto que el bien jurídico que acostumbra protegerse con la

contraseña es lo suficientemente importante para que el daño producido sea grave.

Destrucción de Datos.
Son daños causados en la red mediante la introducción de virus, bombas lógicas y demás actos de sabotaje informático.

Infraccion de los Derechos de Autor.
Es la interpretación de los conceptos de copia, distribución, cesión y comunicación pública de los programas de ordenador utilizando la red.

Infracción del Copyright de Bases de Datos.
Aún no existe una protección uniforme de las bases de datos en los países que tienen acceso a Internet.

Intercepción de e-mail.
Constituye una violación de correspondencia, y la intercepción de telecomunicaciones, de forma que la lectura de un mensaje electrónico ajeno revista la misma gravedad.

Estafas Electronicas.
La proliferación de las compras telemáticas permite que aumenten también los casos de estafa. Se trataría en este caso de una dinámica comisiva que cumpliría todos los requisitos del delito de estafa, ya que además del engaño y el "animus defraudandi" existiría un engaño a la persona que compra.-

Transferencia de Fondos.

Este es el típico caso en el que no se produce engaño a una persona determinada sino a un sistema informático.- Como se puede observar, muchas de estas conductas no son irreales, es decir, las encontramos de una manera palpable, y cualquier persona que tenga conocimientos básicos de informática puede llegar a cometerlos.

CRYPTOME.Org publico el texto integro del informe sobre delitos en el ciberespacio que fue presentado en la sesión plenaria del comité europeo sobre delitos, celebrada del 18 a 22 de junio de 2001.

Este informe ha sido desarrollado por una comisión de expertos (Comité Europeo de Crímenes en el Ciberespacio) se compone de dos partes: por un lado, el borrador de la convención sobre el crimen en Internet y por el otro el borrador de un memorando acerca los problemas originados por el crimen en Internet.

Esta convención tiene como objetivo facilitar un marco común que sirva para la unificación de las políticas relacionadas con los delitos en el ciberespacio de los diferentes países miembros de la Unión Europea.

Los delitos tipificados son agrupados en dos grandes marcos:

Medidas a tomar a nivel nacional y medidas que requieren la cooperación internacional.

Entre los primeros se describen los siguientes delitos:

"Acceso ilegal, Intercepción ilegal, Interferencia de datos, Interferencia de sistemas ,Mala utilización de dispositivos, Falsificación de datos, Fraude (alteración, supresión o borrado de datos y interferencias con el funcionamiento normal de los sistemas),Delitos relacionados con la pornografía infantil, Delitos relacionados con la infracción del Copyright y derechos relacionados."[39]

Dentro del apartado de medidas que precisan de una cooperación a nivel internacional se describen los principios generales relacionados con la extradición, indicando que los delitos tipificados en el apartado de medidas de carácter nacional deben ser incluidos en la relación de delitos que permiten la extradición.

Igualmente se indica la importancia de la cooperación entre las fuerzas del orden de los diversos países miembros.

Delitos convencionales que pueden trasladarse al ciberespacio.
Nos referimos a aquellos que tradicionalmente se han venido dando en la "vida real", sin el empleo de medios informáticos y que con la irrupción de las autopistas de la información se ha producido también en el ciberespacio.

---

[39] http://www.liderdigital.com/documentos/Boletin_Derecho_y_Sociedad_de_la_Informacion_n5. 12/01/03

Por mencionar algunos delitos, pueden ser :

-El robo,
-El espionaje a través de un acceso no autorizado a sistemas informáticos gubernamentales, interceptación de correo electrónico del servicio secreto,
-El espionaje industrial,
-El terrorismo mediante la existencia de hosts que ocultan la identidad del remitente, convirtiendo el mensaje en anónimo, siendo aprovechado por grupos terroristas para remitirse consignas y planes de actuación a nivel internacional,
-El propio narcotráfico ya que se ha utilizado a la red para la transmisión de fórmulas para la fabricación de estupefacientes, para el bloqueo de dinero y para la coordinación de entregas y recogidas;
-Tráfico de armas,
-Proselitismo de sectas,
-Propaganda de grupos extremistas,
-Secuestros y cualquier otro delito que pueda ser trasladado de la vida real al ciberespacio o al revés.

2.5 CONDUCTAS DELICTIVAS POR MEDIO DE INTERNET

En los años 60, se denominaba dentro del ámbito informático "hacker" a toda persona altamente capacitada, que tenía los conocimientos para llevar a los sistemas existentes, mediante modificación del código que lo compone, a nuevas y más productivas instancias.

Ya entrados los 70, y debido a un descuido fortuito de una compañía telefónica y un premio de una caja de cereales un usuario llamado John Draper alias "Capitán Crunch" logra realizar una llamada de larga distancia introduciendo un tono preciso dentro de una línea abierta de teléfono, de allí el término "phone hacker" que después deriva en "phreaker."

Los phreakers toman un nivel insospechado de popularidad, considerándoselos responsables de invaluables defraudaciones. Se llegaron hasta fundar asociaciones que brindaban dichos servicios, como el Homebrew Computer Club, cuyos socios comercializaban cajas con la capacidad de violar sistemáticamente los sistemas de protección de llamadas telefónicas.

Dos de sus miembros cuyos alias eran "Berkeley Blue" (Steve Jobs) y "Oak Toebark" (Steve Wozniak), más tarde decidieron fundar una empresa cuyo nombre marcaría un giro en la forma del manejo de las microcomputadoras: "Apple Computers Inc."

En el principio de los 80, comienza el auge de las microcomputadoras y los sistemas protegidos para las copias de los usuarios, generando un movimiento en contra de esta actitud.

Los desde ese momento denominados crakers, "rompían" el código fuente de los programas eliminando las líneas que efectuaban las comprobaciones de protección. Se funda la revista "2600: The Hacker Quarterly", semanario que incluye técnicas para efectuar phreaking.

A mediados de los 80, las redes corporativas toman características abiertas y se empieza a ver como individuos de muy alta capacidad empiezan a penetrarlas, no hubo desde aquel entonces empresa y/u oficinas gubernamentales que estuviesen a salvaguardo, en honor de aquellos que otrora se los consideraba genios por entrar ("hack in") al código para mejorarlo, se les siguió dando el seudónimo de "hackers".

Se les comienza a llamar "piratas" a aquéllos que sólo les interesaba lucrar con los sistemas ya desprotegidos, para diferenciarlos de aquéllos que podían efectuar el "hackeo" o "crackeo".

Desde cualquier época hasta hoy, existen infinidad de ejemplos de como los sistemas considerados de máxima seguridad han sido violados, modificados, borrados, y desprotegidos.

La Oficina de Contabilidad General de E.E.U.U, determinó que sólo en 1995 soportó 250.000 de estos intentos. (Cuadro 7)

7 de Septiembre de 1999. Asociacion Internacional de Contraterrorismo y Profesionales de la Seguridad
20 de Agosto de 1999 . American Broadcasting Company (ABC)
1 de Agosto de 1999 Base Aérea de Nellis E.E.U.U
4 de Julio de 1999 .

Proyecto de búsqueda de vida inteligente extraterrestre (SETI)
24 de Junio de 1999 . Base Militar de Monmouth E.E.U.U
8 de Junio de 1999 . Ejército de los E.E.U.U.
19 de Junio de 1999 . Centro de Guerra de Superficie de la Marina de E.E.U.U
11 de Junio de 1999 . Senado de los E.E.U.U
31 de Mayo de 1999 . Departamento del Interior de los E.E.U.U
10 de Mayo de 1999 . La Casa Blanca
1 de Abril de 1999 . (día de los inocentes en E.E.U.U)Hackers News Network
27 de Enero de 1999 . Green Peace Internacional
27 de Enero de 1999 . Klu Klux Klan

Cuadro No. 7

Durante el tercer congreso del Instituto de Seguridad de Computadoras celebrado por el FBI (división especial de Crimen Internacional Computadorizado), **se determinó que** ***"el número de ataques sufridos por las empresas va en aumento, y que son debidos en su gran mayoría a hackers externos más que a compotidores u***

organismos gubernamentales, durante el año 1997 se estimaron pérdidas cercanas a los 111 millones de dólares."[40]

Ataque electrónico denominada "ghost hacking o ghosthack", que consiste en la adulteración de información sin que el usuario pueda percibirlo.

En el caso de un Banco estos sistemas, penetran en la red con el fin de detectar dentro de las millones de transacciones electrónicas realizadas, cual es el error de aproximación matemática inapreciable, una vez establecido, le quitan a toda operación esos milésimos, y dicha quita la suman dentro de una sola cuenta, generando grandes sumas de dinero.

En el caso de un usuario final, generalmente introducen programas que graban todo tipo de información que el usuario escriba: nombres de usuario, números de teléfono, números de tarjetas de crédito, etc. Cuando el usuario se reconecte al lugar desde donde le fue insertado el programa, éste se encargará de enviar toda la información acumulada.

Otra operatoria similar, con generalmente resultados de catástrofe, son los denominados "virus informáticos", cuyo nombre proviene de su símil biológico por su habilidad para enfermar al "computador", e infectar todo lugar asignado autoreproduciéndose.

[40] http://www.monografias.com/trabajos/legisdelinf/legisdelinf.shtml 12/01/03

La denominada "enfermedad" del computador puesta de manifiesto bajo ciertas circunstancias (fechas determinadas, cantidad de horas desde la llegada del virus, etc.) suele ir desde un aviso simple que el computador ha sido infectado con determinado virus, hasta el borrado sistemático de toda información existente.

Para un pormenorizado detalle de los lugares y situaciones a los que fueron sometidas diferentes entidades privadas y gubernamentales, con un histórico de como fue el efecto causado, recomiendo recorrer la página web de la HNN (Hackers News Network), dicho sea de paso página que también fue víctima de un ataque.

2.5.1 HACKER.

Es quien intercepta dolosamente un sistema informático para dañar, apropiarse, interferir, desviar, difundir, y/o destruir información que se encuentra almacenada en ordenadores pertenecientes a entidades públicas o privadas. El término de hacker en castellano significa "cortador". Las incursiones de los piratas son muy diferentes y responden a motivaciones dispares, desde el lucro económico a la simple diversión.

Los "Hackers", son fanáticos de la informática, generalmente jóvenes, que tan sólo con un ordenador personal, un módem, gran paciencia e imaginación son capaces de acceder, a través de una red pública de transmisión de datos, al sistema informatizado de una empresa o entidad pública, saltándose todas las medidas de seguridad, y leer

información, copiarla, modificarla, preparando las condiciones idóneas para realizar un fraude, o bien destruirla.

Se pueden considerar que hay dos tipos; 1) los que sólo tratan de llamar la atención sobre la vulnerabilidad de los sistemas informáticos, o satisfacer su propia vanidad; 2) los verdaderos delincuentes, que logran apoderarse por este sistema de grandes sumas de dinero o causar daños muy considerables.

Hackers

"Son programadores y suelen ser jóvenes deseosos de conocer el funcionamiento de los diferentes sistemas. El Hacker aprovecha los agujeros, los fallos de los sistemas de seguridad. Sus intereses se centran en el conocimiento del funcionamiento de los sistemas. Rigen su actividad por un código ético (netiquettes)."[41]

Principios de la ética hacker.

1. Toda la información debe ser libre.
2. Entrégate siempre al imperativo de transmitir el acceso a las computadoras o a cualquier otra cosa que pueda enseñarte como funciona el mundo, esto debe ser ilimitado y total.
3. Desconfía de las autoridades, promueve la descentralización.
4. Los hackers deben ser juzgados por su hacking, no por criterios de edad, títulos, raza o posición.

[41] http://www.inicia.es/de/pazenred/delin2.htm#c 20/01/03

5. Puedes crear verdad y belleza en una computadora.
6. Las computadoras pueden mejorar tu vida.

2.5.2 CRACKER:

Para las acciones nocivas existe la más contundente expresión, "Cracker" o "rompedor", sus acciones pueden ir desde simples destrucciones, como el borrado de información, hasta el robo de información sensible que se puede vender; es decir, presenta dos vertientes, el que se cuela en un sistema informático y roba información o produce destrozos en el mismo, y el que se dedica a desproteger todo tipo de programas, tanto de versiones shareware para hacerlas plenamente operativas como de programas completos comerciales que presentan protecciones anticopia.

Crackers .
"Es el que se cuela en un sistema informático y roba información o produce destrozos en el mismo. Desprotege todo tipo de programas (hardware)para hacerlas plenamente operativas como de programas completos comerciales que presentan protección anticopia"[42]

Esto es relativamente normal cuando se trata de analizar las posibles modalidades de intervención penal en nuevos ámbitos (también ha sucedido así con la manipulación genética). Pero la intervención penal ha de basarse en hechos y no en conceptos de autor (derecho penal

[42] http://www.derechotecnologico.com/hackers.html 20/01/03

de autor). (La propia sentencia del caso Hispahack cae en la tentación de definir "autores" más que hechos).

Las clasificaciones de delitos informáticos adolecen todas de una tendencia a sancionar y reclamar la intervención penal para proteger "algunos" intereses pero olvidan absolutamente la protección de los intereses de los usuarios frente a estas mismas empresas y frente a las empresas de servicios de internet (servidores, buscadores, portales, etc.)

2.5.3 PIRATA INFORMATICO.

Es quien reproduce, vende o utiliza en forma ilegítima un software que no le pertenece o que no tiene licencia de uso, conforme a las leyes de derecho de autor.

Phreaker.

"El que emplea sus conocimientos para poder utilizar las telecomunicaciones gratuitamente. Acceden a la red utilizando "vías" gratuitas de las que disfrutan ilícitamente o de forma no autorizada".[43]

2.5.4 VIRUCKER.

Consiste en el ingreso doloso de un tercero a un sistema informático ajeno, con el objetivo de introducir "virus" y destruir, alterar y/o

---

[43] http://www.inicia.es/de/pazenred/delin2.htm#c 20/01/03

inutilizar la información contenida. Existen dos tipos de virus, los benignos que molestan pero no dañan, y los malignos que destruyen información o impiden trabajar. Suelen tener capacidad para instalarse en un sistema informático y contagiar otros programas e, inclusive, a otros ordenadores a través del intercambio de soportes magnéticos, como disquetes o por enlace entre ordenadores.

"Virucker proviene de la unión de los términos virus y hackers y se refiere al creador de un programa insertado en forma dolosa en un sitema de computo que destruye dañe o inutilice un sistema de información perteneciente a organizaciones con o sin fines de lucro y de diversa indole"[44]

[44] http://www.ua-ambit.org/soi/bol142.hym 20/01/03

CAPITULO III . LEGISLACION INTERNACIONAL Y NACIONAL SOBRE DELITOS INFORMATICOS.

3.1 LEGISLACION INTERNACIONAL

En el contexto internacional, son pocos los países que cuentan con una legislación apropiada en delitos infromaticos . Entre ellos, se destacan, Estados Unidos, Alemania, Austria, Gran Bretaña, Holanda, Francia, Argentina y Chile.

3.1.1 ALEMANIA

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

1.-Espionaje de datos (202 a);

2.-Estafa informática (263 a);

3.-Falsificación de datos probatorios (269) junto a modificaciones complementarias del resto de falsedades documentales como el engaño en el tráfico jurídico mediante la elaboración de datos, falsedad ideológica, uso de documentos falsos (270, 271, 273);

4.-Alteración de datos (303 a) es ilícito cancelar, inutilizar o alterar datos inclusive la tentativa es punible;

5.-Sabotaje informático (303 b), destrucción de elaboración de datos de especial significado por medio de destrucción, deterioro, inutilización, eliminación o alteración de un sistema de datos. También es pubible la tentativa;
6.-Utilización abusiva de cheques o tarjetas de crédito (266 b).

Por lo que se refiere a la estafa informática, la formulación de un nuevo tipo penal tuvo como dificultad principal el hallar un equivalente análogo al triple requisito de acción engañosa, causa del error y disposición patrimonial, en el engaño del computador.

Así como en garantizar las posibilidades de control de la nueva expresión legal, quedando en la redacción que el perjuicio patrimonial que se comete *"consiste en influir en el resultado de una elaboración de datos por medio de una realización incorrecta del programa, a través de la utilización de datos incorrectos o incompletos, mediante la utilización no autorizada de datos, o a través de una intervención ilícita."*[45]

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

---

[45] http://www.tiny.uasnet.mx/prof/cln/der/silvia/leyint.htm 22/01/03

En el caso de Alemania, se ha señalado que a la hora de introducir nuevos preceptos penales para la represión de la llamada criminalidad informática el gobierno tuvo que reflexionar acerca de dónde radicaban las verdaderas dificultades para la aplicación del Derecho penal tradicional a comportamientos dañosos en los que desempeña un papel esencial la introducción del proceso electrónico de datos, así como acerca de qué bienes jurídicos merecedores de protección penal resultaban así lesionados.

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

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

En otro orden de ideas, las diversas formas de aparición de la criminalidad informática propician además, la aparición de nuevas lesiones de bienes jurídicos merecedoras de pena, en especial en la medida en que el objeto de la acción puedan ser datos almacenados o transmitidos o se trate del daño a sistema informáticos.

El tipo de daños protege cosas corporales contra menoscabos de su sustancia o función de alteraciones de su forma de aparición.

3.1.2 ARGENTINA

Contenido del Anteproyecto

Antes de avanzar sobre el comentario del articulado se vuelve necesario remarcar la importancia, para la real aplicabilidad de los tipos ya definidos y los que en el futuro se puedan crear, de demarcar claramente dos conceptos centrales para esta ley. Cabe referirse a las definiciones de "sistema informático" y "dato informático o información".

La Comisión ha podido comprobar, fruto del debate que tuvo lugar en su seno y alimentado por los debates que se producen en otras latitudes, que la inmensa cantidad de las conductas ilegitimas que se buscan reprimir atentan ya sea contra uno u otro de estos dos conceptos definidos.

Despues se decidió - siguiendo la Convención del Consejo de Europa sobre Cyber crime- que, demarcando con nitidez ambos conceptos y haciéndolos jugar dentro de la tipologia elegida, se lograba abarcar en mayor medida las conductas reprochables, sin perder claridad ni caer en soluciones vedadas por principios centrales del derecho penal: a saber, Principio de legalidad y Principio de Prohibición de la Analogía.

El anteproyecto se estructura en tres figuras fundamentales y disposiciones comunes a ellas. La incriminación de las conductas descriptas es el producto de la sistematización a la que hemos llegado luego de analizar exhaustivamente proyectos e iniciativas que han tenido lugar en distintos países. A saber:

"a) Acceso ilegítimo informático
b) Daño informático
c) Fraude informático
d) Disposiciones comunes" [46]

En el primero de los casos se acuña el tipo básico de todo acceso ilegítimo a sistemas o datos informáticos, figura que contempla el llamado hacking, delito que vulnera la confidencialidad de la información (en sus dos aspectos, intimidad y exclusividad) y que puede ser la antesala de otros delitos más graves, por ejemplo el daño, o el fraude informático.

Dicha figura se complementa con dos agravantes según si el autor divulga o revela la información, o sí el sistema accedido concierne a la seguridad, defensa nacional, salud pública o la prestación de servicios públicos.

En el segundo de los casos el tipo penal incrimina legislativamente el llamado daño informático, también conocido como sabotaje

[46] http://www.Dpi.bioetica.org/sofnotas1.htm 22/01/03

informático o cracking, acción dirigida a dañar sistemas o datos informáticos.

Como en el supuesto anterior se redactó una figura básica y tres incisos que prevén distintas agravantes, contemplando el tercero de ellos una pena máxima para el caso que se produzcan las consecuencias dañosas previstas en la ley.

El fraude informático consta de una figura básica que tiene como carácter distinto del daño, el ánimo de lucro que persigue el autor del hecho, quién se vale de manipular sistemas o datos informáticos, o utiliza cualquier artificio tecnológico semejante para procurar la transferencia no consentida de cualquier activo patrimonial de un tercero.

O perjudica a la Administración Pública Nacional o Provincial, o a entidades financieras la pena se eleva de dos a ocho años de prisión.

El proyecto se completa con disposiciones comunes que se dirigen a penalizar las conductas de los responsables de la custodia, operación, mantenimiento o seguridad de un sistema o dato informático y a definir estos dos últimos conceptos.

Comisión de Delitos Informáticos. Buenos Aires, 24 de septiembre de 2001.

3.1.3 AUSTRIA

Ley de reforma del Código Penal de 22 de diciembre de 1987.
Esta ley contempla los siguientes delitos:

Destrucción de datos (126). En este artículo se regulan no sólo los datos personales sino también los no personales y los programas.

Estafa informática (148). En este artículo se sanciona a aquellos que con dolo causen un perjuicio patrimonial a un tercero influyendo en el resultado de una elaboración de datos automática a través de la confección del programa, por la introducción, cancelación o alteración de datos por actuar sobre el curso del procesamiento de datos.

3.1.4 CHILE

Chile fue el primer país latinoamericano en sancionar una Ley contra delitos informáticos, la cual entró en vigencia el 7 de junio de 1993. Según esta ley, la destrucción o inutilización de los de los datos contenidos dentro de una computadora es castigada con penas desde un año y medio a cinco años de prisión. Asimismo, dentro de esas consideraciones se encuentran los virus.

Esta ley prevé en el Art. 1º, el tipo legal vigente de una conducta maliciosa tendiente a la destrucción o inutilización de un sistema de tratamiento de información o de sus partes componentes o que dicha

conducta impida, obstaculice o modifique su funcionamiento. En tanto, el Art. 3º tipifica la conducta maliciosa que altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información .

3.1.5 ESTADOS UNIDOS

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

Consideramos importante destacar las enmiendas realizadas a la Sección 502 del Código Penal relativas a los delitos informáticos en la que, entre otros, se amplían los sujetos susceptibles de verse afectados por estos delitos, la creación de sanciones pecuniarias de $10,000 por cada persona afectada y hasta $50,000 el acceso imprudencial a una base de datos, etcétera."[47]

El objetivo de los legisladores al realizar estas enmiendas, según se infiere, era la de aumentar la protección a los individuos, negocios, y agencias gubernamentales de la interferencia, daño y acceso no autorizado a las bases de datos y sistemas computarizados creados legalmente. Asimismo, los legisladores consideraron que la proliferación de la tecnología de computadoras ha traído consigo la

[47] http://www.aaba.or.ar/bi180p32.htm 25/01/03

proliferación de delitos informáticos y otras formas no autorizadas de acceso a las computadoras, a los sistemas y las bases de datos y que la protección legal de todos sus tipos y formas es vital para la protección de la intimidad de los individuos así como para el bienestar de las instituciones financieras, de negocios, agencias, gubernamentales y otras relacionadas con el estado de California que legalmente utilizan esas computadoras, sistemas y bases de datos.

Es importante mencionar que en uno de los apartados de esta ley, se contempla la regulación de los virus (computer contaminant) conceptualizándose aunque no los limita a un grupo de instrucciones informáticas comúnmente llamados virus o gusanos sino que contempla a otras instrucciones designadas a contaminar otros grupos de programas o bases de datos, modificar, destruir, copiar o transmitir datos o alterar la operación normal de las computadoras, los sistemas o las redes informáticas.

En 1994 aclara que el creador de un virus no escudarse en el hecho que no conocía que con su actuar iba a causar daño a alguien o que él solo quería enviar un mensaje.

En opinión de los legisladores estadounidenses, la nueva ley constituye un acercamiento más responsable al creciente problema de los virus informáticos, específicamente no definiendo a los virus sino describiendo el acto para dar cabida en un futuro a la nueva era de ataques tecnológicos a los sistemas informáticos en cualquier forma en que se realicen.

Diferenciando los niveles de delitos, la nueva ley da lugar a que se contemple qué se debe entender como acto delictivo.

Este país adoptó en 1994 del Acta Federal de Abuso Computacional (18 U.S.C. Sec .1030) que modificó al Acta de Fraude y Abuso Computacional de 1986.

"Con la finalidad de eliminar los argumentos hipertécnicos acerca de qué es y que no es un virus, un gusano, un caballo de Troya y en que difieren de los virus, la nueva acta proscribe la transmisión de un programa, información, códigos o comandos que causan daños a la computadora, a los sistemas informáticos, a las redes, información, datos o programas (18 U.S.C.: Sec. 1030 (a) (5) (A). La nueva ley es un adelanto porque está directamente en contra de los actos de transmisión de virus."[48]

El Acta de 1994 diferencia el tratamiento a aquellos que de manera temeraria lanzan ataques de virus de aquellos que lo realizan con la intención de hacer estragos. Definiendo dos niveles para el tratamiento de quienes crean virus:

a) Quien intencionalmente cause un daño por la transmisión de un virus, el castigo de hasta 10 años en prisión federal más una multa
b) Para los que lo transmiten sólo de manera imprudencial la sanción fluctúa entre una multa y un año en prisión.

[48] http://www.calle22.com/articulo/2024/ 02/02/03

La nueva ley constituye un acercamiento más responsable al creciente problema de los virus informáticos, específicamente no definiendo a los virus sino describiendo el acto para dar cabida en un futuro a la nueva era de ataques tecnológicos a los sistemas informáticos en cualquier forma en que se realicen.

Diferenciando los niveles de delitos, la nueva ley da lugar a que se contemple qué se debe entender como acto delictivo.

Asimismo, en materia de estafas electrónicas, defraudaciones y otros actos dolosos relacionados con los dispositivos de acceso a sistemas informáticos, la legislación estadounidense sanciona con pena de prisión y multa, a la persona que defraude a otro mediante la utilización de una computadora o red informática.

En el mes de Julio del año 2000, el Senado y la Cámara de Representantes de este país, tras un año largo de deliberaciones- establece el Acta de Firmas Electrónicas en el Comercio Global y Nacional.

La ley sobre la firma digital responde a la necesidad de dar validez a documentos informáticos -mensajes electrónicos y contratos establecidos mediante Internet- entre empresas (para el B2B) y entre empresas y consumidores (para el B2C).

3.1.6 FRANCIA

En enero de 1988, este país dictó la Ley relativa al fraude informático, la cual prevé penas de dos meses a dos años de prisión y multas de diez mil a cien mil francos por la intromisión fraudulenta que suprima o modifique datos.

Asimismo, esta ley establece en su artículo 462-3 una conducta intencional y a sabiendas de estar vulnerando los derechos de terceros que haya impedido o alterado el funcionamiento de un sistema de procesamiento automatizado de datos.

Por su parte el artículo 462-4 también incluye en su tipo penal una conducta intencional y a sabiendas de estar vulnerando los derechos de terceros, en forma directa o indirecta, haya introducido datos en un sistema de procesamiento automatizado o haya suprimido o modificado los datos que éste contiene, o sus modos de procesamiento o de transmisión.

También la legislación francesa establece un tipo doloso y pena el mero acceso, agravando la pena cuando resultare la supresión o modificación de datos contenidos en el sistema, o bien en la alteración del funcionamiento del sistema (sabotaje).

Por último, esta ley en su artículo 462-2, sanciona tanto el acceso al sistema como al que se mantenga en él y aumenta la pena correspondiente si de ese acceso resulta la supresión o modificación

de los datos contenidos en el sistema o resulta la alteración del funcionamiento del sistema.

Ley número 88-19 de 5 de enero de 1988 sobre el fraude informático.

Acceso fraudulento a un sistema de elaboración de datos (462-2).Se sanciona tanto el acceso al sistema como al que se mantenga en él y aumenta la sanción correspondiente si de ese acceso resulta la supresión o modificación de los datos contenidos en el sistema o resulta la alteración del funcionario del sistema.

Sabotaje informático (462-3). Se sanciona a quien impida o falsee el funcionamiento de un sistema de tratamiento automático de datos.

Destrucción de datos (462-4). Se sanciona a quien intencionadamente y con menosprecio de los derechos de los demás introduzca datos en un sistema de tratamiento automático de datos o suprima o modifique los datos que éste contiene o los modos de tratamiento o de transmisión.

Falsificación de documentos informatizados (462-5). Se sanciona a quien de cualquier modo falsifique documentos informatizados con intención de causar un perjuicio a otro.

Uso de documentos informatizados falsos (462-6). Se sanciona a quien conscientemente haga uso de documentos falsos haciendo referencia al artículo 462-5.

3.1.7 ITALIA

En Italia existen los siguientes Delitos Informáticos:

a) Acceso Abusivo. Se configura exclusivamente en caso de sistemas informáticos y telemáticos protegidos por dispositivos de seguridad (contraseñas o llaves de hardware) que indiquen claramente la privacidad del sistema y la voluntad del derechohabiente de reservar el acceso a aquél sólo a las personas autorizadas. La comisión de este delito se castiga con reclusión de hasta tres años, previendo agravantes.

b) Abuso de la calidad de operador de sistemas. Este delito es un agravante al delito de acceso abusivo y lo comete quien tiene la posibilidad de acceder y usar un sistema informático o telemático de manera libre por la facilidad de la comisión del delito.

c) "*Introducción de virus informáticos. Es penalmente responsable aquel que cree o introduzca a una red programas que tengan la función especifica de bloquear un sistema, destruir datos o dañar el disco duro, con un castigo de reclusión de hasta dos años y multas considerables*"[49]

d) Fraude Informático.- Cuando por medio de artificios o engaños, induciendo a otro a error, alguien procura para sí o para otros un

[49] http://www.alfa-redi.org/upload/documento/110801-20-6LA%20AUTORIA%20MEDIATA%MEDIATA 02/02/03

injusto beneficio, ocasionando daño a otro. También se entiende como tal la alteración del funcionamiento de sistemas informáticos o telemáticos o la intervención abusiva sobre datos, informaciones o programas en ellos contenidos o pertenecientes a ellos, cuando se procure una ventaja injusta, causando daño a otro. La punibilidad de este tipo de delito es de meses a tres años de prisión, más una multa considerable.

e) Intercepción abusiva.- Es un delito que se comete junto con el delito de falsificación, alteración o supresión de comunicaciones telefónicas o telegráficas. Asimismo, es la intercepción fraudulenta, el impedimento o intrusión de comunicaciones relativas a sistemas informáticos o telemáticos, además de la revelación al público, mediante cualquier medio, de la información, de esas publicaciones; este delito tiene una punibilidad de 6 meses a 4 años de prisión. Asimismo, se castiga el hecho de realizar la instalación de equipo con el fin anterior.

f) Falsificación informática. Es la alteración, modificación o borrado del contenido de documentos o comunicaciones informáticas o telemáticas. En este caso, se presupone la existencia de un documento escrito (aunque se debate doctrinariamente si los documentos electrónicos o virtuales pueden considerarse documentos escritos). En este caso, la doctrina italiana tiene muy clara la noción de "documento informático", al cual define como cualquier soporte informático que contenga datos, informaciones o programas específicamente destinados a elaborarlos.

g) Espionaje Informático.- Es la revelación del contenido de documentos informáticos secretos o su uso para adquirir beneficios propios, ocasionado daño a otro.

h) Violencia sobre bienes informáticos. Es el ejercicio arbitrario, con violencia, sobre un programa, mediante la total o parcial alteración, modificación o cancelación del mismo o sobre un sistema telemático, impidiendo o perturbando su funcionamiento.

i) Abuso de la detentación o difusión de Códigos de acceso (contraseñas).

j) Violación de correspondencia electrónica, la cual tiene agravantes si causare daños.

3.1.8 PORTUGAL

Por su parte, la Constitución de la República Portuguesa, hace mención sobre la utilización informática, la cual fue aprobada por la Asamblea Constituyente el 2 de abril de 1976, y la cual menciona:

Artículo 35: " Utilización de la Informática.
1. Todos los ciudadanos tienen derecho a conocer lo que constare acerca de los mismos en registros mecanográficos, así como el fin a que se destinan las informaciones, pudiendo exigir la rectificación de los datos y su actualización.

2. La informática no podrá ser usada para el tratamiento de datos referentes a convicciones políticas, fe religiosa o vida privada, excepto cuando se tratare del proceso de datos no identificables para fines estadísticos.
3. Queda prohibida la atribución de un número nacional único a los ciudadanos.

En diferentes países se han preocupado por el mal uso que pueda tener los grandes avances tecnológicos, el cual sin una reglamentación adecuada pueden desbordarse y salir de un control, así pues, la apremiante necesidad de que en nuestro Código Penal vigente, se contemplen de una forma u otra.

Cada país contempló dichas normas de acuerdo a sus necesidades propias, (ya que algunos países se enfocaron propiamente a proteger el derecho a la privacidad, y a la propiedad intelectual, o como el que disponga de informaciones nominativas y haga un mal uso de ello; otros tantos a proteger al patrimonio de las personas afectadas como en los fraudes informáticos etcétera).

Sin embargo como se mencionó con anterioridad, nos ayudan y nos dan la pauta para que nuestros legisladores contemplen las figuras delictivas de "delitos informáticos", de acuerdo a nuestra realidad.

3.1.9 DELITOS INFORMATICOS RECONOCIDOS POR LA ORGANIZACIÓN DE NACIONES UNIDAS

Por su parte, el "Manual de la Naciones Unidas para la Prevención y Control de Delitos Informáticos" señala que cuando el problema se eleva a la escena internacional, se magnifican los inconvenientes y las insuficiencias, por cuanto los delitos informáticos constituyen una nueva forma de crimen transnacional y su combate requiere de una eficaz cooperación internacional concertada.

Asimismo, la ONU resume de la siguiente manera a los problemas que rodean a la cooperación internacional en el área de los delitos informáticos:

1.- Falta de acuerdos globales acerca de que tipo de conductas deben constituir delitos informáticos.
2.-Ausencia de acuerdos globales en la definición legal de dichas conductas delictivas.
3.-Falta de especialización de las policías, fiscales y otros funcionarios judiciales en el campo de los delitos informáticos.
4.-Falta de armonización entre las diferentes leyes procesales nacionales acerca de la investigación de los delitos informáticos.
5.-Carácter transnacional de muchos delitos cometidos mediante el uso de computadoras.
6.-Ausencia de tratados de extradición, de acuerdos de ayuda mutuos y de mecanismos sincronizados que permitan la puesta en vigor de la cooperación internacional.

En síntesis, es destacable que la delincuencia informática se apoya en el delito instrumentado por el uso de la computadora a través de redes telemáticas y la interconexión de la computadora, aunque no es el único medio.

Las ventajas y las necesidades del flujo nacional e internacional de datos, que aumenta de modo creciente aún en países latinoamericanos, conlleva también a la posibilidad creciente de estos delitos; por eso puede señalarse que *"la criminalidad informática constituye un reto considerable tanto para los sectores afectados de la infraestructura crítica de un país, como para los legisladores, las autoridades policiales encargadas de las investigaciones y los funcionarios judiciales."*[50]

Tipos de Delitos Informáticos reconocidos por la Organización de las Naciones Unidas:

Los Fraudes cometidos mediante manipulación de computadoras: este tipo de fraude informático conocido también como sustracción de datos, representa el delito informático más común.

La manipulación de programas; este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas que tienen conocimiento especializados en programación informática.

[50] Organización de Naciones Unidas. REVISTA INTERNACIONAL POLITICA CRIMINAL. . Nos. 43 y 44. Naciones Unidas, Nueva York.1994

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

Fraude efectuado por manipulación informáticas de los procesos de cómputo.

Falsificaciones informáticas; cuando se alteran datos de los documentos almacenados en forma computarizada.

Como instrumentos; las computadoras pueden utilizarse también para efectuar falsificación de documentos de uso comercial.

Sabotaje Informático; es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema.

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

Los Gusanos; los cuales son análogos al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse.

La Bomba lógica o cronológica; la cual exige conocimientos especializados ya que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro.

Acceso no autorizado a servicios u sistemas informáticos; esto es por motivos diversos desde la simple curiosidad, como en el caso de muchos piratas informáticos (hackers) hasta el sabotaje o espionaje informático.

Reproducción no autorizada de programas informáticos de protección legal; la cual trae una perdida económica sustancial para los propietarios legítimos.

Existe un Tratado de Cooperación Internacional para la Regulación del Internet y de la Represión e Investigación de los Delitos Cibernéticos.

Artículo 2 . La UNESCO será el organismo fundamental para llevar a cabo la lucha contra delincuentes cibernéticos a través de la comisión para la regulación de Internet (COMPRI) cuya función principal seria supervisar y vigilar el uso y manejo adecuado de la red , por parte del publico en general.....

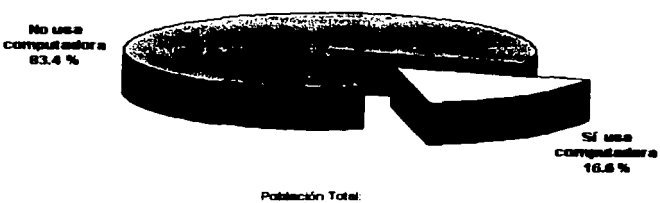
Artículo 7. Cuando la conducta se haya realizado en un país miembro y tenga efectos en uno que sea miembro o viceversa será competente el Tribunal Federal del país o la Corte Internacional de justicia de la O.N.U. a petición de los ofendidos que no sean miembros , y para los que forma parte, cuando no exista disposición legal en dicho pais.

3.2 LEGISLACION NACIONAL SOBRE DE DELITOS INFORMATICOS .

El Instituto Nacional de Estadística , Geografía e Informática realizo un censo en el año 2001 en todo el país, en donde el principal objetivo era dar datos estadísticos acerca de cuantas personas utilizaban computadoras en México y estos fueron los resultados.

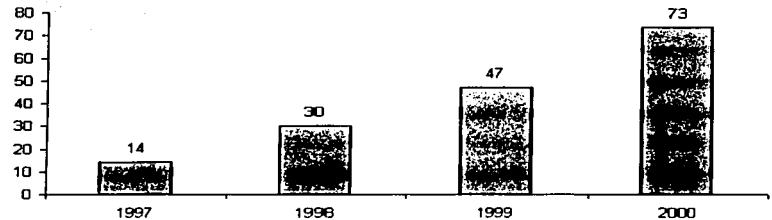
Para el año 2001 existía una población aproximada de 88,400,346 habitantes de los cuales mas de 14,674,000 personas ocupan computadoras, esto representa el 16.6 % del total de la población (Cuadro No 8).

POBLACIÓN QUE USA COMPUTADORA EN EL HOGAR 2001



Cuadro No.8

USUARIOS GUBERNAMENTALES DE INTERNET EN MEXICO
(MILES)



Fuente: Select-IDC

Por GLADYS SANCHEZ / Grupo Reforma

Ciudad de México (27 marzo 2003).-

México ocupa el octavo lugar como país utilizado por hackers para atacar sitios de Internet, según Hervért Hurtado, director general de Tráfico y Contrabando de la Policía Federal Preventiva.

Según la PFP , han sido desmanteladas 200 comunidades en Internet dedicadas a la pornografía infantil. Esto porque el País ha sido utilizado por "hackers" (piratas informáticos) para atacar o sabotear diversos sitios de Internet, dijo este jueves en el marco del Segundo Congreso Panamericano de Seguridad celebrado en la capital mexicana.

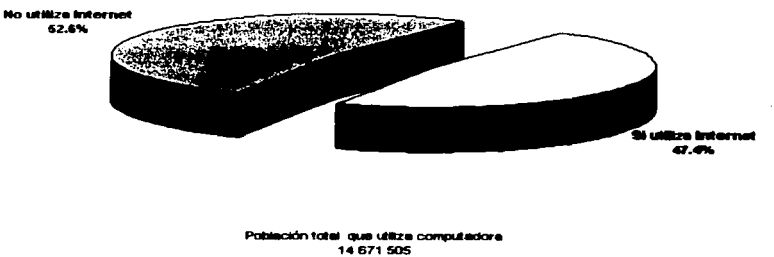
Por ello, argumentó, deben tomarse medidas para prevenir los delitos informáticos. De ahí que, recordó, fue creada la DC-México, grupo interdisciplinario que investiga delitos informáticos en el que participan la PFP, la Agencia Federal de Investigación, la Procuraduría capitalina, empresas de seguridad privada, académicos de diversas universidades y firmas de telecomunicaciones.

Los integrantes del grupo, señaló, trabajan en estrecho contacto con autoridades de Estados Unidos y de países de América Latina. Como parte de sus tareas, comentó, hacen "patrullajes en el ciberespacio" y entre los principales delitos que persiguen están la pornografía infantil, el fraude, la clonación de tarjetas inteligentes y el robo de señales televisivas, entre otros.

En el rubro de pornografía infantil, dijo Hurtado, se han detectado 257 comunidades que intercambian información, de las que 200 ya fueron desmanteladas.
Asimismo se localizaron 2 mil 317 correos electrónicos implicados con ese delito, de los que el 10 por ciento son proveedores de pornografía.Copyright ©
Grupo Reforma Servicio Informativo.

Del total de computadoras 14,671,505. Se calcula que el 47.4% utilizan Internet; es decir mas 6,954,000 personas utilizan internet dentro de sus actividades diarias como lo muestra el Cuadro No. 9

POBLACIÓN QUE UTILIZA INTERNET 2001



Cuadro No. 9

Según estadísticas realizadas por el Instituto Nacional de Estadística Geografía e Informática en el año 2001. La la iniciativa privada es la que tiene el mayor numero de adeptos a equipos de computo y al servico de internet después le sigue la administración y por último se encuentra el uso residencial.

El 70 por ciento de las operaciones de comercio electrónico en México se realizan en el segmento empresa - empresa. En México se estima también que hay más de 4 mil empresas que han incorporado a sus operaciones transacciones a través de medios electrónicos.

La mayoría de estas empresas utilizan el intercambio electrónico de datos (EDI) y muy pocas realizan transacciones a través de Internet.
El gobierno también juega en este proceso un papel importante en la tarea de promoción y desarrollo en el uso de la informática para mejorar el servicio a los usuarios.

La utilización de sistemas electrónicos e informáticos que hagan más eficientes las relaciones entre gobierno- empresas y ciudadanía en general, tiene un impacto positivo en la economía del país. En ese sentido, las dependencias gubernamentales trabajan para ofrecer mejores servicios a través de diferentes sistemas que están al servicio de los empresarios y entre los que destacan: el Sistema de Compras Gubernamentales.

COMPRANET; el Sistema de Información Empresarial, SIEM; el Sistema de Modernización Registral, SIGER; el Sistema de Comercialización, Precios y Promoción Interna, SICOMEPIPI, y el Registro Nacional de Vehículos, RENAVE.

3.2.1 CONSTITUCION POLITICA DE LOS ESTADOS UNIDOS MEXICANO.

A pesar de que día con día el uso de la computadora y de Internet va en aumento, quienes conforman la Asamblea Legislativa del Distrito Federal, minimizan el concepto y la magnitud del delito informático pero sobre todo; la importancia que en nuestros días tiene este medio de comunicación para gran parte de la población y en especial para el Estado por manejar la base de datos mas grande del país.

A continuación se mencionan algunos artículos Constitucionales y tratados que México a firmado a nivel internacional con otras Naciones que tienen relación con los Delitos Informáticos:

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

En nuestro país existe una regulación administrativa sobre las conductas ilícitas relacionadas con la informática, es por ello importante recurrir a aquellos tratados internacionales de los que el Gobierno de México es parte en virtud de que el artículo 133 Constitucional establece que todos los tratados celebrados por el Presidente de la República y aprobados por el Senado serán Ley Suprema de toda la Unión.

Artículo 133.

Esta Constitución, las leyes del Congreso de la Unión que emanen de ella y todos los tratados que estén de acuerdo con la misma, celebrados y que se celebren por el Presidente de la República, con aprobación del Senado, serán la Ley Suprema de toda la Unión.

Los jueces de cada Estado se arreglarán a dicha Constitución, leyes y tratados, a pesar de las disposiciones en contrario que pueda haber en las Constituciones o leyes de los Estados.

Entre los tratados más importantes que México ha firmado se encuentra el que fue realizado con Estados Unidos y Canadá.

Tratado de Libre Comercio de América del Norte (T.L.C.A.N.)

El sistema informático y/o de telecomunicaciones incluye básicamente software de diversas clases incluso de telecomunicaciones más sus redes, junto con información lógicamente organizada, o sea que incluye soporte lógico, soporte electromagnético e información.

Las tres cosas son los bienes jurídicos distintos o el objeto material diverso, que están previstos por normas específicas, y que no nos harían incurrir técnicamente en los llamados "tipos penales en blanco", porque:

1. En el caso de los programas o software la norma jurídica a la que remite el presente tipo penal, está contenida en la Ley Federal de

Derechos de Autor en su artículo 7° inciso "j" además de en otras disposiciones internacionales válidas en México como la Convención de Berna y la Convención Interamericana, y el TLC.

2. Y en el caso de los bancos de datos, entendidos como la "organización pertinente, combinación o arquitectura de programas y datos destinados a la consulta pertinente por un usuario", se encuentra protegida tanto por la Ley Federal de Derechos de Autor en su propio artículo 7° inciso "k", como por el Tratado de Libre Comercio de América del Norte bajo la calidad de compilación autoral, en su artículo 1705, 1, "b", e incluye tanto los programas que organizan y permiten la consulta, como la información almacenada a la que se da acceso, así como las comunicaciones, lo que configura el sistema de información propiamente dicho, y constituye el bien jurídico protegido por el tipo aquí propuesto.

3. La información, como quedó definida en la glosa al tipo 2.

El comité voto aprobatoriamente por introducir este tipo penal tal como se encuentra.Posteriormente los asesores del c. Subprocurador de control de procesos, de la P.G.R. dictaminaron la conveniencia de definir dentro del propio articulo, lo que es un sistema informático o de cómputo, así como también definir el sistema telemático o de teleinformática. Las definiciones que aquí se ofrecen deberán ser compulsadas con las existentes en los protocolos de la U.I.T.

Tratado subscrito por México, y en los demás tratados internacionales.

Este instrumento internacional firmado por el Gobierno de México, de los Estados Unidos y Canadá en 1993, contiene un apartado sobre propiedad intelectual, a saber la Sexta Parte, Capítulo XVII, en el que se contemplan los derechos de autor, patentes, otros derechos de propiedad intelectual y procedimientos de ejecución.

En términos generales, puede decirse que en ese apartado se establecen como parte de las obligaciones de los Estados signatarios en el área que se comenta, que deberán protegerse los programas de cómputo como obras literarias y las bases de datos como compilaciones, además de que deberán conceder derechos de renta para los programas de cómputo.

De esta forma, debe mencionarse que los tres Estados Parte de este Tratado también contemplaron la defensa de los derechos de propiedad intelectual (artículo 1714) a fin de que su derecho interno contenga procedimientos de defensa de los derechos de propiedad intelectual que permitan la adopción de medidas eficaces contra cualquier acto que infrinja los derechos de propiedad intelectual comprendidos en el capítulo específico del tratado.

En este orden y con objeto de que sirva para demostrar un antecedente para la propuesta que se incluye en el presente trabajo, debe destacarse el contenido del párrafo 1 del artículo 1717 denominado Procedimientos y Sanciones Penales en el que de forma expresa se contempla la figura de piratería de derechos de autor a escala comercial.

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

Asimismo, debe mencionarse que en el artículo 1711, relativo a los secretos industriales y de negocios sobre la provisión de medios legales para impedir que estos secretos sean revelados, adquiridos o usados sin el consentimiento de la persona que legalmente tenga bajo su control la información.

Llama la atención que en su párrafo 2 habla sobre las condiciones requeridas para otorgar la protección de los secretos industriales y de negocios y una de ellas es que éstos consten en medios electrónicos o magnéticos.

En resumen, las provisiones insertas en el articulado del TLC se ocupan básicamente de la protección a la propiedad intelectual, dejando a las legislaciones de cada país las sanciones a los delitos que se desprendan de las acciones contra los mencionados derechos.

Los organismos internacionales han tenido una intensa actividad para enfrentar la problemática de los delitos informáticos a fin incorporar a la vida jurídica la regulación de dichas conductas, tal es el caso de las siguientes organizaciones:

Organización de Cooperación y Desarrollo Económico (O.C.D.E.).

En este orden, debe mencionarse que durante los últimos años se ha ido perfilando en el ámbito internacional un cierto consenso en las valoraciones político - jurídicas de los problemas derivados del mal uso que se les da a las computadoras, lo cual da lugar a que en algunos casos, se modifiquen las leyes de Derecho Penal de algunos países.

En un primer término, debe considerarse que en 1983, la OCDE inició un estudio de la posibilidad de aplicar y armonizar en el plano internacional las leyes penales a fin de luchar contra el problema del uso indebido de los programas computaciones.

Las posibles implicaciones económicas de la delincuencia informática, su carácter internacional y el peligro de que la diferente protección jurídico - penal nacional pudiera perjudicar el flujo internacional de información, condujeron en consecuencia a un intercambio de opiniones y de propuestas de solución.

Sobre la base de las posturas y de las deliberaciones surgió un análisis y valoración iuscomparativista de los derechos nacionales aplicables así como de las propuestas de reforma.

Las conclusiones política - jurídicas desembocaron en una lista de las acciones que pudieran ser consideradas por los Estados, por regla general, como merecedoras de pena.

La Organización de Cooperación y Desarrollo Económico que en 1986 publicó un informe titulado Delitos de Informática:

Análisis de la Normativa Jurídica, en donde se reseñaban las normas legislativas vigentes y las propuestas de reforma en diversos Estados Miembros y se recomendaba una lista mínima de ejemplos de uso indebido que los países podrían prohibir y sancionar en leyes penales (Lista Mínima).

Por ejemplo el fraude y la falsificación informáticos, la alteración de datos y programas de computadora, sabotaje informático, acceso no autorizado, interceptación no autorizada y la reproducción no autorizada de un programa de computadora protegido.

La mayoría de los miembros de la Comisión Política de Información, Computadoras y Comunicaciones recomendó también que se instituyesen protecciones penales contra otros usos indebidos (Lista Optativa o Facultativa).

Como espionaje informático, utilización no autorizada de una computadora, utilización no autorizada de un programa de computadora protegido, incluido el robo de secretos comerciales, y el acceso o empleo no autorizado de sistemas de computadoras.
Con objeto de que se finalizara la preparación del informe de la OCDE, el Consejo de Europa inició su propio estudio sobre el tema a fin de elaborar directrices que ayudasen a los sectores legislativos a determinar qué tipo de conducta debía prohibirse en la legislación

penal y la forma en que debía conseguirse ese objetivo, teniendo debidamente en cuenta el conflicto de intereses entre las libertades civiles y la necesidad de protección.

La Lista Mínima preparada por la OCDE se amplió, añadiéndose a ella otros tipos de abuso que se estimaba merecían la aplicación de la legislación penal.

El Comité Especial de Expertos sobre Delitos Relacionados con el Empleo de las Computadoras, del Comité Europeo para los Problemas de la Delincuencia, examinó esas cuestiones y se ocupó también de otras, como la protección de la esfera personal, las víctimas, las posibilidades de prevención, asuntos de procedimiento como la investigación y confiscación internacional de bancos de datos y la cooperación internacional en la investigación y represión del delito informático.

Una vez desarrollado todo este proceso de elaboración de las normas a nivel continental, el Consejo de Europa aprobó la recomendación R(89)9 sobre delitos informáticos, en la que se "recomienda a los gobiernos de los Estados Miembros que tengan en cuenta cuando revisen su legislación o preparen una nueva, el informe sobre la delincuencia relacionada con las computadoras .

Y en particular las directrices para los legisladores nacionales". Esta recomendación fue adoptada por el Comité de Ministros del Consejo de Europa el 13 de septiembre de 1989.

Las directrices para los legisladores nacionales incluyen una lista mínima, que refleja el consenso general del Comité, acerca de determinados casos de uso indebido de computadoras y que deben incluirse en el Derecho Penal, así como una lista facultativa que describe los actos que ya han sido tipificados como delitos en algunos Estados pero respecto de los cuales no se ha llegado todavía a un consenso internacional en favor de su tipificación.

Adicionalmente, en 1992, la OCDE elaboró un conjunto de normas para la seguridad de los sistemas de información, con intención de ofrecer las bases para que los Estados y el sector privado pudieran erigir un marco de seguridad para los sistemas informáticos.

Organización Mundial De Comercio (O.M.C.)

Al inicializar el contenido de este apartado, debemos aclaran que si bien la institución del GATT se transformó en lo que hoy conocemos como la Organización Mundial de Comercio (OMC), todos los acuerdos que se suscribieron en el marco del GATT siguen siendo vigentes.

En este entendido, cabe mencionar que el Gobierno de México es parte de este acuerdo que se celebró en el marco de la Ronda Uruguay del Acuerdo General de Aranceles Aduaneros y Comercio (GATT) manteniendo su vigencia hasta nuestros días.

Es de destacarse el hecho de que en este acuerdo, en el artículo 10 relativo a los programas de ordenador y compilaciones de datos, se establece que este tipo de programas, ya sean fuente u objeto, serán protegidos como obras literarias de conformidad con el Convenio de Berna de 1971 para la Protección de Obras Literarias y Artísticas, y que las compilaciones de datos posibles de ser legibles serán protegidos como creaciones de carácter intelectual.

Además, en la parte III sobre observancia de los derechos de propiedad intelectual, en la sección I de obligaciones generales, específicamente en el artículo 41, se incluye que los miembros del Acuerdo velarán porque en su respectiva legislación nacional se establezcan procedimientos de observancia de los derechos de propiedad intelectual.

Asimismo, en la sección 5, denominada Procedimientos Penales, en particular el artículo 61, se establece que para los casos de falsificación dolosa de marcas de fábrica o de comercio o de piratería lesiva del derecho de autor a escala comercial, se establecerán procedimientos y sanciones penales además de que, "los recursos disponibles comprenderán la pena de prisión y/o la imposición de sanciones pecuniarias ".

Finalmente, en la parte VII, denominada Disposiciones Institucionales, Disposiciones Finales, en el artículo 69 relativo a la cooperación internacional, se establece el intercambio de información y la cooperación entre las autoridades de aduanas en lo que se refiere al

comercio de mercancías de marca de fábrica o de comercio falsificadas y mercancías pirata que lesionan el derecho de autor.

Como se observa, el tratamiento que los dos instrumentos internacionales que se han comentado otorgan a las conductas ilícitas relacionadas con las computadoras es en el marco del derecho de autor.

En este entendido, cabe destacar que el mismo tratamiento que le han conferido esos acuerdos internacionales a las conductas antijurídicas antes mencionadas, es otorgado por la Ley Federal del Derecho de Autor .

Ley Federal de Derechos de Autor en México.

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

Esta ley regula todo lo relativo a la protección de los programas de computación, a las bases de datos y a los derechos autorales relacionados con ambos.

Se define lo que es un programa de computación, su protección, sus derechos patrimoniales, de arrendamiento, casos en los que el usuario podrá realizar copias del programa que autorice el autor del mismo,

las facultades de autorizar o prohibir la reproducción, la autorización del acceso a la información de carácter privado relativa a las personas contenida en las bases de datos, la publicación, reproducción, divulgación, comunicación pública y transmisión de dicha información, establece las infracciones y sanciones que en materia de derecho de autor deben ser aplicadas cuando ocurren ilícitos relacionados con los citados programas y las bases de datos, etcétera.

En este sentido, consideramos importante detenernos en los artículo 102 y 231, el primero de ellos, regula la protección de los programas de computación y señala además que los programas de cómputo que tengan por objeto causar efectos nocivos a otros programas o equipos, lógicamente no serán protegidos.

El segundo en su fracción V sanciona el comercio de programas de dispositivos o sistemas cuya finalidad sea desactivar dispositivos electrónicos de protección de un programa de cómputo.

3.2.2 LEY ORGANICA DE LA ADMINISTRACION PUBLICA FEDERAL

La Ley Orgánica de la Administración Publica a través de sus Secretarias debería de vigilar el contenido de todo aquello que se transmite o publica a través de equipos de computo y de Internet como lo hace la Secretaria de Gobernación en trasmisiones de radio y televisión .

Por otro lado la Secretaria de Relaciones Exteriores será una fuente importante para actualizar nuestra legislación.

A través de estos convenios, acuerdos y tratados podremos darle un enfoque diferente a los delitos informáticos, porque podremos unificar conceptos o delitos que tan bien se han sucitado en otros países o que podríamos prevenir .

ARTÍCULO 27.- A la Secretaría de Gobernación corresponde el despacho de los siguientes asuntos:

I.-.....
II.-.....
III.-.....
IV.-.....
V.-.....
XXI.- Vigilar que las publicaciones impresas y las transmisiones de radio y televisión, así como las películas cinematográficas, se mantengan dentro de los límites del respeto a la vida privada, a la paz y moral pública y a la dignidad personal, y no ataquen los derechos de terceros, ni provoquen la comisión de algún delito o perturben el orden público;

ARTÍCULO 28.- A la Secretaría de Relaciones Exteriores corresponde el despacho de los siguientes asuntos:
I.- Promover, propiciar y asegurar la coordinación de acciones en el exterior de las dependencias y entidades de la administración pública

federal; y sin afectar el ejercicio de las atribuciones que a cada una de ellas corresponda, conducir la política exterior, para lo cual intervendrá en toda clase de tratados, acuerdos y convenciones en los que el país sea parte;

3.2.3 CODIGOS PENALES DE LOS ESTADOS DE LA REPUBLICA MEXICANA.

Actualmente dos Estados de la Republica Mexicana regulan el delito informático dentro de sus supuestos penales, en ambos casos en delitos contra el patrimonio, pero esto nos hace reflexionar que nuestro país no es inmune a los Delitos Informáticos .

CÓDIGO PENAL Y DE PROCEDIMIENTOS PENALES DE SINALOA.

Libro Segundo.
Título Décimo "Delitos Contra el Patrimonio" .

Capítulo V. **Delito Informático** .
Artículo 217. Comete delito informático, la persona que dolosamente y sin derecho:

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

II. Intercepte, interfiera, reciba, use, altere, dañe o destruya un soporte lógico o programa de computadora o los datos contenidos en la misma, en la base, sistema o red. Al responsable de delito informático se le impondrá una pena de seis meses a dos años de prisión y de noventa a trescientos días multa.

CODIGO PENAL DE AGUASCALIENTES.

Libro Segundo.
Titulo Vigésimo Primero. Delitos contra la seguridad en los medios informáticos y magnéticos.

Capitulo I. **Acceso sin Autorización**.
Artículo 223.- El Acceso sin Autorización consiste en interceptar, interferir, recibir, usar o ingresar por cualquier medio sin la autorización debida o excediendo la que se tenga a un sistema de red de computadoras, un soporte lógico de programas de software o base de datos.

Al responsable de Acceso sin Autorización se le sancionará con penas de 1 a 5 años de prisión y de 100 a 400 días multa.
Cuando el Acceso sin Autorización tengan por objeto causar daño u obtener beneficio, se sancionará al responsable con penas de 2 a 7 años de prisión y de 150 a 500 días de multa.

También se aplicarán las sanciones a que se refiere el párrafo anterior cuando el responsable tenga el carácter de técnico, especialista o

encargado del manejo, administración o mantenimiento de los bienes informáticos accesados sin autorización o excediendo la que se tenga.

Capitulo II. **Daño Informático**.

Artículo 224.- El Daño Informático consiste en la indebida destrucción o deterioroparcial o total de programas, archivos, bases de datos o cualquier otro elemento intangible contenido en sistemas o redes de computadoras, soportes lógicos o cualquier medio magnético.

Al responsable de Daño Informático se le sancionará de 1 a 5 años de prisión y de 100 a 400 días de multa.
Se le aplicarán de 2 a 7 años de prisión y de 150 a 500 días multa, cuando el responsable tenga el carácter de técnico especialista o encargado del manejo, administración o mantenimiento de los bienes informáticos dañados.

Artículo 225.- Cuando el Acceso sin Autorización o el Daño Informático se cometan culposamente se sancionarán con penas de 1 mes a 3 años de prisión y de 50 a 250 días multa.

Artículo 226.- La Falsificación Informática consiste en la indebida modificación, alteración o imitación de los originales de cualquier dato, archivo o elemento intangible contenido en sistema de redes de computadoras, base de datos, soporte lógico o programas.

Al responsable del delito de Falsificación Informática se le aplicarán de 1 a 5 años de prisión y de 100 a 400 días multa.

Las mismas sanciones se aplicarán al que utilice o aproveche en cualquier forma bienes informáticos falsificados con conocimiento de esta circunstancia.
Se aplicarán de 2 a 7 años de prisión y de 150 a 500 días multa, cuando el responsable tenga el carácter de técnico, especialista o encargado del manejo, administración o mantenimiento de los bienes informáticos falsificados.

Es evidente que el delito informático poco a poco se empieza ha hacer presente a través de supuestos penales que protegen bienes jurídicos tutelados, que puedan ser vulnerados por tecnología informática.

3.2.4 CODIGO PENAL PARA EL DISTRITO FEDERAL. (Derogado y Vigente).

Un gran avance fue considerar el Acceso Ilícito a Sistema y Equipos de Informática como supuestos penales que podían ser susceptibles a una pena o medida de seguridad, era un excelente inicio para legislar en materia de Delitos Informáticos, pero desgraciadamente fueron derogados estos artículos, para dar paso al Nuevo Código Penal para el Distrito Federal .

CODIGO PENAL PARA EL DISTRITO FEDERAL (Derogado).
Libro Segundo.
Titulo Noveno . Revelación de Secretos y Acceso ilícito a Sistemas y

Equipos de Informática. (Derogado)

Capitulo II . **Acceso Ilícito a Sistemas y Equipos de Informática**

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

Artículo 211 BIS 2.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.
Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

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 cincuenta días multa.

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

Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero,

indebidamente copie información que contengan, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

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

Artículo 211 BIS 6.- Para los efectos de los artículos 211 Bis 4 y 211 Bis 5 anteriores, se entiende por instituciones que integran el sistema financiero, las señaladas en el artículo 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.

CODIGO PENAL VIGENTE PARA EL DISTRITO FEDERAL.

Libro Segundo
Titulo Décimo Tercero. Delitos Contra La Intimidad Personal y la Inviolabilidad del Secreto.
Capitulo I. **Violación de la Intimida Personal.**
ARTÍCULO 212. Se impondrá de seis meses a tres años de prisión, al que sin consentimiento de quien esté legitimado para otorgarlo y, para conocer asuntos relacionados con la intimidad de la persona:

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

II. Utilice medios técnicos para escuchar, observar, grabar la imagen o el sonido.
Este delito se perseguirá por querella.

Capitulo II. **Revelación de Secretos**.
ARTÍCULO 213. Al que sin consentimiento de quien tenga derecho a otorgarlo y en perjuicio de alguien, revele un secreto o comunicación reservada, que por cualquier forma haya conocido o se le haya confiado, o lo emplee en provecho propio o ajeno, se le impondrán prisión de seis meses a dos años y de veinticinco a cien días multa.

Si el agente conoció o recibió el secreto o comunicación reservada con motivo de su empleo, cargo, profesión, arte u oficio, o si el secreto fuere de carácter científico o tecnológico, la prisión se aumentará en una mitad y se le suspenderá de seis meses a tres años en el ejercicio de la profesión, arte u oficio.
Cuando el agente sea servidor público, se le impondrá, además, destitución e inhabilitación de seis meses a tres años.

Libro Segundo
Titulo Vigésimo Tercero. Delitos Contra la Seguridad y el Normal Funcionamiento de las Vías de Comunicación y de los Medios de Transporte.

Capitulo I. **Ataques a las Vías de Comunicación y a los Medios de Transporte .**

Articulo 330 .- .....

Artículo 331.- Se impondrá de uno a cuatro años de prisión y de cien a cinco mil días de multa, al que:

I .- Dañe, altere, interrumpa obstaculice, destruya alguna vía o medio local de comunicación, de transporte, público o de transmisión de energía: o

II.- Interrumpa o dificulte el servicio público local de comunicaciones o de transporte obstaculizando alguna vía local de comunicaciones reteniendo algún medio local de transporte publico de pasajeros, de carga o cualquier otro medio local de comunicación.

Si el medio de transporte a que se refiere a este articulo estuviere ocupado por una o mas personas, las penas se aumentaran en una mitad .

Si alguno de los hechos a que se refiere este articulo , se ejecuta por medio de violencia , la pena se aumentara en dos tercios. Estas sanciones se impondrán con independencia de las que procederán si se ocasiona algún otro ilícito.

Capitulo III . **Violación de Correspondencia.**

Articulo 333. Al que abra o intercepte una comunicación escrita que no este dirigida a él, se le impondrá de treinta a noventa dias multa .

No se sancionara a quien en ejercicio de la patria potestad ,tutela o custodia , abra o intercepte la comunicación escrita dirigida a la persona que se halle bajo su patria potestad , tutela o custodia.

Los delitos previstos en este artículo se perseguirán por querella.

Capítulo IV . **Violación de la Comunicación Privada**.
Articulo334.-A quien intervenga comunicaciones privadas sin mandato de autoridad judicial competente , se le impondrán de dos a ocho de prisión y de cien mil días multa.
A quien revele, divulgue (sic) utilice indebidamente, o en perjuicio de otro, información o imágenes obtenidas o en una intervención de comunicación privada, se le impondrá de tres a doce años de prisión y de doscientos a mil multa.

3.2.5 LEY DE VIAS GENERALES DE COMUNICACIÓN.

En la actualidad la Ley de Vías Generales de Comunicación se regula a través Disposiciones Generales como concesiones, permisos y contratos, derechos de expropiación uso de bienes nacionales y franquicias, explotación de vías generales de comunicación etc.

En esta legislación tenemos contemplado al telégrafo que durante mucho tiempo fue un medio de comunicación importante pero en nuestros días esta a punto de volverse obsoleto , es tiempo de dar paso a nuevos medios de comunicación y empezar a legislar en materia informática para evitar posibles delitos que se empiezan a manifestar a nivel mundial.
Hacemos una especial mención en la Ley de Vías Generales de Comunicación porque aun cuando a legislado en materia de la Red

Nacional ,Telégrafos y de el Servicio Postal no a podido actualizar su normatividad a nuevos medios de comunicación como es el caso especifico de la Informática .

3.2.6 LEY FEDERAL DE TELECOMUNICACIONES.

La transferencia de datos tan importante en nuestros días, para estudiantes, empresas y para el mismo Estado, aun no se le ha dado la debida importancia.
La Ley de Telecomunicaciones es fundamental para tomar en consideración las nuevas tecnologías en el caso especifico de Equipos de computo e Internet ,ya que en esta ley se manejan definiciones, aspectos esenciales y generalizados acerca de los medios de comunicación.

El artículo 7 fracción III nos menciona que podrá Expedir las Normas Oficiales Mexicanas en Materia de Telecomunicaciones y otras disposiciones administrativas; este seria el fundamento para crear un Glosario en materia informática como lo hace esta misma ley en su articulo 3, dando definiciones para una mejor comprensión de la ley.

En donde el legislador que se encuentre ante un caso de Delito informático, pueda remitirse para conocer aspectos generales de la informática en donde se especifique que es una computadora , que es software , que es hardware , que es un ISP ,un DNS, un POP, que significa la www, que es un correo electrónico , que significa

Archivo , un disquete , que es un Cd Wrriter, un Cd Rom, DVD , para que sirve un Servidor, que es Servidor Proxy, que es un Router un Swich , y definir la diversidad de virus que existen etc.

Capitulo I .Disposiciones Generales.
Artículo 1.-La presente Ley es de orden público y tiene por objeto regular el uso, aprovechamiento y explotación del espectro radioeléctrico, de las redes de telecomunicaciones, y de la comunicación vía satélite.

Artículo 2.-Corresponde al Estado la rectoría en materia de telecomunicaciones, a cuyo efecto protegerá la seguridad y la soberanía de la Nación.
En todo momento el Estado mantendrá el dominio sobre el espectro radioeléctrico y las posiciones orbitales asignadas al país.

Artículo 3.-Para los efectos de esta Ley se entenderá por:
I. Banda de frecuencias: porción del espectro radioeléctrico que contiene un conjunto de frecuencias determinadas;
II. Espectro radioeléctrico: el espacio que permite la propagación sin guía artificial de ondas electromagnéticas cuyas bandas de frecuencias se fijan convencionalmente por debajo de los 3,000 gigahertz;
III. Estación terrena: la antena y el equipo asociado a ésta que se utiliza para transmitir o recibir señales de comunicación vía satélite;
IV. Frecuencia: número de ciclos que por segundo efectúa una onda del espectro radioeléctrico;

V. Homologación: acto por el cual la Secretaria reconoce oficialmente que las especificaciones de un producto destinado a telecomunicaciones satisfacen las normas y requisitos establecidos, por lo que puede ser conectado a una red pública de telecomunicaciones, o hacer uso del espectro radioeléctrico;

VI. Orbita satelital: trayectoria que recorre un satélite al girar alrededor de la tierra;

VII. Posiciones orbitales geoestacionarias: ubicaciones en una órbita circular sobre el Ecuador que permiten que un satélite gire a la misma velocidad de rotación de la tierra, permitiendo que el satélite mantenga en forma permanente la misma latitud y longitud;

VIII. Red de telecomunicaciones: sistema integrado por medios de transmisión, tales como canales o circuitos que utilicen bandas de frecuencias del espectro radioeléctrico, enlaces satelitales, cableados, redes de transmisión eléctrica o cualquier otro medio de transmisión, así como, en su caso, centrales, dispositivos de conmutación o cualquier equipo necesario;

IX. Red privada de telecomunicaciones: la red de telecomunicaciones destinada a satisfacer necesidades específicas de servicios de telecomunicaciones de determinadas personas que no impliquen explotación comercial de servicios o capacidad de dicha red;

X. Red pública de telecomunicaciones: la red de telecomunicaciones a través de la cual se explotan comercialmente servicios de telecomunicaciones. La red no comprende los equipos terminales de telecomunicaciones de los usuarios ni las redes de telecomunicaciones que se encuentren más allá del punto de conexión terminal;

XI. Secretaría: la Secretaría de Comunicaciones y Transportes;
XII. Servicios de valor agregado: los que emplean una red pública de telecomunicaciones y que tienen efecto en el formato, contenido, código, protocolo, almacenaje o aspectos similares de la información transmitida por algún usuario y que comercializan a los usuarios información adicional, diferente o reestructurada, o que implican interacción del usuario con información almacenada;
XIII. Sistema de comunicación vía satélite: el que permite el envío de señales de microondas a través de una estación transmisora a un satélite que las recibe, amplifica y envía de regreso a la Tierra para ser captadas por estación receptora, y
XIV. Telecomunicaciones: toda emisión, transmisión o recepción de signos, señales, escritos, imágenes, voz sonidos o información de cualquier naturaleza que se efectúa a través de hilos, radioelectricidad, medios ópticos, físicos, u otros sistemas electromagnéticos.

Artículo 4.-Para los efectos de esta Ley, son vías generales de comunicación el espectro radioeléctrico, las redes de telecomunicaciones y los sistemas de comunicación vía satélite

Artículo 5.-Las vías generales de comunicación materia de esta Ley y los servicios que en ellas se presten son de jurisdicción federal.
Para los efectos de esta Ley se considera de interés público la instalación, operación, y mantenimiento de cableado subterráneo y aéreo y equipo destinado al servicio de las redes públicas de telecomunicaciones, debiéndose cumplir las disposiciones estatales y

municipales en materia de desarrollo urbano y protección ecológica aplicables.

Artículo 7.-La presente Ley tiene como objetivos promover un desarrollo eficiente de las telecomunicaciones; ejercer la rectoría del Estado en la materia, para garantizar la soberanía nacional; fomentar una sana competencia entre los diferentes prestadores de servicios de telecomunicaciones a fin de que éstos se presten con mejores precios, diversidad y calidad en beneficio de los usuarios, y promover una adecuada cobertura social.
Para el logro de estos objetivos, corresponde a la Secretaría, sin perjuicio de las que se confieran a otras dependencias del Ejecutivo Federal, el ejercicio de las atribuciones siguientes:

I. Planear, formular y conducir las políticas y programas, así como regular el desarrollo de las telecomunicaciones, con base en el Plan Nacional de Desarrollo y los programas sectoriales correspondientes;
II. Promover y vigilar la eficiente interconexión de los diferentes equipos y redes de telecomunicación;
III. Expedir las normas oficiales mexicanas en materia de telecomunicaciones y otras disposiciones administrativas;
IV. Acreditar peritos en materia de telecomunicaciones;
V. Establecer procedimientos para homologación de equipos;
VI. Elaborar y mantener actualizado el Cuadro Nacional de Atribución de Frecuencias;

Capitulo IX: Infracciones y Sanciones .

IV ARGUMENTOS PARA ADICIONAR LOS DELITOS INFORMÁTICOS EN MATERIA DE VÍAS DE COMUNICACIÓN Y CORRESPONDENCIA DEL CÓDIGO PENAL PARA EL D. F.

4.1 DERECHO A LA LIBERTAD DE EXPRESIÓN Y LIBRE ACCESO A LA INFORMACIÓN

Dos de los derechos mas defendidos en los países en los que existe un avanzado desarrollo en el área de delitos informáticos; es el Derecho a la información y el derecho a la libertad de expresión que nuestra constitución contempla en el articulo sexto y séptimo respectivamente.

En todo momento el legislador deberá tener presente estas dos garantías individuales y sus respectivas restricciones a razón de no causar perjuicio contra los derechos de terceras personas.

Derecho a la Información.

El Derecho a la información se encuentra en nuestra Constitución Política de los Estados Unidos Mexicanos en su Artículo 6º que a la letra dice: La manifestación de las ideas no será objeto de ninguna inquisición judicial o administrativa, sino en el caso de que ataque a la moral, los derechos de tercero, provoque algún delito o perturbe el orden público; el derecho a la información será garantizado por el Estado.

Aun cuando el Derecho a la información en las ultimas décadas ha estado auxiliado de medios tecnológicos, el libre acceso a la información siempre a estado supeditado al Estado, desde tiempos remotos los gobiernos se encargan de limitar la información a sus gobernados y hasta nuestros días no toda la información sale a la luz pública, la verdad es que mucha información no se difunde a la población ,siempre a existido una limitante en cuanto a la información que se debe dar a conocer, para evitar una revuelta social por aspectos políticos, económicos, culturales o de salud etc. solo por mencionar algunos supuestos .

El derecho a la información y la libertad de expresión no debe violar la privacidad del individuo, ni transgredir los derechos de terceras personas, es indispensable hacer una distinción, entre la información de una persona, de una empresa y del Estado.

Libertad de expresión.

Constitución Política de los Estados Unidos Mexicanos Artículo 7º. Es inviolable la libertad de escribir y publicar escritos sobre cualquier materia. Ninguna ley ni autoridad puede establecer la previa censura, ni exigir fianza a los autores o impresores, ni coartar la libertad de imprenta, que no tiene más límites que el respeto a la vida privada, a la moral y a la paz pública. En ningún caso podrá secuestrarse la imprenta como instrumento del delito.
Las leyes orgánicas dictarán cuantas disposiciones sean necesarias para evitar que so pretexto de las denuncias por delitos de prensa,

sean encarcelados los expendedores, "papeleros", operarios y demás empleados del establecimiento de donde haya salido el escrito denunciado, a menos que se demuestre previamente la responsabilidad de aquéllos.

Algo que ha caracterizado al hombre de los demás seres de la naturaleza, es la facultad de concebir ideas y poderlas transmitir a sus semejantes.

Por eso la libertad de expresión es el Derecho que caracteriza al ser humano, la necesidad del hombre para comunicarse a través de medios de comunicación mas sofisticados desde el correo ,el telégrafo, el teléfono , la radio , la televisión, la computadora, los satélites , próximamente, los hologramas virtuales y por supuesto la teletransportación .

La libertad de expresión nunca debe de afectar derechos de terceros, sin embargo ; en el momento que se lanza un virus en una red pública o privada como forma de manifestación en contra de algo o alguien el Derecho a la Libertad de expresión deja de existir .

En los últimos años la COMPUTADORA e INTERNET son sin duda el máximo exponente de la libertad de expresión y al mismo tiempo del derecho a la información puedes encontrar paginas de lo que tu quieras, desde vídeo juegos hasta la pagina de las fuerzas armadas de la nación mas poderosa del mundo y también puedes publicar lo que tu quieras y compartir con los usuarios de la red.

Este tema es muy interesante dado que algunos se interesan mas por ocultar la información y otros se dedican a investigarla a costa de cualquier cosa (Derecho a la Información), los medios de comunicación como radio, televisión y prensa se han encargado de mantener informada a la opinión pública a cerca de los acontecimientos que día con día suceden en el país y en el mundo entero.

La funcionalidad de la computadora y de Internet permitió compartir información de conexiones punto a punto , e inclusive de un país a otro, debido a lo accesible y multifunción al que resultaba utilizarlas, no solo podías almacenar tu información ahora también podías compartirla con otros usuarios (Libertad de Expresión) no importando el tema o la cantidad, así fuese un libro entero escaneado, imagen , audio o vídeo la información a gran escala la tendrías a la mano con un clic de tu mouse.

Debido a la expansión que ha tenido la informática en todo el mundo, empiezan a aparecer múltiples delitos conocidos y tipificados pero con un nuevo "modus operandi", que con ayuda de la computadora se hacen más sencillos de realizar (En cuestión de segundos), esto hace prácticamente imposible detectar este tipo de ilícitos.

La Organización de Naciones Unidas realiza su mejor esfuerzo, pero es indispensable que cada país empiece a regular el delito informático dependiendo de las necesidades de su población ya que no podemos comparar a Estados Unidos con México.

El Código Civil , el de Comercio ,el Fiscal ,La Procuraduría Federal del Consumidor , se preparan para los contratos e impuestos a través de Internet, es indispensable que el Código Penal prevenga por medio de sus supuestos jurídicos, algunas conductas delictivas referentes al delito informático que ya han sido detectadas como, delitos en accesos a sistemas y equipos de informática, clonación de tarjetas de crédito, billetes falsos a través de equipos de computo, piratería de software, falsificación de documentos etc.

4.2 NECESIDAD DE LEGISLAR LAS HERRAMIENTAS DE INTERNET EN LA LEY FEDERAL DE TELECOMUNICACIONES

"Los adelantos científicos y técnicos junto con el desarrollo económico y social dan a los medios de comunicación y a la información un carácter masivo y mundial a tal grado que ningún hombre o nación puede vivir aislado , el crecimiento de la actividad humana en los últimos siglos hace que comunicación e información sean presupuestos básicos para el desarrollo y formación de la conducta individual y social."[51]

Cabe la posibilidad de que en todas las herramientas de Internet puedan cometerse delitos que hasta el momento puedan tipificarse con el Código Penal, el problema radica en que cada vez son mas los delitos que están relacionados con las computadoras.

---

[51] Lopez Aylon, Sergio . EL DERECHO A LA INFORMACION. México. Editorial Porrua. 1984

Las Herramientas de Internet pueden ocultar delitos informáticos es por ello que debemos conocerlas algunas están prácticamente en desuso pero otras cada día tienen mayor importancia .

world wide web .

La www también conocida como la "web" o "w3" es la aplicación mas popular de Internet y la abreviatura world wide web o telaraña de red mundial ,es un gran conjunto de paginas que son identificadas por nombres que son colocados por el propietario, para que las personas lo identifiquen , por el dominio que puede ser de un proveedor de Internet o de la compañía (prodigy , yahoo, telmex) y por ultimo por letras que ha sido asignadas a cada país (mx) .

Pueden contener imágenes y texto del tema relacionadas con otras paginas, de ahí el sobre nombre de Telaraña. Una página puede contener texto, imagen, sonido, video y sobre todo hipermedios enlaces o vínculos con otras paginas, es indispensable llevar un mejor control de paginas en Internet al menos las nacionales, crear una base de datos de cada pagina publicada en México, ya sea por persona física o moral , nacional o internacional,

ya que cada vez son mas las paginas que contienen pornografía infantil o que te enseñan a fabricar petardos y bombas caseras sin que el contenido de las mismas sea analizado y restringido por la Secretaria de Gobernación como lo hacen cada vez que sale algún spot publicitario de algún programa de televisión o radio .

Correo Electrónico

El correo electrónico es el intercambio de mensajes entre usuarios , es mas rápido que el correo normal , mas barato que una conversación telefónica y esta disponible en todo momento.
Un mensaje de correo electrónico esta formado generalmente por un texto, pero también puede añadirse cualquier archivo adjunto (audio, imagen video).

El usuario redacta un mensaje utilizando el software de correo electrónico de su computadora.
El mensaje es recibido por el programa de correo electrónico del proveedor de servicio al cual se encuentra suscrito el remitente.
El mensaje viaja a través de la red.
El programa de correo electrónico de la computadora destino deposita el mensaje en el buzón del destinatario.
El destinatario utiliza el software de correo electrónico para leer los mensajes recibidos.

El correo electrónico tiene muchísimas bondades pero también ha sido una herramienta para cometer delitos de hostigamiento, de robo de los mensajes, de daño a la propiedad a través de virus informáticos que viajan a través del correo electrónico u otro medio y destruyen tu información, además de que en algunas ocasiones dejan inservible la computadora ya que el virus recorre en su totalidad al sistema operativo , a través de ellos se fomenta la pedofilia y un fenómeno llamado snoff (Violencia extrema , real).

El correo electrónico podrá ser revisado por la policía cibernética siempre y cuando exista una orden respaldada por el juez que en ese momento este conociendo de el asunto para poder fincar responsabilidad en el delito que se le acuse .

Transferencia de Archivos FTP

Dentro de la comunidad de Internet el Sistema FTP es un servidor que proviene de servir lo cual es representativo de sus función puesto que un ordenador de este tipo le sirve a usted archivos y programas la abreviatura FTP significa FILE TRANSFER PROTOCOL y son las regulaciones técnicas según las cuales se debe descargar un programa de Internet en su propio ordenador o computadora .

Puedes bajar todo tipo de software desde recetas de cocina, música , juegos y programas que pretenden facilitarle el trabajo, violando en muchos de los casos Derechos de Autor en el caso de publicaciones, de música , de juegos etc. Es por ello que el Derecho de Autor es el principal tema de discusión actualmente de la red de Internet ,es indispensable darles un nuevo enfoque y considerarlo como un bien jurídico tutelado que ha sido afectado por los Delitos Informáticos .

Acceso Remoto (TELNET).

En la actualidad Telnet esta en decadencia pero no a dejado de existir es por ello que se debe poner un énfasis en este tipo de

servicios ya que son usados por delincuentes que son especialistas en materia informática en donde la policía cibernética nada ha podido hacer ya que son códigos complejos que muy pocas veces se sabe en donde van a operar y que son operaciones imposibles de detener pueden mantener un servidor de cualquier compañía sin servicio durante muchísimas horas ya que desde una computadora ubicada en tu hogar puedes entrar .

El caso mas sonado a nivel mundial sucedió en 1982 por un chico de 15 años que se metió a la base de datos del pentágono.
Inclusive han dejado sin servicio telefónico una ciudad entera sin que se sepa el lugar desde donde esta operando el criminal es por ello que son accesos remotos porque desde tu computadora personal puedes dar ordenes al servidor de que hacer o dejar de hacer .

Grupo de Noticias.

Es el medio de comunicación por excelencia para estar informado del acontecer mundial sin embargo algunos grupos de noticias van mas haya del suceso mundial existen desde los noticiarios en Internet al desnudo , noticias de algunas sectas , grupo terrorista o sitios donde se puede comercializar desde pornografía hasta órganos humanos donde por medio de un servidor proxi evitan ser identificado, los casos mas difundidos son las sectas que cuentan con su pagina en Internet en donde convocan a la gente a través de este grupo de noticias y el otro es el de clonaciones humanas donde dan a conocer

en que país nacerá el próximo clon y cuanto costara, fomentando actividades que están prohibidas a nivel internacional .

Charla en Línea (Chat).

Este servicio tan sencillo y tan utilizado en nuestros días por jóvenes y no tan jóvenes a sido el medio para planear un secuestro debido al sondeo que realiza el secuestrador y que el receptor responde. En algunos países existen gentes que se encargan de chatear con la finalidad de indagar datos personales de donde son , como se llaman, a que se dedican ellos y sus padres pidiendo dirección y teléfono y de esta forma cometer el ilícito con mas precisión la mayoría de la veces son menores de edad .

Lo único que se pretende es mostrar el lado negativo de las herramientas de Internet que no solo resuelve problemas ; también ayuda a perfeccionar delitos haciendo muchas veces imposibles de ser detectados .

4.3 DELITOS INFORMÁTICOS EN MATERIA DE VÍAS DE COMUNICACIÓN Y CORREPONDENCIA

El objeto de este trabajo es la protección integral de los sistemas que utilicen tecnologías de información, así como la prevención y sanción de los delitos cometidos contra tales sistemas o cualquiera de sus componentes y contenidos mediante el uso de dichas tecnologías.

La Tecnología de Información es la rama de la tecnología que se dedica al estudio, aplicación y procesamiento de data, lo cual involucra la obtención, creación, almacenamiento, administración, modificación, manejo, movimiento, control, visualización, distribución, intercambio, transmisión o recepción de información en forma automática, así como el desarrollo y uso del "hardware", "firmware", "software", cualesquiera de sus componentes y todos los procedimientos asociados con el procesamiento de data.

De igual manera, las tecnologías de la información han abierto nuevos horizontes al delincuente, incitando su imaginación, favoreciendo su impunidad y potenciando los efectos del delito convencional. A ello contribuye la facilidad para la comisión y encubrimiento de estas conductas disvaliosas y la dificultad para su descubrimiento, prueba y persecución.

Entendiendo que su ataque supone una agresión a todo el complejo de relaciones socio-económico-culturales, esto es, a las actividades que se producen en el curso de la interacción humana en todo sus ámbitos y que dependen de los sistemas informáticos (transporte, comercio, sistema financiero, gestión gubernamental, arte, ciencia, relaciones laborales, tecnologías, etc.).

En esta propuesta se entiende por delitos informáticos a aquellas acciones típicas, antijurídicas y culpables que recaen sobre la información, atentando contra su integridad, confidencialidad o disponibilidad, en cualquiera de las fases que tienen vinculación con

su flujo o tratamiento, contenida en sistemas informáticos de cualquier índole sobre los que operan las maniobras dolosas.

La respuesta de ¿porque legislar en materia de vías de comunicación y correspondencia?, y no con relación a otros delitos como patrimoniales, revelación de secretos, delitos contra la intimidad de las personas o delitos cometidos por servidores públicos .

Es porque estos delitos tiene como característica principal información de tipo económico, político, social, o cultural, la cual se difunde a través de medios de comunicación entre los que se incluye la computadora como uno de los principales medios de comunicación multifuncional puedes tener texto, imagen , video y audio en una solo aparato ,tu computadora y de esta forma puedes abarcar los delitos antes mencionados y otros mas , no solo enfocarte en uno solo ya que prácticamente todos tienen como bien jurídico a la información.

Es importante hacer énfasis en la información que pueda estar resguardada o protegida en un medio informático como una computadora, algún vídeo , grabaciones de voz o audio ,discos duros, correos electrónicos, CD , disquete . No el objeto material (cosa) sino su contenido como objeto jurídico a proteger.

Al igual que el correo , el teléfono, la radio, la televisión, los satélites , han sido objeto de regulación jurídica ,la computadora debe tener la misma importancia o inclusive una mayor, porque todos los medios de comunicación antes mencionados , tiene relación de una u otra

forma con las computadoras y se ha colocado como el medio informático mas importante en las ultimas dos décadas, es por ello que los medios electrónicos, opticos, dactilares y de cualquier otra tecnología se hacen presentes en otras legislaciones como el Código Civil el Código de Comercio a tal grado que la Secretaria de Hacienda te permite declarar impuestos a través de Internet.

Es por eso que nuestro Código Penal Vigente debe empezar a legislar acerca del delito informático en base a supuestos que podrían originarse en el país.

a) Acceso Ilegitimo Informático.
Pena económica por solo acceder al sistema sin autorización sin dañar ninguna información única y exclusivamente acceso .

b) Daño o Sabotaje Informático.
El borrado o destrucción de un programa de computación no es una conducta aprehendida por el delito, pues el concepto de cosa es sólo aplicable al soporte y no a su contenido también a los datos o información almacenada en un soporte magnético.

Al incluir los sistemas y datos informáticos como objeto de delito de daño se busca penalizar todo ataque, borrado, destrucción o alteración intencional de dichos bienes intangibles. Asimismo, la incriminación tiende también a proteger a los usuarios contra los virus informáticos, caballos de troya, gusanos, cáncer routines, bombas lógicas y otras amenazas similares.

c) Fraude Informático.

El medio de comisión del delito de fraude informático consiste en la manipulación o despliegue de cualquier artificio semejante sobre un sistema o dato informático. Se ha optado por definir la conducta que caracteriza este delito como una "manipulación" o "artificio tecnológico semejante" en el entendimiento de que dichos términos comprenden tanto la acción de supresión, modificación, adulteración o ingreso de información falsa en un sistema o dato informático.

El hecho se agrava cuando el fraude informático recae en alguna Administración Pública Nacional o financiera.

d) Extraterritorialidad

Cuando alguno de los delitos previstos en la presente ley se cometa fuera del territorio de la República, el sujeto activo quedará sujeto a sus disposiciones si dentro del territorio de la República se hubieren producido efectos del hecho punible y el responsable no ha sido juzgado por el mismo hecho o ha evadido el juzgamiento o la condena por tribunales extranjeros.

e) Disposiciones Comunes.

El título de Disposiciones Comunes, se ha creado , por el tipo de ley especial de que se trata, redactar un glosario que facilite la comprensión de la terminología utilizada por el Anteproyecto.

Con la suficiente flexibilidad y vocabulario técnico, con el objeto de no generar anacronismos en razón de la velocidad con la que se producen

los cambios tecnológicos, tratando de aprehender todos los fenómenos de las nuevas tecnologías de la información.

Glosario.

Sistema: cualquier arreglo organizado de recursos y procedimientos diseñados para el uso de tecnologías de información, unidos y regulados por interacción o interdependencia para cumplir una serie de funciones específicas, así como la combinación de dos o más componentes interrelacionados, organizados en un paquete funcional, de manera que estén en capacidad de realizar una función operacional o satisfacer un requerimiento dentro de unas especificaciones previstas.

Data: hechos, conceptos, instrucciones o caracteres representados de una manera apropiada para que sean comunicados, transmitidos o procesados por seres humanos o por medios automáticos y a los cuales se les asigna o se les puede asignar significado.
Información: significado que el ser humano le asigna a la data utilizando las convenciones conocidas y generalmente aceptadas.

Documento: registro incorporado en un sistema en forma de escrito, video, audio o cualquier otro medio, que contiene data o información acerca de un hecho o acto capaces de causar efectos jurídicos.
Computador: dispositivo o unidad funcional que acepta data, la procesa

de acuerdo con un programa guardado y genera resultados, incluidas operaciones aritméticas o lógicas.

Hardware: equipos o dispositivos físicos considerados en forma independiente de su capacidad o función, que forman un computador o sus componentes periféricos, de manera que pueden incluir herramientas, implementos, instrumentos, conexiones, ensamblajes, componentes y partes.

Firmware: programa o segmento de programa incorporado de manera permanente en algún componente de hardware.

Software: información organizada en forma de programas de computación, procedimientos y documentación asociados, concebidos para realizar la operación de un sistema, de manera que pueda proveer de instrucciones a los computadores así como de data expresada en cualquier forma, con el objeto de que éstos realicen funciones específicas.

Programa: plan, rutina o secuencia de instrucciones utilizados para realizar un trabajo en particular o resolver un problema dado a través de un computador.

Procesamiento de data o de información: realización sistemática de operaciones sobre data o sobre información, tales como manejo, fusión, organización o cómputo.

Seguridad: Condición que resulta del establecimiento y mantenimiento de medidas de protección que garanticen un estado de inviolabilidad de influencias o de actos hostiles específicos que puedan propiciar el acceso a la data de personas no autorizadas o que afecten la operatividad de las funciones de un sistema de computación.

Virus: programa o segmento de programa indeseado que se desarrolla incontroladamente y que genera efectos destructivos o perturbadores en un programa o componente del sistema.

Tarjeta inteligente: rótulo, cédula o carnet que se utiliza como instrumento de identificación, de acceso a un sistema, de pago o de crédito y que contiene data, información o ambas, de uso restringido sobre el usuario autorizado para portarla.

Contraseña (password): secuencia alfabética, numérica o combinación de ambas, protegida por reglas de confidencialidad utilizada para verificar la autenticidad de la autorización expedida a un usuario para acceder a la data o a la información contenidas en un sistema.

Mensaje de datos: cualquier pensamiento, idea, imagen, audio, data o información, expresados en un lenguaje conocido que puede ser explícito o secreto (encriptado), preparados dentro de un formato adecuado para ser transmitido por un sistema de comunicaciones.

4.3.1 CORREGIR LAS DEFICIENCIAS DE LOS SUPUESTOS PENALES DE ACCESO ILÍCITO A SISTEMAS Y EQUIPOS DE INFORMÁTICA COMO BASE PARA LA CREACIÓN DEL CAPITULO DELITOS INFORMÁTICOS .

Primero que nada corregir el nombre al capitulo sobre delitos informáticos:

ACCESO ILICITO A SISTEMAS Y EQUIPOS DE INFORMATICA.

En muchas de las ocasiones debido al puesto o cargo que desempeñas tienes acceso licito a la información o al medio informatico, hay que dejar el parámetro abierto sobre acceso licito e ilícito , la finalidad es que exista el delito y pueda ser tipificado por el juzgador ya que el abuso de confianza podría ser contemplado como una salida para el delincuente para recibir una pena menor a la merecida en el caso de que sea un empleado de confianza.

El delito informático podría argumentar una mayor penalidad ya que para cometer el delito fue indispensable que el individuo contara con conocimientos en informática, para acceder al sistema o equipo informatico , conocimientos que lo distinguen de un delincuente común y lo convierte en un delincuente potencialmente peligroso.

En este mismo sentido muchas veces ni siquiera tenemos que acceder a otro equipo ya que en el momento que alguien manda un virus a través de un correo electrónico a determinado servidor o

usuario , el virus no afecta hasta que el receptor lo habré el correo en ese momento el servidor o computadora baja el contenido para que puedas visualizarlo pero el virus ya entro a tu computadora y al final el perjudicado es quien dio el acceso desconociendo que el correo estaba infectado con un virus .

El Mecanismo de Seguridad Puede ser tan variado como dinero tengas para invertir por ejemplo ; pasword, candados contra robo, sistema criptógrafo, el inconveniente es que muchas de las ocasiones el monto económico hace imposible que puedas proteger tu información lo que nos hace quedar fuera del algunos supuestos penales, literalmente hablando.

El problema no radica en el mecanismo de seguridad sino en castigar la intromisión y el perjuicio que pueda causar cuando accesa a la información o atenta contra los medios que sirven como soporte técnico para guardar , enviar, transmitir y recibir información

Aun cuando no se toca el punto de la reincidencia parece que la adrenalina de burlar un sistema informático hace que el delincuente cibernético trate de hacerlo una y otra vez , como si fuera un drogadicto o un ebrio . Conductas que son reconocidas a nivel mundial han catalogado a los adictos a burlar sistemas informaticos como , hackers, crackers, phreackers, viruckres .

"Un joven ingles robo 50 000 libras esterlinas de la compañía en la cual trabajaba y luego manipulo los datos de la computadora para

encubrir el robo. El fraude fue descubierto, pero la dirección declino la acusación penal por temor de que la publicidad alarmara a los accionistas de la compañía. el sujeto solicito a la dirección de esa empresa que le proporcionaran una carta de recomendación a lo cual accedieron .

El uso dicha recomendación para obtener trabajo en otra compañía. Cuatro años mas tarde, esta ultima encontró el rastro de un nuevo fraude por 150 000 libras cometido por el mismo héroe. Otra vez la dirección se abstuvo de acusarlo y de nuevo el ladrón solicito una carta de recomendación. Pero el caballero presiono demasiado al pedir 3500 libras como liquidación, la compañía ahora si lo envió a prisión." [52]

Como este caso existen miles alrededor del mundo y México no ha sido la excepción.

[52]MORA ,JOSE LUIS. Molina Enzo. INTRODUCCION A LA INFORMATICA .Editorial Trillas . México 1974.,p.262.

4.3.2 ADICIONAR EL CORREO ELECTRONICO AL CAPÍTULO DE VIOLACIÓN DE CORRESPONDENCIA.

Código Penal para el D. F. (Vigente)
Capitulo III
Violación de Correspondencia.

Artículo 333.- Al que habrá intercepte una comunicación escrita que no esté dirigida a él se le impondrá de Treinta a Noventa días de multa.
No se sancionaran a quien en ejercicio de su patria potestad tutela o custodia, abra o intercepte la comunicación escrita dirigida ala persona que se halle bajo su patria potestad, tutela o custodia.
Los delitos previstos en este articulo se perseguirán por querella.

El correo electrónico en nuestros días a pasado de ser una herramienta juvenil a ser una macro herramienta para particulares, empresas y para el Estado en donde puedes mandar desde texto , audio, imagen, video, etc.,en cuestión de segundos de un país a otro, considerando a esta servicio digno de protección penal .

El Correo tradicional en México ya no tiene la misma rentabilidad en nuestros días puesto que la tecnología prácticamente a dejado atrás a este servicio pero ahora es indispensable retomar algunos conceptos en cuanto a la violación de correspondencia ya que prevalece el mismo espíritu de la norma que es comunicar pero con la seguridad de que esa información será de emisor a receptor sin

ningún intermediario simplemente debe ser actualizada, en donde el Estado seguirá siendo el encargado de proporcionar la seguridad jurídica.

Cada día es mayor la correspondencia que se trasmite en el país creada y enviada a través de medios informáticos, es decir que la correspondencia tradicional que prácticamente fue desplazada por el teléfono, ahora está dando paso a la utilización masiva de un nuevo medio de comunicación, el e-mail.

Es por ello que el correo electrónico no debe limitarse a dos párrafos y un renglón, la protección del correo electrónico abarca su creación, transmisión y almacenamiento.

El correo electrónico es toda transmisión de información enviada a través de una red de interconexión entre dispositivos electrónicos con capacidad de procesamiento, a una dirección o casilla de correo electrónico.

Es así como la apertura, apoderamiento, desvío o supresión indebidas del correo electrónico o la difusión por cualquier medio de su contenido, cuando el mismo no tuviere por fin tal difusión, deben ser sancionados y protegidos en igual medida que la violación de los papeles privados y la correspondencia tradicional.

El que tenga una correspondencia o un correo electrónico no destinado a la publicidad, y lo hiciere publicar indebidamente, aunque

haya sido dirigida a él, si el hecho causare o pudiere causar perjuicios a terceros tendrá que ser sancionado.

Cuando la dirección o casilla de correo electrónico sea provista por el empleador para uso del empleado, aunque no estén consignados los datos de este último como usuario, se entenderá que la provisión se ha realizado para su uso exclusivo, alcanzándole a esa casilla o dirección la confidencialidad.

El empleador deberá notificar fehacientemente al empleado su política respecto del acceso y uso del sistema de correo electrónico en el lugar de trabajo.

El empleado de correos o telégrafos que, abusando de su empleo, se apoderara de una carta, de un pliego, de un telegrama, de un correo electrónico o de otra pieza de correspondencia, se enterara de su contenido, lo entregare o comunicaré a otro que no sea el destinatario, lo suprimiera, lo ocultare o cambiare su texto será sancionado.

4.3.3 DISTINGUIR ENTRE LOS DELITOS INFORMÁTICOS QUE ATENTEN CONTRA EL ESTADO , LAS EMPRESAS Y EL PARTICULAR.

Es importante hacer una distinción de la información de carácter público y privado .
Las dimensiones de un delito informático a nivel personal o privado no se compara en nada a lo que podría hacer uno de carácter público que de alguna manera atenta contra la protección que el Estado debe proporcionar a los habitantes.

Delitos informáticos en contra de la Defensa Nacional, Investigaciones Científicas, Salud Pública , la Prestación de Servicios Públicos y el Sistema Financiero deberá defenderse con penas ejemplares con la finalidad de prevenir este tipo de ilícitos a través de medios de informáticos

La medios informáticos de carácter empresarial en la actualidad cuentan con tecnología de punta mucho mas eficaz que la del Estado , como pudieran ser los medios ópticos, dactilares, tarjetas maestras, micro chips, reconocimiento del tono de voz .

Solo por mencionar el mas usual claves o pasword pero no por ello se deben pasar por alto este tipo de ilícitos porque al brindar la protección jurídica necesaria estaremos contribuyendo a que cada vez mas empresas sigan invirtiendo en tecnología de punta en nuestro país.

Tal vez la protección de los particulares podría pensarse que es la mas sencilla, por que realmente los daños no serian muy grandes económicamente hablando , pero en realidad se convierte en el mas complejo de los tres , porque el valor del daño o perjuicio es mas que nada estimativo.

CONCLUSIONES

Primero.- El Delito Informático existe en México.

Segundo .- El legislador debe tener en todo momento presente los siguientes artículos de la Constitución Política de los Estados Unidos Mexicanos, artículo 6° referente al Derecho a la información y el artículo 7° referente a la libertad de expresión y el artículo 133 con referencia a los tratados internacionales para legislar en Materia de delitos informaticos y de esta manera no limitar o perjudicar los derechos de la sociedad.

Tercero.- La Ley de Vías Generales de Comunicación a través de la Secretaria de Comunicaciones y Transportes deberá regular, vigilar e inspeccionar a las empresas que presten servicios públicos o privados de comunicación para no fomentar Delitos contra la intimidad, revelación de secretos, facturaciones inexistentes, falsificación de documentos, a través de estos medios tecnológicos.

Cuarto .- La Ley Federal de Telecomunicaciones a través de la Comisión Federal de Telecomunicaciones se hará responsable de la protección de la información en equipos de computo y tecnología informática . En Internet cada uno de los proveedores tendrá la obligación de contar con una base de datos de todos sus usuarios , en caso de ser necesario proporcionar claves y contraseñas de la persona o empresa que se este investigando a la autoridad judicial cuando le sean requeridas.

Quinto .- Retomar el capitulo de acceso ilícito a sistemas y equipos de informática que fueron derogados, como base para la creación de nuevos supuestos penales en materia de delitos Informaticos .

Sexto.- El Delito Informático puede tener diferentes modos de operar, no solo en Delitos Contra el Patrimonio , también lo podemos encontrar en otros Delitos Contra la Moral Pública , Delitos Contra la Intimidad y la Inviolabilidad del Secreto ,Delitos contra la seguridad Colectiva, Delitos Contra la Fe Publica , Contra la Seguridad y el Normal Funcionamiento de las Vías de Comunicación.

Séptimo.- La Policía Cibernética podrá investigar y denunciar la apropiación de propiedad intelectual cuando alguna persona que sin autorización de su propietario y con el fin de obtener algún provecho económico, reproduzca, modifique, copie, distribuya o divulgue un software u otra obra del intelecto que haya obtenido mediante el acceso a cualquier sistema que utilice tecnologías de información.

Octavo.-La Policía Cibernética mediante orden judicial será la única que pueda mediante el uso de tecnologías de información, acceder, capturar, interceptar, interferir, reproducir, desviar pero nunca modificar o eliminar mensajes de datos , señales de transmisión o comunicaciones ajenas.

Noveno.-La principal tarea de la policía cibernética, como hasta nuestros días será investigar a el que por cualquier medio que involucre el uso de tecnologías de información, utilice a la persona o

imagen de un niño, niña o adolescente con fines exhibicionistas o pornográficos teniendo acceso a redes publicas o privadas siempre respaldados por autoridad judicial

Décimo .- La cosa material puede ser restituida, pero la información contenida en los soportes que almacenan datos, en muchas ocasiones cuando son alterados o destruidos ya no se pueden recuperar, es decir que la información que se encuentra respaldada en estos soportes que almacenan datos no cuentan con la debida la protección jurídica en nuestro Código Penal.

Décimo Primero.-Es necesario legislar las herramientas de Internet, ya que cada una de ellas puede ayudar a perfeccionar el delito sin ser detectado a tiempo.

Décimo Segundo.- El Juez impondrá en la sentencia una indemnización en favor de la víctima por un monto equivalente al daño causado. Para la determinación del monto de la indemnización de carácter estimativo, el Juez requerirá del auxilio de expertos.

Décimo Tercero.- El Correo electrónico podrá ser vigilado y registrado con una orden girada por el juez que este conociendo del caso, en donde podrán indagar correos electrónicos y todos los soportes de respaldo de información como disco duro , disquete , cd etc.

Décimo Cuarto- Todos las empresas deberán responsabilizarse del mal uso que se le pueda dar a Internet, a sus redes internas, al correo

electrónico, y a las paginas publicadas en su nombre y bajo su dominio ,también sobre el software y hardware instalados en sus equipos de computo.

Décimo Quinto.- En el ámbito del Derecho Internacional se podrá pedir la extradición de la persona que haya cometido en otro país el delito informático con repercusiones graves en México este es el caso especifico de los virus que son creados en determinado país y luego lanzados a la red Internet, perjudicando diferentes sectores de la población en diferentes países.

Décimo Sexto.- La Posesión de equipo para falsificaciones será confiscado por el estado para investigar el uso y manejo de la tecnología de punta con la cual trabajan los falsificadores y de esta forma detectar todo tipo documentos falsos.

Décimo Séptimo.- Se formara una base de datos de todas las paginas de Internet creadas en México bajo las siglas (mx),en donde previamente los proveedores tendrán registrados los datos del dueño de la pagina responsabilizándose de la información contenida en la pagina en donde la Secretaria de Gobernación definirá si el contenido es el apropiado.

BIBLIOGRAFIA

1.- Amuchategui Requena , Irma. PRIMERO Y SEGUNDO CURSO DE DERECHO PENAL. México. Editorial Harla, 1994.

2.- Azzolini, Alicia; De la Barreda Solórzano, Luis .EL DERECHO PENAL MEXICANO AYER Y HOY. 1ª ed. México. Instituto de Capacitación de la PGR., 1993.

3.-Barragán, Julia. INFORMATICA Y DECISION JURIDICA. 1ªed. México Distribuciones Fontamara, 1994.

4.-Barrios Garrido Gabriela, Muñoz de Alba M Marcia, Pérez Bustillos Camilo. INTERNET Y DERECHO EN MEXICO. México, Editorial Mc Graw Hill, 1998.

5.-Becaria, Cesar TRATADO DE LOS DELITOS Y DE LAS PENAS. México Editorial Porrua, 1952.

6.-Betancourt López, Eduardo. TEORIA DEL DELITO. México. Editorial Porrua ,1994.

7.-Carranca y Trujillo, Raul .Carranca y Rivas ,Raul. DERECHO PENAL MEXICANO.21ª ed México. Editorial Porrua ,2001.

8.-Castellanos Tena, Fernando. LINEAMIENTOS ELEMENTALES DEL DERECHO PENAL. 19 ed. México. Editorial Porrua.1984.

9.-Correa, Carlos Maria .INFORMATICA Y DERECHO. Buenos Aires.Editorial Depalma, 1987.

10.-Cortes Ibarra , Miguel Angel. DERECHO PENAL. 4ª ed. México. Editorial Cárdenas Editor y Distribuidor,1996.

11.-DICCIONARIO DE LA MICROCOMPUTACION. Tomo II. España . Editorial Alfa Homega, 1999

12.-Frezze T. Hill. COMPUTACION BASICA . Argentina .Editorial MIG., 1994.

13.-García Ramón ,Pelayo y Gross .ENCICLOPEDIA METODICA LAROUSSE, Tomo. V México. Editorial Larousse.1998ª

14.-García Ramírez , Sergio. DERECHO PENAL . México .Editorial Mc Graw Hill, 1998.

15.-González de la Vega, Francisco. DERECHO PENAL MEXICANO. México Editorial. Porrua , 1996.

16.- González Quintanilla, José Arturo. DERECHO PENAL MEXICANO. México .Edit. Porrua, 1993 .

17.- Jiménez de Asua ,Luis . LA LEY Y EL DELITO. 3ª ed. Buenos Aires. Editorial Sudamericana,1989.

18.-Lacherbaue , Ingo TODO SOBRE INTERENET. España Editorial Boixcreu, 2000.

19.-Lima de la Luz, Maria . DELITOS ELECTRONICOS .Academia Mexicana de Ciencias Penales. Editorial Porrua ,1984 .

20.-López Aylon ,Sergio . DERECHO ALA INFORMACION .México. Editorial Porrua ,1984.

21.-López Betancourt. HISTORIA DEL DERECHO. México Editorial Porrua, 2001.

22.-Luna Castro ,José Nieves. EL CONCEPTO DE TIPO PENAL EN MEXICO. México Editorial Porrua,2001.

23.-Malo Camacho, Gustavo. DERECHO PENAL MEXICANO. Editorial Porrua S.A. México.1998

24.-Mc Quail. INTRODUCCION A LA TEORIA DE COMUNICACIÓN DE MASAS. Barcelona .Paidos Comunicación, 1983.

25.-Mora José Luis, Molina Enzo. INTRODUCCION A LA INFORMATICA. México. Editorial Trillas, 1974.

26.-Orellano Wiarco, Octavio Alberto. CURSO DE DERECHO PENAL México. Editorial Porrua 1999.

27.-Pavón Vasconcelos , Francisco MANUAL DE DERECHO PENAL MEXICANO México .Editorial Porrua 1998.

28.-Reyes Echandis, Alfonso. DERECHO PENAL. 11ª ed. Colombia. Editorial Temus, 1990.

29.-Romero Coloma, Aurelia Maria. DERECHO A LA INFORMACION Y LIBERTAD EXPRESION . Editorial Bosh .1984.

30.-Soberanes Hernández, José Luis . HISTORIA DEL DERECHO MEXICANO. México. Editorial Porrua , 1993.

31.-Suprema Corte Justicia Nación .DERECHO A LA INFORMACION. México. Serie de debates del Pleno SCJN. 2000.

32.-Téllez Valdes Julio. DERECHO INFORMATICO.2ª ed. México. Editorial Mc Graw Hill. , 1996.

33.-Ureña Lopez L. Alfonso FUNDAMENTOS DE LA INFORMATICA .Madrid . Editorial Alfa Homega, 1999 .

34.-Villalobos, Ignacio. DERECHO PENAL MEXICANO. México. Editorial Porrúa, 1975.

LEGISLACION

CONSTITUCION POLITICA DE LOS ESTADOS UNIDOS MEXICANOS.
LEY ORGANICA DE LA ADMINISTRACION PÚBLICA FEDERAL.
CODIGO PENAL PARA EL DISTRITO FEDERAL (VIGENTE Y DEROGADO).
CODIGO PENAL DEL ESTADO DE SINALOA.
CÓDIGO PENAL DEL ESTADO DE AGUASCALIENTES.
LEY FEDERAL DE DERECHOS DE AUTOR.
LEY DE ESTADISTICA GEOGRAFIA E INFORMATICA.
LEY DE VIAS GENERALES DE COMUNICACIÓN.
LEY FEDERAL DE TELECOMUNICACIONES.

PAGINAS WEB

http://www.asamblealegislativa.gob.mx
http://www.aaba.org.ar/bi180p43.htm
http://www.cyberangels.org/international/sp/hacking/info.html
http://www.delitosinformaticos.com/
http://www-derecho.unex.es/biblioteca/derpenal.htm
http://www.el-mundo.es/navegante/98/junio/18/delitoinformatico.html
http://www.liderdigital.com/documentos/Boletin_Derecho_y_Sociedad_de_la_Informacion_n5.
http://www.monografias.com/trabajos/legisdelinf/legisdelinf.shtml
http://www.delitosinformaticos.com/
http://www.usdoj.gov/criminal/cybercrime/

GLOSARIO

ADN
(Advanced Digital Network)—Comúnmente se refiere a una línea de 56Kbs.

Anonymous FTP (Ver: FTP)

Archie
Un herramienta de Internet *(software)* para encontrar archivos almacenados en sites anónimos de FTP. Se requiere saber el nombre exacto del archivo a buscar para poder hacer uso de el.

ARPANet
(Advanced Research Projects Agency Network)—El precursor de lo que actualmente se conoce como Internet. Desarrollado en los finales de los 60's y principios de los 70's por Departamento de Defensa de los Estados Unidos como un Experimento de redes de grandes áreas (WAN) que sobreviría una guerra nuclear.
Ver también: Internet.

ASCII
(American Standard Code for Informations Interchange)—Esta es el estándar mundial para el código de los números usados por la computadora para representar las mayúsculas y minúsculas de las letras, números , puntuación, etc., latinas. Existen 128 códigos del estándar ASCII que pueden ser representados cada uno por un número binario de siete dígitos: 0000000 hasta el 1111111.

B

Backbone
Una línea de alta velocidad o una serie de conexiones que forman un mayor ancho de banda en una red. El término es relativo de un Back-bone en una pequena red, mucho más pequena, que muchas líneas no back-bones en una red grande.
Ver también: Network (red)

Bandwidth (Ancho de banda)
La cantidad de datos se pueden transferir a través de una conexión. Comúnmente medida en bits- por- segundo. Una página entera de texto en espanol es aproximadamente de 15,000 bits por segundo. Pantallas de movimiento total requiere un mínimo aproximado de 10,000,000 bits- por- segundo dependiendo de la compresión.
Ver también: 56K Line, Bps, Bit, T-1

Baud (Baudio)
En el uso común el "baud rate" de un módem es la cantidad de bits que puede enviar y recibir en un segundo. Técnicamente, un baudio es el número de veces por segundo que el carrier cambia de valor – por ejemplo un módem de 1200 bits por segundo corre normalmente a 300 baudios, pero este mueve 4 bits por baudio (4 X 300 = 1200 bits por segundo).
Ver también: Bit, Módem

BBS
(Bulletin Board Systems) Un boletín computarizado y sistema de anuncios que permite a las personas establecer mesas de debates, transferencia de archivos *(upload, download)*, y realiza anuncios con las personas conectadas al mismo tiempo. Estos son miles *(millones?)* de BBS's en todo el mundo, la mayoría son muy pequenos, que emplean un solo clon IBM PC con 1 ó 2 líneas telefónicas. Algunos son muy grandes y las líneas entre el BBS y un sistema como CompuServe se cruzan en algún punto, pero no esta claramente senalado.

Binhex
(BINary HEXadecimal) Un método para convertir archivos que no están en código ASCII a este código. Esto es necesario porque el correo electrónico (e mail) de internet solo se puede manejar en código ASCII.
Ver también: ASCII, MIME, UUENCODE

Bit
(Binary DigIT) Un solo dígito o número en base-2, en otras palabras, es o un 1 ó un cero. La unidad más pequena de almacenamiento de datos en un sistema computarizado. El ancho de banda *(Bandwith)* es comúnmente medido en bits- por- segundo.
Ver también:Bandwidth, Bps, Byte, Kilobyte, Megabyte

BITNET
(Because It's Time NETwork (Because It's There NETwork)) una red de sites educativos separados de Internet, pero el correo electrónico es libremente intercambio entre BITNET e Internet. Los conocidos como "Listservs", son los grupos de discusión más importantes vía e-mail,, originados en BITNET. Las máquinas BITNET son mainframes que corren con un sistema operativo VMS, y la red es probablemente en la red internacional que se esta encogiendo.

Bps (Bits-por –segundo)
(Bits- Per- Second) Una medida de velocidad de transmisión de datos de un lugar a otro. Un módem de 28.8 puede transferir 28,800 bits por segundo.
Ver también: Bandwidth, Bit

Browser
Un sofhware de cliente que es empleado para aprovechar diversos recursos de Internet.
Ver también: Cliente, URL,WWW, Netscape, Mosaic, Home Page

BTW
(By The Way) Una abreviatura que significa "a propósito" empleada de sobremanera en foros de Internet.
Ver también:: IMHO, TTFN

Byte
Un conjunto de Bits que representan un solo carácter. Comúnmente son 8 bits en un byte, dependiendo de cómo se esta realizando la medición.
Ver también: Bit

C

CGI
(Common Gateway Interface) Un Conjunto de reglas que describen como un servidor de la red *(Web Server)* se comunica con otra pieza de software en la misma máquina, y cómo esta otra pieza de software *(el programa CGI)* se comunica con el servidor de red. Toda pieza de software puede ser un programa CGI si esta maneja entradas y salidas *(input, output)* de acuerdo a los estándares CGI.

Comúnmente un programa CGI es un pequeno programa que toma información de un servidor de red y realiza alguno operación con ella, como el poner el contenido en forma de e-mail ó transformando la información en una base de datos.

Se puede observar que un programa CGI se esta empleando viendo el mensaje "cgi-bin" en un URL, pero no siempre.
Ver también: cgi-bin, Web

Cgin-bin
El directorio más común en un servidor de red en donde se almacena programas CGI.

La parte "bin" del cgi-bin es una abreviatura de binario, debido a que erróneamente la mayoría de los programas eran llamados binarios. En la vida real la mayoría de los programas encontrados en directorios cgi-bin son archivos de texto. (escritos que son ejecutados por binarios localizados en otra parte de la misma maquina.
Ver también: CGI

Client (cliente)
Software empleado para contactar y obtener información de otro software ubicado en un servidor de red de otra computadora, a menudo a grandes distancias. Cada programa "cliente" es disenado para trabajar con uno a más programas de servidores, y cada servidor requiere de un especifico tipo de cliente. Un Browser de red es un tipo específico de cliente.
Ver también: Browser, Server

Cookie
El significado más común de cookie en Internet se refiere a un pedazo de información enviada por un Servidor de Red a un Browser de red en donde el Browser espera almacenar y enviar de regreso al servidor cuando el browser solicite más información del servidor.

Dependiendo del tipo de cookie usada, y de la configuración del browser, el browser podrá aceptar o no a la cookie, y la podrá salvar por periodos largos o cortos.

Ejemplos de cookies usan información de registro o encuestas.

Cuando el servidor recibe una solicitud del browser que incluye una cookie, el servidor es capaz de emplear la información almacenada en la cookie para una variedad de cosas.

Las cookies típicamente salvar información en memoria hasta que el browser es cerrado y son entonces salvadas al disco.

Las cookies NO leen el disco duro y envían tu expediente a las autoridades, pero esto puede ser usado para reunir más información sobre un usuario que podría ser posible sin ellos.
Ver también: Browser, Server

Cyberpunk
Cyberpunk era originalmente un género sub-cultural de ciencia ficción que tomaba lugar en dystopian no muy distante *(sociedad sobre-industrializada)*. El término creció del trabajo de William Gibson y Brece Sterling y surge ahora como el cruzamiento de muchos tipos de seres humanos, máquinas y actitudes punk. Incluye también vestuario y estilos de vida.
Ver también: Cyberspace

Cyberspace
Término originado del autor William Gibson en su novela "Neuromancer" la palabra Cyberspace es actualmente usada para describir el rango entero de recursos informáticos disponibles a través de todas las redes de cómputo.

D

Domain Name
El nombre único que identifica un site Internet. El Domain Name siempre tiene dos o más partes, separadas por puntos. La parte de la izquierda es la más especifica, la de la derecha es la más general. Una máquina podrá tener más de un Domain Name pero no para más de una máquina. Por ejemplo, los domain manes:

- Comdi.net
- Mail.comdi.net
- Telecomunicaciones.co mdi.net

Se refieren todos a la misma máquina, pero cada domain name no se puede referir a más de una sola máquina.
Comúnmente, todas las maquinas de una red tienen la misma en la parte derecha del domain name *(cindu.net en ejemplo anterior)*. También es posible que para que un Domain Name exista no debe estar conectado a una máquina. En estos casos una máquina internet deberá llevar control del correo de dicho Domain Name.
Ver también: IP Number

E-mail (correo electrónico)
(Electronic Mail) Mensajes, comúnmente texto,

enviado por una persona a otra a través de la computadora. El correo electrónico *(e-mail)* puede ser también enviado automáticamente y simultáneamente a una número mayor de direcciones *(lista de correos "Mailing List")*.
Ver también:: Listserv. Maillist

Ethernet
Un método muy común de establecer redes en una LAN *(red no muy grande "local area network)* Ethernet maneja aproximadamente 10,00,000 bits – por – segundo y puede ser usado con casi todo tipo de computadora.
Ver también: Bandwidht, LAN

F

FAQ
(Trequently Asked Questions) FAQs son documentos que en listan y responde las preguntas más comunes de un tema en particular. Existen cientos o miles de FAQs de miles de distintos temas y son comúnmente usados por personas que han tratado de responder las mismas preguntas constantemente.

FDDI
(Fiber Distributed Data Interface) Un estándar de transmisión de datos empleando fibra óptica con un rango de 100,000,000 bits – por –segundo *(10 veces más rápido que una red ethernet, alrededor del doble de rápido que un T-3)*
Ver también: Bandwidht, Ethernet, T-1,T-3

Finger
Un software de internet para localizar gente en sites Internet. El software Finger es también usado para dar acceso a información no personal, pero el uso más común es el de localizar usuarios o a su cuenta en un site Internet. Algunos servidores no permiten el uso del finger pero la mayoría si lo permiten

Fire Wall
Una combinación de hardware y software que separa una LAN *(local area network)* en dos o más partes por motivos de seguridad
Ver también: Network (red), LAN

Flame (flama)
Originalmente, flame significaba el llevar un debate a favor de manera muy apasionada. Flames se refiere recientemente a cualquier comentario derogatorio.
Ver también: Flame War

Flame War
Cuando un debate en línea se degenera en una serie de ataques personales en contra de los expositores y sus posturas respecto a cierto tema. Un intercambio muy caluroso.
Ver también: Flame

FTP
(File Transfer Protocol) Un método muy común de transferir archivos a través de sites Internet. FTP es una manera especial de establecer contacto *(login)* con otros sites Internet con propósito de obtener ó enviar archivos. Existen muchos sites Internet que ofrecen archivos publicitarios ó con otras intenciones que pueden ser obtenidos mediante FTP, estableciendo contacto *(login)* con el nombre de usuario anónimo *(anonymous)*, es por esto que estos sites son llamados "anonymous ftp servers".

G

Gateway
El significado técnico se refiere a un hardware o software que traduce dos protocolos distintos o no compatibles, por ejemplo Prodigy tiene un gateway que traduce su formato interno de correo electrónico a el formato Internet del e-mail. Otro significado menos correcto de gateway es el describir cualquier mecanismo para proveer acceso a otro sistema por ejemplo, AOL puede ser llamado un gateway hacia Internet.

Gopher
Un método muy famoso de realizar menús de materiales disponibles en Internet. Gopher es un programa del estilo Cliente/ Servidor, que requiere que el usuario tenga un software cliente Gopher. Sin embargo el Gopher se expandió alrededor del mundo en un par de anos y ha sido ahora reemplazado por el Hypertext, también conocido como WWW (World Wide Web). Existen aún miles de servidores Gopher en Internet pero su estancia no será muy larga.
Ver también: Cliente, Servidor, WWW, Hypertext

H

Home Page (Homepage) Existen distintos significados para este término. Originalmente, es la página que tu Browser empleara al iniciarlo. El significado más común se refiere a aquella página que es considerada la principal para cierta entidad (organización, persona, etc.) ó simplemente la página principal de un cierto conjunto de páginas. Otro significado no tan correcto se refiere a prácticamente cualquier página de un site.
Ver también: Browser, Web

Host
Cualquier computadora en una red que es fuente de servicios disponibles a otras computadoras en cierta red. Es muy común el tener una máquina host que provee diversos servicios, tal como WWW y USENET.
Ver también: Node, Network

HTML
(HyperText Markup Language) El lenguaje de código que emplea par crear documentos Hypertext para uso en WWW. El código HTML parece un código viejo de tecleado, donde se llena un bloque de texto que indican como debe aparecer el documento, adicionalmente en HTML se puede especificar que un bloque de texto, o una letra este unida a otro archivo en Internet. Los archivos HTML son para ser vistos empleando un software Cliente del WWW, como el Internet Explorer de Microsoft, el famoso Netscape o Mosaic.
Ver también: Cliente, Servidor, WWW

HTTP
(HyperText Transport Protocol) El protocolo para transferir archivos tipo hypertext a lo largo de todo Internet. Requiere un programa cliente HTTP en un lado de la conexión y del otro un programa servidor HTTP. Este protocolo es el más importante usado en World Wide Web *(WWW)*.
Ver también: Cliente, Servidor, WWW

Hypertext
Generalmente, cualquier texto que contenga links a otros documentos – letras o frases en el documento que pueden ser elegidas por un lector que produce que sea llamado y desplegado otro documento.

IMHO
(In My Humble Opinion) Una abreviatura muy empleada en los foros Internet que significa "en mi humilde opinión". IMHO indica que el escritor esta enterado que se esta estableciendo un punto de vista debatible, probablemente de un tema que ya esta en discusión.
Ver también: TTFN,BTW

Internet
(mayúscula) La vasta colección de redes interconectadas que emplean en general protocolos que emergen del ARPANET a finales de los 60's y principios de los 90's. Internet es ahora *(Julio 1995)* una gran conexión que tiene aproximadamente un mínimo de 60,000 redes independientes en todo el mundo creando una gran red global.
Ver también: internet

internet
(minúscula) Cualquier vez que se conecten 2 o más redes *(networks)*, se tiene un internet-como inter-nacional ó inter-estatal.
Ver también: Internet, Network (red)

Intranet
Una red privada dentro de una organización que emplea el mismo tipo de software que se encontrara en la red pública Internet, pero es de uso interno exclusivamente.
A medida que Internet se ha hecho más famoso, muchas de las herramientas empleadas en Internet están siendo empleadas ahora en redes privadas, por ejemplo, muchas compañías tienen servidores de red que están disponibles solo para sus empleados y/o clientes.
Es importante senalar que un Intranet no es un internet---- es simplemente un red más compleja.
Ver también: internet, Internet, Network (red)

IP Number
A menudo llamado "dotted quad". Es un número único que consisten en cuatro partes separadas por puntos.

- Ejemplo: 165.113.245.2

Cada máquina que esta en Internet tiene un número único IP, este número no esta realmente

en Internet. La mayoría de las máquinas tienen uno o más Domain Names que son más fáciles de recordar.
Ver también: Domain Name, Internet

IRC
(Internet Relay Chat) Básicamente un inmenso modo chat muti-usuario. Existe un número servidor de IRC mayores que están unidos *(links)* entre sí. Cualquier persona puede crear un canal y todo lo que se teclea es visto en ese canal por todas las personas conectadas al mismo. Los canales privados pueden *(y son)* creados por varias personas en canales en conferencia.

ISDN
(*Integrated Services Digital Network)* Básicamente es la manera de mover datos en líneas telefónicas regulares. ISDN esta siendo rápidamente disponible a la mayoría de Estados Unidos y en muchos mercados esta costeando muy similarmente a circuitos estándar analógicos. Provee una velocidad mínima de 128,000 bits – por – segundo en líneas telefónicas regulares. En la práctica, la mayoría de las personas serán limitadas a 56,000 ó 64,000 bits – por –segundo

ISP
(Internet Service Provider) Una institución que provee acceso a Internet de alguna forma con intenciones lucrativas.
Ver también: Internet

Java
Java es un nuevo lenguaje de programación creado por Sun Microsystems que esta especificamente diseñado para elaborar programas que puedan ser bajados *(download)* con mucha seguridad a una computadora mediante Internet y que corra inmediatamente sin tener problemas de virus o de daños en archivos. Al usar pequeños programas de elaborados con Java llamados *("Applets")*, la página de Internet *(Web pages)* pueden incluir funciones como animaciones, calculadoras, y muchas otras aplicaciones.

Se puede esperar una gran variedad de características y ventajas agregadas a la Red empleando Java, ya que se pueden elaborar programas de cualquier tipo y que cualquier computadora puede realizar con Java y después incorporarlo a una página de Internet.

K

Kilobyte
Son mil bytes. Comúnmente ahora son 1024 (2 –10) bytes.
Ver también: Byte, Bit

L

LAN
(Local Area Network) Una red de computadoras limitados por el área que rodea a la red, comúnmente un edificio un piso de un edificio.
Ver también: 56K Line, T-1, T-3

Listserv
La manera mas común de listas de correo *(maillist)*, los Listserv eran originados en BITNET pero ahora son más comunes en Internet.
Ver también: BITNET, E-mail, Maillist

línea de 56K
Una conexión a través de una línea teléfono digital capaz de llevar 56,000 bits- por segundo. A esta velocidad, un Megabyte se llevara aproximadamente 3 minutos en transferirse. Esta velocidad es 4 veces ,más rápido que un módem de 14,000bps.

Login
Sustantivo o verbo. Sustantivo: el nombre de la cuenta empleada para tener acceso a un sistema de cómputo. No es secreto (a diferencia del password)

Verbo: El acto de entrar a un sistema de cómputo, por ejemplo: Login a COMDI e ir después a al conferencia MUX.
Ver también: Password

M

Maillist (lista de correo) *(Mailing List)* Un sistema comúnmente autorizado que permite a las personas enviar correo electrónico a una dirección, donde el mensaje es copiado y enviado a otros subscriptores de las lista. De esta manera, las personas que tienen distintas formas de acceso a el correo electrónico puedan participar en discusiones colectivas.

Megabyte
Un millón de bytes.
Ver también: Byte, Bit, Kilobyte

MIME
(Multipurpose Internet Mail Extensions) El estándar para adherir archivos que no son de texto a archivos de correo electrónico de Internet. Los archivos que nos son de texto a archivos de correo electrónicos de Internet. Los archivos que no son de texto incluyen gráficos, hojas de cálculo, documentos, archivos de sonido, etc.

Un programa e-mail es un compilador de MIME si recibe y envía archivos empleando en estándar MIME.

Cuando estos archivos *(no de texto)* son enviados con el estándar MIME son convertidos *(codificados)* a texto que no es leíble. Este estándar generalmente es la manera de especificar como es el archivo al enviarse y como debe de ser regresado a su forma original al ser solicitado.

Además de el software e-mail, el estándar MIME es también universalmente usado por los servidores de red para identificar a los archivos que son enviados a los clientes de este servidor, de esta forma al acomodar nuevos formatos de archivos se hace simplemente actualizando los pares de tipos MIME del Browser y el software apropiado para manejar cada tipo.
Ver también: Browser, Cliente, Servidor, Binhex, UUENCODE

Modem
(Modulator, DEModulator) Un dispositivo que conecta una computadora a una línea telefónica y permite a la computadora comunicarse con otras computadoras mediante el sistema telefónico. Básicamente, los módem son para las computadoras como los teléfonos para los humanos.

MOO
(Mud, Object Oriented) Uno de varios tipos de tipos de ambientes muti-usuario de tipo role-playing, hasta ahora solo basados en texto.
Ver también: MUD

Mosaic
El primer browser para WWW disponible para Macintosh, Windows y Unix todos con la misma interface. Mosaic fue el que inicio la popularidad de la red. Ahora se han desarrollado mejor software como el Internet explorer de Microsoft y el Nestcape.
Ver también: Browser, Cliente, WWW

MUD
(Multi-User Dungeon ó Dimensión) Comúnmente basado en texto, es un simulador de ambiente. La mayoría para el entretenimiento y otros para desarrollo de software y educativos.
Ver también: MOO,MUD

N

Netiquette
La etiqueta en el Internet.
Ver también: Internet

Netizen
Derivado del término citizen, hace referencia a un citizen en Internet, o alguien que emplea recursos de redes. El término conecta responsabilidades civiles y la participación.
Ver también: Internet

Netscape
Un browser para WWW y el nombre de un compañía. El Browser Netscape fue originalmente basado en el Mosaic desarrollado en "National Center for Supercomputing Applications *(NCSA)*", y fue creciendo agregando características que pronto le dieron el lugar del mejor Browser existente. La compañía Netscape también produce software para servidores de red.

Netscape ofrecía mas adelantos en la conexión de interface sobre todos los demás Browsers, y a generados debates al agregar nuevos elementos al lenguaje HTML – pero estos elementos no son universalmente aceptados.

El principal autor del Netscape, Mark Andreessen, fue contratado por NCSA por Jim Clark y juntos fundaron la compañía llamada Mosaic Communications y pronto cambiaron el nombre a Netscape Communications Corportation.

Newsgroup (grupo de noticias)
El nombre que se le da a los grupos de discusión en USENET.
Ver también: USENET

NIC
(Networked Information Center)
Generalmente, cualquier oficina que maneje información de una red. El más famoso de estos en Internet es el InterNIC, que es donde los nuevos Domain Names son registrados

Node (nodo)
Cualquier computadora por si sola conectada a una red.
Ver también: Network, Internet, internet

P

Packet Switching
El método empleado para transportar datos en Internet, toda la información proveniente de una máquina es dividida en pedazos y cada uno de estos tiene una dirección hacia donde se dirige y hacia donde va. Esto permite a los pedazos de información de distintos lugares mezclarse en la misma línea, es por eso que varias persona pueden usar simultáneamente una sola línea.

Password (contraseña)
Un código empleado para tener acceso aun systema restringido. Las contraseñas mas efectivas contienen letras y números con siete dígitos.
Ver también: Login

POP
Dos significados comunes: Point of Presence y Post Office Protocol. La primera, Point of Presence, se refiere a una ciudad o localidad donde una red puede conectarse comúnmente con líneas dial-up. Entonces si una compañía anuncia que pronto tendrá un POP en Monterrey, significa que ellos tendrán pronto un teléfono local en Monterrey y/o un lugar donde líneas dedicadas podrán conectarse a su red.

El segundo significado, Post Office Protocol, se refiere a la manera en que el software del correo electrónico como el Eudora recibe el correo de un servidor. Cuando se obtiene un SLIP,PP ó una cuenta shell casi siempre se obtiene una cuenta POP junto, y esta cuenta POP será la que se le indicara a el software del correo electrónico que use
Ver también: SLIP, PPP

PORT **(puerto)**
3 significados. Primero y más general, un lugar donde la información entra o sale de una computadora. (ej.: puerto serial)

En Internet un puerto se refiere a un número que es parte de un URL, y aparece después del colón(:) después del Domain Name. Cada

servicio en servidores Internet en lista un número estándar de un puerto por ejemplo, los servidores de red normalmente tienen el puerto 80. Los servicios pueden ser también enlistados en puertos no estándar, este es el caso donde el puerto debe estar especificado en un URL cuando se accesa al servidor, es por esto que se puede encontrar un URL como el siguiente:Gopher://peg.cwis.uci.edu:7000/

Enseña un servidor gopher que corre en un puerto no estándar (el puerto gopher es 70).

Por último, un puerto se refiere en traducir un pedazo de software de un tipo de computadora a otro, por ejemplo el traducir un programa de Windows de tal manera que corra en una Macintosh.
Ver también: Domain Name, Server, URL

Posting
Un solo mensaje introducido a una red de un sistema de comunicación.
Ver también: Newsgroup (grupo de noticias)

PPP
(Point to Point Protocol) El protocolo conocido como aquel que permite a una computadora el usar un teléfono común y un módem para hacer conexiones TCP/IP y entonces accesar Internet.
Ver también: IP Number, Internet, SLIP, TCP/IP

R

Red (Network)
Cualquier vez que se conecten 2 o más computadoras de tal manera que puedan compartir recursos, se tiene entonces una red. Si se conectan 2 o más redes y se tienen una internet.
Ver también: internet, Internet, Intranet

Router (ruteador)
Una computadora o software específico que maneja la conexión entre dos o mas redes. Los ruteadores pasan todo el tiempo observando las direcciones de destino de los paquetes que pasan por ellos y deciden por que ruta serán enviados.
Ver también: Packet Switching

S

Server (servidor)
Una computadora, o un paquete de software, que provee un tipo específico de servicio a un software de cliente ubicado en otras computadoras. El término se puede referir a una pieza específica de software, como es el caso del servidor de WWW, o a la máquina en donde el software este corriendo, por ejemplo; un servidor de correo esta fuera de servicio el día de hoy, es por eso que no hay correo saliente. Un solo servidor puede contener distintos tipos de paquetes de software corriendo, esto provee muchos servidores a los clientes de la red.
Ver también: Cliente, Red

SLIP
(Serial Line Internet Protocol) Un estándar para emplear una línea telefónica común (*una línea Serial)* y un Modem para conectar una computadora a un site Internet. SLIP esta siendo gradualmente reemplazado por el PPP.
Ver también: Internet, PPP

SMDS
(Switched Multimegabit Data Service) Un nuevo estándar para transmisores de datos de alta velocidad.

Spam (ó Spamming)
Un intento inapropiado de usar un mailing list *(lista de correo)*, ó USENET u otro medio comunicativo de tipo "broadcast".

Ejemplo: Jessica " spammed" 50 grupo USENET al enviar el mismo mensaje a cada uno.
Ver también: Maillist, USENET

Sysop (sistema operador) *(System Operator)* Cualquier responsable de operaciones físicas en un sistema de cómputo ó en un recurso de red. Un Administrador de Sistema decide que tan seguido de deben de realizar respaldos de información y procedimientos de mantenimiento y los Sysop realizan estas actividades.

T

T-1
Una línea arrenada o dedicada capaz de transferir datos a 1,544,000 bits – por-segundo. Teóricamente una T-1 a su máxima capacidad de transmisión transporta un megabyte en menos de 10 segundos. Sin embargo, esto no es lo suficiente rápido para pantallas completas con movimiento general, para las cuales se requiere al menos 10,00,000 bits- por-segundo. Una T-1 es el medio más rápido comúnmente usado para realizar conexiones a Internet.
Ver también: 56Line, Bandwidth,Bit,Byte,Ethernet, T-3

T-3
Un línea dedicada capaz de transferir datos a 44,736,000 bits-por-segundo. Esto es más que suficiente para pantalla completas que requieran movimiento general.
Ver también: 56Line, Bandwidth,Bit,Byte,Ethernet,,T-1

TCP/IP
(Transmission Contrl Protocol/Internet Protocol) El protocolo que mejor describe a internet. Originalmente diseñado para sistemas operativos UNIX, el software TCP/IP es ahora disponible para cualquier sistema operativo mayor. Para poder tener una conexión a Internet una computadora requiere TCP/IP.
Ver también: IP Number, Internet, UNIX

Telnet
El comando empleado para realizar un login de un site Internet a otro. El comando/software telnet da acceso a el prompt login del servidor al que de se desea conectar.

Terminal
Un dispositivo que permite enviar comandos a una computadora ubicada en otro lugar. Como mínimo esto es un teclado y una pantalla y un conjunto sencillo de circuitos. Comúnmente se usa el software de una terminal en una computadora personal—el software pretende ser (emular) una terminal física y permite teclear comandos a una computadora lejana.

Terminal Server (servidor terminal) Una computadora específica que permite conectar varios módems de uno de sus lados y una conexión a una red LAD o a otro servidor del otro lado. La mayoría de estos servidores proveen servicios PPP y SLIP si están conectados a Internet. Este servidor contesta llamadas en los módems y las transfiere a los nodos adecuados.
Ver también: LAN, Modem, Host, Nodo,PPP, SLIP

TTFN
(Ta Ta For Now) Una abreviatura de un comentario realizado en un foro Internet.
Ver también: IMHO, BTW

U

UNIX
Un sistema operativo diseñado para ser usado por un grupo de varias personal al mismo tiempo(multi-usuario) que maneja TPC/IP. Es el

sistema operativo más común en los servidores Internet.

URL
(Uniform Resource Locator) La manera estándar de asignar direcciones de cualquier recurso en Internet que forma parte del WWW. URL se parece a lo siguiente:

http://www.matisse.net/seminars.html

ó telnet://well.sf.ca.us

ó
news:new.newusers,questions etc.

El modo más común de emplear un URL es al emplear un Browser del WWW como el Explorer y el Netscape.
Ver también: Browser,WWW

USENET
Grupos de discusión alrededor del mundo, con comentarios a través de cientos de miles de máquinas. No todas las máquinas USENET se encuentran en Internet. USENET es completamente descentralizado, con alrededor de 10,000 áreas de discusión, llamados newsgruops (grupo de noticias).
Ver también: Newsgruop

UUENCODE
(Unix to Unix Encoding) Un método para convertir archivos de código Binario a ASCII *(texto)* de tal manera que puedan ser enviados en Internet vía e-mail.
Ver también: Binhex, MIME

V

Veronica
(Very Easy Rodent Oriented Net-wide Index to Computerized Archives) Desarrollado en la Universidad de Nevada, Veronica es una base de datos constantemente actualizada de nombres de casi todos los menús de miles de servidores gopher. La base de datos Veronica por la mayoría de los servidores gopher.
Ver también: Gopher

W

WAIS
(Wide Area Information Servers) Un software comercial que permite asignar categorías a grandes cantidades de información, para después poder tener acceso con índices a información en Internet. Una de las principales características del WAIS es que los resultados de búsqueda que se hacen en ella despliegan los resultados por orden de importancia donde los resultados van del más acertado al menor.

WAN
(Wide Area Network) Una red internet que cubre un área mayor a un solo edificio, edificio o campus.
Ver también: Internet, internet, LAN, Red

Web
Ver: WWW

WWW
(World Wide Web) Dos significados- Primero, no muy común: la constelación entera de recursos que pueden ser accesados empleando Gopher, FTP,HTTP,telnet, USENET, WAIS y otras herramientas. Segundo, el universo de servidores hypertext (*servidores HTTP*) que son los servidores que permiten mezclar texto, gráficos, archivos de sonido, etc