UNIVERSIDAD DEL VALLE DE MATATIPAC, S.C.
CON ESTUDIOS INCORPORADOS A LA UNAM CLAVE 8854

"ADICIÓN DEL FRAUDE INFORMÁTICO AL CÓDIGO PENAL PARA EL ESTADO DE NAYARIT"

TESIS

QUE PARA OBTENER EL TITULO DE

LICENCIADO EN DERECHO

PRESENTA:

OCTAVIO GONZÁLEZ GAONA

ASESORES:

MTRO. DANIEL SALVADOR GARZA CÁCERES

ASESOR TÉCNICO.

LIC. IRMA CARMINA CORTES HERNANDEZ

ASESOR METODOLÓGICO

TEPIC, NAYARIT; JUNIO DE 2007.

D E D I C A T O R I A

A Dios: *Por haberme dado vida para lograr llegar hasta este momento y poderlo compartir con todos mis seres queridos.*

A mis padres: *se que mis logros son sus logros, y es un orgullo poder compartir con ustedes este paso tan importante, el camino para llegar hasta este momento no fue sencillo, pero la carga fue mas ligera por que siempre me ayudaron a soportarla y me impulsaron a seguir adelante. Todo cuanto soy se los debo a ustedes, a su ayuda, a sus enseñanzas, a su ejemplo y a la manera en que me han guiado cuando más lo he necesitado, ahora es mi turno de retribuirles un poco de lo mucho que me han dado y de agradecerles el estar siempre ahí para mi. Gracias.*

A mis Hermanas: *Por el apoyo incondicional que siempre me han brindado y por estar conmigo como siempre en los buenos y malos momentos.*

A mi familia: *La familia es el núcleo de la sociedad, mi familia es el núcleo de mi vida, la encargada de resaltar mis atributos pero también de hacerme notar mis errores, gracias por el apoyo, los consejos que siempre me han dado y por estar ahí cuando es necesario.*

A mis Maestros: *Quienes con gran acierto supieron transmitirnos sus conocimientos, y darnos las herramientas necesarias para enfrentarnos a la vida profesional.*

A mi Institución: *Por haberme dado una formación académica de excelencia.*

C O N T E N I D O

INTRODUCCIÓN.....I
PRÓLOGO.....VI

CAPÍTULO PRIMERO

ANTECEDENTES

1.1. EL DELITO DE CUELLO BLANCO----------1
1.2. EL FRAUDE----------3
1.3. LA INFORMÁTICA Y LOS DELITOS INFORMÁTICOS.----------4
1.3.1. Fraudes Cometidos Mediante Manipulación de Computadoras.----------9
1.3.2. Falsificaciones Informáticas.----------10
1.3.3. Daños o Modificaciones de Programas o Datos Computarizados----------11
1.4. EL FRAUDE ELECTRÓNICO Y EL PHISHING.----------12

CAPÍTULO SEGUNDO

DESARROLLO DEL FRAUDE.

2.1. DESARROLLO HISTÓRICO----------14
2.2. ESTUDIO DOGMÁTICO DEL FRAUDE----------21
2.2.1. Clasificación del Delito.----------21
2.2.2. Imputabilidad e Inimputabilidad.----------24
2.2.3. Conducta y su Ausencia.----------25
2.2.4. Tipicidad y Atipicidad.----------27
2.2.5. Antijuricidad Y Causas de Justificación.----------29
2.2.6. Culpabilidad e Inculpabilidad.----------29
2.2.7. Condiciones Objetivas de Punibilidad y su ausencia.----------30
2.2.8. Punibilidad y Excusas Absolutorias.----------30
2.3. ASPECTOS COLATERALES DEL DELITO----------31
2.3.1. Vida del Delito.----------31
2.3.2. Participación.----------32
2.3.3. Concurso de Delitos.----------33

2.3.4. Acumulación.----------33

CAPÍTULO TERCERO

DERECHO COMPARADO.

3.1. Legislación Nacional.----------34
3.1.1. Código Penal para el Estado de Aguascalientes----------35
3.1.2. Código Penal para el Estado de Baja California----------37
3.1.3. Código Penal para el Distrito Federal----------38
3.1.4. Código Penal para el Estado de México----------41
3.1.5. Código Penal para el Estado de De Morelos----------42
3.1.6. Código Penal para el Estado de Puebla----------44
3.1.7. Código Penal para el Estado de Quintana Roo----------45
3.1.8. Código Penal para el Estado de Tabasco----------46
3.1.9. Código Penal para el Estado de Sinaloa----------48
3.1.10. Código Penal para el Estado de Tamaulipas----------48
3.1.11. Código Penal para el Estado de Yucatán----------50
3.2. TRATAMIENTO Y LEGISLACIÓN INTERNACIONAL----------51
3.2.1. Organismos Internacionales (OCDE)----------51
3.2.2. Tratado de Libre Comercio de América del Norte (TLC)----------57
3.2.3. Legislación en otros países----------59

CAPÍTULO CUARTO

PATRIMONO E INFORMÁTICA.

4.1. EL BIEN JURÍDICO TUTELADO.----------67
4.1.1. Patrimonio como Bien Jurídicamente Tutelado.----------68
4.1.2. Delitos contra el Patrimonio.----------69
4.2. LA INFORMÁTICA Y EL DERECHO.----------73
4.2.1. Informática Jurídica.----------74
4.2.2. Derecho de la Informática.----------75
4.2.3. El Desarrollo del Sistema Jurídico Informático en México y la Regulación Jurídica del Internet.----------76

4.2.4. Descripción de Los Términos en La Informática: Los Url, I.P y El Top Level Domain----------79

CAPÍTULO QUINTO

EL FRAUDE INFORMÁTICO EN PARTICULAR.

5.1. AUSENCIA DE LA TIPICIDAD.----------83
5.2. EL PHISHING----------85
5.2.1. Respuesta Social Ante El Phishing.----------88
5.2.2. Respuestas Legislativas Y Judiciales Ante El Fraude Informático.----------89
5.3. FRAUDE GENÉRICO EN EL ESTADO DE NAYARIT.----------93
5.4. ESTUDIO DOGMÁTICO DEL DELITO DE FRAUDE INFORMÁTICO----------96

CONCLUSIONES----------102
PROPUESTAS----------104
ANEXOS----------106
GLOSARIO----------109
BIBLIOGRAFÍA----------115

INTRODUCCIÓN

Mucho se habla de los beneficios que los medios de comunicación y el uso de la Informática han aportado a la sociedad actual, pero a su vez, se ha abierto la puerta a conductas antisociales y delictivas que se manifiestan de formas que hasta ahora no era posible imaginar. Los sistemas de informáticos ofrecen oportunidades nuevas y sumamente complicadas formas de infringir la ley, y han creado la posibilidad de cometer delitos de tipo tradicional en formas no tradicionales.

Los llamados delitos informáticos no son cometidos por la computadora, sino que es el hombre quien los comete con ayuda de aquella. En ese entendido, este trabajo se dirige al análisis de las posibles medidas preventivas, ya sean de carácter administrativo o penal que consideramos 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 dado en otros países.

Uno de esos delitos, es el fraude informático, el cual es cometido por una persona con amplios conocimientos en materia de informática, encaminado a provocar un menoscabo en el patrimonio de una o más personas, utilizando medios informáticos para lograrlo, alcanzando un lucro indebido para si o para otro.

En el Capítulo I de esta investigación, se presentan los antecedentes del delito, de los delitos de cuello blanco, un acercamiento a los delitos informáticos, al delito de fraude y a su nueva vertiente conocida como el Fraude Informático, y a la conducta denominada Phishing.

Acto seguido, en el Capítulo II, se abordará el desarrollo histórico del delito de fraude, desde sus primeros días, cuando era conocido como Estelionato, hasta llegar a un Estudio

Dogmático del mismo, para conocer sus clasificaciones, cuando es imputable e inimputable el sujeto activo, la conducta y la ausencia de esta, la tipicidad y atipicidad.

Después se analizará en el Capítulo III, la legislación que regula administrativa y penalmente las conductas ilícitas relacionadas con la informática, pero que aún no contempla el fraude informático. En este entendido, se considera pertinente 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.

A continuación, en el Capítulo IV, se expondrá la definición del bien jurídico tutelado, para así llegar a las definiciones de patrimonio y de informática; todo esto para dar un antecedente al tema de este trabajo de investigación. En cuanto al patrimonio, se evocarán los conceptos proveídos por el derecho civil y por el derecho penal, analizando dichos conceptos, para lograr un mayor entendimiento en cuanto al Patrimonio; se analizarán los delitos en contra del patrimonio que contiene el Código Penal del Estado de Nayarit. Se presentará el vínculo que guarda el Patrimonio y la Informática y en cuanto a esta última, se señalarán definiciones de informática, de los medios utilizados para la conexión virtual entre ordenadores en todo el mundo y de las formas en que se regula por el derecho en la actualidad.

Para finalizar la presente investigación, se abordará en el Capítulo V las definiciones de Atipicidad y de la ausencia de esta, de la conducta atípica conocida como "Phishing", la respuesta social ante el Phishing, las respuestas Legislativas y judiciales ante fraude informático, así como los antecedentes en cuanto a los castigos de los primeros delitos informáticos y los primeros ataques, casos en concreto; se revisará al delito de Fraude Genérico en el Estado de Nayarit y se realizará un estudio dogmático preliminar de lo que trata el delito de Fraude Informático, delito el cual se presenta la conducta que causa una deficiencia en la aplicación de la justicia, al no encontrarse establecida en la norma penal.

En Nayarit no existe el tipo penal en cuanto al Fraude informático, así como lo aparece en otros Estados de la Republica los cuales cuentan en sus respectivos Código Penal. Es por la imposibilidad de adecuación al tipo penal del fraude informático, en el Estado de Nayarit, que se dirige esta investigación al análisis de la tipificación del mismo, logrando evitar la comisión de este tipo de infracciones o delitos en el Estado.

Es por todo lo expuesto en este trabajo que es absolutamente necesaria la existencia del tipo penal correspondiente al Fraude Informático en las letras de la legislación Penal del Estado de Nayarit, para evitar que la comisión de este tipo de conducta delictiva continúe llevándose a cabo impunemente en el Estado.

PRÓLOGO

Los últimos cincuenta años de la historia de la humanidad se caracterizan por un grado de avance tecnológico que deja atrás, de manera avasallante, los avances tecnológicos de mil años atrás.

Resultaría impensable imaginar un mundo como el actual sin el apoyo de los ordenadores o computadoras. Miles y miles de procesos diarios, de todas clases y naturalezas, serían irrealizables sin el apoyo de este tipo de tecnología.

De la misma manera, la realización de actividades que buscan producir resultados benéficos para la humanidad, en ocasiones se ven empañadas por acciones humanas que utilizan esta tecnología para causar el mal.

Son este tipo de acciones las que motivan a los estudiosos del Derecho a realizar estudios que le permita al sistema de justicia seguir el avance, primero, de la tecnología, y después, de los procesos sociales que serán fuente e inspiración de la norma.

Este trabajo es fruto del esfuerzo constante y atento de Octavio González Gaona, emprendedor, tenaz alumno y compañero; inquieto estudiante y excelente amigo; acucioso investigador y, en general, una persona valiosa en todos los sentidos.

Ha logrado un trabajo recepcional que servirá perfectamente parar lograr el objetivo de la obtención del grado de licenciatura; no dudo ni por un instante de la sustentación del examen profesional que ha de seguir como consecuencia de la realización de este documento; tampoco dudo que obtendrá éxito en su desempeño profesional, porque éstas son las características más visibles del carácter de Octavio González Gaona: su perseverancia y anhelo de superación.

CARLOS EDUARDO HERRERA LOPEZ.

CAPÍTULO I. ANTECEDENTES

En este capítulo primero, se presentará las definiciones tanto de delito de cuello blanco, como acto antijurídico cometido por personas de alto nivel intelectual y técnico, el de fraude cometido por medio del dolo y del engaño para lograr un acto antijurídico, de los delitos informáticos cuyo nivel de conocimiento va más allá del conocimiento técnico y, una vez analizados los tres anteriores se llegará a una definición provisional del delito que funge como título a este trabajo de tesis, el fraude informático y señalar una de las prácticas delictuosas más cercana al tipo que se pretende incorporar al tipo penal del fraude, esta es "El Phishing".

1.1 EL DELITO DE CUELLO BLANCO

Como delito se entiende el acto típicamente antijurídico, imputable a una persona y cometido en agravio de otras personas o leyes, y que se encuentra sancionado por una ley. En 1939 cuando el importante sociólogo de la escuela de Chicago, Edwin Hardin Sutherland publicó un libro llamado *The white collar criminal,* en el cual explica su investigación con la que demostró que la delincuencia no está directamente relacionada con la pobreza ni con otras condiciones como las sociales o psicológicas con las que comúnmente se asocia.

Edwin H. Sutherland, definió el delito de cuello blanco como " un delito cometido por una persona de respetabilidad y estrato social alto en el curso de su ocupación"[1], dicho autor señala grandes números de conductas que considera como delitos de cuello blanco, aun cuando muchas de tales conductas no se encuentran tipificadas en la norma como delitos, y dentro de las cuales es prudente señalar las quiebras fraudulentas, la evasión de impuestos, la clonación de tarjetas de crédito, el robo de identidad o de cualquier otra información.

[1] SUTHERLAND Edwin H. *the white collar criminal*, nomadas, revista critica de ciencias sociales y juridicas | issn 1578-6730

Para Sutherland, la delincuencia de cuello blanco es un acto socialmente perjudicial, que afecta directamente, pues aunque exista conciencia de tales delitos la mayoría de las veces no se logra una trascendencia en el castigo, ya que la ley penal no es aplicada con igualdad debido a que el sujeto activo de estos delitos, en la gran mayoría de estos, son personas de un nivel económico más elevado de lo normal y con conocimientos superiores a los de la mayoría de la población.

Los múltiples delitos de cuello blanco se pueden dar en diferentes ámbitos; generalmente se ven en la política, en la medicina así como en la industria y el comercio, aunque no se está exento de encontrar actos corruptos en otras áreas. Estos son ilícitos como lo son los fraudes, la malversación o desviación de fondos, sobornos, tráfico de influencias, abuso de autoridad, prácticas laborales injustas, estafas, extorsión, incumplimientos, abuso y/o violación de confianza, que como se ve, son cometidos por personas de negocios "respetables" y profesionales como empresarios, políticos, banqueros, magistrados, servidores públicos, incluso profesores, entre otros, que gozan de una imagen de prestigio por ser profesionistas titulados o aquellos a los que la sociedad otorga su confianza, suelen tratarse de personas indiscutiblemente inteligentes, mas a su vez inmorales, ya que conocen bien la profesión o cargo que desempeñan así como la forma en que pueden cometer sus delitos sin ser descubiertos, pues conocen la ley así como sus capacidades y limitaciones.

Como todo criminal, los criminales de cuello blanco tienen un perfil o características en común, entre las cuales destacan el narcisismo, el egocentrismo, el materialismo, la hipocresía y la peligrosidad, puesto que al cometer los delitos, estos buscan además del lucro o el daño que logran, el renacimiento de otras personas del mismo nivel que los alientan a sobresalir en sus cometidos.

Uno de los muchos delitos de cuello blanco que existen, es el denominado como Fraude, cuya definición más común se encuentra en el Codigo Penal Federal en su artículo trescientos ochenta y seis (386) mismo que versa de la siguiente manera: "Comete el delito de fraude el

que engañando a uno o aprovechándose del error en que éste se halla se hace ilícitamente de alguna cosa o alcanza un lucro indebido"[2].

1.2 EL FRAUDE.

El fraude como delito, según Eduardo López Betancourt se contempla como "Una Conducta delictiva que lesiona el patrimonio de las personas, y que está reglamentado en nuestro Código Penal Federal".[3] Para Eduardo López Betancourt el fraude es una acción cuya finalidad es evadir toda norma o disposición legal, siempre que con ello se logre un perjuicio en contra del estado o contra terceros. En el Código Penal para el Estado de Nayarit, se contempla el fraude como "el que engañando a alguno o aprovechándose del error en que éste se halla, se haga ilícitamente de una cosa o alcance un lucro indebido para sí o para otro"[4]; los elementos que distinguen al fraude, son señalados por los juristas como el engaño o aprovechamiento del error; Mariano Jiménez Huerta señala la esencia del delito de fraude, la cual "es el engaño de que se vale el sujeto activo para hacerse, en perjuicio de otro, de un objeto de ajena pertenencia"[5]; el engañar significa dar apariencia de verdad a lo que es mentira; provocar una falsa concepción de algo. Un rasgo característico del delito de fraude es que carece de medios violentos; además, para la integración del delito de fraude debe existir una relación inmediata y directa entre los dos elementos, el engaño o aprovechamiento del error debe ser previo a la obtención ilícita de la cosa o al alcance del lucro indebido y al mismo tiempo, la causa determinante de una o de otra.

El fraude implica una dinámica comisiva más ideológica, que permite incluir dentro de ella transferencias de fondos, operaciones bancarias y créditos, que suponen un desplazamiento patrimonial con independencia de la materialidad del traslado real. Giuseppe Maggiore, usa como referencia el Código Penal Italiano, nos indica cuales son los delitos contra el patrimonio, cometidos mediante el fraude, siendo estos la estafa, la insolvencia fraudulenta, engaño a

---

[2] *Código Penal Federal*, México, Ed. Isef.
[3] LOPEZ BETANCOURT, Eduardo, *Delitos en Particular*, tomo I, Ed. Porrúa, México 2004, p.p.305.
[4] *Código Penal para El Estado de Nayarit,* México, Ed. Don Pepe.
[5] JIMENEZ HUERTA, Mariano, *Derecho Penal Mexicano.* Parte Especial, tomo IV, Ed. Antigua Librería Robredo, México 1963, p.p. 148 y 149.

personas incapaces, usura, apropiación indebida y receptación. El mismo Maggiore formula un concepto de fraude el cual "consiste en el hecho de quien, al inducir a otro a error por medio de artificios o engaños, obtiene para sí mismo o para otros algún provecho injusto, con perjuicio ajeno"[6]. El penalista Francesco Carrara denomina al delito como Estelionato, en virtud de que considera que el fraude es una característica de varios delitos patrimoniales; nos dice al respecto del estelionato "que su carácter es precisamente configurar un despojo injusto de la propiedad ajena, que no es ni verdadero hurto ni verdadero abuso de confianza, ni verdadera falsedad, pero que participa del hurto, porque ataca injustamente la propiedad ajena; del abuso de confianza, porque se abusa de la buena fe de otros, y de la falsedad, porque a ella se llega mediante engaños y mentiras"[7].

1.3 LA INFORMÁTICA Y LOS DELITOS INFORMÁTICOS:

La Real Academia Española de la Lengua proporciona una definición de Informática[8] "es el conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de ordenadores".n Las redes de comunicación electrónica y los sistemas de información forman parte integrante de la vida diaria de los ciudadanos en el mundo y desempeñan un papel fundamental en el éxito de la economía universal. Cada vez están más interconectadas y es mayor la convergencia de los sistemas de información y las redes. Esta tendencia implica sin duda, numerosas y evidentes ventajas, pero va acompañada también de un riesgo inquietante de ataques malintencionados contra los sistemas de información. Estos ataques pueden adoptar distintas formas, como el acceso ilegal, la difusión de programas perjudiciales, robos de identidad, acceso no autorizado y fraudes electrónicos.

Los ataques contra los sistemas de información constituyen una amenaza para la creación de una sociedad de la información más segura y de un espacio de libertad, seguridad y justicia.

---

[6] MAGGIORE, Giussepe, *Derecho Penal.* Parte Especial, volumen V, Ed. Temis, Bogotá Colombia 1989, p. 122.
[7] CARRARA, Francesco, *Programa de Derecho Criminal,* tomo 6, Ed. Temis, Bogotá Colombia 1966, p413.
[8] Real Academia de la Lengua Española. (http://www.rae.es/)

A nivel doctrinal no existe una definición uniforme de delito informático, de manera que un sector de los juristas considera que los delitos informáticos, como tales, no existen, pues argumentan que estos sólo son delitos normales cuya única diferenciación de otro delito cualquiera, es en las herramientas empleadas o en los objetos sobre los que se producen. Para otro grupo de juristas, existen muchos delitos que difícilmente pueden quedar definidos bajo los tipos penales de la mayoría de los ordenamientos actuales y por consecuencia, éstos se tendrán que adaptar o redactar acorde a los nuevos tiempos, con el afán de evitar impunidad de conductas transgresoras del orden social que ameritan un reproche de naturaleza penal.

Un delito informático, son todas aquellas conductas encaminadas a la comisión de hechos ilícitos que hacen uso indebido de cualquier medio informático, y que son susceptibles de ser sancionadas por el derecho penal.

Dichos delitos son conductas delictivas de cuello blanco (white collar crimes)[9], en tanto que sólo determinado número de personas con ciertos conocimientos técnicos, pueden llegar a cometerlos. Son acciones ocupacionales porque muchas veces se realizan cuando el sujeto está en el trabajo, y de oportunidad debido a que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico. Los delitos informáticos provocan serias pérdidas económicas para los afectados y casi siempre producen beneficio de más de cinco cifras para aquellos que los realizan; los delitos informáticos ofrecen facilidades de tiempo y espacio, ya que en milésimas de segundo y sin la necesaria presencia física pueden llegar a cometerse. Estos delitos se presentan en su mayoría dolosos o intencionales, presentan grandes dificultades para su comprobación, esto por su carácter técnico, y tienden a proliferar cada vez más entre los menores de edad.

Las personas que cometen los Delitos informáticos poseen ciertas características que no presenta el denominador común de los delincuentes; de ahí que se asemejan a los delitos de cuello blanco, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos

[9] SUTHERLAND Edwin H. *the white collar criminal*, nómadas, revista critica de ciencias sociales y jurídicas | issn 1578-6730

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. Con el tiempo se ha podido comprobar que los autores de los delitos informáticos son muy diversos y que lo que los diferencia entre sí es la naturaleza de los cometidos. De esta forma, la persona que entra en un sistema informático sin intenciones delictivas es muy diferente del empleado de una institución financiera que desvía fondos de las cuentas de sus clientes. El nivel típico de aptitudes del delincuente es tema de controversia ya que para algunos en el nivel de aptitudes no es indicador de delincuencia informática en tanto que otros aducen que los posibles delincuentes informáticos son personas listas, decididas, motivadas y dispuestas a aceptar un reto tecnológico, características que pudieran encontrarse en un empleado del sector de procesamiento de datos.

Argibay Molina señala que "delitos informáticos son todas aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio informático"[10]. El delito informático implica actividades criminales que en un primer momento los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robo, fraudes, falsificaciones, perjuicios, estafa, sabotaje, etc.; sin embargo, debe destacarse que el uso indebido de las computadoras es lo que ha propiciado la necesidad de regulación por parte del derecho.

La Asamblea General de las Naciones Unidas, en su resolución 52/91 de 12 de diciembre de 1997, decidió que uno de los cuatro cursos prácticos que se celebrarían en el marco del Décimo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente versaría sobre el tema de los delitos relacionados con la red informática.

La Asamblea, en su resolución 53/110 de 9 de diciembre de 1998, hizo suyo el programa de trabajo del Décimo Congreso, que incluía cuatro cursos prácticos de carácter técnico, uno de ellos referente a los delitos relacionados con la red informática. En esa misma resolución, la

[10] MOLINA, Argibay, *<http://www.aaba.org.ar/bi180p32.htm>* Consulta 30 de Marzo de 2007)

Asamblea subrayó la importancia de los cursos prácticos e invitó a los estados miembros, las organizaciones no gubernamentales y otras entidades pertinentes a que apoyaran los preparativos de los cursos prácticos en los planos financiero, de organización y técnico, incluida la elaboración y distribución de documentación de antecedentes conexa.

La aparición de redes internacionales informáticas, como Internet, permite a los usuarios entablar comunicaciones, actividades y transacciones con otros usuarios de todo el mundo. Dado que las computadoras y las redes pueden ser objeto a la vez de uso legítimo y de uso ilícito, se impone la conclusión de que entre quienes exploran las oportunidades del nuevo medio hay personas y grupos impulsados por motivos delictivos. La lucha contra la delincuencia en el actual entorno de redes informáticas internacionales se complica debido a tres causas principales":

a) El comportamiento delictivo puede producirse en un entorno electrónico. La investigación de los delitos cibernéticos, es decir, de cualquier delito cometido en una red electrónica, exige conocimientos técnicos especializados, procedimientos de investigación y facultades legales de que tal vez carezcan las autoridades encargadas de hacer cumplir la ley del Estado interesado;

b) Las redes informáticas internacionales, como Internet, son medios abiertos que permiten que los usuarios actúen más allá de las fronteras del Estado en el que están situadas. Pero la labor investigadora de las autoridades encargadas de hacer cumplir la ley deben circunscribirse en general al territorio de su propio Estado. Esto significa que, la lucha contra la delincuencia en las redes de computadoras abiertas requiere una intensificación de la cooperación internacional;

c) Las estructuras abiertas de las redes informáticas internacionales ofrecen a los usuarios la oportunidad de elegir el entorno jurídico que mejor se ajuste a sus propósitos. Los usuarios pueden elegir un país en el que determinadas formas de comportamiento que puedan

desarrollarse en un entorno electrónico no se hayan tipificado como delitos. Esto puede atraer la actividad de personas de otros estados en cuyos ordenamientos jurídicos esas mismas actividades constituyan un delito. La existencia de "paraísos informáticos" estados que no dan prioridad a la reducción o prevención del uso ilícito de las redes de computadoras, o donde no se han elaborado leyes de procedimiento eficaces- puede obstaculizar los esfuerzos de otros países por combatir los delitos relacionados con las redes de computadoras".

El examen que figura a continuación se centra en la manera de lograr una acción internacional coordinada para facilitar, mejorar y perfeccionar los actuales métodos de lucha contra la delincuencia cibernética. Reviste particular interés el papel que pueden desempeñar las Naciones Unidas u otras organizaciones internacionales.[11] Se proporciona información general acerca del curso práctico sobre delitos relacionados con las redes informáticas.

Además, se esbozan los tipos de delito previstos con respecto a las redes electrónicas internacionales y se exploran las razones por las cuales esos delitos requieren una atención y esfuerzos combinados internacionales. La definición de tales delitos debería facilitar una interpretación internacional común y orientar las políticas penales nacionales en esa esfera.

El delito informático está en relación con todo comportamiento ilegal que atente contra la seguridad de sistemas y datos mediante operaciones electrónicas. La seguridad de los sistemas y datos informáticos puede determinarse en función de tres principios: garantía de confidencialidad, integridad o disponibilidad de los datos y funciones de procesamiento. De conformidad con la lista de la Organización de Cooperación y Desarrollo Económicos, de 1985 y la Recomendación formulada en 1989 por el Consejo de Europa, que es más detallada, los delitos contra la confidencialidad, la integridad o la disponibilidad incluyen:

[11] 10º CONGRESO DE LAS NACIONES UNIDAS SOBRE PREVENCION DEL DELÍTO Y TRATAMIENTO DEL DELINCUENTE

1.3.1.- Fraudes Cometidos Mediante Manipulación de Computadoras:

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

La manipulación de programas. Es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente debe tener conocimientos técnicos concretos de informática. Este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas. Un método común utilizado por las personas que tiene conocimientos especializados en programación informática es el denominado Caballo de Troya, que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.

Manipulación de los datos de salida. Se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos. Tradicionalmente esos fraudes se hacían a base de tarjetas bancarias robadas, sin embargo, en la actualidad se usan ampliamente el equipo y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.

Fraude efectuado por manipulación informática. Que aprovecha las repeticiones automáticas de los procesos de cómputo. Es una técnica especializada que se denomina "técnica de salchichón" en la que "rodajas muy finas" apenas perceptibles, de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra.

1.3.2.- Falsificaciones Informáticas.

Como objeto. Cuando se alteran datos de los documentos almacenados en forma computarizada.

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

Acceso no autorizado a sistemas o servicios informáticos: este se da por motivos diversos: desde la simple curiosidad, como en el caso de muchos piratas informáticos (hackers) hasta el sabotaje o espionaje informático.

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

Reproducción no autorizada de programas informáticos de protección legal: puede entrañar una pérdida económica sustancial para los propietarios legítimos. Algunas

jurisdicciones han tipificado como delito esta clase de actividad y la han sometido a sanciones penales. El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones modernas.

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

Sabotaje informático. Es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema. Las técnicas que permiten cometer sabotajes informáticos son:

Virus. Es una serie de claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos. Un virus puede ingresar en un sistema por conducto de una pieza legítima de soporte lógico que ha quedado infectada, así como utilizando el método del Caballo de Troya.

Gusanos. Se fabrica en forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse. En términos médicos podría decirse que un gusano es un tumor benigno, mientras que el virus es un tumor maligno. Ahora bien, las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus; por ejemplo, un programa gusano que subsiguientemente se destruirá puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita.

Bomba lógica o cronológica. Exige conocimientos especializados ya que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro. Ahora bien, al revés de los virus o los gusanos, las bombas lógicas son difíciles de detectar antes de que exploten; por eso, de todos los dispositivos informáticos criminales, las bombas lógicas son las que poseen el máximo potencial de daño. Su detonación puede programarse para que cause

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

1.4 El Fraude Electrónico Y El Phishing.

Ajustándose en el tipo penal del fraude, en el que se tutela el patrimonio; este tipo penal es de comisión necesariamente dolosa, en el que, además, se encuentra presente un dolo específico del autor tendiente a la obtención ilícita de la cosa. La gran diferencia entre el robo y el fraude es que, en el primer supuesto, el bien es obtenido por el agente del delito sin el consenso del pasivo. Por eso, el verbo típico rector de la figura delictiva es apoderarse, mientras que en el segundo, el pasivo entrega voluntariamente la cosa, en virtud del engaño o del aprovechamiento de error que vician su voluntad.

Según la corriente dominante, en el delito de fraude, el engaño o aprovechamiento de error tiene que dirigirse necesariamente contra una persona, en virtud de que la nota distintiva del delito es que el paciente del delito vea viciada su voluntad y entregue la cosa, por tanto, no puede verificarse el fraude sobre máquinas ni sobre personas privadas de razón e, incluso, la doctrina menciona que contra los incapaces tampoco; en el robo y abuso de confianza, dicha circunstancia no es necesaria. El objeto materia del apoderamiento ilícito en el robo y la cosa de que dispone el activo en el abuso de confianza deben forzosamente tener el carácter de bienes muebles (robo equiparado); en el caso del fraude, el objeto material es mucho más amplio ya que el activo puede obtener cualquier prestación, no necesariamente una cosa, pues el término lucro denota cualquier ventaja de carácter patrimonial.

Consecuentemente, si se parte de la idea de que una máquina no puede ser objeto de engaño, no puede hablarse en estos casos de que pueda verificarse el verbo típico consistente en engañar o aprovecharse del error en que alguien se encuentra, característicos del fraude, mientras que, con independencia de establecer si puede hablarse de un apoderamiento ilícito, lo

cierto es que en este tipo de conductas que se verifican mediante el empleo de medios informáticos el objeto sobre el que recae la conducta no es en todos los casos un bien mueble, más aun, cuando lo que obtiene el agente del delito es un servicio, de lo que se sigue entonces que en estos casos existen serias dudas para encuadrar los hechos bajo el tipo penal de fraude como en el tipo penal de robo.

El término phishing proviene de la palabra en inglés *fishing* que significa pesca haciendo alusión al acto de pescar usuarios mediante señuelos cada vez más sofisticados, y de este modo obtener información financiera y contraseñas. Quien lo practica es conocido con el nombre de phisher, y también se dice que el término "*phishing*" es la contracción de "*password harvesting fishing*" (cosecha y pesca de contraseñas), aunque esto probablemente es un acrónimo retroactivo.

Los intentos más recientes de phishing han tomado como objetivo a clientes de bancos y servicios de pago en línea. Aunque el ejemplo que se muestra en la primera imagen es enviado por phishers de forma indiscriminada con la esperanza de encontrar a un cliente de dicho banco o servicio, estudios recientes muestran que los phishers en un principio son capaces de establecer con qué banco una posible víctima tiene relación, y de ese modo enviar un e-mail, falseado apropiadamente, a la posible víctima. En términos generales, esta variante hacia objetivos específicos en el phishing se ha denominado *spear phishing* (literalmente *phishing con lanza*). Los sitios de Internet con fines sociales también se han convertido en objetivos para los phishers, dado que mucha de la información provista en estos sitios puede ser utilizada en el robo de identidad. Algunos experimentos han otorgado una tasa de éxito de un 70% en ataques phishing en redes sociales.

A finales del 2006 un gusano informático se apropió de algunas páginas del sitio web MySpace logrando redireccionar los enlaces de modo que apuntaran a una página web diseñada para robar información de ingreso de los usuarios.

CAPÍTULO II. DESARROLLO DEL FRAUDE.

En el presente capítulo se abordarán el desarrollo histórico del delito de fraude, desde sus primeros días, cuando era conocido como Estelionato, hasta llegar a un Estudio Dogmático del mismo, para conocer sus clasificaciones, cuando es imputable e inimputable el sujeto activo, la conducta y la ausencia de esta, la tipicidad y atipicidad.

2.1. DESARROLLO HISTÓRICO.

Durante el Imperio Romano, el delito de fraude se separó de la figura delictiva del Hurto; dando entonces surgimiento al estelionato. Así, la estafa y la apropiación indebida figuraban, entre los romanos dentro del concepto general del fraude o Estelionato.

El fraude era definido como el dolo en el Digesto, siendo así toda astucia, falacia o maquinación empleada para engañar, burlar y cegar a otros. Giuseppe Maggiore en su obra de nombre Derecho Penal, decía que el estelionato "Comprendía todo atentado fraudulento contra el patrimonio ajeno, mediante alguna improbidad y perfidia (quedam perfidia et improbitas). Su pena era el trabajo, las minas para los humiliores y el destierro corporal para los honestiores"[11].

Maggiore tenia la idea de que en el derecho germánico y en el canónico se reprimen varios casos de fraude, pero que a falta de una doctrina unitaria del delito, estos casos son ignorados. El derecho medieval no presentó mejor tributo, las legislaciones modernas se esforzaron por distinguir entre el fraude punible y el dolo puramente civil.

[11] MAGGIORE, Giuseppe, *Derecho Penal,* op. Cit., p. 11. Ed. Janniti

En la Legislación Española en las Siete Partidas, así como en la legislación toscaza, el delito de Estelionato, no se definía, pero se daban las formas de cómo se podía realizar, en las cuales se distinguían los artificios delictuosos.

Mariano Jiménez Huerta, en su obra El Derecho Penal Mexicano, cuenta que "El Código del Manú castigaba al que vendía grano malo por bueno, cosa vil por fragrante, cristal de roca colorado por piedra preciosa, hilo de algodón por hilo de seda, hierro por plata, etc; el Código de Hamumurabit sancionaba las falsificaciones de pesas y medidas; las leyes hebraicas sancionaban a los comerciantes ávidos de abusar de los compradores necesitados; y el Corán a los que se aprovechaban de las condiciones del comprador para venderle, o del vendedor para comprarle, a precio, respectivamente mayor o menor del justo valor de la cosa o hacían uso de cualquier artificio dirigido a acrecentar el aparente valor de la merced"[12].

En la Época Precortesiana, el delito de fraude tiene su antecedente más antiguo entre los aztecas, quienes castigaban la alteración en el mercado de las medidas establecidas por los jueces con la pena de muerte sin demora, en el lugar de los hechos. En la Época Colonial estaba reglamentado en las Siete Partidas.

El 07 de Diciembre de 1871, conocido como Código de Martínez de Castro pues esta obra de una comisión presidida por Antonio Martínez de Castro, aparece el Primer Código Penal Mexicano en materia federal. Dicho ordenamiento regulaba dos ilícitos en cuanto al fraude: el Fraude contra la propiedad y la Quiebra Fraudulenta, en sus Capítulos V y VI respectivamente, del Título Primero Delitos contra la Propiedad y en su Libro Tercero De los Delitos en Particular.

[12] JIMENEZ HUERTA, Mariano. "*Derecho Penal Mexicano"*, op. Cit., p.147.

En su exposición de motivos, en el capítulo que trata del fraude se halla el Artículo 430, en que se prohíbe a los hacendados y a los dueños de fábricas y talleres, da a los operarios, en pago de su salario o jornal, tarjas, plachuelas de cualquier materia u otra cosa que no corra como moneda en el comercio, bajo la pena de pagar como multa el doble de la cantidad a que ascienda la raya de la semana en que se haya hecho el pago de esa manera. Esta prevención tuvo por objeto cortar el escandaloso abuso que cometían en algunas haciendas, fábricas y talleres, de hacer así los pagos para obligar á los jornaleros á que compraran allí cuanto necesitaban dándoles efectos de mala calidad y a precios muy altos. Por falta de una disposición semejante se ha ido arraigando este mal, a pesar de las quejas que alguna vez llegaron hasta el Supremo Gobierno.

Conforme a la quiebra, en la misma exposición de motivos se enuncia que siendo ya muy frecuente el delito de quiebra fraudulenta é inadecuadas las penas de la legislación que regia, era necesario señalar otras y fijar reglas para el castigo de ese grave delito, como lo fue la comisión en el Capitulo IV del Título I.

Dicha código establecía dentro del Capítulo de Fraude contra la Propiedad, que había tal, siempre que engañando a uno, o aprovechándose del error en que éste se halla, se hace otro ilícitamente de alguna cosa o alcanza un lucro indebido, con perjuicio de aquél. (Art. 413).

Dentro de este mismo capítulo, regulaba que el fraude tomaba el nombre de estafa, cuando el que quiere hacerse de una cantidad de dinero en numerario, en papel moneda o billetes de banco, de un documento que importa obligación, liberación o transmisión de derechos, ó de cualquiera otra cosa ajena mueble, logra que se la entreguen por medio de maquinaciones ó artificios que no constituyan un delito de falsedad. Esto al reglamentarse se equiparaba al delito de robo sin violencia.

Sancionaba dentro de este capítulo, al que por título oneroso enajenare una cosa y entregara intencionalmente otra distinta de la que contrató (Art. 418); el que por título oneroso enajenara una cosa en precio mayor del que realmente tenía (419); cuando intervenía a nombre del dueño otra persona y cometiera el engaño (Art. 420); al que engañara al comprador sobre la cantidad o peso de la cosa vendida (Art. 421); el que se propusiera defraudar sin acuerdo con el falseador haciendo uso de moneda falsa o alterada, de pesas o medidas falsas o alteradas, o de algún documento falso, agravándose la pena si se tratara de empleado público (Art. 222); al que vendiera medicinas o comestibles falsos, entre otros[13]

Dentro del Capítulo de la Quiebra Fraudulenta, se establecía que al comerciante á quien se declare alzado, se le impondrán cinco años de prisión, si el deficiente que resultare de su quiebra no excediere de mil pesos. Cuando exceda de esa cantidad, se formará el término medio de la pena aumentado á los cinco años un mes más de prisión, por cada cien pesos de exceso; pero sin que dicho término medio pueda pasar de diez años (Art. 434)[14]

El 30 de septiembre de 1929, aparece un nuevo Código Penal que deroga al anterior de 1871, que también fue como Código Almaraz, y que estuvo vigente hasta 1932; dicho ordenamiento suprimió la denominación de fraude contra la propiedad y, en su mismo Capítulo V pone en su lugar el nombre de Estafa a la misma conducta delictiva que el código de 1872 regulaba, sólo agregó un caso más en que habría estafa, quedando el artículo 1151 de la siguiente manera:

"Artículo 1151.- Hay estafa:

1. *Siempre que engañando a uno, o aprovechándose del error en que éste se halla, se hace otro ilícitamente de alguna cosa, o alcanza un lucro indebido con perjuicio de aquél;*

[13] CÓDIGO PENAL MEXICANO DE 1871.
[14] Idem

2. *Cuando el que quiere hacerse de una cantidad de dinero en numerario, en papel moneda o en billetes de banco de un documento que importe obligación, liberación o transmisión de derechos, o de cualquier otra cosa ajena mueble, logra que se la entreguen por medio de maquinaciones, engaños o artificios"*[15].

Dicha ley, fusionaba lo que hoy en día son los delitos de fraude y estafa, toda vez que en aquel tiempo, no existía la definición del tipo penal de fraude, en un mismo artículo, en dos fracciones, y a los dos se los consideró como estafa.

En el Capítulo IV, cambia su denominación al delito De la Quiebra Culpable o Fraudulenta, modificando su concepto, estableciendo en el Artículo 1171: *"Al comerciante quebrado que fulgare o se ausentare sin motivo grave y justificado y sin dejar en su establecimiento persona autorizada para representarlo y con los elementos necesarios para hacer los pagos debidos, se le impondrán cinco años de segregación, si el deficiente que resultare de su quiebra no excediere de mil pesos. Cuando exceda de esta cantidad, se formará el término medio de la sanción, aumentando a los cinco años un mes de segregación por cada cien pesos de exceso; pero sin que dicho término medio pueda pasar de doce años. La misma sanción se impondrá al comerciante quebrado que hubiere destruido, inutilizado u ocultado todos o parte de los libros de su contabilidad"*[16].

También en este capítulo castigaba al fallido que hubiere ocultado o enajenado sus bienes en fraude de sus acreedores, o para favorecer a uno de ellos con perjuicio de los otros (Art. 1172); al corredor o agente de cambio y a cualquier persona mayor de edad que, teniendo prohibición legal de comerciar, comerciaren y quebraren

[15] CÓDIGO PENAL DE 1929
[16] Idem

fraudulentamente o culpablemente (Art. 1176); señala quiénes serán cómplices en la quiebra fraudulenta (Art. 1177).

El 14 de Agosto de 1931, se publicó en el Diario Oficial de la Federación un nuevo Código Penal Federal que entra en vigor a partir del 17 de septiembre de 1931, mismo que continúa vigente. Dicho código elimina las denominaciones de los anteriores ordenamientos, dejando en su Capítulo III, del Título Vigésimo Segundo el delito de fraude, donde aparece el concepto de fraude genérico como se encuentra en la legislación vigente, pero en este ordenamiento se presenta dentro de un listado de conductas delictivas, entre los fraudes específicos, menos de los actualmente establecidos. Así, el Artículo 386 en su fracción I establece: "se impondrá de una multa de cincuenta a mil pesos y prisión de seis meses a seis años:

1. Al que engañando a uno, o aprovechándose del error en que éste se halla, se haga ilícitamente de alguna cosa o alcance un lucro indebido"[17].

El código de 1931, con anterioridad a las reformas actuales, para la aplicación de sanciones, no tomaba en cuenta el valor de lo defraudado establecido en las tres fracciones del Artículo 386 del Código Penal vigente, pues solamente en el artículo 388 ordenaba que cuando el valor de lo defraudado no excediera de cincuenta pesos, se castigaba el delito con multa de cinco a cincuenta pesos y prisión de tres días a seis meses, o ambas sanciones según era el caso, actualmente este artículo ha sido reformado por completo.

[17] Código Penal Federal 1932

El Código Penal Federal vigente al 20 de Febrero del 2007, estipula lo siguiente en su Artículo 386:

"Artículo 386. Comete el delito de fraude el que engañando a uno o aprovechándose del error en que éste se halla se hace ilícitamente de alguna cosa o alcanza un lucro indebido. El delito de fraude se castigará con las penas siguientes:

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

II. Con Prisión de 6 meses a 3 años y multa de 10 a 100 el salario, cuando el valor de lo defraudado excediera de 10, pero no de 500 veces el salario.

III. Con prisión de tres a doce años y multas hasta de ciento veinte veces el salario, si el valor de lo defraudado fuere mayor de quinientas veces el salario"[18].

Dicho ordenamiento, como se menciona en párrafos anteriores, toma en cuenta el valor de lo defraudado, dando a cada uno una pena en proporción.

En el Código Penal para el Estado de Nayarit, se menciona el Fraude en el Capítulo IV, artículo 368, el cual enuncia que:

"ARTÍCULO 368.- Comete el delito de fraude, el que engañando a alguno o aprovechándose del error en que éste se halla, se haga ilícitamente de una cosa o alcance un lucro indebido para sí o para otro.

[18] CODIGO PENAL FEDERAL Legislación Federal (Vigente al 20 de febrero de 2007), México, Ed. ISEF

El delito de fraude se sancionará con las penas siguientes:

I. Con prisión de tres días a dos años y multa de diez a treinta días de salario, cuando el valor de lo defraudado no exceda de cien veces del salario mínimo vigente.

II. Con prisión de dos a seis años y multa de quince a sesenta días de salario, cuando el valor de lo defraudado excediera de cien pero no de quinientas veces el salario.

III. Con prisión de seis a doce años y multa hasta de veinte a cien días de salario, si el valor de lo defraudado fuere mayor de quinientas veces el salario.

Cuando el sujeto pasivo entregue la cosa de que se trata a virtud no solo de engaños, sino de maquinaciones o artificios que para obtener esa entrega se hayan empleado, la pena señalada en las fracciones anteriores, se aumentará con prisión de tres días a dos años.[19]*"*

Dicho artículo enuncia en los mismos preceptos que el Código Penal Federal, haciendo una breve aclaración en cuanto al uso de maquinaciones o artificios, aumentando la pena, gracias al uso de estos.

2.2 ESTUDIO DOGMÁTICO DEL DELITO DE FRAUDE.

A continuación se presenta la clasificación dogmática propia del delito de fraude.

2.2.1 Clasificación Del Delito.

[19] CODIGO PENAL PARA EL ESTADO DE NAYARIT, Código publicado en la Segunda Sección del Periódico Oficial del Estado de Nayarit, el sábado 22 de Agosto de 1981.

Por su Gravedad: Es un delito, porque viola una norma jurídica, siendo sancionado por la autoridad judicial.

Según la conducta del agente: está se separa en dos preceptos:

1.- De Acción.- El fraude es un delito de acción a virtud de que con la conducta del agente se produce un hecho, consistente en el engaño.

2.- De Comisión por omisión.- También se puede presentar mediante una omisión, cuando éste produce un resultado material. Se puede presentar respecto al aprovechamiento del error.

Por el Resultado:

1.- Material: El fraude es un delito de resultado material, porque con su acción (engaño) o su comisión por omisión (aprovechamiento del error), se produce un mutuamiento en el mundo exterior, lesionando el bien jurídicamente tutelado por la norma penal, consistente en el daño patrimonial. Este resultado material se fundamente en dos hipótesis: que el sujeto se haga ilícitamente de una cosa o que alcance un lucro indebido.

Por el daño que causa:

1.- De Lesión: el fraude provoca un daño directo y efectivo al bien jurídicamente tutelado, que en este caso, provoca la disminución del patrimonio del ofendido.

Por su Duración:

1.- Instantáneo: esto es, porque se consuma cuando el agente se hace de una cosa o alcanza un lucro indebido.

Por el elemento interno:

1.- Dolo: el delito de fraude sólo puede presentarse en forma dolosa mediante el dolo directo, es decir, el agente al producir el resultado, coincide con su voluntad de delinquir.

Por su estructura:

1.- Simple: porque tutela un solo bien jurídico: El patrimonio de las personas.

Por el número de Actos:

1.- Unisubsistente: porque el delito se consuma en un solo acto.

Por el número de sujetos:

1.- Unisubjetivo: este delito requiere para su integración la participación de un sujeto.

Por su forma de persecución:

1.- De Querella: es un delito que se persigue a petición de parte ofendida en todas sus modalidades.

El Artículo 370, párrafo segundo establece respecto a la persecución del fraude:

"Los delitos equiparables a la figura delictiva de fraude en las fracciones IV, V, VI y VII señaladas en el artículo 369, solamente se perseguirán a petición de parte ofendida, siendo, aplicable además en lo conducente los artículos 349, 353 y 356."[20].

En función de su materia.

1.- Federal: en virtud de que se encuentra regulado en nuestro Código Penal Federal, es de aplicación Federal.

[20] CODIGO PENAL DEL ESTADO DE NAYARIT

2.- Común: Será de esta clase, cuando el delito en estudio se ejecute en el ámbito local, sujetándose a la ley penal correspondiente.

Clasificación Legal.

Título Vigésimo Segundo "Delitos contra las personas en su patrimonio", del Código Penal Federal. Y Título Vigésimo "Delitos contra el Patrimonio" del Código Penal para el Estado de Nayarit.

2.2.2 Imputabilidad e Inimputabilidad.

Será imputable del delito de fraude el agente con capacidad de querer y entender en el ámbito del derecho, que no padezca de ningún trastorno mental o desarrollo intelectual retardado. Los Menores de edad son imputables, solamente están sujetos a otro régimen jurídico.

Las acciones libres en su causa se pueden presentar en el delito de fraude cuando el agente se coloque en estado de inimputablidad, como lo establece el Artículo 15 fracción VII del Código Penal Federal y el artículo 20 del Código Penal para el Estado de Nayarit; los cuales excluyen al delito cuando el agente padece de trastorno mental o desarrollo intelectual retardado, especificando después; a no ser que el agente hubiere provocado su trastorno mental dolosa o culposamente, en cuyo caso responderá por el resultado típico simple y cuando lo haya previsto o le fuere previsible.

La inimputabilidad, se da cuando a un sujeto no se le puede hacer responsable de un delito, a virtud de su incapacidad mental o minoría de edad para algunos autores. Las causas de inimputabilidad son, aludiendo al artículo 15, fracción VII del Código Penal Federal, cuando:

"VII. 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 agente hubiere provocado su trastorno mental dolosa o culposamente, en cuyo caso responderá por el resultado típico siempre y cuando lo haya previsto o le fuere previsible.

Cuando la capacidad a que se refiere el párrafo anterior sólo se encuentre considerablemente disminuida, se estará a lo dispuesto en el artículo 69 bis de este Código".

En el Código Penal para el Estado de Nayarit, se enuncia lo siguiente:

"CAPÍTULO VII
CAUSAS DE INIMPUTABILIDAD
ARTÍCULO 20.- Son causas de inimputabilidad:

I. la condición de personas menores de dieciséis años;

II. El trastorno mental; y

III. III. La sordomudez y la ceguera de nacimiento o que sobrevenga antes de los siete años de edad, cuando haya falta de instrucción.

2.2.3 Conducta y su Ausencia.

2.2.3.1: Conducta: esta presenta una clasificación:

1.- Acción.- el fraude es un delito de acción respecto al elemento del engaño, a virtud de que el agente requiere realizar un acto positivo, consistente en un movimiento corporal, para que produzca el resultado.

2.- Comisión por omisión: También se puede presentar el delito de fraude por comisión por omisión, cuando se trata del aprovechamiento.

2.2.3.2: Sujetos: estos son activo y Pasivo.

1.- Activo: en el delito de fraude genérico regulado por el artículo 386, así como en los de fraude específico regulados por el artículo 387 en sus fracciones I, II, III, IV, V, VI, VII, VIII, IX, X, XI, XIV, XVIII, XXI; 388, 388 bis y 389 bis, será cualquier persona que engañe o se aproveche del error en que se encuentra otro, para hacerse ilícitamente de alguna cosa o alcanzar un lucro indebido. En los casos de los artículos 387 fracción XII, XIII y 389, serán respectivamente el fabricante, empresario, contratista o constructor de una obra cualquiera; el vendedor de materiales de construcción o cualquier especie; los constructores o vendedores de edificios en condominio; quien tenga un cargo en el gobierno en una empresa descentralizada o de participación estatal o de cualquier agrupación de carácter sindical, o que tenga relaciones con los funcionarios o dirigentes de dichos organismos.

2.- Pasivo: En el delito de Fraude genérico y en los específicos, con excepción del artículo 387 fracciones VII y XIX tercer párrafo, el sujeto pasivo puede ser cualquier persona física o moral, quien sufre el daño patrimonial. En el caso del 387 fracciones VII y XIX tercer párrafo, los sujetos pasivos serán respectivamente el primero o segundo comprador y las personas morales.

2.2.3.3 Objetos: estos son material y jurídico:

1.- Material: será la cosa obtenida ilícitamente por el agente, o el lucro indebido.

2.- Jurídico: el objeto jurídico en el delito de fraude es el patrimonio.

2.2.3.4: Lugar y Tiempo de la Comisión del Ilícito.

De acuerdo al sistema penal vigente en Nayarit, si el delito de fraude se cometiera en territorio extranjero por un mexicano contra mexicano o contra extranjero, por un extranjero contra mexicano, serán penados en el Estado de Nayarit, con arreglo a las leyes federales, siempre que concurran los requisitos establecidos por el Código Penal para el Estado de Nayarit, en su artículo 2:

"ARTÍCULO 2o.- Se aplicará asimismo por los delitos que se inicien, preparen o cometan fuera del Estado, cuando se produzcan o se pretenda tengan efectos en el territorio de Nayarit, si los hechos delictuosos tienen ese carácter en la Entidad en que se ejecuten y en el Estado de Nayarit, siempre que no se haya sentenciado definitivamente por ellos al responsable en la localidad en que delinquió o en otro lugar"[21].

2.2.3.5: Ausencia de conducta. Se puede presentar como causa de ausencia de conducta, en un caso extremo, el hipnotismo.

2.2.4 Tipicidad y Atipicidad:

1.- Tipicidad:

[21] *Código Penal para el Estado de Nayarit*, México, Ed. Don Pepe

a).- Tipo: se encuentran descritos, tanto el fraude genérico como el específico, respectivamente en el artículo 368 -370 del Código Penal para el Estado de Nayarit.

b).- Tipicidad: se presentará en el delito de fraude cuando se adecue la conducta a cualquiera de los tipos mencionados con antelación, es decir, a los elementos descritos en el precepto legal.

c).- Clasificación:

- Por su composición: Es un tipo anormal, porque además del elemento objetivo contiene elementos normativos. El hacerse ilícitamente de una cosa o alcanzar un lucro indebido.
- Por su ordenación Metodológica: el fraude es un delito fundamental o básico, por tener plena independencia y estar formado con una conducta ilícita sobre un bien jurídicamente tutelado, es decir, no contiene circunstancia alguna que agrave o atenúe la penalidad.

- En función de su autonomía: el fraude es un tipo autónomo ya que tiene vida propia, no depende de la realización de ningún otro tipo penal para su perpetración.

- Por su formulación: es casuístico en virtud a que está formado por dos hipótesis, se puede cometer el delito de fraude por engaño o aprovechamiento del error.

- Por el daño: es de lesión porque el resultado material daña directamente al bien jurídicamente tutelado que es el patrimonio de las personas.

2.- Atipicidad:

a).- Ausencia de calidad exigida por la ley en cuanto a los sujetos activos.

b).- Por falta del objeto material, es decir, que no exista la cosa o el lucro indebido.

c).- Por falta de objeto jurídico: el patrimonio de las personas.

d).- Al no realizarse el hecho por los medios comisitos específicamente señalados.

2.2.5 Antijuricidad y causas de Justificación.

1.- Antijuricidad: al cometer el delito de fraude está realizando una conducta antijurídica, es decir, contraria a derecho. Para que esta antijuricidad se presente, el agente no debe haber actuado bajo ninguna causa de justificación.

2.- Causas de Justificación: obediencia jerárquica.

2.2.6 Culpabilidad e Inculpabilidad.

1.- Culpabilidad: el delito de fraude, como ya se mencionó, sólo se puede presentar mediante dolo directo.

2.- Inculpabilidad:

a).- Error esencial de hecho invencible: la inculpabilidad se puede presentar por error de tipo y error de licitud (eximentes putativas); por error de tipo cuando el agente por error esencial e invencible no sabe que está realizando alguno de los elementos del tipo; por error de licitud cuando el sujeto cree actuar bajo alguna causa de legalidad.

b).- No exigibilidad de otra conducta: cuando se atenta las circunstancias que concurren en la realización de una conducta ilícita, no sea racionalmente exigible al agente de una conducta diversa a la que realizó, en virtud de no haberse podido determinar a actuar conforme a derecho (Art. 15 Fracc. IX).

2.2.7 Condiciones Objetivas de Punibilidad y su ausencia.

No se presentan, por consiguiente, hay ausencia de condiciones objetivas de punibilidad.

2.2.8 Punibilidad y Excusas Absolutorias.

1.- Punibilidad: se encuentra establecida en los artículos:
Artículo 368.- El delito de fraude se sancionará con las penas siguientes:

I. Con prisión de tres días a dos años y multa de diez a treinta días de salario, cuando el valor de lo defraudado no exceda de cien veces del salario mínimo vigente.

II. Con prisión de dos a seis años y multa de quince a sesenta días de salario, cuando el valor de lo defraudado excediera de cien pero no de quinientas veces el salario.

III. Con prisión de seis a doce años y multa hasta de veinte a cien días de salario, si el valor de lo defraudado fuere mayor de quinientas veces el salario.

Cuando el sujeto pasivo entregue la cosa de que se trata a virtud no solo de engaños, sino de maquinaciones o artificios que para obtener esa entrega se hayan empleado, la pena señalada en las fracciones anteriores, se aumentará con prisión de tres días a dos años."[22]

2.- Excusas Absolutorias: No existen.

2.3 ASPECTOS COLATERALES DEL DELITO.

2.3.1 Vida del Delito.

a).- Fase Interna: Se presenta en la psique del agente cuando surge la idea de cometer el delito de fraude, después la delibera y finalmente decide ejecutarla.

b).- Fase Externa: Es cuando el agente exterioriza su idea, prepara todos los elementos necesarios para la realización del ilícito y finalmente lo ejecuta.

c).- Ejecución: el delito de fraude se consuma en el momento en que el agente por medio del engaño o aprovechamiento del error, se hace ilícitamente de alguna cosa o alcanza un lucro indebido.

d).- Tentativa: se puede presentar en el delito de fraude, la tentativa acabada e inacabada.

---

[22] *Código Penal para el Estado de Nayarit.* México, Ed. Don Pepe

- Tentativa Acabada: Se presenta cuando la gente tiene el propósito de cometer el delito de fraude pero no se efectúa por causas ajenas a su voluntad, es el delito frustrado. Es decir, en la tentativa acabada hay realización de todos los actos de ejecución, sin que se consuma el delito por causas ajenas a la voluntad del agente.

- Tentativa Inacabada: se presenta en el delito de fraude cuando por causas independientes a la voluntad del sujeto, el delito no se realiza, esto es, el agente omite ejecutar uno o varios actos que eran necesarios para el resultado previsto.

2.3.2 Participación.

a).- Autor Material: perpetra directamente en el delito de fraude.

b).- Coautor: En unión del autor material comete el ilícito, realizando conductas descritas en el tipo penal.

c).- Autor Intelectual: prepara la realización del delito e induce a otro a su ejecución.

d).- Autor Mediato: No comete directamente el hecho delictivo, acude a otra persona extraña que utiliza como instrumento para su realización.

e).- Cómplice: Se presente en este tipo penal cuando un individuo ayuda al agente en acciones secundarias encaminadas a su ejecución.

f).- Encubridor: Oculta al culpable, los efectos, objetos o instrumentos del hecho criminoso.

2.3.3 Concurso de Delitos.

a).- Ideal.- El concurso ideal se presenta cuando con una conducta se cometen varios delitos.

b).- Material: es el concurso de delitos en el que, con varias conductas, se cometen varios delitos distintos.

2.3.4 Acumulación.

El Sistema Jurídico Mexicano, en caso de acumulación de delitos, utiliza el método de acumulación jurídica, que consistirá en tomar como base para la imposición de la sanción el delito mayor, al que se le irán sumando proporcionalmente las sanciones de los demás ilícitos cometidos, si que exceda de los máximos señalados por la ley penal.

CAPÍTULO III DERECHO COMPARADO.

Para el desarrollo de este capítulo se analizará la legislación que regula administrativa y penalmente las conductas ilícitas relacionadas con la informática, pero que aún no contempla el fraude informático. En este entendido, se considera pertinente 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 de toda la Unión.

3.1 LEGISLACIÓN NACIONAL

La Constitución Política de los Estados Unidos Mexicanos, consagra la garantía de la protección del derecho a la información y el derecho a la privacidad de las comunicaciones previstas en el artículo 6, la legislación mexicana cuenta escasamente con once tipos penales previstos en el Código Penal Federal, en su Título Noveno denominado Revelación del Secreto y Acceso Ilícito a Sistemas y Equipos de Informática específicamente en los artículos 210, 211 y 211-bis al 211-Bis-7, Título vigésimo Sexto denominado Delitos en materia de Derechos de Autor, artículo 424-Bis.

Existen algunas disposiciones jurídicas que regulan de alguna forma el fenómeno informático y se encuentran contempladas en otros ordenamientos como el Código de Comercio, Código Fiscal de la Federación, diversas leyes federales como la Ley Federal de Derechos de Autor, Ley Federal de Protección al Consumidor, Ley Federal de Estadística, Geografía e Historia y en la reciente Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

En las legislaciones locales solamente once entidades contemplan en sus ordenamientos penales algunas modalidades de los delitos informáticos, estas entidades son: Aguascalientes, Baja California, Distrito Federal, Estado de México, Morelos, Puebla, Quintana Roo, Sinaloa, Tabasco, Tamaulipas y Yucatán, tal y como se aprecia en las siguientes tablas:

3.1.1 Código Penal para el Estado de Aguascalientes[23]:

"TÍTULO DÉCIMO PRIMERO; DELITOS EN CONTRA DE LA CONFIDENCIALIDAD

CAPITULO I: Revelación de Secretos

ARTÍCULO 195.- La Revelación de Secretos consiste en el aprovechamiento de archivos informáticos personales o en la revelación de una comunicación reservada que se conozca o que se haya recibido por motivo de empleo, cargo o puesto, sin justa causa, con perjuicio de alguien y sin consentimiento del que pueda resultar perjudicado.
Al responsable de Revelación de Secretos se le aplicarán de 3 meses a 1 año de prisión y de 15 a 30 días multa.

ARTÍCULO 196.- Si el inculpado de la Revelación de Secretos presta sus servicios profesionales o técnicos, o se trata de un servidor público; o el secreto revelado es de carácter industrial o científico, la punibilidad será de 1 a 5 años de prisión y de 30
a 50 días multa.

TÍTULO VIGÉSIMO PRIMERO; DELITOS CONTRA LA SEGURIDAD EN LOS MEDIOS INFORMÁTICOS Y MAGNÉTICOS

CAPÍTULO I: Acceso sin Autorización
ARTICULO 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.

---

[23] *Código Penal para el Estado de Aguascalientes,* México. Porrúa

Cuando el Acceso sin Autorización tenga 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.

CAPÍTULO II: Daño Informático

ARTICULO 224.- El Daño Informático consiste en la indebida destrucción o deterioro parcial 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”

3.1.2 Código Penal para el Estado de Baja California[24]:

"LIBRO SEGUNDO; PARTE ESPECIAL; SECCIÓN PRIMERA; DELITOS CONTRA EL INDIVIDUO; TITULO TERCERO; DELITOS CONTRA LA INVIOLABILIDAD DEL SECRETO

CAPÍTULO UNICO: REVELACIÓN DEL SECRETO

ARTÍCULO 175.- Fue reformado por Decreto No. 161, publicado en el Periódico Oficial No. 24, de fecha 12 de junio de 1998, Sección I, Tomo CV, expedido por la H. XV Legislatura, siendo Gobernador Constitucional del Estado, el C. Lic. Héctor Terán Terán, 1995-2001; para quedar vigente como sigue:

ARTÍCULO 175.- Tipo y punibilidad.- Al que sin consentimiento de quien tenga derecho a otorgarlo revele un secreto, de carácter científico, industrial o comercial, o lo obtenga a través de medios electrónicos o computacionales o se le haya confiado, y obtenga provecho propio o ajeno se le impondrá prisión de uno a tres años y hasta cincuenta días multa; si de la revelación del secreto resulta algún perjuicio para alguien, la pena aumentará hasta una mitad más. Al receptor que se beneficie con la revelación del secreto se le impondrá de uno a tres años de prisión y hasta cien días multa.

REVELACION DEL SECRETO: Se entiende por revelación de secreto cualquier información propia de una fuente científica, industrial o comercial donde se generó, que sea transmitida a otra persona física o moral ajena a la fuente.

QUERELLA: El delito de revelación de secreto se perseguirá por querella de la persona afectada o de su representante legal.

---

[24] *Código Penal para el Estado de Baja California.* México. Porrúa

SECCION CUARTA; DELITOS CONTRA EL ESTADO; TÍTULO PRIMERO; DELITOS CONTRA LA SEGURIDAD INTERIOR DEL ESTADO

CAPÍTULO IV: TERRORISMO

ARTÍCULO 279 BIS.- Subtipo y Punibilidad.- Se impondrá pena de uno a tres años de prisión y hasta ciento cincuenta días multa, a quien por cualquier forma, ya sea escrita, oral, electrónica, o medio de comunicación, anuncie a un servidor público o particular a sabiendas de su falsedad, la existencia de explosivos, sustancias tóxicas, biológicas, incendiarias o de cualquier otro medio capaz de causar daños en instalaciones públicas o privadas, que produzcan alarma, temor o terror a las personas que se encuentren en su interior, perturben la paz pública o suspendan un servicio.

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".

3.1.3 Código Penal para el Distrito Federal[25]:

"DISTRITO FEDERAL LIBRO SEGUNDO; TÍTULO NOVENO REVELACIÓN DE SECRETOS Y ACCESO ILÍCITO A SISTEMAS Y EQUIPOS DE INFORMATICA

CAPÍTULO II ACCESO ILÍCITO A SISTEMAS Y EQUIPOS DE INFORMATICA

ARTÍCULO 211 bis 1.- Al que sin autorización modifique, destruya o provoque perdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de

[25] *Código Penal Para El Distrito Federal*. México, Porrúa

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 perdida de información contenida en sistemas o equipos de informática del estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.

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

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

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

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

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

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 perdida de información que contengan, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

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

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

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 aumentaran hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno”

3.1.4 Código Penal del Estado de México[26]:

"LIBRO SEGUNDO; TÍTULO PRIMERO; DELITOS CONTRA EL ESTADO; SUBTÍTULO CUARTO; DELITOS CONTRA LA FE PÚBLICA

CAPÍTULO IV
FALSIFICACIÓN Y UTILIZACIÓN INDEBIDA DE TÍTULOS AL PORTADOR, DOCUMENTOS DE CRÉDITO PÚBLICO Y DOCUMENTOS RELATIVOS AL CRÉDITO

Artículo 174.- Se impondrán de cuatro a diez años de prisión y de ciento cincuenta a quinientos días de salario mínimo de multa al que:

I. Produzca, imprima, enajene aún gratuitamente, distribuya, altere o falsifique tarjetas, títulos o documentos para el pago de bienes y servicios o para disposición de efectivo, sin consentimiento de quien esté facultado para ello;

II. Adquiera, utilice, posea o detente indebidamente, tarjetas, títulos o documentos para el pago de bienes y servicios, a sabiendas de que son alterados o falsificados;

III. Adquiera, utilice, posea o detente indebidamente, tarjetas, títulos o documentos auténticos para el pago de bienes y servicios, sin consentimiento de quien esté facultado para ello;

IV. Altere los medios de identificación electrónica de tarjetas, títulos o documentos para el pago de bienes y servicios; y

V. Acceda indebidamente a los equipos de electromagnéticos de las instituciones emisoras de tarjetas, títulos o documentos para el pago de bienes y servicios o para disposición de efectivo.

Las mismas penas se impondrán a quien utilice indebidamente información confidencial o reservada de la institución o persona que legalmente esté facultada para emitir tarjetas, títulos o

[26] *Código Penal del Estado de México.* México, Porrúa.

documentos utilizados para el pago de bienes y servicios. Si el sujeto activo es empleado o dependiente del ofendido, las penas aumentarán en una mitad.

En el caso de que se actualicen otros delitos con motivo de las conductas a que se refiere este artículo se aplicarán las reglas del concurso

CAPÍTULO II DELITOS CULPOSOS

ARTÍCULO 62.- Los delitos culposos se sancionarán con hasta la mitad de las sanciones asignadas al delito doloso que corresponda, salvo que la ley ordene otra cosa. En estos casos, la sanción privativa de libertad no podrá exceder de la dispuesta en el artículo 128. Cuando se trate de sanción alternativa que incluya una no privativa de la libertad, esta circunstancia aprovechará al infractor. Al responsable de delito culposo se le impondrá, igualmente, en su caso, suspensión hasta de cinco años o privación definitiva de los derechos, cargos o funciones correspondientes la actividad en cuyo ejercicio cometió el delito.

ARTÍCULO 63.- Al imponer la sanción correspondiente al delito culposo, el juez tomará en cuenta las reglas generales de individualización previstas en este Código y calificará la gravedad de la culpa, considerando los datos siguientes:
VI. Cualesquiera elementos relevantes, apreciables técnicamente, para la determinación de la gravedad de la culpa cuando los hechos ocurrieron con motivo del funcionamiento de equipos o aparatos eléctricos, electrónicos o mecánicos. A este respecto, se considerará el estado del equipo, vías y demás condiciones de funcionamiento, tratándose de infracciones cometidas con motivo del tránsito de vehículos. Asimismo, en este caso se tomaran en cuenta las condiciones del tiempo y las personales del sujeto cuando se cometió el delito".

3.1.5 Código Penal para el Estado de Morelos[27].

TITULO DUODÉCIMO; DELITOS CONTRA LA MORAL PÚBLICA

[27] *Código Penal para el Estado de Morelos.* México, Porrúa.

CAPÍTULO I

ULTRAJES A LA MORAL PÚBLICA (REFORMADO, P.O. 18 DE OCTUBRE DE 2000)

ARTÍCULO 213.- Se aplicará prisión de seis meses a tres años y de trescientos a quinientos días multa:

II.- Al que realice exhibiciones públicas obscenas por cualquier medio electrónico, incluyendo Internet, así como las ejecute o haga ejecutar por otro;

CAPÍTULO III

CORRUPCIÓN DE MENORES E INCAPACES (ADICIONADO, P.O. 18 DE OCTUBRE DE 2000)

ARTICULO 213 QUATER.- …Si además del delito citado resultase cometido otro, se aplicarán las reglas de acumulación.

Al que procure, facilite o induzca por cualquier medio a un menor, o a un incapaz, a realizar actos de exhibicionismo corporal, lascivos o sexuales, con el objeto y fin de videograbarlo, fotografiarlo o exhibirlo mediante anuncios impresos o electrónicos, incluyendo la Internet, se le impondrá de seis a quince años de prisión y de cien a quinientos días-multa. Se duplicará la sanción a la persona que cometa o consienta cualquiera de las conductas descritas, si fuere ascendiente, hermano, hermana, padrastro, madrastra, tutor, tutora o todo aquel que tenga sobre el menor el ejercicio de la patria potestad.

CAPÍTULO III

FRAUDE PROCESAL

ARTÍCULO 300.- Al que para obtener un beneficio indebido para sí o para otro, simule un acto jurídico o un acto o escrito judicial, o altere elementos de prueba y los presente en juicio, o realice cualquier otro acto tendiente a inducir a error ante autoridad judicial o administrativa, con el fin de obtener sentencia, resolución o acto administrativo contrario a la ley, se le impondrá de seis meses a cinco años de prisión y de cincuenta a cuatrocientos días multa".

3.1.6 Código Penal para el Estado de Puebla[28].

TÍTULO SEPTIMO; SECCION SEGUNDA
CORRUPCION DE MENORES E INCAPACES

Artículo 224 Ter. Quien por cualquier medio, sea directo, mecánico o con soporte informático, electrónico o de cualquier otro tipo, venda, publique, distribuya, exhiba y difunda; transporte o posea con algunos de estos fines, material pornográfico infantil, se le impondrá prisión de dos a cinco años y multa de diez a cien días de salario.

CAPÍTULO DÉCIMO; FALSEDAD; SECCIÓN PRIMERA
FALSIFICACIÓN DE ACCIONES, OBLIGACIONES Y OTROS DOCUMENTOS DE CREDITO PÚBLICO.

Artículo 245 bis.-Se impondrá prisión de tres a nueve años y multa de ciento cincuenta a cuatrocientos días de salario:

I.- Al que produzca, imprima, enajene aún gratuitamente, distribuya o altere tarjetas, títulos, documentos o instrumentos utilizados para el pago de bienes y servicios o para disposición de efectivo, sin consentimiento de quien esté facultado para ello;

II.-Al que adquiera, utilice o posea, tarjetas, títulos, documentos o instrumentos para el pago de bienes y servicios o para disposición de efectivo, a sabiendas de que son alterados o falsificados;

III.- Al que adquiera, utilice, posea o detente indebidamente, tarjetas, títulos o documentos auténticos para el pago de bienes y servicios o para disposición de efectivo, sin consentimiento de quien esté facultado para ello;

---

[28] *Código Penal para el Estado de Puebla.* México, Porrúa.

IV.- Al que adquiere, copie o falsifique los medios de identificación electrónica, cintas o dispositivos magnéticos de tarjetas, títulos, documentos o instrumentos para el pago de bienes y servicios o para disposición de efectivo; y

V.- Al que acceda indebidamente a los equipos y sistemas de cómputo o electromagnéticos de las Instituciones emisoras de tarjetas, títulos, documentos o instrumentos, para el pago de bienes y servicios o para disposición de efectivo.

Las mismas penas se impondrán, a quien utilice indebidamente información confidencial o reservada de la Institución o persona que legalmente esté facultada para emitir tarjetas, títulos, documentos o instrumentos para el pago de bienes y servicios o para disposición de efectivo.

Si el sujeto activo es empleado o dependiente del ofendido, las penas aumentarán en una mitad.

En caso de que se actualicen otros delitos con motivo de las conductas a que se refiere este artículo, se aplicarán las reglas del concurso

3.1.7 Código Penal para el Estado de Quintana Roo[29].

TÍTULO TERCERO; DELITOS CONTRA LA FE PÚBLICA;

CAPÍTULO II
FALSIFICACIÓN DE DOCUMENTOS Y USO DE DOCUMENTOS FALSOS

ARTÍCULO 189-BIS.- Se impondrá hasta una mitad más de las penas previstas en el artículo anterior, al que:

[29] *Código Penal para el Estado de Quintana Roo*. México, Porrúa.

I.- Produzca, imprima, enajena aún gratuitamente, distribuya o altere tarjetas, títulos, documentos o instrumentos utilizados para el pago de bienes o servicios o para disposición en efectivo, sin consentimiento de quien esté facultado para ello.

II.- Adquiera, posea o detente ilícitamente tarjetas, títulos, documentos o instrumentos para el pago de bienes y servicios o para disposición de efectivo a sabiendas que son alterados o falsificados.

III.- Copie o reproduzca, altere los medios de identificación electrónica, cintas o dispositivos magnéticos de documentos para el pago de bienes o servicios para disposición en efectivo.

IV.- Acceda indebidamente los equipos y sistemas de cómputo o electromagnéticos de las instituciones emisoras de tarjetas, títulos, documentos o instrumentos para el pago de bienes y servicios o para disposición de efectivo.

Las mismas penas se impondrán a quien utilice indebidamente información confidencial o reservada de la institución o persona que legalmente esté facultada para emitir tarjetas, títulos, documentos o instrumentos para el pago de bienes y servicios o para disposición de efectivo.

Si el sujeto activo es empleo o dependiente del ofendido, las penas se aumentarán hasta en una mitad más.

En el caso de que se actualicen otros delitos con motivo de las conductas a que se refiere este artículo se aplicarán las reglas del concurso

3.1.8 Código Penal para el Estado de Tabasco[30]:

"CAPITULO V
VIOLACION DE LA COMUNICACION PRIVADA

[30] *Código Penal para el Estado de Tabasco.* México, Porrúa

ARTÍCULO 316.- Al que intervenga la comunicación privada de terceras personas, a través de medios eléctricos o electrónicos, se le aplicará prisión de uno a cinco años

CAPITULO II
DAÑO INFORMATICO

ARTÍCULO 326 bis

1 .- A quien sin autorización modifique, destruya o deteriore en forma parcial o total, archivos, bases de datos o cualquier otro elemento intangible contenido en computadoras personales, sistemas o redes de cómputo, soportes lógicos, o cualquier otro medio magnético, se le sancionará con penas de uno a cinco años de prisión y de cien a cuatrocientos días multa.
Cuando el activo tenga el carácter de encargado del manejo, administración o mantenimiento de los bienes informáticos dañados, las penas se incrementarán en una mitad más.

CAPITULO III
FALSIFICACION INFORMATICA

ARTÍCULO 326 bis 2.- Se impondrán penas de uno a cinco años de prisión, al que copie o imite los originales de cualquier dato, archivo o elemento intangible contenido en una computadora personal o en un sistema de redes de computadoras, base de datos, soporte lógico, siempre que para ello se requiera autorización y no la obtenga.
Las mismas sanciones se aplicarán al que utilice o aproveche en cualquier forma, los bienes informáticos falsificados, previstos en este Título.

ARTÍCULO 326 bis 3.- Cuando los ilícitos previsto en este Título se comentan utilizando el equipo de cómputo de terceras personas, las penas se incrementarán en una mitad. "

3.1.9 Código Penal para el Estado de Sinaloa[31].

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".

Cabe señalar que en Sinaloa se ha contemplado al delito informático como uno de los delitos contra el patrimonio, siendo este el bien jurídico tutelado.

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

3.1.10 Código Penal para el Estado de Tamaulipas[32]

TÍTULO SÉPTIMO

---

[31] *Código Penal para el Estado de Sinaloa*. México, Porrúa
[32] *Código Penal para el Estado de Tamaulipas* México, Porrúa

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

CAPÍTULO II

ACCESO ILICITO A SISTEMAS Y EQUIPOS DE INFORMATICA

ARTÍCULO 207-Bis.- Al que sin autorización modifique, destruya, o provoque pérdida de información contenida en sistemas o equipo de informática protegidos por algún mecanismo de seguridad o que no tenga derecho de acceso a el, se le impondrá una sanción de uno a cuatro años de prisión y multa de cuarenta a ochenta días salario.

ARTÍCULO 207-Ter.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistema o equipo de informática de alguna dependencia pública, protegida por algún mecanismo se le impondrá una sanción de dos a seis años de prisión y multa de doscientos a seiscientos días salario.

ARTÍCULO 207-Quater.- Al que sin autorización conozca o copié información contenida en sistemas o equipos de informática de alguna dependencia pública, protegida por algún mecanismo se le impondrá una sanción de dos a cinco años de prisión y multa de cien a trescientos días salario.

ARTÍCULO 207-Quinquies .- Al que estando autorizado para acceder a sistemas y equipos de informática de alguna dependencia pública, indebidamente modifique, destruye o provoque pérdida de información que contengan se impondrá una sanción de tres a ocho años de prisión y multa de trescientos a ochocientos días salario.

ARTÍCULO 207-Sexies. - Al que estando autorizado para acceder a sistemas y equipos de informática de alguna dependencia pública, indebidamente copie, transmita o imprima información que contengan se le impondrá de uno a cuatro años de prisión y multa de cien a trescientos días salario.

Los delitos previstos en este titulo serán sancionados por querella de la parte ofendida”

3.1.11 Código Penal para el Estado de Yucatán[33]:

TÍTULO SÉPTIMO; DELITOS CONTRA LA MORAL PÚBLICA; CAPÍTULO II CORRUPCIÓN DE MENORES E INCAPACES, TRATA DE MENORES Y PORNOGRAFÍA INFANTIL

ARTÍCULO 211. Al que procure o facilite por cualquier medio que uno o más menores de dieciséis años, con o sin su consentimiento, los obligue o induzca a realizar actos de exhibicionismo corporal, lascivos o sexuales, con objeto y fin de videograbarlos, fotografiarlos o exhibirlos mediante anuncios impresos o electrónicos, con o sin el fin de obtener un lucro, se le impondrán de cinco a diez años de prisión y de cuatrocientos a quinientos días-multa.

Al que fije, grabe o imprima actos de exhibicionismo corporal, lascivos o sexuales en que participen uno o más menores de dieciséis años, se le impondrá la pena de diez a catorce años de prisión y de cuatrocientos a quinientos días-multa. La misma pena se impondrá a quien con fines de lucro o sin él, elabore, reproduzca, venda, arriende, exponga, publicite o transmita el material a que se refieren las acciones anteriores.

Se impondrá prisión de ocho a dieciséis años y de cuatrocientos cincuenta a quinientos días-multa, así como el decomiso de los objetos, instrumentos y productos del delito, a quien por sí o a través de terceros, dirija, administre o supervise cualquier tipo de asociación delictuosa con el propósito de que se realicen las conductas previstas en los dos párrafos anteriores con menores de dieciséis años.

Para los efectos de este artículo se entiende por pornografía infantil, la representación sexualmente explícita de imágenes de menores de dieciséis años"

---

[33] *Código Penal para el Estado de Yucatán.* México, Porrúa.

3.2 TRATAMIENTO Y LEGISLACIÓN INTERNACIONAL

3.2.1. Organismos Internacionales (ONU y OCDE)

El objetivo de este capítulo es presentar todos aquellos elementos que han sido considerados tanto por organismos gubernamentales internacionales así como por diferentes Estados, para enfrentar la problemática de los delitos informáticos a fin de que contribuyan al desarrollo de nuestro trabajo.

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 hace las computadoras, lo cual ha dado lugar a que, en algunos casos, se modifiquen los derechos penales nacionales.

La Organización de las Naciones Unidas ha reconocido que los delitos por computadora constituyen un grave problema, ya que las leyes, los sistemas que imparten justicia y la cooperación internacional no se han adecuado a los cambios tecnológicos. La propia organización instó a los Estados miembros a intensificar esfuerzos para combatir este tipo de conductas.[34] Para la O.N.U, Existen dos subcategorías de delitos cibernéticos:

a) Delito cibernético en sentido estricto ("delito informático"): todo comportamiento ilícito que se valga de operaciones electrónicas para atentar contra la seguridad de los sistemas informáticos y los datos procesados por ellos;

b) Delito cibernético en sentido lato ("delito relacionado con computadoras"): todo comportamiento ilícito realizado por medio de un sistema o una red informáticos, o en relación

[34] Décimo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente Viena, 10 a 17 de abril de 2000.

con ellos; incluidos los delitos como la posesión, el ofrecimiento o la distribución ilegales de información por medio de un sistema o una red informáticos.

El delito informático está en relación con todo comportamiento ilegal que atente contra la seguridad de sistemas y datos mediante operaciones electrónicas. La seguridad de los sistemas y datos informáticos puede determinarse en función de tres principios: garantía de confidencialidad, integridad o disponibilidad de los datos y funciones de procesamiento. De conformidad con la lista de la Organización de Cooperación y Desarrollo Económicos, de 1985 y la Recomendación formulada en 1989 por el Consejo de Europa, que es más detallada, los delitos contra la confidencialidad, la integridad o la disponibilidad incluyen:

a) El acceso no autorizado, o bien, el acceso sin derecho a un sistema o una red informáticos violando medidas de seguridad;

b) El daño a los datos o a los programas informáticos, es decir el borrado, la descomposición, el deterioro o la supresión de datos o de programas informáticos sin derecho a ello;

c) El sabotaje informático, es la introducción, la alteración, el borrado o la supresión de datos o de programas informáticos, o la interferencia en sistemas informáticos, con la intención de obstaculizar el funcionamiento de un sistema de computadoras o de telecomunicaciones;

d) La interceptación no autorizada, es decir, la interceptación, realizada sin autorización y por medios técnicos, de comunicaciones destinadas a un sistema o a una red informáticos, provenientes de ese sistema o esa red o efectuadas dentro de dichos sistema y red;

e) El espionaje informático, es conocido como la adquisición, la revelación, la transferencia o la utilización de un secreto comercial sin autorización o justificación legítima, con la intención de causar una pérdida económica a la persona que tiene derecho al secreto o de obtener un beneficio ilícito para sí mismo o para una tercera persona.

El fraude relacionado con la informática ha sido definido por el Consejo de Europa como la introducción, la alteración, el borrado o la supresión de datos o de programas informáticos, u otra interferencia en el curso del procesamiento de datos que cause una pérdida económica o de bienes poseídos por otra persona con la intención de obtener una ganancia económica ilícita para sí mismo o para otra persona. Esta disposición se refiere a la situación en que el autor del delito interfiere -con o sin derecho- en el funcionamiento correcto del procesamiento de datos de una computadora con el efecto especificado en la definición de fraude. No abarca las conocidas estratagemas para estafar a las personas urdidas por medio de representaciones o comunicaciones electrónicas a través de Internet, como los ofrecimientos de venta de acciones a precios favorables; las inversiones inmobiliarias en un Estado extranjero; los empréstitos con un tipo de interés excepcionalmente alto; el pago anticipado de artículos descritos con vaguedad; o los incentivos para participar en planes de pirámides.

La Organización de Cooperación y Desarrollo Económico (OCDE) inició en 1983, 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 computacionales.

Las posibles implicaciones económicas de la delincuencia informática, su carácter internacional y, a veces, incluso transnacional 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 político-jurídicas desembocaron en una lista de las acciones que pudieran ser consideradas por los Estados, por regla general, como merecedoras de pena.

De esta forma, la OCDE 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 reformas 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), como 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, Computadores y Comunicaciones recomendó también que se instituyesen protecciones penales contra otros usos indebidos (Lista optativa o facultativa), espionaje informático, utilización no autorizada de una computadora, utilización no autorizada de un programa 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 informa 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 considerablemente, 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 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 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 Estado pero respecto de los cuales no se ha llegado todavía a un consenso internacional en favor de su tipificación.

Adicionalmente debe mencionarse que 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 el mismo año.

En este contexto, consideramos que si bien este tipo de organismos gubernamentales ha pretendido desarrollar normas que regulen la materia de delitos informáticos, ello es resultado de las características propias de los países que los integran, quienes, comparados con México y otras partes del mundo, tienen un mayor grado de informatización y han enfrentado de forma concreta las consecuencias de ese tipo de delitos.

Por otra parte, a nivel de organizaciones intergubernamentales de carácter universal, debe destacarse que en el seno de la Organización de las Naciones Unidas (ONU), en el marco del Octavo Congreso sobre Prevención del Delito y Justicia Penal, celebrado en 1990 en la Habana Cuba, se dijo que la delincuencia relacionada con la informática era consecuencia del mayor empleo del proceso de datos en las economías y burocracias de los distintos países y que por ello se había difundido la comisión de actos delictivos.

Además, la injerencia transnacional en los sistemas de proceso de datos de otros países, había traído la atención de todo el mundo. Por tal motivo, si bien el problema principal —hasta

ese entonces era la reproducción y la difusión no autorizada de programas informáticos y el uso indebido de los cajeros automáticos, no se habían difundido otras formas de delitos informáticos, por lo que era necesario adoptar medidas preventivas para evitar su aumento.

En general, se supuso que habría un gran número de casos de delitos informáticos no registrados. Por todo ello, en vista que los delitos informáticos eran un fenómeno nuevo, y debido a la ausencia de medidas que pudieran contrarrestarlos, se consideró que el uso deshonesto de las computadoras podría tener consecuencias desastrosas. A este respecto, el Congreso recomendó que se establecieran normas y directrices sobre la seguridad de las computadoras a fin de ayudar a la comunidad internacional a hacer frente a estas formas de delincuencia.

Partiendo del estudio comparativo de las medidas que se han adoptado a nivel internacional para atender esta problemática, deben señalarse los problemas que enfrenta la cooperación internacional en la esfera del delito informático y el derecho penal, a saber: la falta de consenso sobre lo que son los delitos informáticos, falta de definición jurídica de la conducta delictiva, falta de conocimientos técnicos por parte de quienes hacen cumplir la ley, dificultades de carácter procesal, falta de armonización para investigaciones nacionales de delitos informáticos. Adicionalmente, deben mencionarse la ausencia de la equiparación de estos delitos en los tratados internacionales de extradición. Teniendo presente esa situación, se consideró indispensable resaltar que las soluciones puramente nacionales serán insuficientes frente a la dimensión internacional que caracteriza este problema. En consecuencia, es necesario que para solucionar los problemas derivados del incremento del uso de la informática, se desarrolle un régimen jurídico internacional donde se establezcan las normas que garanticen su compatibilidad y aplicación adecuada. Durante la elaboración de dicho régimen, se deberán de considerar los diferentes niveles de desarrollo tecnológico que caracterizan a los miembros de la comunidad internacional.

En otro orden de ideas, debe mencionarse que la Asociación Internacional de Derecho Penal durante un coloquio celebrado en Wurzburgo en 1992, adoptó diversas recomendaciones respecto a los delitos informáticos. Estas recomendaciones contemplaban que en la medida en que el derecho penal tradicional no sea suficiente, deberá promoverse la modificación de la definición de los delitos existentes o la creación de otros nuevos, si no basta con la adopción de otras medidas (principio de subsidiaridad). Además, las nuevas disposiciones deberán ser precisas, claras y con la finalidad de evitar una excesiva tipificación deberá tenerse en cuenta hasta qué punto el derecho penal se extiende a esferas afines con un criterio importante para ello como es el de limitar la responsabilidad penal con objeto de que éstos queden circunscritos primordialmente a los actos deliberados.

Asimismo, considerando el valor de los bienes intangibles de la informática y las posibilidades delictivas que pueden entrañar el adelanto tecnológico, se recomendó que los Estados consideraran de conformidad con sus tradiciones jurídicas y su cultura y con referencia a la aplicabilidad de su legislación vigente, la tipificación como delito punible de la conducta descrita en la "lista facultativa", especialmente la alteración de datos de computadora y el espionaje informático; así como que por lo que se refiere al delito de acceso no autorizado precisar más al respecto en virtud de los adelantos de la tecnología de la información y de la evolución del concepto de delincuencia.

Además, señala que el tráfico con contraseñas informáticas obtenidas por medios inapropiados, la distribución de virus o de programas similares deben ser considerados también como susceptibles de penalización.

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

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 6a. 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 exponerse 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 titulado 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, titulado defensa de la propiedad intelectual, se estableció que México haría su mayor esfuerzo por cumplir tan pronto como fuera posible con las obligaciones del Artículo 1718 relativo a la defensa de los derechos de propiedad intelectual en la frontera, haciéndolo en un plazo que no excedería a tres años a partir de la fecha de la firma del TLC.

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 segúndo habla sobre las condiciones requeridas para otorgar la protección de los secretos industriales y de negocios y una de ellas es que estos consten en medios electrónicos o magnéticos.

3.2.3. Legislación en otros países

Se ha dicho que algunos casos de abusos relacionados con la informática deben ser combatidos con medidas jurídico-penales. No obstante, para aprehender ciertos comportamientos merecedores de pena con los medios del Derecho penal tradicional, existen, al menos en parte, relevantes dificultades. Estas proceden en buena medida, de la prohibición jurídico-penal de analogía y en ocasiones, son insuperables por la vía jurisprudencial. De ello surge la necesidad de adoptar medidas legislativas. En los Estados industriales de Occidente existe un amplio consenso sobre estas valoraciones, que se refleja en las reformas legales de los últimos diez años.

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

ALEMANIA

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

- Espionaje de datos (202 a);
- Estafa informática (263 a);

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

- 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;

- 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, causación 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.

Sobre el particular, cabe mencionar que esta solución en forma parcialmente abreviada fue también adoptada en los Países Escandinavos y en Austria.

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

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.

AUSTRIA

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

- Destrucción de datos (126). En citado 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. Además contempla sanciones para quienes cometen este hecho utilizando su profesión.

FRANCIA

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). En este 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). En este artículo se sanciona a quien impida o falsee el funcionamiento de un sistema de tratamiento automático de datos.

- Destrucción de datos (462-4). este artículo 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). En este 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). Este sanciona a quien conscientemente haga uso de documentos falsos haciendo referencia al artículo 462-5.

ESTADOS UNIDOS

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

Con la finalidad de eliminar los argumentos hipertécnicos acerca de qué es y qué no es un virus, un gusano, un Caballo de Troya, etcétera 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, al sistema 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.

El Acta de 1994 diferencia el tratamiento a aquellos que de manera temeraria lanzan ataques de virus de aquellos que lo realizan con la intención de hacer estragos. El acta define dos niveles para el tratamiento de quienes crean virus estableciendo para aquellos que intencionalmente causan un daño por la transmisión de un virus, el castigo de hasta 10 años en

prisión federal más una multa y para aquellos que lo transmiten sólo de manera imprudencial la sanción fluctúa entre una multa y un año en prisión.

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

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.

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.

Se Considera 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.

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 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.

VENEZUELA.

La Asamblea Nacional de la República Bolivariana de Venezuela decretó en la Gaceta Oficial nº 37.313 de fecha 30 de octubre de 2001, una ley que alude al tema de esta investigación. De nombre Ley Especial Contra Delitos Informáticos, dicha ley tiene por objeto 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 o los cometidos mediante el uso de dichas tecnologías, en los términos previstos en esta ley.

Es necesario que 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.

Las sanciones por los delitos previstos en la Ley Especial Contra Delitos Informáticos serán principales y accesorias.

Las sanciones principales concurrirán con las accesorias y ambas podrán también concurrir entre sí, de acuerdo con las circunstancias particulares del delito del cual se trate, en los términos indicados en la presente ley

Si los delitos previstos en la Ley fuesen cometidos por los gerentes, administradores, directores o dependientes de una persona jurídica, actuando en su nombre o representación, éstos responderán de acuerdo con su participación culpable.

La persona jurídica será sancionada en los términos previstos en esta Ley, en los casos en que el hecho punible haya sido cometido por decisión de sus órganos, en el ámbito de su actividad, con sus recursos sociales o en su interés exclusivo o preferente.

CAPÍTULO IV. PATRIMONO E INFORMÁTICA.

En este capítulo, se expondrá la definición del bien jurídico tutelado, para así llegar a las definiciones de patrimonio y de informática; todo esto para dar un antecedente al tema de este trabajo de investigación. En cuanto al patrimonio, se evocarán los conceptos proveídos por el derecho civil y por el derecho penal, analizando dichos conceptos, para lograr un mayor entendimiento en cuanto al Patrimonio; se analizarán los delitos en contra del patrimonio que contiene el Código Penal para el Estado de Nayarit. Se presentará el vínculo que guarda el Patrimonio y la Informática y en cuanto a esta última, se señalarán definiciones de informática, de los medios utilizados para la conexión virtual entre ordenadores en todo el mundo y de las formas en que se regula por el derecho en la actualidad.

4.1 EL BIEN JURÍDICO TUTELADO.

Para que la sociedad pueda convivir es necesario proteger, a través del Derecho Penal, los bienes jurídicos que son la vida, la libertad, patrimonio, entre otras cosas, pues cada Código Punitivo hace referencia en cada uno de sus títulos a algún bien jurídico. El bien jurídico tutelado es el derecho o facultad protegida por la norma jurídica; es a través de las normas jurídicas que se pretende garantizar la preservación de los bienes jurídicos. Es aquello que la sociedad defiende como un derecho individual y personalísimo de todos los ciudadanos. Para Olga Islas el "bien jurídico es el concreto interés individual o colectivo protegido por el particular tipo penal"[35].

El bien jurídicamente tutelado, es el bien o el derecho que es protegido por las leyes penales, el cual puede ser la vida, la integridad corporal, la libertad sexual, la propiedad privada. El objeto jurídico tutelado en el delito de fraude, es el patrimonio y

[35] ISLAS y MAGALLANES, Vera Olga "*Temas actuales de justicia penal*". Sextas Jornadas sobre Justicia Penal. IIJ-UNAM. 2006

la propiedad, entendiendo que como patrimonio, se tiene a los bienes o posesiones que puede tener una persona y como propiedad, la capacidad de enajenarlas

4.1.1 Patrimonio Como Bien Jurídicamente Tutelado.

El patrimonio es la posibilidad de adquirir bienes, muebles o inmuebles, que nace con la persona y muere con ella. Ese patrimonio está compuesto por las pertenencias que posee una persona, ya sea física o jurídica y de las cuales es propietario. La persona tiene el derecho de administrarlo su patrimonio como mejor le parezca. El patrimonio es el conjunto de bienes, derechos y obligaciones que constituyen los medios económicos y financieros a través de los cuales ésta puede cumplir sus fines. Para Rafael de Pina y Rafael de Pina Vara, el patrimonio es "el Conjunto de Derechos y Obligaciones que corresponde a un solo titular; suma de bienes y riquezas que pertenecen a una persona"[36].

En el Derecho Civil, el patrimonio para Marcel Planiol, era "el conjunto de derechos y de obligaciones pertenecientes a una persona, estimables en dinero"[37]. Para Planiol, existe un lazo entre la persona y el patrimonio, siendo que solo las personas pueden tener un patrimonio, pues que son capaces de ser sujetos activos y pasivos de los derechos; por lo consiguiente solo las personas tienen aptitud para poseer bienes, o para tener créditos u obligaciones.

Josserand define al patrimonio "como un conjunto de valores pecuniarios positivos o negativos pertenecientes a una misma persona y que figuran unos en el activo y otros en el pasivo"[38]. Es decir, de todos los derechos y obligaciones

---

[36] DE PINA, Rafael y DE PINA VARA, Rafael. *Diccionario de Derecho*, ed. Porrúa, Vigesimonovena edición. 2000

[37] PLANIOL, Marcel " *Tratado de Derecho Civil*', ed. Harla p.p 355-359

[38] JOSSERAND, Louis "*Derecho Civil*' ed. Harla, p.p 560

pertenecientes a una persona, se incluyen solamente aquellos de carácter patrimonial, ya que son apreciables en dinero. El activo se compone con derechos reales y derechos personales; en cambio el pasivo se conforma con obligaciones, es decir, el lado pasivo de los derechos personales. El lado pasivo de los derechos reales no se cuantifica.

Toda persona tiene necesariamente un patrimonio, aunque pueda poseer muy pocas cosas, sin embargo este tiene un patrimonio inherente a ella. Cada persona no tiene más de un patrimonio. En tanto la persona viva, no se puede efectuar una transmisión de su patrimonio a otra persona; no se puede enajenar más que los elementos, uno después de otro. Es por ello por lo que todas las transmisiones que se hacen entre vivos son a título particular. La transmisión de la totalidad del patrimonio no puede hacerse sino hasta después de la muerte de la persona.

Es notorio el que la mayor parte de los elementos que componen el patrimonio, tanto los derechos reales como los derechos de crédito, son susceptibles de perderse por el efecto de una prescripción extintiva, cuando no se hace uno de ellos durante un tiempo prolongado. Pero a estos derechos, de cualquiera naturaleza, que son prescriptibles, se oponen otros derechos que su titular puede dejar de ejercitar sin peligro de que se pierdan, por largo que sea el tiempo que se les abandone, a estos últimos se les conoce como facultades; las facultades son el derecho de cambiar la forma de explotación de su propiedad, el derecho de construir en un terreno, el derecho de adquirir más bienes, etc.

4.1.2 Delitos Contra El Patrimonio.

En el Derecho penal, el patrimonio puede ser afectado por un sin número de delitos, los cuales, se encuentran tipificados dentro de los Códigos Penales del país, Así mismo que en el Código Penal para el Estado de Nayarit, se enuncian en el Título

Vigésimo denominado Delitos Contra el Patrimonio, estos comprenden del artículo 343 al 380, mismos que se exponen a continuación:

"TÍTULO VIGÉSIMO. DELITOS CONTRA EL PATRIMONIO.

- **ROBO (Art. 343):** lo comete el que se apodera de una cosa ajena, mueble, sin derecho y sin consentimiento de las personas que pueden disponer de ella con arreglo a la Ley.

- **ABIGEATO (Art. 357):** Comete el delito de abigeato el que se apodera de una o más cabezas de ganado ajeno cualquiera que sea su especie, sin consentimiento de quien legalmente puede disponer de ellas.

- **ABUSO DE CONFIANZA (Art. 364)**: lo comete el que, con perjuicio de alguien, disponga para sí o para otro, de cualquier cosa ajena mueble, de la que se le haya transmitido la tenencia y no el dominio, se le sancionará con prisión hasta de dos años y multa de diez a treinta días de salario, cuando el monto del abuso no exceda cien veces del salario.

- **FRAUDE (Art. 368)**: Comete el delito de fraude, el que engañando a alguno o aprovechándose del error en que éste se halla, se haga ilícitamente de una cosa o alcance un lucro indebido para sí o para otro. Este delito cuenta con casos especiales de defraudación que se sancionarán conforme a lo dispuesto en el artículo que trata al Fraude (Son 15 Fracciones)

- **ADMINISTRACIÓN FRAUDULENTA (Art. 371):** Comete el delito de administración fraudulenta el que teniendo a su cargo el manejo, la administración o el cuidado de bienes ajenos, con engaño o aprovechamiento del error del ofendido, perjudique a su titular o a un tercero con legítimo interés, o altere en sus cuentas los precios o condiciones de los contratos,

suponiendo operaciones o prestaciones o exagerando las que hubiere hecho ocultando o reteniendo bienes, o empleare abusivamente los bienes o la firma que se le hubiere confiado.

- **USURA (Art. 372):** Se impondrá prisión de seis meses a cinco años y multa de tres a diez días de salario**:**
    - **I.** Al que abusando de la apremiante necesidad de una persona, realizare cualquier préstamo, aún encubierto con otra forma contractual con intereses mayores en dos por ciento mensuales a los autorizados por el Banco de México, u otras ventajas evidentemente desproporcionadas, para sí o para otro;
    - **II.** Al que abusando de la apremiante necesidad ajena, procurase un préstamo cualquiera cobrando una comisión evidentemente desproporcionada, para sí o para otra; y
    - **III.** Al que haya adquirido un préstamo usurario o una comisión usuraria con conocimiento de causa para enajenarlo o hacerlo valer.

- **DESPOJO DE INMUEBLES Y AGUAS (Art. 372):** se aplicarán las sanciones de uno a cinco años de prisión y multa de tres a diez días de salario:
    - **I.** Al que de propia autoridad y haciendo violencia física o moral a las personas, o furtivamente, o empleando amenazas o engaño, ocupe un inmueble ajeno, o haga uso de él o de un derecho real que no le pertenezca;
    - **II.** Al que de propia autoridad y haciendo uso de cualquiera de los medios indicados en la fracción anterior ocupe un inmueble de su propiedad, en los casos en que la Ley no se lo permita por hallarse en poder de otra persona, o ejerza actos de dominio que lesionen derechos legítimos del ocupante; y
    - **III.** Al que en los términos de las fracciones anteriores, cometa despojo de aguas.

- **DAÑO EN PROPIEDAD AJENA (Art. 375):** Se impondrá de cuatro a ocho años de prisión y multa de cinco a veinte días de salario a los que causen incendio, inundación o explosión con daño o peligro de:
    - **I.** Un edificio, vivienda o cuarto donde se encuentre alguna persona;
    - **II.** Ropas, muebles u objetos en tal forma que puedan causar daños a las personas;
    - **III.** Archivos públicos o notariales;
    - **IV.** Bibliotecas, museos, escuelas o edificios o monumentos públicos; y
    - **V.** Montes, bosques, selvas, pastos, mieses o cultivos de cualquier otro género. Si la plantación estuviere en tierras ejidales, las sanciones aplicables serán de seis a doce años de prisión y multa de cinco a veinte días de salario.

- **OCUPACIÓN ILEGAL DE EDIFICIOS E INMUEBLES DESTINADOS A UN SERVICIO PÚBLICO (Art. 380):** Se impondrá de seis meses a tres años de prisión y multa hasta el equivalente de treinta días de salario al que de propia autoridad y haciendo uso de la violencia física en las personas o en las cosas, se apodere de un edificio destinado a un servicio público cualquiera que este sea."[39]

La descripción citada anteriormente, enuncia los delitos que afectan al patrimonio de las personas, mismos que se contiene en el Código Penal para el Estado de Nayarit. Los citados delitos, le sirven al juzgador en el Estado de Nayarit, para explicar o tipificar conductas delictivas que atacan, ya sea directa o indirectamente, al bien jurídico tutelado, que en este caso es el patrimonio de las personas; aunque a la vez, representa un problema en el Estado, toda vez que no todas las conductas delictivas que se encaminan a dañar el patrimonio encuadran en los tipos penales expuestos anteriormente, lo cual representa un grave problema al momento de aplicar correctamente la ley; dichas conductas son realizadas gracias a los avances

[39] *Código Penal para el Estado de Nayarit.* México, Ed. Delma

tecnológicos que se presentan en la actualidad, logrando con ello que dichos delitos no encuadren en el tipo penal, al no contener los elementos que clasifican a una conducta. Es por ello que es necesario, tanto para esta investigación, como para los órganos encargados de administrar la ley y la justicia, que abunden en conocimientos encaminados a evitar o corregir los huecos legislativos que evitan administrar justicia a dichas conductas delictivas que siguen sin encuadrar en el tipo penal.

4.2 LA INFORMÁTICA Y EL DERECHO.

La Real Academia de la Lengua Española proporciona una definición de Informática "es el conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de ordenadores"[40]; la informática surge de la misma inquietud racional del hombre, el cual, ante la continua y creciente necesidad de información para una adecuada toma de decisiones, es impulsado a formular nuevos postulados y desarrollar nuevas técnicas que satisfagan dichos propósitos. La Informática surge en 1959 en Estados Unidos, y ha sufrido cambios a la par de la evolución del derecho. Las primeras investigaciones en materia de recuperación de documentos jurídicos en forma autorizada se remontan a los años cincuenta, época en que se comenzaba a utilizar las computadoras no sólo con fines matemáticos sino también lingüísticos. Dichos esfuerzos fueron realizados en el Health Law Center de la Universidad de Pittsburg, Pensylvania, quien el entonces director del centro, John Horty, estaba convencido de la necesidad de encontrar medios satisfactorios para tener acceso a la información legal. Para 1959, el centro colocó los ordenamientos legales de Pensylvania en cintas magnéticas. El sistema fue demostrado posteriormente en 1960, ante la American Association Boreau of Lawyers en la reunión anual en Washington, D.C. Esta fue la primera demostración de un sistema legal automatizado de búsqueda de información. La palabra informática, es un neologismo derivado de los vocablos información y automatización, sugerido en el año de 1962 por

[40] Real Academia de la Lengua Española. (http://www.rae.es/)

Phillipe Dreyfus, quien fue el Director del Centro Nacional de Cálculo Electrónico de la Sociedad Bull y un pionero en la Informática Francesa. En sentido general, la Informática se define como un conjunto de técnicas encaminadas al tratamiento lógico y automatizado de la información para una adecuada toma de decisiones, está es más una técnica que una ciencia, debido a su carácter eminentemente pragmático.

La informática, como uno de los fenómenos más importantes en la actualidad, influye en prácticamente todas las áreas del conocimiento humano, dentro de las cuales el Derecho no es excepción. El Derecho Informático, es una disciplina de continuo desarrollo, la cual considera a la informática como instrumento y objeto de estudio. La clasificación del Derecho Informático obedece a dos vertientes fundamentales: la Informática Jurídica y el Derecho de la Informática.

4.2.1 Informática Jurídica.

En lato sensu, la informática jurídica es el conjunto de aplicaciones de la informática en el ámbito del derecho. Para Julio Téllez Valdés, la informática Jurídica se define como "la técnica interdisciplinaria que tiene por objeto el estudio e investigación de los conocimientos de la Informática general, aplicables a la recuperación de información jurídica, así como la elaboración y aprovechamiento de los instrumentos de análisis y tratamiento de información jurídica necesarios para lograr dicha recuperación[41]. La interrelación entre la informática y el Derecho, ha dado lugar a un sin número de denominaciones, entre las que destacan las siguientes:

1. **JURIMETRICS.-** en español Jurimetría, creada por el juez estadounidense Lee Loevigner en 1949.
2. **GIUSCIBERNÉTICA.-** En español juicibernética, de Mario G. Losano, quien en su libro Giuscibernética sostiene que la cibernética aplicada al

[41] TÉLLEZ VALDÉS, Julio. "*Derecho Informático"* Ed. Mc Graw Hill, 3ª Edición.

> derecho no solo ayuda a la depuración cuantitativa de este, sino también a la cualitativa. En su obra expone la fundamentación filosófica de la relación del Derecho con la informática[42].

Desde hace años la informática jurídica ha permitido un mejor conocimiento de los fenómenos jurídicos, por lo que muchos juristas, anteriormente escépticos e indiferentes, han encontrado en la computadora un instrumento eficaz para el desarrollo de sus actividades. En este sentido, debido a la informatización en el campo del derecho, se han constituido diferentes tipos de archivos (legislativos, de jurisprudencia, doctrinales, bibliográficos, etc), los cuales representan un potencial informativo insospechado, además de que constituyen un apoyo rápido y eficaz al realizar actividades de gestión, así como una ayuda en la toma de decisiones en la educación e investigación, lo que representa un hecho sin precedente en el campo del derecho.

4.2.2 Derecho de la Informática.

A finales de los años setenta y Luego de diez años de aplicaciones comerciales de las computadoras, empezaron a surgir las primeras inquietudes respecto a las eventuales repercusiones negativas motivadas por el fenómeno informático las cuales requerían de un tratamiento especial. Julio Téllez Valdés define al derecho de la Informática, como el conjunto de leyes, normas y principios aplicables a los hechos y actos derivados de la Informática[43]. Es decir, es un conjunto de leyes, normas y principios con alusión específica al fenómeno informático. El objetivo principal del derecho de la informática es el de regular ciertos fenómenos socio informáticos que no están legislados. La autonomía de esta disciplina jurídica proviene de aquellas fuentes de donde surge el derecho. A nivel interdisciplinario, están aquellas provistas por el mismo derecho, como es el caso de la legislación, que es incipiente al respecto, sin

---

[42] LOSANO, Mario "*Nouvi Siuluppi Della Sociología del Diritto",* 1960, p101.
[43] TÉLLEZ VALDÉS, Julio. "*derecho informático"* Ed. Mc Graw Hill, 3ª Edición.

embargo, cabe señalar aquellas disposiciones caracterizadas por guardar un vinculo con respecto a la informática, como es el caso de los ordenamientos en materia constitucional, civil, penal, laboral, fiscal, administrativo, procesal, internacional, entre otras. Asimismo, en cuanto a la jurisprudencia y la doctrina, existen algunos pronunciamientos, teorías y artículos respecto a los problemas jurídicos suscitados por la informática.

4.2.3 El Desarrollo del Sistema Jurídico Informático en México l La Regulación Jurídica del Internet.

Para poder ubicarse en el desarrollo del sistema jurídico en México, deben ser analizados tres procesos interdependientes, a través de los cuales va dirigida la actualización de la legislación en materia de informática y la consolidación del acceso a la información.

El primer proceso es el desarrollo del sistema informático en las relaciones entre los gobernados, ya que como un reclamo de las actividades cotidianas de la sociedad, hubo la necesidad de implementar medidas de seguridad que dieran certidumbre jurídica a los actos realizados a través de la internet u otros sistemas de intercomunicación informáticos dando lugar a crear en la legislación expresiones como las siguientes: medios electrónicos, ópticos, remotos y de cualquier otra tecnología, trayendo consigo una modificación de la legislación tanto civil como mercantil que han propiciado la validación de sistemas de movimientos bancarios, formas contractuales, sistemas de compras, diversas firmas, certificaciones, para ello se realizaron las reformas en los códigos civiles, en los códigos de procedimientos civiles, código de comercio, en la ley de instituciones de crédito, en la ley federal de protección al consumidor, a este proceso se le llama adecuación del marco jurídico para la aplicación de los sistemas informáticos entre los gobernados.

El segundo de los elementos, trata de los sistemas de seguridad de las creaciones de sistemas y desarrollos informáticos en materia de propiedad industrial y de derechos de autor, como son los secretos industriales, conocimientos técnicos, registros de marcas, registro de los esquemas de trazado de circuitos integrados así como la inscripción de sus transmisiones y licencias de uso y explotación, regulado por la Ley de la Propiedad Industrial; y como parte de este elemento que también protege la Ley Federal del Derecho de Autor el cual protege los programas de cómputo, las bases de datos y su documentación; y una tercera a través del código que complementa las leyes sustantivas ya citadas y que, es el Código Penal, ya que establece las posibles conductas constitutivas de delito en la materia así como las sanciones a quienes, por ejemplo, crean los virus de computadora, a los que alteran indebidamente los archivos magnéticos, o se infiltran indebidamente a los sistemas o bases de datos, a este conjunto de normas que componen el segundo elemento se les puede clasificar como garantes del desarrollo del sistema informático.

El tercer elemento es la legislación que a favorecido el acceso a la información, que toma como base el desarrollo de los dos elementos anteriores, este a su vez se ha desarrollado bajo dos vertientes:

El acceso a la información comercial que registra el estado en su función de fedatario público de los actos jurídicos de los gobernados y el acceso a la información pública gubernamental, regulado por la ley, como actividades meramente de gobierno, es decir actos administrativos; a este tercer elemento le podemos denominar aprovechamiento del sistema informático como proceso técnico para el acceso a la información.

La Internet es una colección de circuitos y rutinas, como un conjunto de recursos compartidos o incluso como una disposición a intercomunicarse; es decir,

como una mega red, una red de redes de computadoras. Otro punto de vista, es pensar en las redes como el medio a través del cual se envía y acumula información. Internet puede ser interpretado como la información y los servicios que circulan por esta red; como un sistema distribuido de información, una red global de redes de ordenadores, pues cada red está compuesta por docenas de miles de ordenadores. Internet es tanto un conjunto de comunidades como de tecnologías, y su éxito se atribuye a la satisfacción de las necesidades básicas de la comunidad y a la utilización de un modo efectivo para impulsar la infraestructura. Es a la vez, un medio de difusión mundial, un mecanismo de propagación de la información y un medio de colaboración e interacción entre los individuos y sus ordenadores, independientemente de su localización geográfica. El número total de usuarios de la Internet asciende hoy en día a varios millones, y su crecimiento es exponencial. Este alto nivel de conectividad ha creado un grado de comunicación, colaboración, acceso a la información e intercambio de recursos sin precedentes en la historia de la humanidad.

El Internet cambia para el derecho, la noción de tiempo y de espacio, puesto que es posible realizar enlaces inmediatos a tiempo real sin importar el lugar del mundo donde se encuentren las partes. Se debe considerar, la posibilidad del nacimiento del derecho internacional de la informática como medio adecuado para la regulación de Internet, en donde el derecho internacional podría reducirse a un gran sistema de reglas de elección de la ley a aplicar a la resolución de un caso. Existe un elemento, en la postura de crear un Derecho Consuetudinario del Ciberespacio, cuyo atractivo es la de sostener un derecho suficientemente flexible para acompañar el rápido devenir del cambio tecnológico y por ende legal, que es propio del medio.

En estos años, han surgido iniciativas provenientes de la misma sociedad civil y de las empresas que marcaron la pauta en Internet y que han comenzado a adaptar políticas de autocensura, como la mayoría de las compañías que ofrecen portales gratuitos, prohíben la publicación de imágenes pornográficas, y grupos de discusión o

chats, que desalientan el uso de lenguaje impropio, ambos en sus términos de uso, con miras a desarrollar y estructurar la red de modo armónico y equilibrado para que responda a vitales intereses de la comunidad y a las necesidades esenciales del hombre actual. Uno de los primeros países en introducir códigos deontológicos o de buena conducta en la red, es Francia con sus netiquettes o reglas de etiqueta en la red; Inglaterra ha adoptado mecanismos de autorregulación, donde se han elaborado códigos de conducta y creado organismos independientes como la Safety Net Foundation, que mantiene una línea directa en la que se pueden recibir denuncias de aquellos contenidos, ideologías o actividades que se consideran ilícitas. También se ha hecho común los programas filtro o cerrojo, o de selección de contenidos que bloquean el acceso a determinados sitios web, que es el mecanismo técnico más adecuado para evitar la existencia de contenidos ilícitos, limitando o impidiendo el acceso a dichos contenidos más no ideas que reclama la libertad de expresión, pero se bloquean al mismo tiempo acceso a determinados contenidos expuestos en sitios web, respetándose así la diferencia de criterios, valores y costumbres morales.

4.2.4 Descripción de los Terminos en la Informática: Los Url, I.P Y El Top Level Domain

Una dirección de Internet o web address es lo que en el vocabulario técnico se conoce como URL, significa Uniform Resource Locator, es decir, localizador uniforme de recurso. El URL es la cadena de caracteres con la cual se asigna una dirección única a cada uno de los recursos de información disponibles en la internet. Existe un URL único para cada página de cada uno de los documentos de la World Wide Web. Hacemos uso de las direcciones de web cuando se escribe en el navegador de web el sitio a donde se quiere llegar, o cuando se hace "click" en un hipervínculo. Básicamente lo que hace una dirección de web es decirle al programa navegador que se dirija a cierta computadora o red de computadoras en cualquier parte del mundo usando cierto protocolo de comunicación y muestre o ejecute un cierto archivo. Las direcciones web más sencillas contienen básicamente 3 partes: el protocolo, el nombre de dominio, y la

ruta y nombre de archivo; la tercera parte puede o no existir. Tómese como ejemplo el URL de la Universidad Simón Bolívar, http://www.usb.ve. La primera parte es la definición del Protocolo, esta dice cual es el tipo de servidor al cual se refiere el URL y cuál es el protocolo a utilizar para la transferencia de los archivos desde el servidor en donde éstos se encuentran hasta el computador del usuario. Los tipos más comunes de URL son los siguientes:

- **https:** Secure HTTP (HTTP Seguro. Protocolo de http con ciertas especificaciones usado en sitios seguros (sitios que requieren contraseñas), como websites de bancos, correo basado en todas las páginas web con extensión .html o .htm usualmente están almacenadas en un servidor de tipo WWW, y este servidor usa el protocolo http.

- **ftp:** File Transfer Protocol (Protocolo de Transferencia de Archivos), es el utilizado en la transferencia de archivos almacenados en un servidor de FTP. Normalmente estos archivos son para descargar, y "no son páginas web" sino de otro tipo, como archivos con extensiones .exe, .pdf, .zip, etc. Por ejemplo, el servidor de ftp de la DST ftp://ftp.dst.usb.ve.

- **Mail to:** Indica que se trata de una dirección de correo electrónico. Al escribirla en su navegador web inmediatamente se abre el programa predeterminado de correo electrónico en su computadora, como por ejemplo Outlook Express, Netscape Messenger, Microsoft Outlook o cualquier otro.

- **News:** este señala que el URL apunta a algún Usenet Newsgroup o Grupo de Noticias. Al igual que con mail to al introducir una dirección que comience por news:// se abre el programa indicado para manejarla.

- **Telnet:** Al introducirla se ejecutará un programa separado de cliente telnet.

- **Gopher:** Utilizado cuando se desea navegar por servidores de directorios Gopher.

- **Wais:** Se utiliza para navegar por los servidores WAIS.
- **File:** Los navegadores de web también pueden navegar a través de los archivos de nuestra propia computadora, para ello es necesario ingresar en el URL el indicativo de protocolo file:/// (en este caso con tres barras "/") seguido del camino o path hacia el directorio que se desea ver.

Cada computadora que se encuentra conectada a la internet está identificada con un número llamado Dirección IP, esta es un número que identifica de manera lógica y jerárquica a una interfaz de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP (Internet Protocol), como por ejemplo 159.90.90.200, y es habitual que un usuario que se conecta desde su hogar a Internet utilice una dirección IP. A través de Internet, los ordenadores se conectan entre sí mediante sus respectivas direcciones IP. Sin embargo, a los seres humanos nos es más cómodo utilizar otra notación más fácil de recordar y utilizar, como los nombres de dominio; la traducción entre unos y otros se resuelve mediante los servidores de nombres de dominio DNS.

El Nombre de Dominio tiene adicionalmente una parte llamada "Dominio de Más Alto Nivel" o "Top Level Domain", que son las terminaciones de dos o tres letras al final de la dirección. Un dominio de **Internet** es un nombre de equipo que proporciona nombres más fácilmente recordados en lugar de la IP numérica. Permiten a cualquier servicio moverse a otro lugar diferente en la topología de Internet, que tendrá una dirección IP diferente. El significado de cada uno se explica a continuación:

- **.com:** Comercial o de negocios.
- **.org:** Organizaciones sin fines de lucro.
- **.net:** Proveedor de conexión o redes internas.
- **.edu:** Instituciones educativas.
- **.gov:** Instituciones gubernamentales.

- **.mil:** Cuerpos militares.
- **.xx:** En donde xx representa el identificador de país o territorio, por ejemplo .mx (México).

Es necesario explicar lo anteriormente expuesto, toda vez que una persona encaminada a cometer un ilícito utilizando medios informáticos, como requisito mínimo, debe tener extraordinarios conocimientos sobre el uso y desarrollo de las direcciones web, I.P. y el top level domain, para poder acceder a redes especiales o a otros equipos, con el fin de atacar el patrimonio de otras personas o simplemente comprobar a otras personas afines a su conducta, un tipo de competencia en la que, acceder sitios o dominios restringidos, genera para estas personas un nivel de status o jerarquía más elevada; por lo mismo que la autoridad competente, debe contar con conocimientos aún más amplios para lograr con ello, regular y aplicar la justicia correctamente.

CAPÍTULO V. EL FRAUDE INFORMÁTICO EN PARTICULAR.

En el presente capítulo se abordarán las definiciones de atipicidad y de la ausencia de esta, de la conducta atípica conocida como "Phishing", la respuesta social ante el Phishing, las respuestas legislativas y judiciales ante fraude informático, así como los antecedentes en cuanto a los castigos de los primeros delitos informáticos y los primeros ataques, casos en concreto; se revisará al delito de Fraude Genérico en el Estado de Nayarit y se realizará un estudio dogmático preliminar de lo que trata el delito de Fraude Informático, delito el cual se presenta la conducta que causa una deficiencia en la aplicación de la justicia, al no encontrarse establecida en la norma penal.

5.1 AUSENCIA DE LA TIPICIDAD.

La atipicidad es el aspecto negativo del delito y se da cuando no se integran los elementos descritos en el tipo real, es decir la atipicidad es la ausencia de la adecuación de la conducta al tipo[44].

Es común la diferenciación que existe entre la ausencia de tipo y de atipicidad; en la primera, la ausencia de tipo se lleva a cabo cuando el legislador, deliberadamente o en forma inadvertida, no describe una conducta que según el sentir general debería ser incluida y descrita en la norma escrita; la atipicidad, se da cuando la conducta realizada por el sujeto activo no se encuadra en el tipo penal, porque falta alguno de sus elementos. en toda atipicidad existe la ausencia del tipo; si un hecho específico no encuadra perfectamente en el tipo descrito en la ley, entonces en ese hecho, no existe tipo penal. algunas causas de la atipicidad son las siguientes:

- Ausencia de calidad exigida por la ley en cuanto a los sujetos activo y pasivo.

[44] CASTELLANOS Tena Fernando; *Lineamientos Elementales de Derecho Penal*; Ed. Porrúa, México, D.F.; 1997.

- Si faltan el objeto material y el objeto jurídico.
- Cuando no se dan las referencias temporales o espaciales requeridas en el tipo.
- Al no realizarse el hecho por los medios comisivos específicamente señaladas en la Ley.
- Si faltan los elementos subjetivos del injusto legalmente exigidos y.,
- Por no darse en su caso la Antijuricidad especial.

En cuanto al Fraude Informático, al existir coincidencia en la doctrina, en el sentido de que el engaño o aprovechamiento de error no pueden dirigirse contra las máquinas, al carecer estas de discernimiento, pero si en contra de las personas que las manejan; es claro que no podría considerarse fraude en aquellos casos en los que se manipula el sistema informático para hacerse de un determinado bien; sin embargo, el tipo penal de robo tampoco ofrece una solución al problema, pues aún y cuando la conducta del sujeto pudiera forzadamente concebirse como un apoderamiento, consumado en el momento en que tiene acceso al bien, lo cierto es que en muchos de los casos el activo no obtendrá una cosa mueble ajena como lo exige el tipo penal, sino más bien un lucro indebido, como cuando se obtiene un servicio. Así entonces, se corre el riesgo de que exista atipicidad en conductas en las que se utiliza la informática para hacerse del patrimonio ajeno.

En algunas ocasiones, el tipo describe el comportamiento bajo ciertas condiciones de tiempo o de lugar, como cuando la ley exige condiciones de como debe ser realizado el hecho pudiendo ser este; en persona, directa o indirectamente, o presentando cierta conducta diferente.

Las consecuencias que se producen cuando existe una atipicidad, se divide en tres hipótesis:

- **No hay integración del tipo**.- En esta hipótesis se da la atipicidad cuando no se integra alguno de los elementos constitutivos del delito.

- **Existencia de otro delito.-** En esta hipótesis se da la traslación del tipo, o sea a la existencia de otro delito, como en el caso de que falte la relación o parentesco exigido del tipo.

- **Existencia del delito imposible.-** La tentativa imposible se da cuando falta por ejemplo, el bien jurídico tutelado o el objeto material.

Por lo tanto al no existir una adecuación de la conducta a la norma jurídica, se encuentra lo que se llama atipicidad; en la tipicidad es necesario que exista una adecuación de la acción u omisión en el tipo, y en la atipicidad no existe dicha adecuación; por otra parte, cuando existe una la conducta que no encuadra en el tipo, esta conducta nunca podrá ser delictuosa aunque el sentimiento social diga lo contrario, puesto que no existe en la norma jurídica.

5.2 EL PHISHING.

El phishing es una modalidad de fraude diseñada con la finalidad de robar la identidad de un usuario, la cual consiste en obtener información, tal como números de tarjetas de crédito, contraseñas, información de cuentas u otros datos personales por medio de engaños[45]. Este tipo de fraude se recibe habitualmente a través de mensajes de correo electrónico o de ventanas emergentes. El término phishing proviene de la palabra en inglés fishing que significa pesca haciendo alusión al acto de pescar usuarios mediante señuelos (engaños) cada vez más sofisticados, y de este modo obtener información financiera y contraseñas bancarias. Quien lo practica es conocido con el nombre de phisher; también se dice que el término "phishing" es la contracción de "password harvesting fishing" (cosecha y pesca de contraseñas). (Ver Anexo 01).

[45] http://www.microsoft.com/latam/seguridad/hogar/spam/phishing.mspx

En esta modalidad de fraude, el usuario malintencionado envía millones de mensajes falsos que parecen provenir de sitios Web reconocidos o de confianza, como un banco o la empresa de tarjeta de crédito del usuario común, mismo que contesta y brinda la información sin saber que es victima de un engaño. Dado que los mensajes y los sitios Web que envían estos usuarios parecen oficiales, logran engañar a muchas personas haciéndoles creer que son legítimos. La gente confiada normalmente responde a estas solicitudes de correo electrónico con sus números de tarjeta de crédito, contraseñas, información de cuentas u otros datos personales.

Para que estos mensajes parezcan aun más reales, el estafador suele incluir un vínculo falso que parece dirigir al sitio Web legítimo, pero en realidad lleva a un sitio falso o incluso a una ventana emergente que tiene exactamente el mismo aspecto que el sitio Web oficial. Estas copias se denominan "sitios Web piratas". Una vez que el usuario está en uno de estos sitios Web, introduce información personal sin saber que se transmitirá directamente al delincuente, que la utilizará para realizar compras, solicitar una nueva tarjeta de crédito o robar su identidad.

La primera mención del término phishing data de enero de 1996 en grupo el de noticias de hackers Alt.2600, aunque el término apareció tempranamente en la edición impresa del boletín de noticias hacker "2600 Magazine". El término phishing fue adoptado por crackers que intentaban "pescar" cuentas de miembros de AOL (America On Line); ph es comúnmente utilizado por hackers para sustituir la f, como raíz de la antigua forma de hacking conocida como "phone phreaking".

El phishing en AOL se encontraba estrechamente relacionado con la comunidad de warez que intercambiaba software apócrifo. Un cracker se hacía pasar como un empleado de AOL y enviaba un mensaje instantáneo a una víctima potencial. Para poder engañar a la víctima de modo que diera información confidencial, el mensaje podía contener textos como "verificando cuenta" o "confirmando información de factura". Una vez el usuario enviaba su contraseña, el atacante podía tener acceso a la cuenta de la víctima y podia utilizarla para varios propósitos

criminales, incluyendo el spam. Tanto el phishing como el warezing en AOL requerían generalmente el uso de programas escritos por crackers, como el AOLHell.

En 1997 AOL reforzó su política respecto al phishing y los warez fueron terminantemente expulsados de los servidores de AOL. Durante ese tiempo el phishing era tan frecuente en AOL que decidieron añadir en su sistema de mensajería instantánea, una línea de texto que indicaba: "no one working at AOL will ask for your password or billing information" que en español significa que nadie que trabaje en AOL le pedirá a usted su contraseña o información de facturación. Simultáneamente AOL desarrolló un sistema que desactivaba de forma automática una cuenta involucrada en phishing, normalmente antes de que la víctima pudiera responder. Los phishers se trasladaron de forma temporal al sistema de mensajería instantáneo de AOL (AIM o American Instant Messenger), debido a que no podían ser expulsados del servidor de AIM. El cierre obligado de la escena de warez en AOL causó que muchos phishers dejaran el servicio, y en consecuencia la práctica.

Los intentos más recientes de phishing han tomado como objetivo a clientes de bancos y servicios de pago en línea. Aunque el ejemplo que se muestra en la primera imagen es enviado por phishers de forma indiscriminada con la esperanza de encontrar a un cliente de dicho banco o servicio, estudios recientes muestran que los phishers en un principio son capaces de establecer con qué banco una posible víctima tiene relación, y de ese modo enviar un e-mail, falseado apropiadamente, a la posible víctima. En términos generales, esta variante hacia objetivos específicos en el phishing se ha denominado spear phishing (literalmente phishing con lanza). Los sitios de Internet con fines sociales también se han convertido en objetivos para los phishers, dado que mucha de la información provista en estos sitios puede ser utilizada en el robo de identidad. Algunos experimentos han otorgado una tasa de éxito de un 70% en ataques phishing en redes sociales. A finales del 2006 un gusano informático se apropió de algunas páginas del sitio web MySpace logrando redireccionar los enlaces de modo que apuntaran a una página web diseñada para robar información de ingreso de los usuarios.

Los daños causados por el phishing oscilan entre la pérdida del acceso al correo electrónico a pérdidas económicas sustanciales. Este tipo de robo de identidad se está haciendo cada vez más popular por la facilidad con que personas confiadas normalmente revelan información personal a los phishers, incluyendo números de tarjetas de crédito y números de seguridad social. Una vez esta información es adquirida, los phishers pueden usar datos personales para crear cuentas falsas utilizando el nombre de la víctima, gastar el crédito de la víctima, o incluso impedir a las víctimas acceder a sus propias cuentas.

Se estima que entre mayo del 2004 y mayo del 2005, aproximadamente 1.2 millones de usuarios de computadoras en los Estados Unidos tuvieron pérdidas a causa del phishing, lo que suma a aproximadamente $929 millones de dólares estadounidenses. Los negocios en los Estados Unidos perdieron cerca de 2000 millones de dólares al año mientras sus clientes eran víctimas. El Reino Unido también sufrió el alto incremento en la práctica del phishing. En marzo del 2005, la cantidad de dinero reportado que perdió el Reino Unido ha causa de esta práctica fue de aproximadamente £12 millones de libras esterlinas. (Ver Anexo 01).

5.1.1 Respuesta Social Ante El Phishing.

Una estrategia para combatir el phishing adoptada por algunas empresas es la de entrenar a los empleados de modo que puedan reconocer posibles ataques phishing. La nueva táctica de phishing donde se envían correos electrónicos de tipo phishing a una compañía determinada, conocido como spear phishing, ha motivado al entrenamiento de usuarios en varias localidades, incluyendo la Academia Militar de West Point en los Estados Unidos. En un experimento realizado en junio del 2004 con spear phishing, el 80% de los 500 cadetes de West Point a los que se les envió un e-mail falso fueron engañados y procedieron a dar información personal[46]. Ver Anexo (03)

[46] Bank, David: *"'Spear Phishing' Tests Educate People About Online Scams",* The Wall Street Journal, 17 de agosto del 2005.

Una vez que a un usuario se le contacta mediante un mensaje electrónico, y en dicho mensaje se hace mención sobre la necesidad de "verificar" una cuenta electrónica propiedad del usuario, este puede contactar con la compañía que supuestamente le envía el mensaje, o puede escribir la dirección web de un sitio web seguro en la barra de direcciones de su navegador para evitar usar el enlace que aparece en el mensaje sospechoso de phishing. Muchas compañías, incluyendo eBay y PayPal, siempre se dirigen a sus clientes por su nombre de usuario en los correos electrónicos, de manera que si un correo electrónico se dirige al usuario de una manera genérica como ("Querido miembro de eBay") es probable que se trate de un intento de phishing.

5.1.2 Respuestas Legislativas y Judiciales ante el Fraude Informático

El 26 de enero de 2004, la FTC (Federal Trade Commission, "Comisión Federal de Comercio") de Estados Unidos llevó a juicio el primer caso contra un phisher sospechoso. El acusado, un adolescente de California, supuestamente creó y utilizó una página web con un diseño que aparentaba ser la página de American Online para poder robar números de tarjetas de crédito.[47] Tanto Europa como Brasil siguieron la práctica de los Estados Unidos, rastreando y arrestando a presuntos phishers. A finales de marzo del 2005, un hombre estonio de 24 años fue arrestado utilizando una backdoor, a partir de que las víctimas visitaron su sitio web falso, en el que incluía un keylogger que le permitía monitorear lo que los usuarios tecleaban[48]. Del mismo modo, las autoridades arrestaron al denominado phisher kingpin, Valdir Paulo de Almeida, líder de una de las más grandes redes de phishing que en dos años había robado entre $18 a $37 millones de dólares estadounidenses [49]. En junio del 2005 las autoridades del Reino Unido arrestaron a dos hombres por la práctica del phishing[50], en un caso conectado a la denominada Operation Firewall del Servicio Secreto de los Estados Unidos, que buscaba sitios web notorios que practicaban el phishing. (Ver Anexo 02)

[47] Legon, Jeordan: "'Phishing' scams reel in your identity", CNN, 26 de enero de 2004.
[48] Leyden, John: "Trojan phishing suspect hauled in", *The Register*, 4 de abril del 2005.
[49] Leyden, John: "Brazilian cops net 'phishing kingpin'", *The Register*, 21 de marzo del 2005
[50] "UK Phishers Caught, Packed Away," *eWEEK*, junio 27 del 2005.

En los Estados Unidos, el senador Patrick Leahy introdujo el Acta Anti-Phishing del 2005 el 1 de marzo del 2005. Esta ley federal de anti-phishing establecía que aquellos criminales que crearan páginas web falsas o enviaran spam a cuentas de e-mail con la intención de estafar a los usuarios podrían recibir una multa de hasta $250,000 USD y penas de cárcel por un término de hasta cinco años[51].

La compañía Microsoft también se ha unido al esfuerzo de combatir el phishing. El 31 de marzo del 2005, Microsoft llevó a la Corte del Distrito de Washington 117 pleitos federales. En algunos de ellos se acusó al denominado phisher "John Doe" por utilizar varios métodos para obtener contraseñas e información confidencial. Microsoft espera desenmascarar con estos casos a varios operadores de phishing de gran envergadura. En marzo del 2005 también se consideró la asociación entre Microsoft y el gobierno de Australia para educar sobre mejoras a la ley que permitirían combatir varios crímenes cibernéticos, incluyendo el phishing.

En la sesión de la comisión permanente del miércoles 20 de julio de 2005, aparece en la Gaceta Parlamentaria del H. Congreso de La Unión, una propuesta por parte del Partido de la Revolución Democrática, en la cual se propuso legislar en materia de delitos informáticos; de dicha sesión se desprende que los bienes jurídicos que se protegen son la información contenida en sistemas o equipos de informática que tengan un mecanismo de seguridad, el patrimonio, el mercado nacional, la fe pública y privada, la privacidad de los datos.

En dicha sesión, se tomó en cuenta que las nuevas tecnologías de la comunicación han provocado que cada vez más conductas criminales sean perpetradas a través de la informática y que estas queden impunes por falta de tipos penales aplicables ante las limitaciones impuestas por el principio de legalidad penal que proscribe la analogía y la interpretación extensiva.

[51] "Phishers Would Face 5 Years Under New Bill," Information Week, 2 de marzo del 2005

La Comisión Nacional Para La Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF), trata el Fraude Informático con un enfoque encaminado a Operaciones Bancarias; para esta, dentro de los llamados ilícitos patrimoniales más frecuentes en contra de Instituciones Bancarias, resalta el fraude en sus diversas modalidades. Entre los más importantes está el fraude genérico, específico e informático; el fraude con el uso de tarjetas de débito o de crédito falsas, el uso de cheques falsos, de cheques originales obtenidos de forma ilícita; el desvío de fondos destinados al pago de impuestos y los accesos indebidos a los sistemas informáticos de las Instituciones Financieras, con la finalidad de realizar transferencias ilegales de recursos. La prolija imaginación para ejecutar estos delitos es abundante.

Simplemente, en materia de tarjetas bancarias se encuentra la falsificación integral de las mismas, incluido el copiado total de la banda magnética, que permite el traslado de los datos registrados en la original hacia otro plástico, de manera que se tiene un duplicado exacto de la verdadera. Los fraudes con cheques no se quedan atrás. En muchos de los casos se trata de documentos apócrifos derivados de la falsificación integral de los esqueletos que los componen. El uso de la tecnología de punta para este propósito es algo común, así como para la elaboración de identificaciones falsas para hacer los cheques cobrables.

A decir de los expertos, el fraude que más se ha popularizado es el perpetrado en contra de los contribuyentes de impuestos. Algunas personas que trabajan en bancos, coludidas con los empleados de las recaudadoras fiscales, realizan toda una serie de maniobras para desviar los pagos de personas físicas y morales hacia otras cuentas bancarias.

Una modalidad de fraude que está alcanzando dimensiones preocupantes es el realizado a través de transferencias electrónicas sobre el soporte de la red mundial. El defraudador se hace del Número de Identificación Personal (NIP) del titular de la cuenta y, por medio del servicio de banca por Internet, transfiere los recursos de la cuenta hacia alguna otra para disponer de ese dinero. Dado que es difícil determinar quién ha sido el autor del fraude, la

legislación considera a los titulares como partícipes de "lavado de dinero" y, por tanto, culpables de disponer ilícitamente de recursos ajenos. No obstante que pueden darse situaciones de riesgo en las instituciones bancarias, el usuario debe tener la certeza de que cuenta con el respaldo por parte de la institución y del Instituto para la Protección al Ahorro Bancario (IPAB) cuando sea el caso.

Ante eso, en mayo de 2000, la Oficina Federal de Investigaciones de Estados Unidos (FBI), junto con el departamento de Justicia y el Centro Nacional de Delitos Cometidos por Trabajadores no Manuales de ese país, anunciaron la creación del Centro de Denuncias de Fraudes en la Internet (Internet Fraud Complaint Center o IFCC). Este Centro tiene por objetivo permitir a los consumidores de diversos servicios financieros accesibles a través de Internet, que sospechan de un fraude en ese medio, buscar información para tener mayores elementos que le permitan estar alerta ante una eventualidad de este tipo. Entre esos delitos se encuentra el fraude bancario[52].

Además de ello, independientemente del combate a la criminalidad por parte de las instituciones bancarias, trabajan para formar un frente común en contra de la delincuencia con base en medidas más severas, como mayor capacitación al personal que labora en sus diferentes sucursales, criterios más estrictos para la selección de sus empleados, controles informáticos cada vez más eficientes de monitoreo y detección de los Usuarios de estos servicios, aplicación de auditorias sorpresivas, entre muchas otras

En el Estado de Nayarit, existen antecedentes de que el fraude informático se ha cometido en numerosas ocasiones, como se puede constatar en el Exp: 180/06 del Juzgado Penal de Acaponeta en el cual el indiciado de Nombre Baltasar Ojeda Morales, cometió en agravio de la querellante Banco Nacional de México, un delito de fraude que le importo problemas al juzgador a la hora de encuadrarlo en el tipo penal de fraude, toda vez que no encajaba con los elementos comunes que constituyen al delito de fraude, en su modalidad

[52] http:www.ifccfbi.gov.

genérica y especifica. Lo curioso de este caso, fue la forma en la que el indiciado se hacia de cuantiosas cantidades en una cuenta de banco de su propiedad, con un movimiento bancario de nombre devolución de Mercancía en el Extranjero, y que continuó logrando acumular dicha cantidad a expensas de la querellante.

5.3 FRAUDE GENÉRICO EN EL ESTADO DE NAYARIT.

En el Código Penal para el Estado de Nayarit, se encuentra en su Artículo 368, la definición específica del delito de fraude, la cual es "Comete el delito de fraude, el que engañando a alguno o aprovechándose del error en que éste se halla, se haga ilícitamente de una cosa o alcance un lucro indebido para sí o para otro"[53], dicho es sancionado con las siguientes penas:

"I. Con prisión de tres días a dos años y multa de diez a treinta días de salario, cuando el valor de lo defraudado no exceda de cien veces del salario mínimo vigente.

II. Con prisión de dos a seis años y multa de quince a sesenta días de salario, cuando el valor de lo defraudado excediera de cien pero no de quinientas veces el salario.

III. Con prisión de seis a doce años y multa hasta de veinte a cien días de salario, si el valor de lo defraudado fuere mayor de quinientas veces el salario.

Cuando el sujeto pasivo entregue la cosa de que se trata a virtud no solo de engaños, sino de maquinaciones o artificios que para obtener esa entrega se hayan empleado, la pena señalada en las fracciones anteriores, se aumentará con prisión de tres días a dos años".

Este delito cuenta con casos especiales de defraudación, los cuales se contemplan en el Artículo 369 del mismo Código; estos comprenden 15 fracciones de conductas diferentes que se

[53] *Código Penal para el Estado de Nayarit.* México. Ed. Delma.

sancionarán conforme a lo dispuesto en el artículo que trata al Fraude. Dichas conductas son las siguientes:

"I. Al que obtenga, dinero, valores o cualquier otra cosa, ofreciendo encargarse de la defensa de un procesado o de un reo, si no realiza ésta o la abandona sin causa justificada;

II. Al que por título oneroso enajene alguna cosa con conocimiento de que no tiene derecho para disponer de ella, o la arriende, hipoteque, empeñe o grave de cualquier otro modo, si ha recibido el precio, el alquiler, la cantidad en que la grave, parte de ellos o un lucro equivalente;

III. Al que obtenga de otro una cantidad de dinero o cualquier otro lucro, otorgándole o endosándole a nombre propio o de otro un documento nominativo, a la orden o al portador, contra una persona supuesta o que el otorgante sabe que no ha de pagarle;

IV. Al que se haga servir alguna cosa o admita un servicio en cualquier establecimiento comercial y no pague el importe;

V. Al que compre una cosa mueble ofreciendo pagar su precio al contado y rehúse después de recibirla, a hacer el pago o devolver la cosa si el vendedor le exige lo primero dentro de quince días de haber recibido la cosa el comprador;

VI. Al que hubiere vendido una cosa mueble y recibido su precio, si no la entrega dentro de los quince días del plazo convenido o no devuelve su importe en el mismo término, en caso de que se le exija esto ultimo;

VII. Al que venda a dos o más personas una misma cosa, sea mueble o raíz y reciba el precio de la primera, de la segunda o siguientes enajenaciones o de dos o más de ellas o parte del precio, o cualquier otro lucro con perjuicio del primero o de los siguientes compradores;

VIII. Al que simulare un contrato, un acto o escrito judicial, con perjuicio de otro;

IX. Al que por sorteos, rifas, loterías, promesas de venta o por cualquier otro medio se quede con todo o parte de las cantidades respectivas, sin entregar la mercancía u objeto ofrecido;

X. Al fabricante, empresario contratista o constructor de una obra cualquiera, que emplee en la construcción de la misma, materiales en cantidad o calidad inferiores a las convenidas, mano de obra inferior a la estipulada, siempre que haya recibido el precio o parte de él;

XI. Al vendedor de material de construcción de cualquiera especie, que habiendo recibido el precio de los mismos, no los entregue en su totalidad o calidad convenidos;

XII. Al que explote la superstición o la ignorancia de una persona por medio de supuesta evocación de espíritus, adivinaciones o curaciones;

XIII. Al que habiendo recibido mercancías con subsidio o franquicia para darles un destino determinado, la distrajere de este destino o en cualquier forma desvirtúe los fines perseguidos por el subsidio o la franquicia;

XIV. Al que para eludir todo o parcialmente el pago de un impuesto, contribución, multa o cualquier otra prestación fiscal legalmente decretada, emplee simulaciones, engaños o cualquier otro procedimiento que tienda a ocultar, variar o desnaturalizar la causa o sujeto del impuesto, multa o prestación o a inducir a error en alguna forma a las autoridades fiscales; y

XV. Al que obtenga de cualquier persona o institución una suma de dinero o cosas determinadas en concepto de refacción, habilitación o avío y no los aplique al objeto u obras convenidos. Cuando el dinero o cosas hayan sido recibidas por una persona moral, los responsables del delito serán las personas físicas que suscriban los documentos relativos sin perjuicio de decretar la suspensión de la persona jurídica en sus actividades, hasta por un año"[54].

[54] *Código Penal para el Estado de Nayarit.* México. Ed. Delma.

5.4 ESTUDIO DOGMÁTICO DEL DELITO DE FRAUDE INFORMÁTICO.

A continuación se presenta la clasificación del delito que atañe a esta investigación, lo cual es necesario para comprender las diferencias que existen ente este último y el delito de fraude genérico y específico, y como en un futuro podría aparecer en el catálogo de delitos del Estado de Nayarit.

Clasificación del Delito de Fraude Informático:

I. **Por su gravedad:** Es un delito, porque viola una norma jurídica, siendo sancionado por la autoridad judicial.

II. **Por la conducta del agente:** De acción y de comisión por omisión.

III. **Por su resultado:** Material.

IV. **Por el daño que causa:** De lesión

V. **Por su duración:** Instantáneo

VI. **Por el elemento interno:** Doloso

VII. **Por su estructura:** Simple

VIII. **Por el número de actos: MULTISUBSISTENTE**: Porque el delito se consuma en un determinado número de actos.

IX. **Por el número de sujetos: MULTISUBJETIVO:** Porque para su integración, no solo requiere de la participación de un sujeto, sino que pueden participar aún mas.

X. **Por su forma de persecución:** De Querella y De Oficio.

XI. **En función de su materia:** Común.

XII. **Clasificación legal:** Título Vigésimo "Delitos contra el patrimonio", del Código Penal Para el Estado de Nayarit.

Imputabilidad e inimputabilidad.

I. **Imputabilidad:** Será imputable, el agente con grandes capacidades en materia de informática, menores de edad.

II. **Inimputabilidad:** Incapacidad mental o desarrollo intelectual retardado.

CONDUCTA Y SU AUSENCIA.

I. **Conducta:**
   a. Acción.- el fraude informático es un delito de acción respecto al elemento del engaño, a virtud de que el agente requiere realizar un acto positivo, consistente en un movimiento corporal e incorporeo, para que produzca el resultado.
   b. Comisión por omisión: No se presenta.

II. **Sujetos:** Activo y Pasivo.
   a. **Activo:** en el delito de fraude específico regulados por el artículo 368 en sus fracciones I, II, III, IV, V, VI, VII, VIII, IX, X, XI, XII, XIII, XIV, XV y 370, será cualquier persona que engañe o se aproveche del error en que se encuentra otro, para hacerse ilícitamente de alguna cosa o alcanzar un lucro indebido.
   b. **Pasivo:** En el delito de Fraude específico, sujeto pasivo puede ser cualquier persona física o moral, quien sufre el daño patrimonial.

III. **Objetos**: estos son material y jurídico:
   a. **Material:** Será la cosa obtenida ilícitamente por el agente, o el lucro indebido.

b. **Jurídico:** El objeto jurídico en el delito de fraude es el patrimonio.

IV. Lugar y Tiempo de la Comisión del Ilícito: Artículo 1, 2, 3 y 4 del Código Penal Para el Estado de Nayarit.

V. Ausencia de conducta. No se presenta ninguna causa de ausencia de conducta

Tipicidad y Atipicidad:

I. Tipicidad:

a. Tipo: Actualmente no se encuentra descrito en el tipo penal de fraude especifico pero es la propuesta de este trabajo de tesis, la creación de la fracción XVI del Artículo 370 del Código Penal para el Estado de Nayarit.

b. Tipicidad: se presentará en el delito de fraude cuando se adecue la conducta a cualquiera de los tipos mencionados con antelación, es decir, a los elementos descritos en el precepto legal.

c. Clasificación:

i. Por su composición: Es un tipo anormal, porque además del elemento objetivo contiene elementos normativos. El hacerse ilícitamente de una cosa o alcanzar un lucro indebido;

ii. Por su ordenación Metodológica: el fraude informático es un delito fundamental o básico, por tener plena independencia y estar formado con una conducta ilícita sobre un bien jurídicamente tutelado, es decir, no contiene circunstancia alguna que agrave o atenúe la penalidad;

iii. En función de su autonomía: el fraude es un tipo autónomo ya que tiene vida propia, no depende de la realización de ningún otro tipo penal para su perpetración,

iv. Por su formulación: es casuístico en virtud a que está formado por dos hipótesis, se puede cometer el delito de fraude por engaño o aprovechamiento del error;

v. Por el daño: es de lesión porque el resultado material daña directamente al bien jurídicamente tutelado que es el patrimonio de las personas.

II. Atipicidad:

a. Ausencia de calidad exigida por la ley en cuanto a los sujetos activos;

b. Por falta del objeto material, es decir, que no exista la cosa o el lucro indebido;

c. Por falta de objeto jurídico: el patrimonio de las personas;

d. Al no realizarse el hecho por los medios comisitos específicamente señalados; y

e. Si faltan los elementos subjetivos del injusto legalmente exigidos.

Antijuricidad y causas de justificación.

I. Antijuricidad: al cometer el delito de fraude está realizando una conducta antijurídica, es decir, contraria a derecho. Para que esta antijuricidad se presente, el agente no debe haber actuado bajo ninguna causa de justificación.

II. Causas de justificación: No existen causas de justificación para este delito.

Culpabilidad e inculpabilidad.

I. Culpabilidad: dolo directo.

II. Inculpabilidad:

i. Error esencial de hecho invencible de tipo y de licitud.

ii. No exigibilidad de otra conducta.

Condiciones objetivas de punibilidad y su ausencia: No se presentan, por lo consiguiente, hay ausencia de condiciones objetivas de punibilidad.

Punibilidad y Excusas Absolutorias.

I. **Punibilidad:** se encuentra establecida en los artículos 368 y 370 del Código Penal para el estado de Nayarit.

II. **Excusas Absolutorias:** No se presenta.

ASPECTOS COLATERALES DEL DELITO.

Vida del Delito:

a).- Fase Interna: Se presenta en la psique del agente cuando surge la idea de cometer el delito de fraude, después la delibera y finalmente decide ejecutarla.

b).- Fase Externa: Es cuando el agente exterioriza su idea, prepara todos los elementos necesarios para la realización del ilícito y finalmente lo ejecuta.

c).- Ejecución:

- Consumación: el delito de fraude se consuma en el momento en que el agente por medio del engaño o aprovechamiento del error, se hace ilícitamente de alguna cosa o alcanza un lucro indebido.

- Tentativa:
  - Tentativa Acabada: no se presenta puesto que sería imperceptible.
  - Tentativa Inacabada: no se presenta puesto que sería imperceptible.

Participación.

a).- Autor Material: perpetra directamente en el delito de fraude.

b).- Coautor: En unión del autor material comete el ilícito, realizando conductas descritas en el tipo penal.

c).- Autor Intelectual: Prepara la realización del delito e induce a otro a su ejecución.

d).- Autor Mediato: No comete directamente el hecho delictivo, acude a otra persona extraña que utiliza como instrumento para su realización.

e).- Cómplice: Se presente en este tipo penal cuando un individuo ayuda al agente en acciones secundarias encaminadas a su ejecución.

f).- Encubridor: No es necesario, toda vez que por los medios en que se comete el delito, existe cierto sigilo.

Concurso de delitos.

a).- Ideal.- El concurso ideal se presenta cuando con una conducta se cometen varios delitos.

b).- Material: es el concurso de delitos en el que, con varias conductas, se cometen varios delitos distintos.

Acumulación.

El Sistema Jurídico Mexicano, en caso de acumulación de delitos, utiliza el método de acumulación jurídica, que consistirá en tomar como base para la imposición de la sanción el delito mayor, al que se le irán sumando proporcionalmente las sanciones de los demás ilícitos cometidos, si que exceda de los máximos señalados por la ley penal.

CONCLUSIONES

Una vez desarrollada la presente investigación es preciso dar a conocer los resultados obtenidos y se procede en consecuencia, al tenor de las siguientes conclusiones:

PRIMERA. Con el apoyo de las fuentes de información y los razonamientos propios se comprobó la hipótesis formulada por el sustentante.

SEGUNDA. Es obligatorio cumplir con la aplicación de los Tratados Internacionales en los que México es parte.

TERCERA. Es necesario que se proteja el Bien Jurídico Tutelado, que en este caso es el patrimonio y la propiedad.

CUARTA.- Que la informática reúne características que la convierten en un medio idóneo para la comisión de muy distintas modalidades delictivas, en especial de carácter patrimonial.

QUINTA.- Es obligatorio tener un mayor control con las nuevas tecnologías que se presentan.

SEXTA. Es inapelable la necesidad de instruir a la autoridad en materia de control de las nuevas tecnologías.

SEPTIMA.- Es impresionante el como el fraude informático ha proliferado hasta el grado de afectar gravemente el patrimonio y la propiedad.

OCTAVA.- Que la conducta delictiva conocida como fraude informático, es cometida por personas con altos conocimientos muy por encima del promedio de la población del estado.

NOVENA.- Que la expansión del comercio electrónico es una de las actividades que obliga a incorporar por lo menos un tipo penal descriptivo de la falsificación o eliminación de documentos o la incorporación de alguno a un sistema que utiliza tecnologías de información.

DECIMA.- Es importante penalizar la conducta delictiva de Fraude Informático en el Código Penal del Estado de Nayarit.

PROPUESTAS.

Una vez teniendo los resultados de la investigación es preciso dar a conocer las propuestas tendentes a resolver el problema de la investigación.

PRIMERA: Establecer los lineamientos y políticas de seguridad de los sistemas informáticos en el Estado de Nayarit.

SEGUNDA: Definir estándares de seguridad en el desarrollo de aplicaciones informáticas.

TERCERA: Definir estándares de seguridad en la instalación de sistemas operativos y bases de datos.

CUARTA: Definir estándares de seguridad en el diseño de redes de computadoras, para que no se cometa el fraude informático.

QUINTA: Desarrollar los mecanismos para salvaguardar el secreto de la información mediante redes o sistemas informáticos y de telecomunicaciones seguros.

SEXTA: Salvaguardar el contenido informacional de las comunicaciones.

SEPTIMA: Salvaguardar la información de carácter confidencial y patrimonial contenida en sistemas y equipos de informática del Estado de Nayarit.

OCTAVA: Impulsar la legislación en materia de delitos informáticos

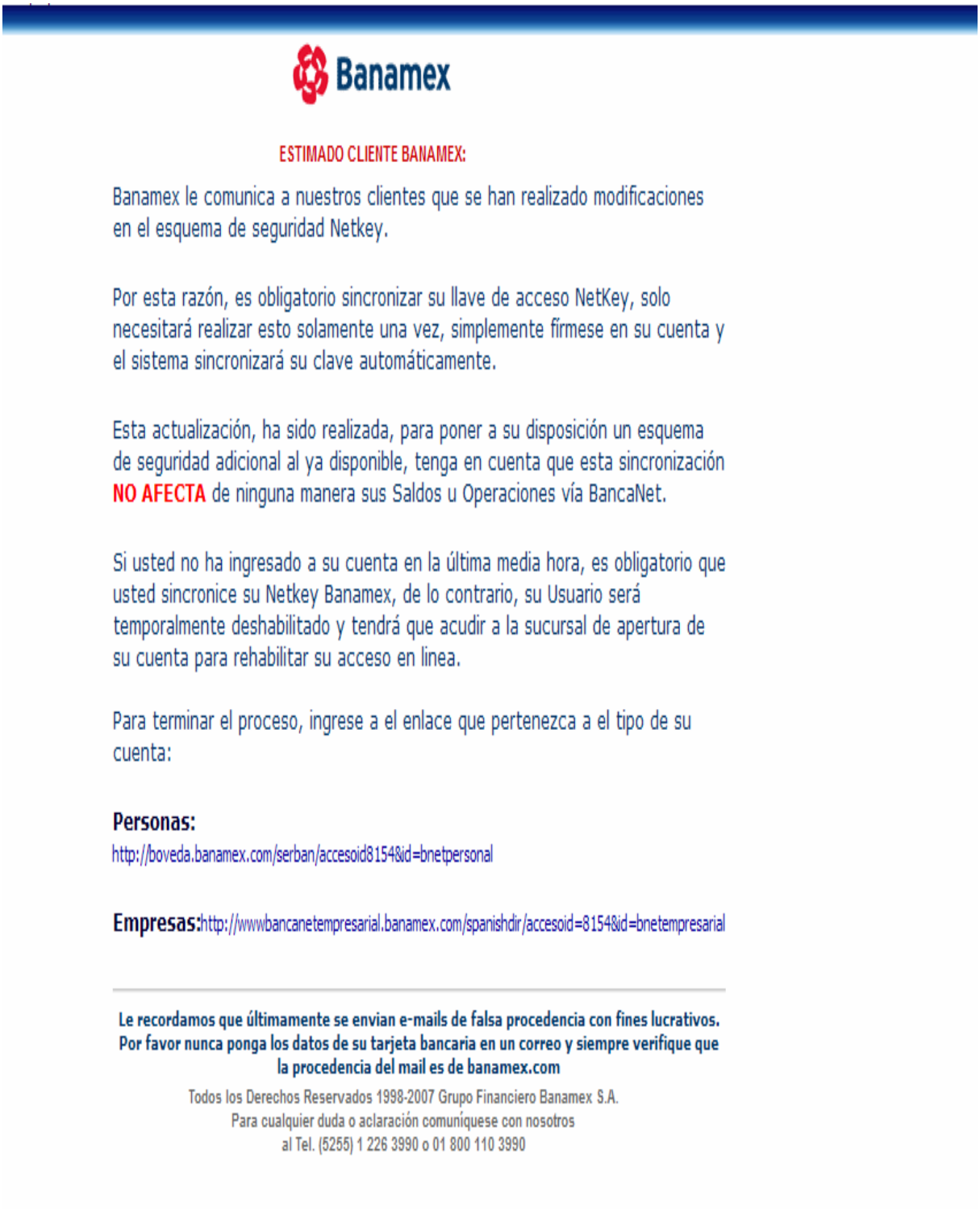
NOVENA: Determinar los métodos de respuesta legal a tomar cuando se identifique el Fraude Informático.

DECIMA: Que se adicione una fracción al artículo 369 del Código Penal para el Estado de Nayarit, al contenido del esquema siguiente o alguno que en esencia sea similar:

TEXTO VIGENTE	TEXTO QUE SE PROPONE
CÓDIGO PENAL PARA EL ESTADO DE NAYARIT. **TÍTULO VIGESIMO** **DELITOS CONTRA EL PATRIMONIO.** **CAPÍTULO IV** **FRAUDE** **Artículo 369**.- *Se considerarán como casos especiales de defraudación y se sancionarán conforme a lo dispuesto en el artículo anterior, los siguientes:* *I, II, III, IV, V, VI, VII, VIII, IX, X, XI, XII, XIII, XIV, XV- ……*	**CÓDIGO PENAL PARA EL ESTADO DE NAYARIT.** **TÍTULO VIGESIMO** **DELITOS CONTRA EL PATRIMONIO.** **CAPÍTULO IV** **FRAUDE** **Artículo 369**.- *Se considerarán como casos especiales de defraudación y se sancionarán conforme a lo dispuesto en el artículo anterior, los siguientes:* *I, II, III, IV, V, VI, VII, VIII, IX, X, XI, XII, XIII, XIV, XV- ……* ***XVI.-*** *El que a través del uso de tecnologías de información, acceda, intercepte, interfiera manipule o use, mediante engaño o aprovechamiento del error, un sistema o medio de comunicación para obtener bienes o valores tangibles o intangibles de carácter patrimonial sustrayéndolos de su tenedor, sin derecho y sin consentimiento de la persona que puede disponer de ellos con arreglo a la ley.*

ANEXO.

Anexo 01.



Banamex

ESTIMADO CLIENTE BANAMEX:

Banamex le comunica a nuestros clientes que se han realizado modificaciones en el esquema de seguridad Netkey.

Por esta razón, es obligatorio sincronizar su llave de acceso NetKey, solo necesitará realizar esto solamente una vez, simplemente fírmese en su cuenta y el sistema sincronizará su clave automáticamente.

Esta actualización, ha sido realizada, para poner a su disposición un esquema de seguridad adicional al ya disponible, tenga en cuenta que esta sincronización NO AFECTA de ninguna manera sus Saldos u Operaciones vía BancaNet.

Si usted no ha ingresado a su cuenta en la última media hora, es obligatorio que usted sincronice su Netkey Banamex, de lo contrario, su Usuario será temporalmente deshabilitado y tendrá que acudir a la sucursal de apertura de su cuenta para rehabilitar su acceso en linea.

Para terminar el proceso, ingrese a el enlace que pertenezca a el tipo de su cuenta:

Personas:
http://boveda.banamex.com/serban/accesoid8154&id=bnetpersonal

Empresas: http://wwwbancanetempresarial.banamex.com/spanishdir/accesoid=8154&id=bnetempresarial

Le recordamos que últimamente se envian e-mails de falsa procedencia con fines lucrativos. Por favor nunca ponga los datos de su tarjeta bancaria en un correo y siempre verifique que la procedencia del mail es de banamex.com

Para cualquier duda o aclaración comuníquese con nosotros
al Tel. (5255) 1 226 3990 o 01 800 110 3990

Anexo 02.


Phishing Reported between October 2004 to June 2005
Incidents Reported
16000
14000
12000
10000
8000
6000
4000
2000
0
6957
8975
8829
12845
13468
12883
14411
14987
15050
October
November
December
January
Febuary
March
April
May
June
2004
2005
Month

Anexo 03. http://seguridad.internautas.org/phishing/

G L O S A R I O

1. **TLC:** Tratado de Libre Comercio de América del Norte.
2. **OCD:** Organización de Cooperación y Desarrollo Económico.
3. **CONDUSEF.** Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros.
4. **NIP.** Número de Identificación Personal.
5. **FBI.** Federal Bureau of Investigations.
6. **IFCFBI.** Internet Crime Complaint Center. Centro de Denuncias de Fraudes en la Internet.
7. **AOL.** America Online.
8. **Hacker.** La palabra deriva de hack, que significa hacha, y es él termino que se usaba para describir la familiar forma en que los técnicos telefónicos arreglaban cajas defectuosas, el bueno y el viejo golpe seco, y la persona encargada de ejecutar esos golpes se le llamaba naturalmente un hacker, este tipo de persona no es considerado propiamente un delincuente, se asemeja más bien a un bromista que disfruta entrando en sistemas informáticos privados y que toma esa actividad como un reto a sus conocimientos.
9. **Cracker.** La significación deriva de la palabra en ingles crack, que significa romper, este tipo de personas trae aparejada la firme intención de provocar un daño en los sistemas informáticos de un tercero, lo cual constituye un auténtico peligro, su terminación er, connota al quebrador, o persona que se dedica a dañar los sistemas informáticos, ya por que se le pagó o por motivos nocivos que bien pueden ser personales.
10. **Phreacker**. En castellano se denomina pirata, que manipula esencialmente los sistemas informáticos de las compañías de teléfonos, ahorrándose una considerable cantidad de dinero, puesto que activa teléfonos convencionales y celulares piratas, constituyendo un grado de peligro para las empresas que manejan esta línea comercial.
11. **Lamer.** Connota a la persona que su especialidad radica en utilizar códigos fuentes de otros programadores para beneficio (una especie de plagio electrónico) propio sin hacer mención del copyright (derechos de autor).
12. **Sniffer.** Del inglés sniff, que significa olfatear, este tipo de personas navega por la línea internet de sistema en sistema, con la intención de descubrir todo tipo de errores que pudieran vender o utilizar en su beneficio (robo de información, acceso a sistemas financieros, a secretos de patentes, al banco de información científica, etc).

13. **Graffitis.** Deriva de la palabra gráfico, y su conducta esencial estriba en rayar los sistemas informáticos, al igual que en nuestra actualidad se rayan las paredes, estos se dedican a decorar la página web con sus creaciones pintorescas.
14. **El caballo de Troya:** consiste en introducir en un programa de uso habitual una rutina o conjunto de instrucciones, por supuesto no autorizado, para que dicho programa actúe en ciertos casos de forma distinta a como estaba previsto. Es un método difícil de detectar pero fácil de prevenir instituyendo estrictos procedimientos de catalogación y descatalogación de programas de forma que sea imposible acceder a ningún programa para su modificación sin los correspondientes permisos, y una vez que éste haya sido modificado, comprobar que el programa funciona correctamente, modificado en lo que se pretendía y que el resto siga igual.
15. **Técnica del salami:** consiste en introducir o modificar unas pocas instrucciones en los programas para reducir sistemáticamente las cuentas bancarias, los saldos de proveedores transmitiéndola a una cuenta virtual. Es de fácil realización y de difícil comprobación.
16. **Técnica del super zaping:** consiste en el uso no autorizado de un programa de utilidad para alterar, borrar, copiar, insertar o utilizar en cualquier forma no permitida los datos almacenados en la computadora. El nombre proviene de un programa de utilidad conocido como SUPERZAP que es como una llave que abre cualquier rincón de la computadora por protegido que pueda estar, es un programa de acceso universal. Generalmente al detectar la alteración de los datos se piensa que es un mal funcionamiento de la computadora.
17. **Técnica de puertas falsas.** Este método consiste en interrupciones producidas que los programadores hacen para el chequeo del programa con lo que se dejan puertas falsas para entrar en él. El problema que se presenta es tener la certeza de que cuando los programas entran en proceso de producción normal todas las puertas falsas hayan desaparecido.
18. **Técnica de creación de bombas lógicas**: consiste en introducir en un programa un conjunto de rutinas generalmente no utilizadas para que en una fecha o circunstancia predeterminada se ejecuten, desencadenando la destrucción de la información almacenada en la computadora distorsionando el funcionamiento del sistema, provocando paralizaciones intermitentes.
19. **Ataques asincrónicos:** la técnica se basa en la forma de funcionar de los sistemas operativos y sus conexiones con los programas de la aplicación a los que sirve y soporta en su ejecución. En virtud de que los sistemas operativos funcionan en forma asincrónica,

estableciendo colas de espera que van desbloqueando en función de la disponibilidad de los datos o recursos que se esperaban. Esta técnica es poco utilizada en virtud de su complejidad.

20. **Aprovechamiento de información residual:** se basa en aprovechar los descuidos de los usuarios o técnicos informáticos para obtener información que ha sido abandonada sin ninguna protección como residuo de un trabajo real efectuado con autorización.
21. **Divulgación no autorizada de datos reservados:** sustracción de información confidencial o espionaje industrial.
22. **Escuchas telefónicas:** técnica en la que para su utilización de requiere de un módem para demodular las señales telefónicas analógicas y convertirlas en señales digitales.
23. **https:** Secure HTTP (HTTP Seguro. Protocolo de http con ciertas especificaciones usado en sitios seguros (sitios que requieren contraseñas), como websites de bancos, correo basado en todas las páginas web con extensión .html o .htm usualmente están almacenadas en un servidor de tipo WWW, y este servidor usa el protocolo http.
24. **ftp:** File Transfer Protocol (Protocolo de Transferencia de Archivos), es el utilizado en la transferencia de archivos almacenados en un servidor de FTP. Normalmente estos archivos son para descargar, y "no son páginas web" sino de otro tipo, como archivos con extensiones .exe, .pdf, .zip, etc. Por ejemplo, el servidor de ftp de la DST ftp://ftp.dst.usb.ve.
25. **Mail to:** Indica que se trata de una dirección de correo electrónico. Al escribirla en su navegador web inmediatamente se abre el programa predeterminado de correo electrónico en su computadora, como por ejemplo Outlook Express, Netscape Messenger, Microsoft Outlook o cualquier otro.
26. **URL.** Uniform Resource Locator. Localizador Uniforme de Recursos.
27. **I.P.** es un número que identifica de manera lógica y jerárquica a una interfaz de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP (*Internet Protocol*), que corresponde al nivel de red o nivel 3 del modelo de referencia OSI.
28. **News:** Indica que el URL apunta a algún Usenet Newsgroup o Grupo de Noticias. Al igual que con mail to al introducir una dirección que comience por news:// se abre el programa indicado para manejarla.
29. **FTC.** Comisión Federal de Comercio, en sus siglas en Ingles "Federal Trade Commssion".
30. **Telnet:** Al intoducirla se ejecutará un programa separado de cliente telnet.

31. **Gopher:** Utilizado cuando se desea navegar por servidores de directorios Gopher.
32. **Wais:** Se utiliza para navegar por los servidores WAIS.
33. **File:** Los navegadores de web también pueden navegar a través de los archivos de nuestra propia computadora, para ello es necesario ingresar en el URL el indicativo de protocolo file:/// (en este caso con tres barras "/") seguido del camino o path hacia el directorio que se desea ver.
34. **..com:** Comercial o de negocios.
35. **..org:** Organizaciones sin fines de lucro.
36. **..net:** Proveedor de conexión o redes internas.
37. **..edu:** Instituciones educativas.
38. **..gov:** Instituciones gubernamentales.
39. **..mil:** Cuerpos militares.
40. **..xx:** En donde xx representa el identificador de país o territorio, por ejemplo .mx (México).
41. **Tecnología de Información:** 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.
42. **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.
43. **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.
44. **Información:** significado que el ser humano le asigna a la data utilizando las convenciones conocidas y generalmente aceptadas.

45. **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.
46. **Computador:** dispositivo o unidad funcional que acepta data, la procesa de acuerdo con un programa guardado y genera resultados, incluidas operaciones aritméticas o lógicas.
47. **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.
48. **Firmware:** programa o segmento de programa incorporado de manera permanente en algún componente de hardware.
49. **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.
50. **Programa:** plan, rutina o secuencia de instrucciones utilizados para realizar un trabajo en particular o resolver un problema dado a través de un computador.
51. **Procesamiento de data o de información:** realización sistemática de operaciones sobre data o sobre información, tales como manejo, fusión, organización o cómputo.
52. **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.
53. **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.
54. **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.
55. **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.

56. **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.

F U E N T E S D E C O N S U L T A

1.- Obras Consultadas:

- DEL PONT K., Luis Marco y NADELSTICHER Mitrania, Abraham, Delitos de cuello blanco y reacción social, Instituto Nacional de Ciencias Penales. México. 1981.
- JIMENEZ DE ASUA, LUIS. Tratado de Derecho Penal, tomo II. Buenos Aire, Argentina. 1950.
- HANCE, Olivier. Leyes y Negocios en Internet. México. De. Mc Gram Hill Sociedad Internet. México. 1996.
- MIR PUIG, S (Comp.) Delincuencia Informática. Promociones y Publicaciones Universitarias. Barcelona, 1992.
- TELLEZ Valdes, Julio. Derecho Informático. 3a. ed. México. Ed. Mc Graw Hill 2006.
- ZAVALA, Antelmo. "El impacto social de la informática jurídica en México". Tesis. México. UNAM. 1996.
- CARRANCA Francesco; Programa del Curso de Derecho Criminal; Temis; Milano, Italia; 1955.
- CARRANCA y Trujillo Raúl, y Carrancá y Rivas Raúl;Derecho Penal parte General; Porrúa; 4ta. Edición; México, D.F.; 1956.
- CARRILLO Montoya Juan; La Legítima Defensa como excluyente de responsabilidad Criminal. Carrillo Hermanos e Impresiones, México D.F.; 1931.
- CASTELLANOS Tena Fernando; Lineamientos Elementales de Derecho Penal; Porrúa, México, D.F.; 1997.
- LÓPEZ, Betancourt Eduardo; Delitos en Particular; Ed. Porrúa 10ma Edición. México, D.F.; 2004.

- LÓPEZ, Betancourt Eduardo; Teoria del Delito; Ed. Porrúa 8a Edición. México, D.F.; 2000.
- BECCARÍA, Luis P. - Rey, Patricio E."La inserción de la Informática en la Educación y sus efectos en la reconversión laboral". Instituto de Formación Docente -SEPA-. Buenos Aires. 1999.

2.- Legislación Internacional:

- Tratado de Libre Comercio (TLC) Parte 3. Diario Oficial de la Federación. Lunes 20 de diciembre de 1993.
- Exposición de motivos del Décimo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente Viena, 10 a 17 de abril de 2000.
- Exposición de motivos de la Comisión de Justicia de la Cámara de Diputados Doc. 184/LVI/96 (I. P.O. Año III) DICT.

3.- Legislación Nacional:

- Constitución Política de los Estados Unidos Mexicanos
- Código Penal para el Estado de Aguascalientes
- Código Penal para el Estado de Baja California
- Código Penal para el Distrito Federal
- Código Penal para el Estado de México
- Código Penal para el Estado de Morelos
- Código Penal para el Estado de Puebla
- Código Penal para el Estado de Quintana Roo

- Código Penal para el Estado de Sinaloa
- Código Penal para el Estado de Tabasco
- Código Penal para el Estado de Tamaulipas
- Código Penal para el Estado de Yucatán

4.- Medios Electrónicos:

- Microsoft® Encarta: Biblioteca Premium Encarta 2007.
- Diccionario Enciclopédico Larousse 2006, Dinamarca 81, México D.F.
- IUS 2006, Actualizado a Marzo 2007

5.- Páginas Web:

- http://www.google.com
- http://es.wikipedia.org/wiki/Portada
- http://www.condusef.gob.mx/
- http://www.juridicas.unam.mx/
- http://200.38.86.53/PortalSCJN/
- http://www.scjn.gob.mx/ius2006/
- http://www.pgr.gob.mx/
- http://www.espacios.net.mx
- http://www.ba.net/aol/ayuda/cursos/15min/español/search/sld03.htm

- http://www.advance.com.ar/usuarios/gragry/recursos/buscador.htm
- http://www.escape.com.ar/busque2.asp
- http://www.generaciond.com/
- http://www.ifccfbi.com