UNIVERSIDAD DE SOTAVENTO A.C.

ESTUDIOS INCORPORADOS A LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INFORMÁTICA

"DELITOS INFORMÁTICOS EN INTERNET Y EL DESAFÍO EN LA PREVENCIÓN Y CONTROL DE LA ERA INFORMÁTICA"

TESIS PROFESIONAL

QUE PARA OBTENER EL TÍTULO DE:

LICENCIADO EN INFORMÁTICA

PRESENTA:

JORGE LUIS OSORIO SANTOS

ASESOR DE TESIS:
LIC. EMILIO DE JESÚS ESPRONCEDA GONZÁLEZ

Coatzacoalcos, Veracruz **2012.**

Dedicatoria

Esta Tesis está dedicada con mucho cariño a mi familia por hacer sido motivación y apoyo para lograr una meta constructiva en mi vida. Dedicada a mi madre que lucho por darme lo mejor, que cuido de mí cuando enfermaba, que se esforzó al máximo por que llegara yo a este momento.

A quien me enseño que era un error el no saber, pero un doble error el no aceptarlo y siempre tuvo la paciencia para aconsejarme y mostrarme cual era el camino correcto, mi ejemplo a seguir Rafael Córdova.

A mi abuelita que siempre a estado conmigo y se convirtió en mi segunda mama gracias a sus cariños, sus preocupaciones, a su gran fortaleza. A mis primos, tíos, tías que me acompañaron en algunos momentos de mi camino.

Le agradezco con mucho cariño a todas las personas que intervinieron directa e indirectamente en el desarrollo, aceptación y presentación de mi tesis.

Le agradezco a Dios por darme la oportunidad de vivir y de regalarme una familia maravillosa la razón para pensar y la inteligencia para aprender y así haber logrado este sueño.

Y a mis profesores y asesores de mi tesis por confiar en mí, por tenerme la paciencia necesaria, por apoyarme en momentos difíciles. Agradezco el haber tenido unos profesores tan buenas personas como lo son ustedes. Nunca los olvidare.

Y no me puedo ir sin antes decirles, que sin ustedes a mi lado no lo hubiera logrado, se que hay mucho camino por recorrer, me falta mucho que aprender y si de algo estoy seguro es que paso a paso llegare a la meta, triunfar.

Índice

Problema

La principal preocupación de las empresas es que su información pueda llegar a manos equivocadas e inadecuadas, especialmente en países con problemas de corrupción, es por eso que surge la problemática de este tan importante y complicado tema, a veces los gobierno obtienen la clave para descifrar los mensajes en código, esto significa que personas no autorizadas que no son del gobierno pueden obtenerlas y utilizarlas.

Pero como detener a los delincuentes mediante internet, es por eso aquí se menciona toda la información de este complejo tema y las maneras en que se pueden detectar los usuarios que usan, manipulan y dañan a las compañías con su principal herramienta que es la información, y las maneras que se podrán utilizar para acabar con esta problemas que es el uso indebido de la información de las empresas.

Hipótesis

La determinación de los delitos informáticos maneja mucho la responsabilidad que representa determinar si la conducta es típica, antijurídica y culpable, dentro de un sistema informático.

Es decir que aquella persona que entre a un sistema de manera indebida, cuando este sistema este protegido como medida de seguridad o se mantenga contra la voluntad de quien tiene derecho a excluirlo incurrirá en un delito y tendrá que pagar con una multa, ante este delito.

Si se logra determinar que un sistema ha sido violado y este tenia un clave de privacidad para personas solo autorizadas se determina como hurto calificado, es decir que si se logra determinar que surgió violencia sobre el equipo.

El objetivo primordial es ofrecer una garantía de seguridad, y los sistemas información deben resguardarse, y si alguien entra a ellos sin ninguna autorización, el usuario o empresa puede reclamar una indemnización por daños y perjuicios.

Objetivo General

- Realizar una investigación profunda acerca del fenómeno de los Delitos Informáticos, analizando el impacto de éstos en la función de Auditoria Informática en cualquier tipo de organización.

Objetivo Específico

- Conceptualizar la naturaleza de los Delitos Informáticos.
- Estudiar las características de este tipo de Delitos.
- Tipificar los Delitos de acuerdo a sus características principales.
- Investigar el impacto de éstos actos en la vida social y tecnológica de la sociedad.
- Analizar las consideraciones oportunas en el tratamiento de los Delitos Informáticos.
- Mencionar las empresas que operan con mayor riesgo de ser víctimas de ésta clase de actos.
- Analizar la Legislatura que enmarca a ésta clase de Delitos, desde un contexto Nacional e Internacional.
- Definir el rol del auditor ante los Delitos Informáticos.
- Presentar los indicadores estadísticos referentes a éstos actos delictivos.

Justificación

La problemática y básicamente la decisión de llevar a cabo este tan relevante tema sobre los delitos informáticos, es la protección, resguardo y privacidad de la información ya se personal o de carácter profesional, es decir a nadie le gusta que sus derechos a la privacidad estén a la deriva, por lo tanto se da a conocer las medidas, los requerimientos y la solución que se puedan tener al respecto sobre la información.

Es por el bien estar de las empresas mas que nada, contar con privacidad en la utilización de manejo de sistemas básicamente manejados por personas autorización y mediante control y capacitación de los mismos, y que esta no llegue a ser manipula de manera incorrecta y derivado de la utilización de esta tan grande información que pueda caer en manos equivocadas es por esto que se debe delimitar, analizar y recurrir a sistemas más complejos para tener mayor control de los mismos, y solo se pueda acceder a ellos personas calificadas, mediante códigos, claves u otros factores.

Introducción

La tecnología digital con información proveniente desde los puntos más lejanos del mundo, o tener el acceso a nuestras cuentas corrientes, o simplemente encontrarnos leyendo las noticias nacionales e internacionales, sin necesidad de recurrir al diario de papel o estar en contacto con nuestros familiares en todo momento, ubicación y situación posible. Todos estos alcances en la comunicación se han ido posicionando en nuestras vidas, lo que para nosotros es nuevo y novedoso, futuras generaciones recordaran estos tiempos como el comienzo de una nueva era, “la era digital y de la globalización de las comunicaciones”.

El desarrollo de toda esta infraestructura en las comunicaciones, informaciones y negocios, que cada día más vemos compenetrados en las actividades políticas, culturales y comerciales, han mostrado un amplio crecimiento y desarrollo de todas las áreas del quehacer nacional, fenómeno mundial que ha ocasionando que el área dedicada a la informática y la computación ganan cada día más un espacio. Las tecnologías de la sociedad de la información pueden utilizarse, y se utilizan, para perpetrar y facilitar diversas actividades delictivas.

En manos de personas que actúan de mala fe, con mala voluntad, o con negligencia grave, estas tecnologías pueden convertirse en instrumentos para actividades que ponen en peligro o atentan contra la vida, la propiedad o la dignidad de los individuos o del interés público. Estas nuevas herramientas son usadas por personas, que por naturaleza humana nos hace enfrentar situaciones que se alejan de un claro comportamiento de convivencia en sociedad, en que con sus acciones utilizan para sí y en desmedro de otras nuevas técnicas de criminalidad para el cometido de sus acciones perturbadoras.

Estas acciones perturbadoras de la convivencia social han nacido al amparo de las nuevas herramientas tecnológicas, ante lo cual en el ámbito mundial, se ha generado una percepción de la seguridad informática, percepción que se ha ido

desarrollando muy por detrás de la realidad de los alcances de los llamados ciberdelitos, pero que ha generado acciones claras y evidentes de una necesidad de control por parte de los organismos de control social formal; es por ello que las experiencias desarrolladas por la Organización de las Naciones Unidas, la Comunidad Europea, los Estados Unidos de Norteamérica, se han dirigido hacia la creación de los organismos necesarios para plantear que el problema del cibercrimen y sus consecuencias en la seguridad de las personas y en sus respectivas economías es un hecho grave y que requiere de urgentes medidas de todo tipo, tanto en el ámbito legislativo, de tecnologías y de socialización.

Esta situación de vulnerabilidad a que nos vemos enfrentados en el área de la protección legal de los derechos de las personas naturales o jurídica, no ha detenido el avance de otros medios, provenientes de la misma área tecnológica, para los resguardos de nuestros bienes jurídicos, tales como la privacidad, bienestar, derechos de autor y tantos otros; como son la aparición en el ámbito privado de servicios que mediante el uso de nuevas tecnologías o metodologías permiten un ambiente de tranquilidad relativa, especialmente en el desarrollo del comercio electrónico.

Capítulo I Generalidades de los Delitos Informáticos

Capítulo I Generalidades de los Delitos Informáticos

1.1. Generalidades

Fraude puede ser definido como engaño, acción contraria a la verdad o a la rectitud. La definición de Delito puede ser más compleja.

Los elementos integrantes del delito son:

- ✓ El delito es un acto humano, es una acción (acción u omisión).
- ✓ Dicho acto humano ha de ser antijurídico, debe lesionar o poner en peligro un interés jurídicamente protegido.
- ✓ Debe corresponder a un tipo legal, definido por La Ley, ha de ser un acto típico.
- ✓ El acto ha de ser culpable, imputable a dolo (intención) o a culpa (negligencia), y una acción es imputable cuando puede ponerse a cargo de una determinada persona
- ✓ La ejecución u omisión del acto debe estar sancionada por una pena.
- ✓ Por tanto, un delito es: una acción antijurídica realizada por un ser humano, tipificado, culpable y sancionado por una pena.

Se podría definir el delito informático como toda acción (acción u omisión) culpable realizada por un ser humano, que cause un perjuicio a personas sin que necesariamente se beneficie el autor o que, por el contrario, produzca un beneficio ilícito a su autor aunque no perjudique de forma directa o indirecta a la víctima, tipificado por La Ley, que se realiza en el entorno informático y está sancionado con una pena.

De esta manera, el autor mexicano Julio TELLEZ VALDEZ señala que los delitos informáticos son "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y

culpables en que se tienen a las computadoras como instrumento o fin (concepto típico)".

1.2. Consideración del Delito Informático

En la actualidad las computadoras se utilizan no solo como herramientas auxiliares de apoyo a diferentes actividades humanas, sino como medio eficaz para obtener y conseguir información, lo que las ubica también como un nuevo medio de comunicación, y condiciona su desarrollo de la informática; tecnología cuya esencia se resume en la creación, procesamiento, almacenamiento y transmisión de datos.

La informática esta hoy presente en casi todos los campos de la vida moderna.

Con mayor o menor rapidez todas las ramas del saber humano se rinden ante los progresos tecnológicos, y comienzan a utilizar los sistemas de Información para ejecutar tareas que en otros tiempos realizaban manualmente.

El progreso cada día más importante y sostenido de los sistemas computacionales permite hoy procesar y poner a disposición de la sociedad una cantidad creciente de información de toda naturaleza, al alcance concreto de millones de interesados y de usuarios.

Las más diversas esferas del conocimiento humano, en lo científico, en lo técnico, en lo profesional y en lo personal están siendo incorporadas a sistemas informáticos que, en la práctica cotidiana, de hecho sin limitaciones, entrega con facilidad a quien lo desee un conjunto de datos que hasta hace unos años sólo podían ubicarse luego de largas búsquedas y selecciones en que el hombre jugaba un papel determinante y las máquinas existentes tenían el rango de equipos auxiliares para imprimir los resultados.

En la actualidad, en cambio, ese enorme caudal de conocimiento puede obtenerse, además, en segundos o minutos, transmitirse incluso documentalmente y llegar al receptor mediante sistemas sencillos de operar,

confiables y capaces de responder casi toda la gama de interrogantes que se planteen a los archivos informáticos.

Puede sostenerse que hoy las perspectivas de la informática no tienen límites previsibles y que aumentan en forma que aún puede impresionar a muchos actores del proceso.

Este es el panorama de este nuevo fenómeno científico tecnológico en las sociedades modernas. Por ello ha llegado a sostenerse que la Informática es hoy una forma de Poder Social.

Las facultades que el fenómeno pone a disposición de Gobiernos y de particulares, con rapidez y ahorro consiguiente de tiempo y energía, configuran un cuadro de realidades de aplicación y de posibilidades de juegos lícito e ilícito, en donde es necesario el derecho para regular los múltiples efectos de una situación, nueva y de tantas potencialidades en el medio social.

Los progresos mundiales de las computadoras, el creciente aumento de las capacidades de almacenamiento y procesamiento, la miniaturización de los chips de las computadoras instalados en productos industriales, la fusión del proceso de la información con las nuevas tecnologías de comunicación, así como la investigación en el campo de la inteligencia artificial, ejemplifican el desarrollo actual definido a menudo como la "era de la información".

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

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

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

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

El espectacular desarrollo de la tecnología informática ha abierto las puertas a nuevas posibilidades de delincuencia antes impensables. La manipulación fraudulenta de los ordenadores con ánimo de lucro, la destrucción de programas o datos y el acceso y la utilización indebida de la información que puede afectar la esfera de la privacidad, son algunos de los procedimientos relacionados con el procesamiento electrónico de datos mediante los cuales es posible obtener grandes beneficios económicos o causar importantes daños materiales o morales. Pero no sólo la cuantía de los perjuicios así ocasionados es a menudo infinitamente superior a la que es usual en la delincuencia tradicional, sino que también son mucho más elevadas las posibilidades de que no lleguen a descubrirse. Se trata de una delincuencia de especialistas capaces muchas veces de borrar toda huella de los hechos.
En este sentido, la informática puede ser el objeto del ataque o el medio para cometer otros delitos. La informática reúne unas características que la convierten en un medio idóneo para la comisión de muy distintas modalidades delictivas, en especial de carácter patrimonial (estafas, apropiaciones indebidas, etc.). La idoneidad proviene, básicamente, de la gran cantidad de datos que se acumulan, con la consiguiente facilidad de acceso a ellos y la relativamente fácil manipulación de esos datos.

La importancia reciente de los sistemas de datos, por su gran incidencia en la marcha de las empresas, tanto públicas como privadas, los ha transformado en

un objeto cuyo ataque provoca un perjuicio enorme, que va mucho más allá del valor material de los objetos destruidos. A ello se une que estos ataques son relativamente fáciles de realizar, con resultados altamente satisfactorios y al mismo tiempo procuran a los autores una probabilidad bastante alta de alcanzar los objetivos sin ser descubiertos.

1.3. Características de los Delitos Informático

Según el mexicano Julio Tellez Valdez, los delitos informáticos presentan las siguientes características principales:

- Son conductas criminales de cuello blanco (white collar crime), en tanto que sólo un determinado número de personas con ciertos conocimientos (en este caso técnicos) puede llegar a cometerlas.
- Son acciones ocupacionales, en cuanto a que muchas veces se realizan cuando el sujeto se halla trabajando.
- Son acciones de oportunidad, ya que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.
- Provocan serias pérdidas económicas, ya que casi siempre producen "beneficios" de más de cinco cifras a aquellos que las realizan.
- Ofrecen posibilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse.
- Son muchos los casos y pocas las denuncias, y todo ello debido a la misma falta de regulación por parte del Derecho.
- Son muy sofisticados y relativamente frecuentes en el ámbito militar.
- Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.
- Tienden a proliferar cada vez más, por lo que requieren una urgente regulación. Por el momento siguen siendo ilícitos impunes de manera manifiesta ante la ley.
- Sistemas y empresas con mayor riesgo.

- Evidentemente el artículo que resulta más atractivo robar es el dinero o algo de valor. Por lo tanto, los sistemas que pueden estar más expuestos a fraude son los que tratan pagos, como los de nómina, ventas, o compras. En ellos es donde es más fácil convertir transacciones fraudulentas en dinero y sacarlo de la empresa.
- Por razones similares, las empresas constructoras, bancos y compañías de seguros, están más expuestas a fraudes que las demás.

Los sistemas mecanizados son susceptibles de pérdidas o fraudes debido a que:

Tratan grandes volúmenes de datos e interviene poco personal, lo que impide verificar todas las partidas.

Se sobrecargan los registros magnéticos, perdiéndose la evidencia auditable o la secuencia de acontecimientos.

A veces los registros magnéticos son transitorios y a menos que se realicen pruebas dentro de un período de tiempo corto, podrían perderse los detalles de lo que sucedió, quedando sólo los efectos.

Los sistemas son impersonales, aparecen en un formato ilegible y están controlados parcialmente por personas cuya principal preocupación son los aspectos técnicos del equipo y del sistema y que no comprenden, o no les afecta, el significado de los datos que manipulan.

En el diseño de un sistema importante es difícil asegurar que se han previsto todas las situaciones posibles y es probable que en las previsiones que se hayan hecho queden huecos sin cubrir.
Los sistemas tienden a ser algo rígidos y no siempre se diseñan o modifican al ritmo con que se producen los acontecimientos; esto puede llegar a ser otra fuente de "agujeros".

Sólo parte del personal de proceso de datos conoce todas las implicaciones del sistema y el centro de cálculo puede llegar a ser un centro de información. Al mismo tiempo, el centro de cálculo procesará muchos aspectos similares de las transacciones.

En el centro de cálculo hay un personal muy inteligente, que trabaja por iniciativa propia la mayoría del tiempo y podría resultar difícil implantar unos niveles normales de control y supervisión.

El error y el fraude son difíciles de equiparar. A menudo, los errores no son iguales al fraude. Cuando surgen discrepancias, no se imagina que se ha producido un fraude, y la investigación puede abandonarse antes de llegar a esa conclusión. Se tiende a empezar buscando errores de programación y del sistema. Si falla esta operación, se buscan fallos técnicos y operativos. Sólo cuando todas estas averiguaciones han dado resultados negativos, acaba pensándose en que la causa podría ser un fraude.

1.4. Delitos en perspectiva

Los delitos pueden ser examinados desde dos puntos de vista diferentes:

- Los delitos que causan mayor impacto a las organizaciones.
- Los delitos más difíciles de detectar.

Aunque depende en gran medida del tipo de organización, se puede mencionar que los Fraudes y sabotajes son los delitos de mayor incidencia en las organizaciones. Además, aquellos que no están claramente definidos y publicados dentro de la organización como un delito (piratería, mala utilización de la información, omisión deliberada de controles, uso no autorizado de activos y/o servicios computacionales; y que en algún momento pueden generar un impacto a largo plazo).

Pero si se examina la otra perspectiva, referente a los delitos de difícil detección, se deben situar a aquellos producidos por las personas que trabajan internamente en una organización y que conocen perfectamente la configuración interna de las plataformas; especialmente cuando existe una cooperación entre empleados, cooperación entre empleados y terceros, o incluso el involucramiento de la administración misma.

1.5. Tipificación de los Delitos Informáticos

1.5.1. Clasificación según la Actividad Informática

Sabotaje Informático

El término sabotaje informático comprende todas aquellas conductas dirigidas a causar daños en el hardware o en el software de un sistema. Los métodos utilizados para causar destrozos en los sistemas informáticos son de índole muy variada y han ido evolucionando hacia técnicas cada vez más sofisticadas y de difícil detección. Básicamente, se puede diferenciar dos grupos de casos: por un lado, las conductas dirigidas a causar destrozos físicos y, por el otro, los métodos dirigidos a causar daños lógicos.

Conductas dirigidas a causar daños físicos

El primer grupo comprende todo tipo de conductas destinadas a la destrucción «física» del hardware y el software de un sistema (por ejemplo: causar incendios o explosiones, introducir piezas de aluminio dentro de la computadora para producir cortocircuitos, echar café o agentes cáusticos en los equipos, etc. En general, estas conductas pueden ser analizadas, desde el punto de vista jurídico, en forma similar a los comportamientos análogos de destrucción física de otra clase de objetos previstos típicamente en el delito de daño.

Conductas dirigidas a causar daños lógicos

El segundo grupo, más específicamente relacionado con la técnica informática, se refiere a las conductas que causan destrozos «lógicos», o sea, todas aquellas conductas que producen, como resultado, la destrucción, ocultación, o alteración de datos contenidos en un sistema informático.

Este tipo de daño a un sistema se puede alcanzar de diversas formas. Desde la más simple que podemos imaginar, como desenchufar el ordenador de la electricidad mientras se esta trabajando con él o el borrado de documentos o datos de un archivo, hasta la utilización de los más complejos programas lógicos destructivos (crash programs), sumamente riesgosos para los sistemas, por su posibilidad de destruir gran cantidad de datos en un tiempo mínimo.

Estos programas destructivos, utilizan distintas técnicas de sabotaje, muchas veces, en forma combinada. Sin pretender realizar una clasificación rigurosa de estos métodos de destrucción lógica, podemos distinguir:

La jurisprudencia francesa registra un ejemplo de este tipo de casos. Un empleado programó el sistema de tal forma que los ficheros de la empresa se destruirían automáticamente si su nombre era borrado de la lista de empleados de la empresa.

Bombas lógicas (time bombs): En esta modalidad, la actividad destructiva del programa comienza tras un plazo, sea por el mero transcurso del tiempo (por ejemplo a los dos meses o en una fecha o a una hora determinada), o por la aparición de determinada señal (que puede aparecer o puede no aparecer), como la presencia de un dato, de un código, o cualquier mandato que, de acuerdo a lo determinado por el programador, es identificado por el programa como la señal para empezar a actuar.

Otra modalidad que actúa sobre los programas de aplicación es el llamado «cáncer de rutinas» («cancer routine»). En esta técnica los programas destructivos tienen la particularidad de que se reproducen, por sí mismos, en otros programas, arbitrariamente escogidos.

Una variante perfeccionada de la anterior modalidad es el «virus informático» que es un programa capaz de multiplicarse por sí mismo y contaminar los otros programas que se hallan en el mismo disco rígido donde fue instalado y en los datos y programas contenidos en los distintos discos con los que toma contacto a través de una conexión.

Fraude a través de computadoras

Estas conductas consisten en la manipulación ilícita, a través de la creación de datos falsos o la alteración de datos o procesos contenidos en sistemas informáticos, realizada con el objeto de obtener ganancias indebidas.

Los distintos métodos para realizar estas conductas se deducen, fácilmente, de la forma de trabajo de un sistema informático: en primer lugar, es posible alterar datos, omitir ingresar datos verdaderos o introducir datos falsos, en un ordenador.

El autor, empleado de una importante empresa, ingresó al sistema informático un programa que le permitió incluir en los archivos de pagos de salarios de la compañía a «personas ficticias» e imputar los pagos correspondientes a sus sueldos a una cuenta personal del autor.

Esta maniobra hubiera sido descubierta fácilmente por los mecanismos de seguridad del banco (listas de control, sumarios de cuentas, etc.) que eran revisados y evaluados periódicamente por la compañía. Por este motivo, para evitar ser descubierto, el autor produjo cambios en el programa de pago de salarios para que los «empleados ficticios» y los pagos realizados, no aparecieran en los listados de control.

Por último, es posible falsear el resultado, inicialmente correcto, obtenido por un ordenador: a esta modalidad se la conoce como manipulación del output.

Una característica general de este tipo de fraudes, interesante para el análisis jurídico, es que, en la mayoría de los casos detectados, la conducta delictiva es

repetida varias veces en el tiempo. Lo que sucede es que, una vez que el autor descubre o genera una laguna o falla en el sistema, tiene la posibilidad de repetir, cuantas veces quiera, la comisión del hecho. Incluso, en los casos de "manipulación del programa", la reiteración puede ser automática, realizada por el mismo sistema sin ninguna participación del autor y cada vez que el programa se active.

En el ejemplo jurisprudencial citado al hacer referencia a las manipulaciones en el programa, el autor podría irse de vacaciones, ser despedido de la empresa o incluso morir y el sistema seguiría imputando el pago de sueldos a los empleados ficticios en su cuenta personal.

Una problemática especial plantea la posibilidad de realizar estas conductas a través de los sistemas de teleproceso. Si el sistema informático está conectado a una red de comunicación entre ordenadores, a través de las líneas telefónicas o de cualquiera de los medios de comunicación remota de amplio desarrollo en los últimos años, el autor podría realizar estas conductas sin ni siquiera tener que ingresar a las oficinas donde funciona el sistema, incluso desde su propia casa y con una computadora personal. Aún más, los sistemas de comunicación internacional, permiten que una conducta de este tipo sea realizada en un país y tenga efectos en otro.

Respecto a los objetos sobre los que recae la acción del fraude informático, estos son, generalmente, los datos informáticos relativos a activos o valores. En la mayoría de los casos estos datos representan valores intangibles (ej.: depósitos monetarios, créditos, etc.), en otros casos, los datos que son objeto del fraude, representan objetos corporales (mercadería, dinero en efectivo, etc.) que obtiene el autor mediante la manipulación del sistema. En las manipulaciones referidas a datos que representan objetos corporales, las pérdidas para la víctima son, generalmente, menores ya que están limitadas por la cantidad de objetos disponibles. En cambio, en la manipulación de datos referida a bienes intangibles, el monto del perjuicio no se limita a la cantidad existente sino que, por el contrario, puede ser «creado» por el autor.

Copia ilegal de software y espionaje informático

Se engloban las conductas dirigidas a obtener datos, en forma ilegítima, de un sistema de información. Es común el apoderamiento de datos de investigaciones, listas de clientes, balances, etc. En muchos casos el objeto del apoderamiento es el mismo programa de computación (software) que suele tener un importante valor económico.

Infracción de los derechos de autor: La interpretación de los conceptos de copia, distribución, cesión y comunicación pública de los programas de ordenador utilizando la red provoca diferencias de criterio a nivel jurisprudencial.

Infracción del Copyright de bases de datos: No existe una protección uniforme de las bases de datos en los países que tienen acceso a Internet. El sistema de protección más habitual es el contractual: el propietario del sistema permite que los usuarios hagan "downloads" de los ficheros contenidos en el sistema, pero prohíbe el replicado de la base de datos o la copia masiva de información.

Uso ilegítimo de sistemas informáticos ajenos

Esta modalidad consiste en la utilización sin autorización de los ordenadores y los programas de un sistema informático ajeno. Este tipo de conductas es comúnmente cometida por empleados de los sistemas de procesamiento de datos que utilizan los sistemas de las empresas para fines privados y actividades complementarias a su trabajo. En estos supuestos, sólo se produce un perjuicio económico importante para las empresas en los casos de abuso en el ámbito del teleproceso o en los casos en que las empresas deben pagar alquiler por el tiempo de uso del sistema.

Acceso no autorizado: La corriente reguladora sostiene que el uso ilegítimo de passwords y la entrada en un sistema informático sin la autorización del propietario debe quedar tipificado como un delito, puesto que el bien jurídico

que acostumbra a protegerse con la contraseña es lo suficientemente importante para que el daño producido sea grave.

1.6. Delitos informáticos contra la privacidad

Grupo de conductas que de alguna manera pueden afectar la esfera de privacidad del ciudadano mediante la acumulación, archivo y divulgación indebida de datos contenidos en sistemas informáticos.

Esta tipificación se refiere a quién, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o cualquier otro tipo de archivo o registro público o privado.

Existen circunstancias agravantes de la divulgación de ficheros, los cuales se dan en función de:

El carácter de los datos: ideología, religión, creencias, salud, origen racial y vida sexual.

Las circunstancias de la víctima: menor de edad o incapaz.
También se comprende la interceptación de las comunicaciones, la utilización de artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen o de cualquier otra señal de comunicación, se piensa que entre lo anterior se encuentra el pinchado de redes informáticas.

Interceptación de e-mail: En este caso se propone una ampliación de los preceptos que castigan la violación de correspondencia, y la interceptación de telecomunicaciones, de forma que la lectura de un mensaje electrónico ajeno revista la misma gravedad.

Capítulo II Delitos Informáticos

Capítulo II Delitos Informáticos

2.1. Concepto de Fraude y Delitos

Fraude puede ser definido como engaño, acción contraria a la verdad o a la rectitud. La definición de delito es más compleja y han sido muchos los intentos de formular una noción de delito que sirviese para todos los tiempos y en todos los países. Esto no ha sido posible, dada la íntima conexión que existe entre la vida social y jurídica de cada sociedad y cada siglo, ya que ambas se condicionan íntimamente.

artículo 231 del distrito federal dispone: “Se impondrán las penas previstas en el artículo anterior, a quien: ... XIV. Para obtener algún beneficio para sí o para un tercero, por cualquier medio accese, entre o se introduzca a los sistemas o programas de informática del sistema financiero e indebidamente realice operaciones, transferencias o movimientos de dinero o valores, independientemente de que los recursos no salgan de la Institución...

En el articulo 11° del Código Penal dice que **“Son delitos y faltas las acciones u omisiones dolorosas o culposas penadas por la ley”.(checar articulo)**

Esta noción de delito es especialmente formal, y no define cuales sean sus elementos integrantes. En cualquier caso, sus elementos integrantes son:

- El delito es un acto humano, es una acción (acción u omisión).
- Dicho acto humano ha de ser antijurídico, ha de estar en oposición con una norma jurídica, debe lesionar u oponer en peligro un interés jurídicamente protegido.
- Debe corresponder a un tipo legal (figura de delito), definido por la ley, ha de ser un acto típico.

- El acto ha de ser culpable, imputable o dolo (intención) o a culpa (negligencia), y un acción es imputable cuando puede ponerse a cargo de una determinada personal.
- La ejecución u omisión del acto debe estar sancionado con una pena.

Los hechos ilícitos que pueden afectar a las organizaciones, se pueden agrupar de la siguiente manera:

- Robo bajo sus distintas modalidades.
- Daño en propiedad ajena.
- Terrorismo.
- Privación ilegal de la libertad.
- El abuso de confianza.
- El fraude.
- La violación de correspondencia.
- La falsificación de documentos.
- La relevación de secretos.

Con la utilización de las computadoras, ha aparecido una nueva tipificación del accionar ilícito, los delitos informáticos.

2.2. Definición de Delito Informático

El delito informático implica actividades criminales que un primer momento los países han tratado de encuadras en figuras típicas de carácter tradicional, tales como robo, hurto, 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.

En la actualidad no existe una definición en la cual los juristas y estudiosos del derecho estén de acuerdo, es decir no existe un concepto propio de los llamadas delitos informaticos. Aun cuando no existe dicha definición con

carácter universal, se han formulado conceptos funcionales atendiendo a las realidades concretas de cada país.

“Delito Informático es toda aquella conducta ilícita que hace uso indebido de cualquier medio Informático, susceptible de ser sancionada por el derecho penal”.

“Cualquier comportamiento criminógeno en el cual la computadora ha estado involucrada como material o como objeto de la acción criminógena, o como mero símbolo”.

“Aquel que se da con la ayuda de la informática o de las técnicas anexas”.

“La realización de una acción que, reuniendo las características que delimitan el concepto de delito, se ha llevado a cabo utilizando un elemento informático o telemático contra los derechos y libertades de los ciudadanos definidos en la Constitución”.

“En sentido amplio, es cualquier conducta criminogenea o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en sentido estricto, el delito informático, es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea con método, medio o fin”.

“Son las conductas típicas antijurídicas y culpables en que se tiene a las computadoras como instrumento o fin”

“Son actitudes ilícitas en que se tiene a las computadoras como instrumento o fin”.

“Todas aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio informáticos”.

“Son todas aquellas conductas ilícitas susceptibles de ser sancionadas por el Derecho penal y que su realización se valen de las computadoras como medio o fin para su comisión”.

“Aquel que esta íntimamente ligado a la informática o a los bienes jurídicos que históricamente se han relacionado con las tecnologías de la información: datos, programas, documentos electrónicos, dinero electrónico, información, etc.”

“Conjunto de comportamientos dignos de reproche penal que tienen por instrumento o por objeto a los sistemas o elementos de técnica informática, o que están en relación significativa con esta, pudiendo presentar múltiples formas de lesión de variados bienes jurídicos”.

“La realización de una acción que, reuniendo las características, que delimitan el concepto de delito, sea llevado a cabo utilizando un elemento informático, y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software”.
“Todos los actos antijurídicos según la ley penal vigente realizados con el empleo de un equipo automático de procesamiento de datos”.

“Cual acto ilegal en relación con el cual el conocimiento de la tecnología informática es esencial para su realización, investigación y persecución”.

“Delito informático, más que una forma especifica de delito, supone una pluralidad de modalidades delictivas vinculadas, de algún modo con las computadoras”.

“Es todo comportamiento ilegal o contrario a la ética o no autorizado que concierne a un tratamiento automático de datos y/o transmisión de datos”.

Algunos lo consideran inscribible en la criminalidad “de cuello blanco”, la delincuencia de cuello blanco es la violación de la ley penal por una persona de alto nivel socio-económico en el desarrollo de su actividad profesional.

“Es cualquier acto ilegal ejecutando con dolo para el que es esencial el conocimiento y uso, propio o ajeno, de la tecnología informática para su comisión, investigación o persecución con la finalidad de beneficiarse con ello.

Una clasificación de los distintos tipos de delincuentes informaticos es la siguiente:

- **Hacker:** Es quien intercepta dolosamente un sistema informático para dañar, apropiarse, interferir, desviar, difundir, y/o destruir información que se concentra almacenada en computadoras perteneciente a entidades publicas o privadas. El termino de hacker en castellano significa “cortador”. Los “Hackers”, son fanáticos de la informática, generalmente jóvenes, que tan solo con un computador personal, un modem, gran paciencia e imaginación son capaces de acceder, a través de una red publica de transmisión de datos, al sistema informatizado de una empresa o entidad púbica, saltándose todas las medidas de seguridad, y leer información, copiarla, modificarla, preparando las condiciones idóneas para llamar la atención sobre la vulnerabilidad de los sistemas informaticos, o satisfacer su propia vanidad.

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

- **Phreaker:** Persona que ingresa al sistema telefónico, teniendo o no equipo de computación, con el propósito de apoderarse, interferir, dañar, destruir, conocer, difundir, hacer actos de sabotaje, o hacer uso de la información accediendo al sistema telefónico, provocando las

adulteraciones que, en forma directa, conlleva este accionar con su consecuente perjuicio económico.

Son tipos con unos conocimientos de telefónica insuperables. Conocen a fondo los sistemas telefónicos incluso más que los propios técnicos de las compañías telefónicas.

Estos tipos han sabido crear todo tipo de cajas de colores con una función determinada. Actualmente se preocupan más de las cajas de prepago, que de las cajas, ya que suelen operar desde cabinas telefónicas o móviles. Un sistema de retos, es capaz de captar los números de abonado en el aire.

De esta forma es posibles crear clones de tarjetas telefónicas a distancia.

Son lo más famosos en los medios de comunicación por los desastres que han hecho a través de los años.

Hace algún tiempo el hacer phreaking fue una actividad semi respetable dentro de la comunicación hacker; había un acuerdo de caballeros donde el hacer phreaking era bien visto como juego intelectual y como una forma de exploración, pero el robo de servicios era tabú.

La modernización de las redes hizo necesario que los phreakers utilizaran técnicas menos éticas, como robar números de calling cards, los obtenían colocándose cerca de algún teléfono público y memorizando el número de tarjeta que marcaba un usuario descuidado.

Una vez obtenido el número y la claves, la información era esparcida de tal manera que en un caso se llevaron a realizar 600 llamadas internacionales en dos minutos antes de que los operadores de seguridad del sistema la cancelaran.

Otra alternativa en la búsqueda de información de los Phone Phreakers es hacer trashing que consiste en escavar en la basura de los edificios de las compañías telefónicas en busca de lista desechadas de claves de acceso.

Con sus habilidades pueden llegar a crear un pequeño aparato que simula el sonido de una moneda cuando entra en el teléfono público, escucha conversaciones privadas y crear cuentas telefónicas ficticias.

- **Virucker:** Esta palabra proviene de la unión de los términos Virus y Hacker, y se refiere al creador de un programa el cual insertado en forma dolorosa en un sistema de cómputo destruya, altere, dañe o inutilice a un sistema de información perteneciente a organizaciones con o sin fines de lucro y de diversa índole.

- **Pirata Informático:** Es aquella persona que copia, reproduce, vende, entrega un programa de software que no le pertenece o que no tiene licencia de uso, a pesar de que el programa esta correctamente registrado como propiedad intelectual en su país de origen o en otro país, esta persona adultera su estructura, su procedimiento de instalación, copiándolo directamente y reproduciendo por cualquier medio de documentación que acompaña al mismo programa.

Los sistemas que pueden estar más expuestos a fraude son lo que tratan pagos, como los de planilla, ventas o compras. En ellos es donde es más fácil convertir transacciones fraudulentas en dinero y sacarlo de la empresa.

Por razones similares, las empresas constructoras, bancos y compañías de seguros, están más expuestas a fraudes que los demás.

Los delitos pueden ser examinado desde dos puntos de vista diferentes:

- Los delitos que causan mayor impacto a las organizaciones.
- Los delitos más difíciles de detectar.

Aunque depende en gran medida del tipo de organización, se puede mencionar que los Fraudes y sabotajes son los delitos de mayor incidencia en las organizaciones. Además, aquellos que no están claramente definidos y publicados dentro de la organización como un delito (piratería, mala utilización de la información, omisión deliberada de controles, uso no autorizado de activos y/o servicios computacionales; y que en algún momento pueden generar un impacto a largo plazo).

Pero si se examina la otra perspectiva, referente a los delitos de difícil detección, se deben situar a aquellos producidos por las personas que trabajan internamente en una organización y que conocen perfectamente la configuración interna de las plataformas; especialmente cuando existe una cooperación entre empleados y terceros, o incluso el involucramiento de la administración misma.

2.3. Terminología sobre Delitos

Existen diferentes términos para definir este tipo de delitos entre los que podemos destacar:

“delitos electrónicos”, “delitos relacionados con la computadora”, “crímenes por computadora”, “delincuencia relacionada por la computadora”, “delincuencia informática”, “criminalidad informática”, “abuso informático”, “computer crime”, “Computerkriminalitat”.

2.4. Clasificación de los Delitos Informaticos

Una Clasificación de los delitos informaticos es en base a dos criterios, como instrumento o medio, o como fin u objetivo es la siguiente:

1) **Como instrumento o medio.** En esta categoría se tiene a las conductas criminales que se valen de las computadoras como método (utilizando métodos electrónicos para llegar a un resultado ilícito), medio o símbolo

(utilizan una computadora como medio o símbolo) en la comisión del ilícito, por ejemplo:

a) Falsificación de documentos vía computarizada (tarjetas de crédito, cheques, etc.).
b) Variación de los activos y pasivos en la situación contable de las empresas.
c) Planeación o simulación de delitos convencionales (robo, homicidio, fraude, etc.).
d) “Robo” de tiempo de computadora.
e) Lectura, sustracción o copiado de información confidencial
f) Modificación de datos tanto en la entrada como en la salida.
g) Aprovechamiento indebido o violación de un código para penetrar a un sistema introduciendo instrucciones inapropiadas (esto se le conoce en el medio como el método del “Caballo de Troya”).
h) Vacilación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa, método conocido como la “técnica de salami”.
i) Uso no autorizado de programas de cómputo.
j) Introducción de instrucciones que “interrupciones” en la lógica interna de los programas, a fin de obtener beneficios, tales como consulta a su distribuidor.
k) Alteración en el funcionamiento de los sistemas, a través de los cada vez más temibles virus informáticos.

2) **Como fin u objetivo.** En esta categoría se enmarcan las conductas criminales que van dirigidas en contra de la computadora, accesorios o programas como entidad física. Algunos ejemplos son los siguientes:

1. Manipulación en los datos e informaciones contenidos en los archivos o soportes físicos informáticos ajenas;
2. Acceso a los datos y utilización de los mismos por quien no esta autorizado para ello:

3. Utilización de la computadora y/o los programas de otra persona, sin autorización, con el fin de obtener beneficios propios y en perjuicio de otro;
4. Introducción de programas o rutinas en otras computadoras para destruir información, datos o programas;
5. Utilización de la computadora con fines fraudulentos y;
6. Agresión a la privacidad mediante la utilización y procedimiento de datos personales con fin distinto al autorizado.
7. Programación de instrucciones que producen un bloqueo total al sistema.
8. Destrucción de programas por cualquier método.
9. Daño a la memoria.
10. Atentado físico contra la maquina o sus accesorios (discos, cintas, terminales, etc.).
11. Sabotaje político o terrorismo en que se destruya o surja un apoderamientos de los centros neurálgicos computarizados.
12. Secuestro de soportes magnéticos en lo que figure información valiosa con fines de chantaje (pago de rescate, etc.).

Otra clasificación de estas conductas catalogadas como delitos informaticos, es la siguiente:

1. *Fraude por manipulaciones de una computadora contra un sistema de procedimiento de datos;*
2. *Espionaje informático y robo de software;*
3. *Sabotaje informático;*
4. *Robo de servicios;*
5. *Acceso no autorizado a sistemas de procesamiento de datos, y*
6. *Ofensas tradicionales en los negocios asistidos por computador.*

Figura 2.4. Clasificación de los Delitos Informaticos

En varios estudios federales de los Estados Unidos, se han concretado manifestaciones de los llamados delitos informáticos o “computer-crime”, como lo son:

1. *Introducción de los datos falsos en el sistema y manipulación de datos;*
2. *Uso no autorizado de instalaciones y elementos físicos de los sistemas informáticos, y*
3. *Atentados contra el patrimonio mediante computadoras*

Figura 2.4.1. Clasificación de los Delitos Informaticos

Otra clasificación, es la que sigue:

1. Delitos económicos vinculados a la informática:

- Fraude mediante manipulaciones contra los sistemas de procesamiento de datos,
- Espionaje Informático y robo (hurto) de software; sabotaje informático;
- Apropiación de servicios,
- Acceso no autorizado a los sistemas informaticos;
- Fraude fiscal informático;

2. Ofensas por medios informaticos contra los desechos individuales de la persona: atentados contra la intimidad y privacidad;

3. Ataques por medio de la informática contra intereses supraindividuales:

- Atentados contra la seguridad nacional;
- Atentados contra la integridad de los procedimientos basados en la informática en los procesamientos de datos,
- Atentados contra la legitimación democrática de las decisiones parlamentarias vinculadas a las computadoras.

Respecto a las distintas formas de delincuencia informática enumeradas, hay una que coincide en las diversas clasificaciones, y es la que se refiere a la manipulación de la computadora, que alude a aquellos comportamientos que afectan las fases de suministro, salida y comunicación de datos e información,

así como su procesamiento, esto es, las alteraciones del programa de la computadora.

La manipulación de los datos e información puede ser cometida, en tres etapas diferentes:

1. *Almacenamiento de los datos o entrada, que es el momento en que se introduce la información, en lenguaje electrónico, a la computadora,*
2. *Procesamiento de datos o programación, que se refiere a las operaciones secuenciales que debe seguir la computadora para dar solución o respuesta a una orden específica.*
3. *Transmisión de los datos del proceso o salida, que se refiere a la información ya procesada, y se presenta por medio de comunicaciones o accesos a periféricos en los que se archiva.*

Figura 2.4.2. Manipulación de la Datos e Información

Entre las técnicas de manipulación de las computadoras podemos mencionar las siguientes:

1. Estafa de datos (Data Diddling),
2. El Caballo de Troya (Trojan Horse);
3. Técnica Salami (Salami techniques o Rouding down);
4. Uso no autorizado de un programa “llave” (Superzapping);
5. Trampas (Trap Doors);
6. Bombas lógicas (Logic Bombs);
7. Ataques asíncronos (Asynchronous Attacks);
8. Limpieza o Recogida de información residual (Scavening);
9. Fuga de datos o Filtración de datos (Data Leakage);
10. Subterfugio o Suplantación o Trasiego de personas (Piggybanking and Impersonation);
11. Interceptación o Pinchado de líneas (Wire Topping);
12. Simulación y modelado de delitos (Simulation and Modeling).

2.5. Peculiaridades de la Criminalidad Informática

En el plano jurídico-penal, la criminalidad informática puede suponer una nueva versión de delitos tradicionales (atentado terrorista contra la computadora que regula el tráfico aéreo) o la aparición de nuevos delitos impensables antes del descubrimiento de las nuevas tecnologías (virus informaticos, accesos

indebidos o procesamiento de datos para alterar su funcionamiento, etc.). Por ello la criminalidad informática obliga a revisar los elementos constitutivos de gran parte de los tipos penales tradicionales. Cabe imaginar el estupor de un penalista del pasado siglo ante la mera alusión, hoy tan frecuente en el lenguaje referido a la criminalidad informática, de situaciones tales como: la posibilidad de que existan fraudes en los que el engaño se realiza sobre una maquina y no sobre una persona, de robos de servicios de la computadora, que se realizan sin fuerza en las cosas; o de hurtos de tiempo de computadora, sin que exista un animo de lucro, sino un mero propósito de juego por quien lo realiza y sin que se prive al titular de la cosa de su posesión.

Por tratarse de un sector sometido a constantes fructuaciones e innovaciones tecnológicas, sus categorías son asimismo efímeras y cambiantes. El hurto de tiempo de computadora fue uno de los supuestos de criminalidad informática en las primeras etapas de este sector jurídico informático. Pero en la medida en que la evolución informática ha permitido sustituir las computadoras voluminosas, costosas y accesibles solo a aquellas empresas o entidades de enorme potencial económico, por las computadoras de la cuarta generación, esos supuestos delictivos han perdido importancia. Hoy toda la persona puede tener acceso a una computadora personal que le permite realizar operaciones que hace 20 años eran privativas de equipos muy costosos y sofisticados.

Con ello se ha dejado de tener relevancia práctica y trascendencia jurídica la utilización de tiempo de computadora.

De otro lado, la criminalidad informática se caracteriza por las dificultades que entraña descubrirla, probarla y perseguirla. A la dificultad de descubrir las conductas informáticas delictivas se añade la facilidad de penetrar en algunos de los sistemas informaticos y la personalidad especial de algunas de los delincuentes que pueden considerarse como un subtipo de la delincuencia de “cuello blanco”. Conviene también reseñar, al considerar estas peculiaridades político-criminales, que en ocasiones, se han avanzado índices de probabilidad delictiva en relación con la informática. Hace algunos años adquirió notoriedad el estudio realizado por dos especialistas norteamericanos en esta materia. En

ese análisis se simbolizaban las Probabilidad de Crimen Informático = P (CI), en función de tres variables: Deshonestidad = D (es decir, la inclinación al delito del personal informaticos); Oportunidad = O (o sea, la falta de medidas de seguridad en los equipos informaticos); y Motivación = M (que se refiere a los conflictos personales o laborales que pueden incitar a delinquir a los empleados informaticos).

La propia precariedad del sistema jurídico penal refuerza la tendencia a no denunciar estos delitos, para evitar la alarma social o el desprestigio que de su conocimiento podría derivarse.

Por ello, las mas de las veces, las victimas prefieren sufrir las consecuencias del delito e intentar prevenirlo para e futuro, antes que iniciar un procedimiento judicial. Esta situación dificulta el conocimiento preciso del número de delitos perpetrados y la planificación de las adecuadas medidas legales sancionadoras o preventivas.

2.6. Tipos de Delincuente Informático: Sujetos Activos y Pasivos

Sujeto Activo, posee ciertas características que no presentan el denominador común de los delincuentes, esto es, los sujetos activos tienen habilidades para el manejo de los sistemas informaticos 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.

Con el tiempo se ha podido comprobar que los autores de los delitos informaticos son muy diversos y que lo que los diferencia entre si es la naturaleza de los delitos 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 Informático es tema de controversia ya que para algunos, dicho nivel no es indicador de delincuencia informática en tanto que otros aducen que los posibles delincuentes informaticos 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.

Sin embargo teniendo en cuenta las características ya mencionadas de la persona que cometen los “delitos informaticos”, estudiosos en la materia lo han catalogado como “delito de cuello blanco” termino introducido por primera vez por el criminólogo Edwin Sutherland en el año 1943.

Este conocido criminólogo señala un sinnúmero de conductas que considera como “delitos de cuello blanco”, aun cuando muchas de estas conductas no están tipificadas en los ordenamientos jurídicos como delitos, y dentro de las cuales cabe destacar las “violaciones a las leyes de patentes y fabrica de derechos de autor, el mercado negro; el contrabando en las empresas, la evasión de impuestos, las quiebras fraudulentas, corrupción de altos funcionarios, entre otros”.

Asimismo, este criminólogo estadounidense dice que tanto la definición de los “delitos informaticos” como la de los “delitos de cuello blanco” no es de acuerdo al interés protegido, como sucede en los delitos convencionales sino de acuerdo al sujeto activo que los comete. Entre las características en común que poseen ambos delitos tenemos que: el sujeto activo del delito es una persona en cierto status socioeconómico, su comisión no puede explicarse por pobreza ni por la mala habitación, ni por carencia de recreación, ni por baja educación, ni por poca inteligencia, ni por inestabilidad emocional.

Es difícil elaborar estadísticas sobre ambos tipos de delitos. La “cifra negra” es muy alta; no es fácil descubrirlo y sancionarlo, en razón del poder económico de quienes lo cometen, pero los daños económicos son altísimos; existe una gran indiferencia de la opinión publica sobre los daños ocasionados a la sociedad; esta no considera delincuentes a los sujetos que cometen este tipo de delitos, no los segrega, no los desprecia, ni los desvaloriza, por el contrario, el autor o autores de este tipo de delitos se considera a sí mismos “respetables”. Otra coincidencia que tienen estos tipos de delitos es que,

generalmente, son objeto de medidas o sanciones de caracteres administrativos y no privativos de la libertad.

Sujeto Pasivo, o víctima del delito es el entre sobre el cual recae la conducta de acción u omisión que realiza el sujeto activa, y en el caso de los “delitos informaticos” las victimas pueden ser individuos, instituciones credicticias, gobiernos, etc, que usan sistemas automatizados de información, generalmente conectados a otros.

El sujeto pasivo del delito es sumamente importante, ya que mediante el podemos conocer los diferentes ilícitos que cometen los delincuentes informaticos, con objeto de prever las acciones antes mencionadas debido a que muchos de los delitos son descubiertos casusticamente por el desconocimiento del modus operandi de los sujetos activos. Dado lo anterior, “ha sido imposible conocer la verdadera magnitud de los “delitos informaticos”, ya que la mayor parte de los delitos no son descubiertos o no son denunciados a las autoridades responsables” y si a esto se suma la falta de leyes que protejan a las víctimas de estos delitos; la falta de preparación por parte de las autoridades para comprender, investigar y aplicar el tratamiento jurídico adecuado a esta problemática; el temor por parte de las empresas de denunciar este tipo de ilícitos por el desprestigio que esto pudiera ocasionar a su empresa y las consecuentes perdidas económicas, entre otras mas, trae como consecuencia que las estadísticas sobre este tipo de conductas se mantenga bajo la llamada “cifra oculta o cifra negra”.

2.7. Categoría de Ataques

Una amenaza es una condición del entorno del sistema de información (persona, maquina, suceso o idea) que, dado una oportunidad, podría dar lugar a que se produjese una violación de la seguridad (confidencialidad, integridad, disponibilidad o uso legitimo).

La política de seguridad y el análisis de riesgos identifican las amenazas que han de ser contrarrestados, dependiendo del diseñador del sistema de seguridad especificar los servicios y mecanismos de seguridad necesarios.
Las amenazas a la seguridad en una red pueden caracterizarse modelando el sistema como un flujo de información desde una fuente, como por ejemplo un archivo a una región de la memoria principal, a un destino, como por ejemplo otro archivo o un usuario. Un ataque no es más que la realización de una amenaza.

Las cuatro categorías generales de amenazas o ataques son las siguientes:

Interrupción

La información del sistema es destruida o llega a ser inutilizable. Este es un ataque sobre la disponibilidad. En este ataque se pueden incluir ejemplos de destrucción de una pieza hardware, como un disco duro o el corte de una línea de comunicación.

Intercepción

Una participación sin autorización por parte de una persona, computadora o programa es una comunicación. Este es un ataque sobre la confidencialidad. Un ejemplo incluido podría ser la copia ilegal de programas o archivos.

Modificación

Una participación sin autorización, pero no solo accediendo a la información sino también alterándola. Este es un ataque sobre la integridad. Los ejemplos incluidos podrían ser los cambios de valores en archivos y programas o la modificación de mensajes transmitidos en una red.

Figura 2.7. Modificación transmitida en una Red

Fabricación

Introducción de objetos falsificados en un sistema sin autorización. Este es un ataque sobre la autenticidad. Un ejemplo seria la introducción de mensajes falsos en una red.

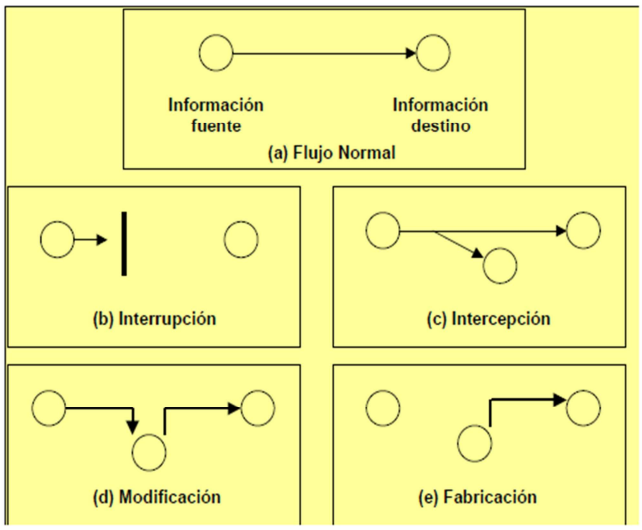

Figura 2.7.1. Fabricación

Estas categorías de ataques se pueden categorizar en dos tipos de ataque, los pasivos y los activos:

Ataques Pasivos

Los ataques pasivos son simplemente observaciones de datos reservados durante una transmisión. La finalidad del intruso es la obtención de la información transmitida. Dentro nos encontramos dos tipos de ataque: la observación del contenido del mensaje y el análisis de tráfico. El primero sería el entendimiento por parte de un intruso del contenido de una transmisión que contiene información confidencial, como una conversación telefónica o correo electrónico.

El análisis de tráfico seria la observación por parte del intruso sobre la longitud del mensaje, la identificación de los usuarios y la frecuencia de transmisión, pero en ningún caso puede entender la información, pues va encriptada. Los ataques pasivos son difícilmente detectados porque no producen una alteración de la información, no obstante son factibles de prevenir.

Ataques Activos

Los ataques activos incluyen alguna modificación del mensaje o la creación de mensajes falsos. Hay varios tipos de ataques:

- **Cambiar la identidad del emisor o receptor:** Ocurre cuando una entidad pretende hacerse pasar por otra

Figura 2.7.2. Ataques Activos

- **Manipulación de datos:** Alteración o eliminación de la información,

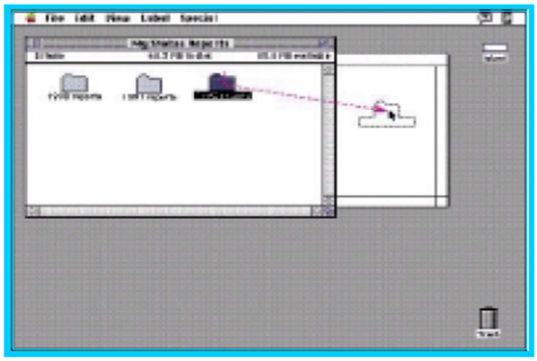

Figura 2.7.3. Manipulación de Datos

- **Repetición:** Capturar una información, guardarla un tiempo y volverla a enviar, produciendo un afecto de no autorización.
- **Denegación de servicio:** Impedir una comunicación, una respuesta, causar un repudio de usuarios
- **Encaminamiento incorrecto:** Atacan a los nodos dentro de la red, pues no están tan protegidos como los terminales.

2.8. Tipos de Delitos Informaticos

Delitos	Características
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 mas 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 tienen 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 partir de tarjetas bancarias robadas, sin embargo, en la actualidad se usan ampliamente equipos y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.
Fraude efectuado por manipulación informática	Aprovecha las repeticiones automáticas de los procesos de cómputo. Es una técnica especializada que se denomina "técnica del salchichón" en la que "rodajas muy finas" apenas perceptibles de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra.

Figura 2.8. Tipos de Delitos Informaticos

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.

Figura 2.8.1. Tipos de Delitos Informaticos

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.
Virus	Es una serie de claves programadas 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 de 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 en donde se halla la bomba.
Acceso no autorizado a Sistemas o Servicios	Por motivos diversos: desde la simple curiosidad, como en el caso de muchos piratas informáticos (Hacker) hasta el sabotaje o espionaje informático.

Figura 2.8.2. Tipos de Delitos Informaticos

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.	Esta 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. Al respecto, consideramos, que la reproducción no autorizada de programas informáticos no es un delito informático debido a que el bien jurídico a tutelar es la propiedad intelectual.

Figura 2.8.3. Tipos de Delitos Informaticos

2.9. Fraude Informático

Contemplando el fraude informático en un sentido amplio se pueden formar varios grandes grupos de figuras delictivas claramente diferenciados:

1. *Fraude informático propiamente dicho.*
2. *Protección del derecho a la intimidad.*
3. *Propiedad intelectual informática.*
4. *Acciones físicas contra la integridad de las computadoras.*
5. *Las acciones de los "hackers".*
6. *Los virus informáticos y programas análogos.*
7. *La sustracción de tiempo de computadora.*

Figura 2.9. Fraude Informático

En el grupo 1, el número de posibles fraudes es amplio, y solo esta limitado por la imaginación del autor, su capacidad técnica y las medidas de seguridad de la instalación.

Los diferentes fraudes los podemos englobar en cuatro grandes grupos básicos:

- Intervención en los datos de entrada al sistema.
- Incorporación de modificaciones no autorizadas en los programas.
- Modificación fraudulenta de la información almacenada en el sistema.
- Intervención en las líneas de transmisión de datos.

Respecto a los **grupos 2 y 3** derecho de la intimidad y la protección de programas.
En el grupo 4, recoge las acciones físicas contra las propias computadoras, caso del robo y sabotaje. El robo, principalmente, se da en unidades o elementos hardware fácilmente transportables, por ejemplo: pantallas, teclados, impresoras, módems, etc, y menos en grandes computadoras.

El sabotaje se presenta de muy diversas maneras: destornillador en el ventilador de la unidad central, silicona en un cajero automático, vaso de bebida en una CPU, bomba de plástico, incendio provocado, etc. Obviamente este tipo de acciones no son exclusivas del mundo informático ya se dan también en otro entornos industriales.

El grupo 5, relacionado con los “hackers”, que ha tenido especial relevancia debido a sus “hazañas”, ya que se han logrado introducirse en sistemas supuestamente sofisticados.

Podemos considerar que hay dos tipos:

- Los que solo tratan de llamar la atención sobre la vulnerabilidad de los sistemas informaticos, o satisfacer su propia vanidad.
- Los verdaderos delincuentes, que logran apoderarse por este sistema de grandes sumas de dinero o causar daños muy considerables.

Ambos tipos son peligrosos, pues vienen a ser en nuestra época como los piratas de tiempos pasados, cuya peligrosidad mayor estaba en la inseguridad que creaban en el tráfico marítimo. En este caso, la inseguridad la crean en el sistema vertebral de la economía.

El grupo 6, tiene que ver con los virus informaticos (un virus, en biología, es un agente productor de enfermedades contagiosas, comúnmente invisible y filtrable, por lo que el nombre elegido es bastante adecuado). Existen dos tipos de virus: Benignos (molestan, pero no dañan), Malignos (destruyen información o impiden trabajar). Suelen tener capacidad para instalarse en un sistema informático y contagiar otros programas e, incluso, a otras computadoras a través del intercambio de soportes magnéticos, como disquetes, o por enlace entre computadoras.

El grupo 7, tiene que ver con el hurto de uso del tiempo de la computadora. Consiste en la utilización sin autorización de una computadora por un empleado o por un tercero durante cierto tiempo, sin moverlo, beneficiándose de ciertos servicios. Puede llegar a tener una cierta importancia económica.

2.10. Comportamiento Delictivo Informático

Espionaje Informático (Industrial o Comercial)

El espionaje Informático (industrial o comercial) debe entenderse como “la obtención, con animo de lucro y sin autorización además, de valor para el trafico económico de la industria o comercio”, todo lo que se refiere a la falsificación en materia informática, reproducción no autorizada de un programa informático protegido.

Sabotaje Informático

El Sabotaje Informático debe entenderse como aquellas “alteraciones causadas en datos computarizados o programas informaticos con la intención de obstaculizar el funcionamiento de un sistema informático o de telecomunicaciones”, siempre que los datos o programas afectados infieran en la actividad de empresa, pues de no ser así afectarían bienes de distinta naturaleza y por ende ajeno al bien jurídico “información”, todo lo que se refiere a la destrucción, modificación o inutilización de archivos y ficheros informatizados, distribución de virus y programas delictivos.

Intromisión Informática

Comportamiento consistente en la introducción a sistemas de información o computadoras infringiendo medidas de seguridad destinadas a proteger los datos contenidos en ella, todo lo que se refiere al acceso no autorizado, intercepción sin autorización, uso no autorizado de una computadora.

Aquí es necesario precisar que, aunque es un inicio, pareciera que Sabotaje Informático e Intromisión fueran comportamientos idénticos, ello no es así pues; mientras en el sabotaje, la intención es obstaculizar el funcionamiento de un sistema informático, en el segundo caso la acción realizada busca únicamente el ingreso a tales sistemas sin dirigir sus actos para producir perjuicio, si se produce es ajeno al comportamiento aunque lo agrave.

a) Delito de Violación a la Intimidad

En el articulo 154 esta tipificado el Delito de violación a la intimidad, el cual establece: “el que viola la intimidad de la vida personal y familiar ya sea observando, escuchando o registrando un hecho, palabra, escrito o imagen, valiéndose de instrumentos, procesos técnicos u otros medios será reprimido con pena privativa de libertad no mayor de dos años. La pena será no menor de uno ni mayor de tres y de treinta a ciento veinte días cuando el agente revela la intimidad conocida de la manera antes prevista”.

El que indebidamente, organiza, proporciona o emplea cualquier archivo que tenga datos referentes a las convicciones políticas o religiosas y otros aspectos de la vida intima de una o mas personas será reprimido con pena privativa de libertad no menor de un año ni mayor de cuatro años. Si el agente es funcionario o servidor publico y comete delito en ejercicio del cargo, la pena será no menor de tres años ni mayor de seis de inhabilitación.

La base de datos computarizadas se considera que están dentro del precepto de “cualquier archivo que tenga datos”, en consecuencia estaría tipificado el delito de violación a la intimidad utilizando la informática y la telemática a través del archivo, sistematización y transmisión de archivos que contengan datos privados que sean divulgados sin consentimiento.

b) Delito de Hurto agravado por Transferencia Electrónica de Fondos, telemática en general y empleo de claves secretas

El que, para obtener provecho, se apodera ilegítimamente de un bien total o parcialmente ajeno, sustrayéndolo del lugar donde se encuentra, será reprimido con pena privativa de libertad no menos de uno ni mayor de tres años. Se equipara a bien mueble la energía eléctrica que tenga valor económico, así como el espectro electromagnético.

El delito de hurto agravado por transferencia electrónica de fondos tiene directa importancia en la actividad informática.

El sistema de transferencia de fondos, en su conjunto, se refiere a la totalidad de las instituciones y practicas bancarias que permiten y facilitan las transferencias interbancarias de fondos. El desarrollo de medios eficientes de transmisión de computadora a computadora de las órdenes de transferencia de fondos ha fortalecido el sistema. Los niveles de calidad y seguridad de las transferencias interbancarias de fondos se han ido acrecentando conforme el avance de la tecnología, no obstante la vulnerabilidad a un acceso indebido es una “posibilidad latente” por tanto además de los sistemas de seguridad de

hardware, software y comunicaciones ha sido necesario que la norma penal tenga tipificada esta conducta criminal.

Uno de los medios de transferencia electrónica de fondos se refiere a colocar sumas de dinero de una cuenta a otra, ya sea dentro de la misma entidad financiera o una cuenta en otra entidad de otro tipo, ya sea pública o privada. Con la frase “telemática en general” se incluye todas aquellas transferencias u operaciones cuantificables en dinero que pueden realizarse en la red informática ya sea con el uso de Internet, por ejemplo en el Comercio Electrónico o por otro medio. Cuando se refiere a “empleo de claves secretas” se esta incluyendo la vulneración de password de niveles de seguridad, de códigos de claves secretas.

c) Delito de Falsificación de Documentos Informaticos

Es la norma que regula el valor probatorio del documento informático, incluyendo en los conceptos de microforma y microduplicado tanto al microfilm como al documento informático. El establece que: “la falsificación y adulteración de microformas, microduplicados y microcopias sea durante el proceso de grabación o en cualquier otro momento, se reprime como delito contra la fe publica, conforme las normas pertinentes del Código Penal”.

En el Código Penal, entre los delitos contra la fe publica, que son aplicables a la falsificación y adulteración de microformas digitales se tiene.

d) Delito de Fraude en la administración de personas jurídicas en la modalidad de uso de bienes informaticos

Puesto que en el patrimonio de la persona están incluidos tanto bienes materiales (hardware) como inmateriales (software, información, base de datos, etc) esta figura delictiva puede aplicarse al campo informático según interpretación.

“Sera reprimido con pena privativa de libertad no menos de uno ni mayor de cuatro años el que, en su condición de fundador, miembro del directivo o del consejo de administración o del consejo de vigilancia, gerente, administrador o liquidador de una persona jurídica, realiza, en perjuicio de ella o de terceros, cualquiera de las actos siguientes.

e) Delito contra los derechos de autor de software

Respecto a los delitos contra los derechos de autor de software, debe tenerse en cuenta que sobre la naturaleza jurídica y la tutela que apunta el derecho de autor sobre el software hay acuerdo general.

Y no puede ser de otro modo, debido a la trascendencia que tiene, dado que la transgresión de índole penal a la actividad intelectual constituye no solo una agresión a la propiedad del autor y afecta los intereses de la cultura, sino que conforma también un ataque al derecho moral sobre la paternidad de la obra.

a) La modifique total o parcialmente.
b) La reproduzca total o parcialmente, por cualquier medio o procedimiento.
c) La distribuya mediante venta, alquiler o préstamo público.
d) La comunique o difunda públicamente por cualquiera de los medios o procedimientos reservados al titular del respectivo derecho.
e) La reproduzca, distribuya o comunique en mayor número que el autorizado por escrito.

Capítulo III El uso de las Nuevas Tecnologías y Riesgo y Oportunidades

Capítulo III El uso de las Nuevas Tecnologías y Riesgo y Oportunidades

El desafío de las nuevas tecnologías nos obliga a observarlas desde una doble óptica. Si bien el temor inicial que suscita lo desconocido ha hecho proliferar una serie de tabúes que han encontrado en Internet el lado más perjudicial, la posibilidad de compartir, en tiempo real, cualquier faceta del saber humano, abre un mundo de oportunidades que, hasta hace poco tiempo, era inimaginable.

La imagen que ofrece Internet, asociada siempre a un espacio en el que resulta difícil aplicar la Ley, contrasta con la situación que se da en la realidad, tras el estudio de las normas de ámbito nacional e internacional y a partir de las experiencias procesales y la jurisprudencia existente hasta el momento.

A pesar de la novedad aparente, la materia a analizar es tan amplia, que obliga a limitar a los siguientes puntos:

- Comercio electrónico,
- Delitos en Internet,
- Medios de Control y Prevención,
- Responsabilidad del proveedor de contenidos,
- Conflictos jurisdiccionales,
- Problemática especifica de los derechos de autor.

3.1. Comercio Electrónico

El hecho de que el comercio electrónico en Internet vaya dirigido prioritariamente al consumo, y en especial, a la compra compulsiva, obliga a tener en cuenta los aspectos jurídicos de la transacción, tanto en la fase de preparación de la oferta, como en la de aceptación.

Las razones que impulsan a un usuario a permanecer en un web no son únicamente la utilidad y el interés de sus contenidos, sino también el atractivo de sus graficas y el nivel de sorpresa que suscita cada sección. Ello conlleva

un esfuerzo creativo que debe ser convenientemente protegido mediante las medidas habituales del Derecho del Autor y de la Propiedad Industrial.

Por otra parte, debe cuidarse el contenido del contrato en línea (usando Correo Electrónico, EDI, Internet), la adecuación de sus clausulas a las especiales características de la contratación electrónica, y la forma en que se efectúa la transacción, con el fin de demostrar que el usuario ha prestado su consentimiento o las condiciones de oferta.

La concurrencia de oferta y aceptación, pago y entrega, puede producirse en tiempo real o de forma diferida. El software, por ejemplo, que constituye el producto más vendido o través de Internet, puede ser transferido mediante ambas modalidades. A través de una transacción en tiempo real, el usuario efectúa un “download” del programa tras cumplimentar el formulario de pedido en un entorno seguro. En el casi de la transacción diferida, recibirá el producto o servicio a través de medios convencionales.

No obstante, no todas las transacciones podrán basarse exclusivamente en medios electrónicos: algunas operaciones bancarias, los negocios que deban formalizarse en documento público y la contratación de seguros de vida, que contengan datos relativos o la salud, exigirán la firma analógica original del usuario.

Los riesgos generados por el comercio electrónico se inician en el momento en que la empresa decide tener presencia en la red a través del correspondiente establecimiento de una tienda virtual.

El dominio que va a identificar a la compañía en Internet puede haber sido reservado de mala fe por un especulador que solicitara una importante suma de dinero para formalizar su transferencia.

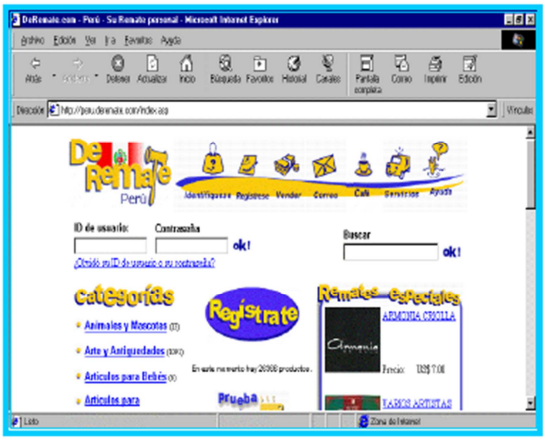

Figura 3.1. Comercio Electrónico

Los pedidos recibidos a través de un formulario electrónico pueden contener datos falsos, generados con programas que simulan el número de una tarjeta de crédito valida.

También puede producirse la interceptación de una transacción con el fin de alterar su contenido o acceder a las claves de las partes que participan en la misma.

Figura 3.1.1. Comercio Electrónico

Por todo ello, antes de poner en marcha un proyecto de comercio electrónico en Internet, es conveniente que se compruebe el cumplimiento, entre otros, de los siguientes requisitos:

- Protección mediante Propiedad Intelectual e Industrial del diseño grafico del web, así como de sus contenidos (texto, gráficos, iconos, fotografías, animaciones, etc.) y código fuente (HTML, JAVA,GGI, etc.).

- Protección del dominio en Internet.
- Establecimiento de los medios de prueba que permitan demostrar la aceptación del usuario.
- Sistemas de certificación que garanticen la confidencialidad, autenticidad, integridad y no repudiación de la transacción.
- Cumplimiento de los requisitos legales de la venta a distancia.
- Medios de prevención de delitos informaticos.
- Clausula de arbitraje.
- Seguro de responsabilidad civil especifico.

3.2. Delitos en Internet

El ciberespacio es un mundo virtual en el que los defectos, miserias y malos hábitos del ser humano se reproducen con la misma fidelidad que las virtudes. El efecto de aldea global generado por el entramado de redes y la proliferación de nodos en todo el planeta ayuda a la difusión inmediata de los mensajes y permite el acceso a cualquier información introducida en la red.
A las reconocidas ventajas que ello supone se unen las disorsiones y los malos usos que pueden tener lugar en el sistema y que confirman una ves más que el mal no está en el medio utilizando sino en la persona que lo utiliza.

Hay necesidad de prevenir y sancionar estos malos usos en la red Internet, lo cual obliga a localizar las distorsiones más habituales que se producen y a analizar los argumentos que se han dado a favor de una legislación que regule el uso de la red y los criterios contrarios a esa regulación.

3.3. Responsabilidad del Proveedor

Existen diversas posiciones sobre la atribución de responsabilidad por los contenidos introducidos en Internet o en una obra multimedia. Es conocida la existencia de una corriente que establece una comparación entre los proveedores de acceso o alojamiento y los editores, en el sentido de que

ambos proporcionan el soporte material que permite a los autores la divulgación de los contenidos generados.

Los proveedores de Servicios de Acceso a Internet (PSI), deben responsabilizarse de los contenidos que publican, al igual que los editores lo hacen con sus obras.

Por el contrario, la segunda corriente asimila los PSI a los propietarios de librerías, de manera que se reconoce la imposibilidad de controlar el entorno volumen de información dinámica o estática que los usuarios introducen en el servidor.

Respecto a la imposibilidad de control de los contenidos de un servidor, cabe distinguir entre foros abiertos y foros cerrados. Sin tener en cuenta las dificultades técnicas de monitorizar todos los foros abiertos que haya en un servidor, podemos decir que no existen obstáculos jurídicos para observar, bloquear, e incluso eliminar los contenidos ilícitos localizados en un entorno WWW, FTP,News, etc.

Por el contrario, la monitorización del correo electrónico y de las conversaciones privadas mantenidas en los foros cerrados del servidor podría construir, en si misma, un delitos de interceptación de las telecomunicaciones.

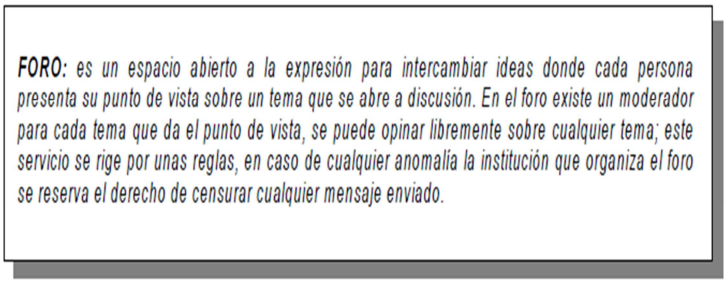

Figura 3.3. Responsabilidad del proveedor

En el foro abierto cualquier persona pueda proponer un tema nuevo, discutir sobre un tema ya existente o comentar las contribuciones de los otros participantes.

La responsabilidad del PSI solo debería apreciarse cuando se demuestre un conocimiento directo de la existencia de los contenidos ilícitos, sin que se haya producido posteriormente un bloqueo de dicha información.

3.4. Medios de control y prevención en Internet

Los proveedores de acceso a Internet y los proveedores de servicios de aplicaciones o alojamiento desempeñan un papel decisivo para dar acceso a los usuarios a los contenidos de Internet. Sin embargo, no se ha de olvidar que la responsabilidad primordial de los contenidos recae sobre los autores y los proveedores de contenidos. Por ello es imprescindible señalar con exactitud la cadena de responsabilidades con el fin de situar la responsabilidad de los contenidos ilícitos en sus creadores.

3.5. Conflictos Jurisdiccionales

El ámbito global de la red genera una dificultad añadida a la hora de perseguir los delitos de Internet.

La proliferación de bancos de datos personales, anónimos y centros de distribución de copias no autorizadas de software, han hecho que los servidores situados en los países que no han ratificado los convenios internacionales de propiedad intelectual o de auxilio a la administración de justicia, aparezcan como refugio para los actos de todo tipo de delitos.

3.6. Problematica de los derechos de autor

La protección de los derechos de autor favorece el crecimiento de la sociedad de la información, ya que contribuye a establecer la certeza de que el autor de una obra verá compensado su esfuerzo con el rendimiento económico que produzca su explotación.

Pensar que los derechos de autor son inaplicables en Internet puede poner en peligro el futuro de la propia red, ya que nadie se atreverá a publicar sus obras en un entorno donde cualquiera puede apropiarse del esfuerzo ajeno.

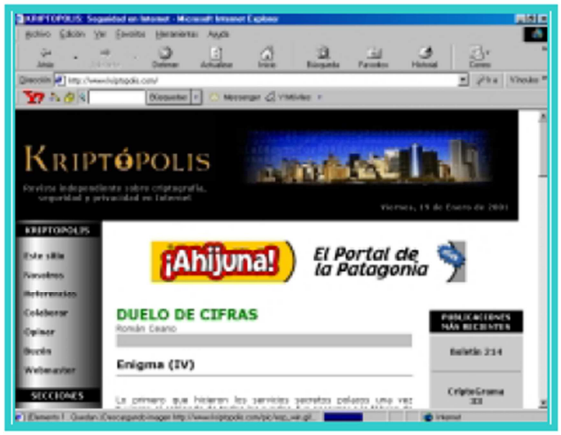

Figura 3.6. Problemática de los derechos de autor

La visión romántica de un ciberespacio libre, sin derechos de autor es un espejismo. Pocos autores aceptaran que su obra pueda ser inscrita en el Registro de la Propiedad Intelectual por otros usuarios y posteriormente puedan encontrarse con una denuncia por plagio de su propio trabajo. Pero actualmente, los mayores perjudicados por la falta de respeto de los derechos de autor en Internet son los productores de software. Los programas por computadora constituyen el producto mas vendido en Internet, también tienen el triste privilegio de ser las obras mas copiadas.

La copia se produce en todas las plataformas posibles:

- Webs Warez (es un termino usado por software “piratas” para describir software del que se ha despojado su protección de copia y hecho disponible para transmitir en Internet),
- FTP Warez,
- Canales del IRC Warez,
- Grupos de noticias Warez.

Pero la modalidad mas extendida es la de los llamados “cracks”, que son pequeños programas que sirven para anular la protección o la limitación de tiempo de una aplicación especifica. Pero la copia no autorizada de software no se limita al ámbito de Internet. La guerra de precios en el sector de las

computadoras clónicos ha generado un submundo de profesionales informaticos dedicados a las instalaciones de copias y distribución de CD-ROM e, incluso, a la falsificación de paquetes completos de las aplicaciones mas conocidas. Pero el comportamiento actual del mercado no contribuye a la mejora de la situación, ya que las posibilidades de crecimiento se ven frustrados por el fraude continuando en software y hardware. En el primer cado porque los usuarios se implican en la actividad de copia no autorizada. En el segundo caso, porque las tácticas que ayudan a ofrecer precios mas bajos se basan en la manipulación de procesadores y en la defraudación del IGV en las importaciones de material informático.

Capítulo IV Los Delitos Informaticos y el Impacto en la Sociedad y Economía

4.1. Concepto de Sociedad

La sociedad es, generalmente, una forma de vida natural y necesaria al hombre en la cual se requiere un ajuste de las funciones y de las actividades de cada individuo, que haga posible la convivencia, evitando choques, resolviendo conflictos y fomentando la cooperación. En consecuencia, si el hombre ha de vivir en sociedad para su conservación y desarrollo, es claro que en esa sociedad, organizada con tales fines, ha de tener posibilidad de hacer todo aquello que sea medio adecuado para llenar sus propias necesidades, hallándose obligado a respetar el ejercicio de iguales facultades en las demás y aun a contribuir con su esfuerzo para la satisfacción de las exigencias colectivas, constituyéndose así el orden jurídico por el conjunto de normas que regulan y hacen posible y beneficia la vida en común.

4.2. Efectos de los Delitos Informaticos en la Sociedad

Los sistemas de cómputo permiten hoy procesar y poner a disposición de la sociedad una cantidad creciente de información de toda naturaleza, a millones de interesados y de usuarios. La mas diversas categorías del conocimiento

humanos, científico, técnico, profesional y personal están siendo incorporados a sistemas informáticos, sin limitaciones, entrega con facilidad a quien desee un conjunto de datos que hasta hace unos años solo podría ubicarse luego de largas búsquedas y selecciones en que el hombre jugaba un papel determinante y las maquinas existentes tenían el rango de equipos auxiliares para imprimir los resultados.

En la actualidad, ese enorme caudal de conocimiento puede obtenerse en segundo o minutos, transmitirse incluso el documento y llegar al receptor, mediante sistemas sencillos de operar, confiables y capaces de responder a casi toda la gama de interrogantes que se planteen a los archivos informáticos. Se afirma que las perspectivas de la informática no tienen límites previsibles, por ello se ha llegado a sostener que la Informática es hoy una forma de Poder Social. Las capacidades que pone a disposición de Gobiernos y de particulares, con rapidez y por consiguiente ahorro de tiempo y energía, configuran un cuadro de realidades de aplicaciones y de posibilidades de juegos lícitos e ilícitos, en donde es necesario el derecho para regular los múltiples efectos de una situación, nueva y de tantas potencialidades en el medio social.

El desarrollo constante de las computadoras, el creciente aumento de las capacidades de almacenamiento y procesamiento, la miniaturización de los chips de las computadoras instalados en productos industriales, la fusión de proceso de la información con las nuevas tecnologías de comunicación, así como la investigación en el campo de la inteligencia artificial, no solo tiene un lado ventajoso sino que plantea también problemas de significativa importancia para el funcionamiento y la seguridad de los sistemas informáticos en los negocios, la administración, la defensa y la sociedad.

Debido a esta vinculación, el aumento de los delitos relacionados con los sistemas informaticos registrados en la última década a nivel mundial, representa una amenaza para la economía de un país y también para la sociedad en su conjunto. El autor o autores de este tipo de delitos se considera a si mismos “respetables” otra coincidencia que tiene estos tipos de delitos en

que, generalmente son objeto de medidas o sanciones de carácter administrativo y no privativos de la libertad.

Este nivel de criminalidad se puede explicar por la dificultad de reprimirla en forma internacional, ya que los usuarios están esparcidos por el mundo y, en consecuencia, existe una posibilidad muy grande de que el agresor y la victima estén sujetos a leyes nacionales diferentes. Además, si bien los acuerdos de cooperación y los tratados intentan remediar algunas de las dificultades ocasionadas por los delitos informativos, sus posibilidades son limitadas.
La violación de la intimidad a través de acceso ilegitimo a bancos de datos informatizados, los fraudes cometidos por medios de computadoras, la reproducción ilícita de software, el espionaje industrial y la introducción de virus dañinos en sistemas informáticos entre otro, son delitos que debe enfrentar la sociedad y que el derecho y especialmente las ciencias criminológicas deben resolver lo antes posible.

Los delitos informáticos hacen que se tenga cierta desconfianza en las transacciones que se realizan mediante Internet, con las tarjetas de crédito, con la confidencialidad de los datos personales, etc. Como se puede alterar la información se pierde credibilidad.

Aquellos que tienen la posibilidad de accesar a información de terceros son tentadas de infiltrarse a dicha información para sacarle provecho, chantajeando o extorsionando a esas personas, vendiéndola a otros, etc.
Los hackers, crackers, etc, tienden a agruparse en comunidades, con el fin de intercambiar experiencias y tratar de lograr objetivos cada vez más inalcanzables.

Los delitos informaticos también afectan en la identidad de las personas, porque sabiendo el password de otra personas se puede suplantar su identidad, hacer transacciones, enviar correos, malograr, eliminar, alterar información, etc, con la identificación de otra persona.

Otra forma que afectan estos delitos es que generan la inseguridad institucional, es decir la inestabilidad en las relaciones entre las personas, un ejemplo podría ser enviar un mensaje anónimo por correo electrónico dentro de una institución, hogar, etc. acusando falsamente a ciertas personas, generando con esto desconcierto, dudas sobre esas personas, creando inestabilidad emocional, desastibiliza el hogar, la familia, instrucciones.

4.3. Efectos de los Delitos Informáticos en la Economía

La Economía, es, sin duda alguna, uno de los bastiones del actual modelo social, la existencia de bloques económicos en tenaz competencia en su afán de acaparar el mercado hace que se requiera de elementos que favorezcan la obtención del lucro requerido, la información se convierte así en un elemento vital para sus aspiraciones.

El fenómeno de la globalización permite en ingreso fluido y constante del material informático, tanto Hardware como Software, en los países, lo que genera la reducción del costo y en consecuencia posibilita mayor empleo por parte de la sociedad.

El mundo digital, a pesar de su creciente tamaño y universalidad no termina en el teclado y en un cable de comunicación, sino que alcanza al mundo físico el cual puede controlar un sistema de transporte colectivo, una línea área, la economía de los diferentes países, y hasta un reactor a planta nuclear. Y por tanto se considera importante que las leyes criminales tengan armas con las cuales poder hacer frente a las consecuencias que dichos actos digitales puedan causar en el mundo físico.

El primer tipo de ataques fue físico: ataques contra computadoras, cables y elementos electrónicos, Internet se defendió en este tipo de ataques.

Los protocolos distribuidos reducen la dependencia de un solo computador. La redundancia elimina la posibilidad de fuentes puntuales de error. Muchos casos

donde caídas físicas de tensión, de datos o de otros tipos, causan problemas, para los que la mayormente se conoce la solución.

Durante las pasadas décadas, la seguridad de las computadoras se concentro en los ataques sintácticos: ataques contra la lógica operativa de las computadoras y las redes. Este tipo de ataques tiene como objetivo las vulnerabilidades en los programas informaticos, problemas con algoritmos de cifrado, protocolos y vulnerabilidades del tipo denegación de servicios, constituyen prácticamente la totalidad de las alertas de seguridad de la última década.

Otro tipo de ataques de red son los ataques semánticos, que tienen como objetivo la manera en que se asigna significado a un contenido. En nuestra sociedad la gente tiende a creerse todo lo que lee.

Uno de los viejos trucos se ha adaptado al correo electrónico y a la Web. Corredores de bolsa sin escrúpulos usan Internet para alimentar sus estrategias de juego sucio. Otro ejemplo de ataques semánticos en Internet es colocar información falsa en boletines informaticos.

No solo colocan información falsa en boletines, también cambian información caduca, lo que puede traer consecuencias serias.
Los ataques semánticos se vuelven incluso más graves cuando se ejecutan contra computadoras. Los procesos informaticos son mucho mas rígidos respecto al tipo de entradas que admiten. Falsificar entradas en una computadora es más devastador, simplemente porque las computadoras no poseen todos los mecanismos de comprobación que la gente una instintivamente.

Ninguno de estos ataques es nuevo. La gente ha sido víctima, durante mucho tiempo de malas estadísticas, leyendas urbanas y falsos rumores. Cualquier medio de comunicación es susceptible de ser utilizado para explorar la ingenuidad, y siempre ha habido gente sacando partido de esto. Las redes informaticos facilitan el comienzo de los ataques y su dispersión, o que un

individuo anónimo se comunique con un gran número de personas a un costo prácticamente nulo.

4.4. Derecho a la Intimidad

El derecho a la intimidad, que incluye el honor, la persona, la familia y la propia imagen tiene en la actualidad un tratamiento jurídico: la privacidad (privacy), que es una libertad positiva, consistente en ejercer un derecho de control sobre los datos referidos a la propia persona, que han salido ya de la esfera de la intimidad para convertirse en elementos de un archivo electrónico privado o público. La privacidad es necesaria para relaciones de intimidad y confianza. En una sociedad en que los individuos no tienen privacidad, la amistad y la confianza no se pueden desarrollar. Si se desea tener tales relaciones, se debe tener privacidad. Es un delicado problema: conciliar el poder estatal y el interés público, con los derechos inviolables de la persona sobre la base de un espíritu democrático y del Estado de Derecho. Es por ello que se requiere prevenir los posibles abusos y peligros que la informática puede generar.

La información sobre las personas se utiliza para tomar decisiones importantes que afectan profundamente a las personas. La información sobre la que se almacena en una base de datos se puede utilizar para decidir si una empresa contrata o no, si o no se concede un préstamo, si o no se llamara a la comisaría de policía para un interrogatorio, un arresto o una persecución; si o no se recibirá una educación, un alojamiento, etc.

El respeto a la intimidad se extiende hoy, en los países de civilización política democrática, a una esfera bastante amplia de la vida privada. No solo a los informes íntimos, sino también a algunos comportamientos personales, a los elementos distintivos de la personalidad, a las opiniones religiosas y políticas. Los datos de este género se denominan sensibles para distinguirlos de los que están a disposición del público.

Se entiende que la privacidad es una necesidad básica, esencial para el desarrollo y mantenimiento de una sociedad libre, así como para la madurez y

estabilidad de la personalidad individual. En consecuencia, se ha de considerar el derecho de toda persona frente a las agresiones contra sí mismo, su hogar, su familia, sus relaciones y comunicaciones con los demás, su propiedad y sus negocios. Así concebido, este derecho incluye la protección frente a utilizaciones no autorizadas de su imagen, de su identidad; su nombre o sus documentos personales.

La información que afecta la intimidad personal y familiar son las que contiene los siguientes datos cuando son divulgados sin autorización o consentimiento de la persona o sin orden juridicial o de la autoridad competente:

a) Datos sensibles, como son el de raza, ideología, estado de salud, creencias, religión.
b) Datos secretos, como son el secreto profesional, secreto comercial, secreto bancario, secreto de confesión, etc.
c) Datos reservados, siendo aquellos que el titular no está obligado a proporcionar para que sean conocidos por terceros, como son: filiación (hijo matrimonial), extramatrimonial, adoptado, delitos contra el honor (difamación, calumnia, injuria), libertad sexual (violación), adulterio, aborto, etc.
d) Datos privados, los que el titular debe proporcionar periódicamente a la autoridad para fines específicamente señalados, como por ejemplo los datos contenidos en una declaración jurada del impuesto a la Renta, solo deben ser utilizados para los fines que específicamente fueron datos, no para fines distintos.

Entre las informaciones que están excluidas por Ley o razones de Seguridad Nacional, se puede mencionar los datos incluidos en el secreto censal, los datos conocidos en sesión secreta del congreso, la información estratégica y de defensa nacional, etc.

4.5. El derecho a la protección de datos

Es preciso enmarcar los conceptos “informática y privacidad” dentro de un equilibrio entre los derechos de quienes utilizan información sobre individuos (normalmente departamentos gubernamentales y corporaciones o empresas) frente a los derechos de aquellas personas sobre las cuales se obtiene información. La privacidad se ha denominado también libertad informática, que consiste en el derecho a la autotutela de la propia identidad informática, es decir, la que resulta de la recogida y de la confrontación de los datos personales insertados en un programa.

La protección de datos es una aplicación específica de principios de privacidad a tecnologías de la información, y tiene como propósito la protección a la autonomía individual sobre los datos personales. La protección de datos ha sido un tema central desde el principio de los setenta coincidiendo con el uso masivo de sistema informaticos.

Capitulo V Seguridad de Sistemas Informáticos

Capitulo V Seguridad de Sistemas Informáticos

5.1. Desarrollando una política de seguridad

Es necesario que la institución cree una política simple y genética para su sistema de forma que los usuarios puedan entenderla y seguirla con facilidad. Esta política deberá proteger los datos y también la privacidad de los usuarios. Algunas preguntas que son necesarias tener en cuenta para la creación de una política de seguridad son las siguientes:

1.- ¿Quién tiene acceso al sistema?
2.- ¿A quién le está permitido instalar software en el sistema?
3.- ¿Quién es el responsable de los datos?
4.- ¿Quién tiene la capacidad de recuperar la máquina de un ataque ya sea por virus o por individuos?
5.- ¿Quién analiza si el sistema está siendo utilizado apropiadamente?

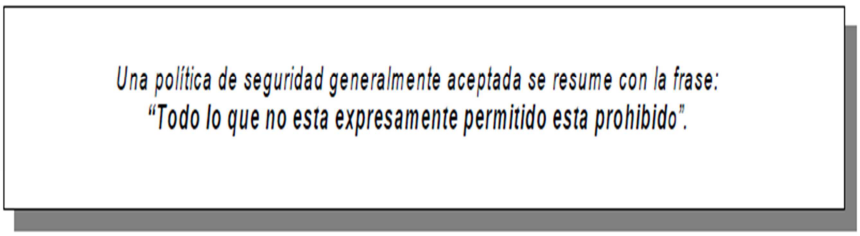

Figura 5.1. Desarrollando una política de seguridad

Esto significa que a menos que la institución proporcione a un usuario acceso a un servicio, ese usuario no debería poder usar ese servicio.

5.2. Formas de asegurar su sistema

Existen diversos métodos con los cuales se puede proteger la información, la maquina, los datos, los usuarios, la red.

Si la empresa tiene una red o está planificando instalar una, hay muchos factores que se deben tener en cuenta antes incluso de instalar la primera máquina.

Las maquinas grandes y conocidas no son el único objetivo: muchos intrusos simplemente desean introducirse en el mayor número posible de sistemas, independiente de su tamaño. Además, pueden usar un agujero de seguridad en su sistema para conseguir acceso a otros a los que esté conectado.

5.2.1. Seguridad Basada en La Maquina

Normalmente el área de la seguridad en la que las instituciones concentran más sus esfuerzos es la seguridad basada en la maquina. Esto normalmente implica asegurarse de que el sistema es seguro, y confiar en que el resto de los administradores de las maquinas de la red hagan lo mismo.

Es necesario tener presente que la contraseña es un punto importante para mantener la seguridad de la maquina, asegurar los servicios locales de red de la PC, mantener el registro de la actividad del sistema y actualizar los programas que tengan agujeros de seguridad, estas son algunas de las responsabilidades del administrador local encargado de la seguridad.

Aunque esto es absolutamente necesario, puede convertirse en una tarea excesivamente laboriosa a medida que su red crezca y dejen de esta compuesta por una pocas maquinas

5.2.2. Seguridad de Red

La seguridad de red es tan necesaria como la seguridad de las maquinas, debido a que varias computadoras se encuentran en la misma red y no se puede esperar que todos y cada uno de estos sistemas sea seguro.
Es necesario asegurarse de que solo los usuarios autorizados pueden usar la red, construir “cortafuegos” o firewalls, usar una fuerte encriptación, y asegurarse de que no haya maquinas inseguras en la red, esta es una actividad o tarea del administrador de seguridad de la red, en la institución.

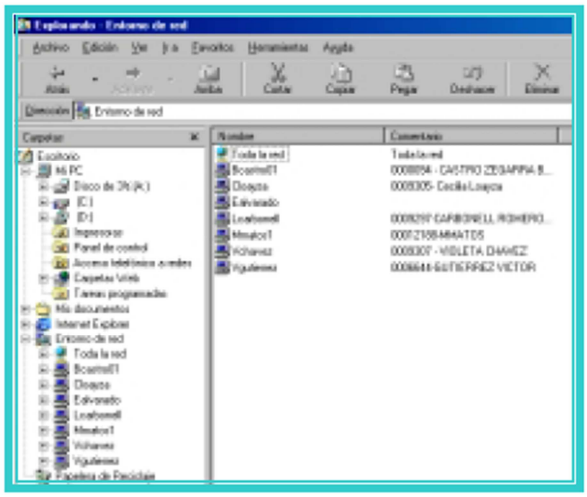

Figura 5.2.2. Seguridad de Red

5.2.3. Seguridad a través de la oscuridad

Una forma de seguridad es la “seguridad a través de la oscuridad”. Esto significa, por ejemplo, mover un servicio con agujeros de seguridad conocidos a un puerto no estándar con la esperanza de que los posibles atacantes no se den cuenta de que está ahí y por consiguiente no puedan explotarlo. La seguridad a través de la oscuridad no es en absoluto segura.

Tener un sistema pequeño, o relativamente poco conocido, no significa que un intruso no vaya a estar interesado en lo que la información de la institución.

5.3. Preparación de la Seguridad

Como primer paso se tiene que chequear el sistema, para que se encuentre lo más seguro que sea posible, posteriormente conectarlo a la red, sin embargo existen algunos puntos importantes que se tiene que tener en cuenta para estar preparando contra una posible intromisión, de manera que la institución pueda rápidamente deshacerse del intruso, y volver a dejar el sistema listo para seguir trabajando normalmente.

5.3.1. Haga una Copia de Seguridad Completa de la Maquina

Aconsejamos lo siguiente:

- Si tiene menos de 650 MB de datos en cada partición, hacer una copia a CD-ROM, debido a que una copia de seguridad en CD es difícil de manipular, y si se guarda de forma adecuada puede durar mucho tiempo.
- Las cintas magnéticas y otros soportes regrabables deben protegerse contra escritura al final el proceso de copia de seguridad, y deben verificarse después, para asegurarse que no ha sido modificados.
- Asegúrese de almacenar las copias de seguridad en un lugar seguro. Una buena copia de seguridad le proporciona un buen punto de partida desde el que restaurar un sistema totalmente destruido.
- Generalmente las instituciones guardan los backups en la misma oficina sin embargo es recomendable guardar las copias de seguridad en un lugar diferente a donde residen físicamente las maquinas,

5.3.2. Planificación una buena Política de Copias de Seguridad

Es necesario realizar un análisis de los documentos e informes que maneja la institución, clasificando la información según la importancia para la entidad, saber a cuales se les debe dar prioridad de mayor a menor.

Posteriormente es necesario decidir cada cuanto tiempo se realizan las copias de los backups, pueden ser anualmente, trimestralmente, mensualmente, semanalmente o diariamente dependiendo de los cambios y la importancia de la información para la institución.
Si en algún momento realiza cambios particularmente importantes en el sistema, una copia completa del sistema seria la recomendable.

5.4. Contingencias Frente al Delito

5.4.1. Copias de Seguridad

Las copias de seguridad de los archivos son el único mecanismo para recuperar la información en caso de la perdida de la misma. La perdida de la información puede ser por diversos motivos desde una persona o intruso hasta

por desastres naturales, por dicha razón, se hace necesario adoptar medidas o políticas de Seguridad Informática, para almacenar y restaurar los backups en el momento deseado y con información actualizada.

Es necesario no solamente realizar las copias de los backups, sino también entregarlo a las personas responsables para que realicen las pruebas necesarias, de esta manera saber si la copia se realizo correctamente, ya que se han encontrado muchos casos donde se realizan las copias, pero no está correcta lo cual perjudica al usuario ya que al momento de querer utilizar las copias, no tienen los datos correctos o hasta ni tienen datos.

Entre una de las recomendaciones básicas para realizar copias de backups, es que la persona de realizar las copias, debe mantener el orden cronológico de cada una de ellas, e ir depurando las que considera que ya no van a ser necesarias, por obsoletas, esta depuración tiene que hacerla acompañado de cada persona responsable de los archivos que se encuentran en el backup, en caso contrario podría eliminar una copia que es necesaria para el usuario.

Otro aspecto que es importante analizar, es que diverso administradores ponen en las etiquetas de las copias de seguridad, detalles del contenido de la misma, sin embargo acá hay un punto muy importante, ya que si alguien consiguiera sustraer la copia, sabría toda la información contenida en la misma.

5.4.2. Contrafuegos (Firewall)

Un firewall es un mecanismo de protección que se puede utilizar para controlar el acceso entre una red segura y una menos segura. Un firewall no es un único componente, es una estrategia diseñada para proteger los recursos de una organización que se pueden alcanzar a través de Internet. Un firewall sirve de “guardián” entre Internet y las redes internas (o corporativos, o Intranet), la principal función de un firewall es la de control de acceso centralizado. Si los usuarios exteriores o remotos pueden acceder a las redes internas sin cruzar el firewall, su efectividad es mínima.

El firewall determina cual de los servicios de red puede ser revisado por usuarios que están dentro o fuera, es decir quién puede entrar para utilizar los recursos de red pertenecientes a la organización.

También un firewall, está considerado como un equipamiento, combinación de hardware y software que muchas empresas u organización instalan entre sus redes internas y el Internet. Un contrafuego permite que solo un tipo específico de mensajes pueda entrar y/o salir de la red interna.

Alcances de los Firewalls

- Proporciona un punto donde concentrar las medidas de seguridad.
- Pueden bloquear tráfico no deseado.
- Pueden dirigir tráfico entrante a sistemas internos preparados para tal fin, más confiables.
- Ayuda a llevar a cabo la política de seguridad:
  - Permite desactivar servicios que se consideran inseguros desde Internet.
  - Permite restringir fácilmente el acceso o la salida desde/hacia determinadas maquinas.
- Permite el registro de información sobre la actividad entre la red interna y el exterior.
- Aísla secciones internas de la red de otras.

Los firewall proporcionan diversos tipos de protección: pueden ocultar sistemas vulnerables que no pueden hacerse fácilmente seguros de Internet, pueden registrar el trafico que sale o que llega a la red privada, pueden ocultar información como nombre de sistemas, topología de red, tipos de dispositivos de red e identificadores de usuarios internos de Internet, pueden proporcionar autentificación más robusta que la de las aplicaciones estándar. Como con cualquier mecanismo de protección, existen compromisos entre conveniencia y seguridad. La transferencia es la visibilidad del firewall tanto para los usuarios de dentro como para los de fuera que atraviesan el firewall. Un firewall se dice que es “transparente” para los usuarios si estos no se dan cuenta, ni se deben detener en el firewall para poder acceder a la red.

Limitaciones de los Firewall

- La información confidencial no solo puede exportarse a través de la red.
- Las acciones indebidas sobre maquinas (accesos no autorizados, introducción de virus, etc.) se pueden realizar aun mas fácilmente desde la red interna.
- No puede impedir ni proteger conexiones que no pasan a través de él.
- No puede proteger contra nuevos tipos de ataque que no tenga catalogados.
- El mayor problema de los firewall es que restringuen mucho el acceso a Internet desde la red protegida. Básicamente, reducen el uso de Internet al que se podría hacer desde un terminal.

5.4.3. Encriptación

Desde años de años se ha venido buscando la manera de poder ocultar o "cifrar" los mensajes mediante diversa técnicas, pero que a su vez volvía los textos ininteligibles. Cifrar un texto o mensaje, conlleva a que si este es interceptado por alguien extraño, el texto no pueda ser descifrado sin la clave correcta. Los sistemas criptográficos se han extendido rápidamente, diversas personas actualmente utilizan la criptografía para "esconder" sus mensajes a la información.
Sin embargo siempre encontraremos personas que trataran de violar los diferentes sistemas de cifrado.

Sistemas de Cifrados

Dentro de los métodos clásicos podemos encontrarnos con varios sistemas como los que siguen a continuación:

- Cifrado Cesar o Monoalfabetico Simple.
- Cifrado Monoalfabetico General.
- Cifrado por Sustitución Polialfabetica
- Cifrado Inverso.

El Sistema de cifrado Cesar o Monoalfabetico Simple

Es un método extremadamente simple y fue empleado por los romanos para encriptar sus mensajes, de ahí el nombre de Cesar, ya que fue en su reinado cuando nació este sistema de cifrado. Este sistema de cifrado se consiste en reemplazar cada letra de un texto por otra que se encuentre a una distancia determinada. Se sabe que Cesar empleaba un distancia de 3, así:

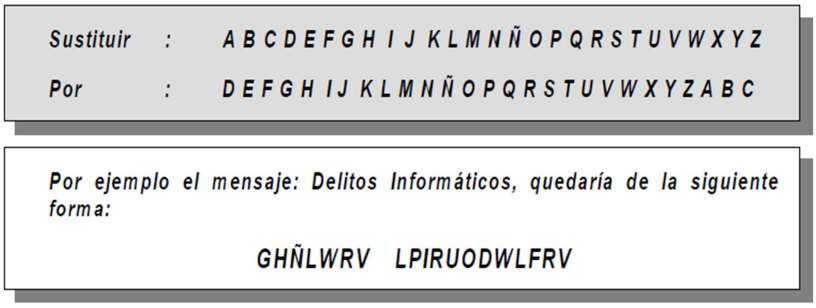

Figura 5.4.3. Encriptación

El sistema de Cifrado Monoalfabetico General

Es un sistema que se basa en sustituir cada letra por otra forma aleatoria. Esto supone un grado más de complejidad en el método de cifrado anterior. Un ejemplo sería el siguiente:

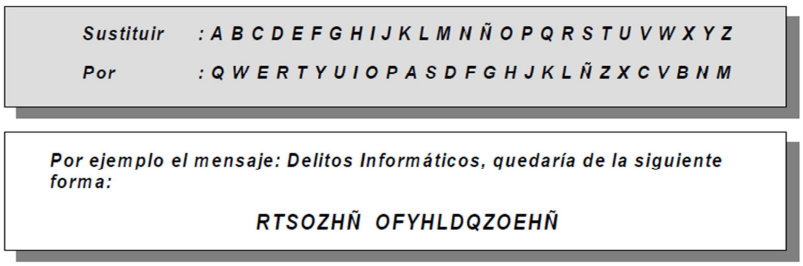

Figura 5.4.3.1. El sistema de Cifrado Monoalfabetico General

El sistema por Sustitución Polialfabetica

Es un método que emplea más de un alfabeto de sustitución. Esto es, se emplean varias cadenas de palabras aleatorias y diferentes entre sí, para después elegir una palabra distinta según una secuencia establecida. Aquí nacen las claves secretas basadas en números. Este sistema es algo más

complejo que los anteriores y a veces resulta difícil descifrar mensajes cuando empleamos más de diez columnas de palabras aleatorias.

El Sistema de Cifrado Inverso

Es considerada una de las formas más simples de cifrar, consiste en escribir al revés, pero lo cierto es que este es un sistema de cifrado. La forma de hacerlo es simplemente escribiendo el mensaje al revés.

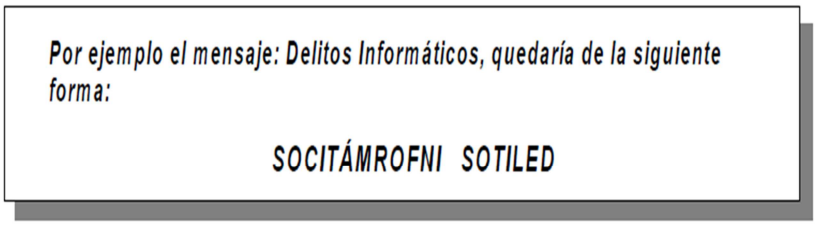

Figura 5.4.3.2. El Sistema de Cifrado Inverso

Con la llegada de las computadoras han surgido nuevos método de encriptación más trabajados y seguros. Algunos de ellos también basados en claves secretas, cuya computación es prácticamente inalcanzable o bastante compleja.

Conclusión

Conclusión

A través del desarrollo del trabajo de la presente tesis, sobre los delitos informáticos, delitos considerados emergentes para el milenio que comienza y por ser de un carácter exploratorio y en base a todos los antecedentes recopilados, bibliografía recopilada y entrevistas realizadas.

Que desde el inicio del proyecto Arpa en el año 1967, el desarrollo de Internet en estos 33 años, ha permitido el surgimiento de una nueva era en las comunicaciones e interrelaciones humanas, comerciales y de gestión.

Que este nuevo paradigma en las relaciones humanas, permite acercar distancias, eliminar barreras y deponer conflictos raciales, religiosos, culturales.

La ley mexicana está trabajando para poder realizar los cambios necesarios para controlar el delito informático, el 17 de mayo del 2000 se publicaron en el diario oficial de la federación, se crearon en la especie, los artículos 211 bis al 211 bis 7 al código penal federal, son leyes para controlar los comportamientos de los llamados hackers o crackers, que atentan sobre los sistemas de computo que pueden o no ser parte del sector financiero mexicano, es decir se ha formado un cuerpo normativo federal. Que sanciona al sujeto que tenga acceso ilegal a dichos sistemas.

Que si bien existe una nueva forma de comunicación social y humana, esto ha dado margen al surgimiento de nuevos hechos o delitos, que valiéndose de la red, de sus computadores como medio o como fin, logran transgredir y superar ampliamente las distintas figuras típicas penales.

Que las técnicas informáticas han creado nuevas posibilidades del uso indebido de las computadoras, lo que ha generado la necesidad de una regulación por parte del derecho.

Se ha generalizado el entendimiento de que “Delitos Informáticos”, son todas aquellas conductas ilícitas susceptibles de ser sancionados por el derecho penal, que hacen uso indebido de cualquier medio informático.

La Criminología, se ha abocado al estudio de los delitos informáticos, desde el punto de vista del delincuente, del delito, la norma y el control social.

Del delincuente, ha determinado que los delincuentes informáticos, son de conductas llamados “delitos de cuello blanco”, ya que no es de acuerdo al interés protegido, sino de acuerdo al sujeto activo que los comete, catalogando al delincuente como persona de cierto status económico, la comisión del delito, no encuentra explicación en la pobreza, ni mala habitación, ni por carencia de recreación, etc.

Se han establecidos algunos acuerdos, tratando de solucionar las posibles implicaciones económicas de la delincuencia informática, ya que tienen carácter internacional e incluso transnacional, cuyo principal problema es la falta de una legislación unificada que, facilita la comisión de los delitos.

En 1986 la OCDE público un informe titulado Delitos de informática: análisis de la normativa jurídica, donde se reseñaban las normas legislativas vigentes y las propuestas de reforma en diversos Estados miembros y se recomendaba una lista mínima de ejemplos de uso indebido que los países podrían prohibir y sancionar en leyes penales.

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

En 1990 la Organización de las Naciones Unidas (ONU) en el Octavo Congreso sobre Prevención del Delito y Justicia Penal, celebrado 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.

Se ha determinado, que el autor de este tipo de delitos no es fácil descubrirlo ni sancionarlo, existe una indiferencia en la opinión pública sobre los daños ocasionados en la sociedad, ya que esta no los considera delincuentes, no los segrega, no los desprecia ni los desvaloriza, por el contrario, el autor se considera respetable y generalmente son sancionados con medidas de carácter administrativo y no privativos de la libertad.

Los problemas jurídicos relacionados con la Internet, se basan especialmente en los nombres de dominio y las marcas comerciales, al existir diferencias en su posesión y administración por parte de sus propietarios; de los derechos de autor, ante la imposibilidad de prohibir las reproducciones no autorizadas de trabajos y elementos de propiedad intelectual, la realización virtual de actividades altamente reguladas en los ámbitos financieros, de compra y venta de valores; al no existir fronteras ni el control adecuado sobre las incipientes instituciones mercantiles, que hacen uso de la red como sustento de su trabajo.

La legislación mexicana regula Comercial y penalmente las conductas ilícitas relacionadas con la informática, pero que aún no contemplan en sí los delitos informáticos.

La ley 111 de Patentes de Invención regula la protección a la propiedad intelectual.
La ley Penal 11723 de "La propiedad Científica, literaria y artística" ha modificado los artículos 71, 72, 72 bis, 73 y 74.
El artículo 71 tipifica como conducta ilícita a "el que de cualquier manera y en cualquier forma defraudare los derechos de propiedad intelectual que reconoce esta ley"

El Art. 72 considera casos especiales de defraudación:

El que edite, venda o reproduzca por cualquier medio o instrumento, una obra inédita o publicada sin autorización de su autor o derecho-habientes.
El que falsifique obras intelectuales, entendiéndose como tal la edición de una obra ya editada, ostentando falsamente el nombre del editor autorizado al efecto.
El que edite, venda o reproduzca una obra suprimiendo o cambiando el nombre del autor, el titulo de la misma o alterando dolosamente su texto.
El Art. 72 bis

El que con fin de lucro reproduzca un fonograma sin autorización por escrito de su productor o del licenciado del productor;
El que con el mismo fin facilite la reproducción ilícita mediante el alquiler de discos fonográficos u otros soportes materiales;
El que reproduzca copias no autorizadas por encargo de terceros mediante un precio.
El que almacene o exhiba copias ilícitas y no pueda acreditar su origen mediante la factura que lo vincule comercialmente con el productor legítimo;
El que importe las copias ilegales con miras a distribución al público.
El decreto 165/94 (B.O. del 8/2/94) incluyó al software dentro de la Ley de Propiedad Intelectual 11723.
También dentro del Código Penal encontraremos sanciones respecto de los delitos contra el honor (109 a 117); Instigación a cometer delito (209), instigación al suicidio (83); estafas (172), además de los de defraudación,

falsificación, tráfico de menores, narcortráfico, etc., todas conductas que pueden ser cometidas utilizando como medio la tecnología electrónica

El comercio electrónico desarrollo gracias a la proliferación de la Internet, los problemas más urgentes se basan en la formación del consentimiento, la seguridad acerca de las identidades de los contratantes y la prueba de las obligaciones.

Glosario

Glosario

Acceso no autorizado: Uso ilegitimo de passwords y la entrada de un sistema informático sin la autorización del propietario.

Arpa: Es el Departamento de Defensa de los Estados Unidos por la Agencia de Proyectos de Investigación Avanzada (ARPA), y cuando el sistema de DNS's comenzó a funcionar los dominios de ARPANET fueron inicialmente convertidos al nuevo sistema añadiéndoles .arpa al final.

Cibercrimen: Son actividades delictuales realizadas con la ayuda de herramientas informáticas, experimenta un fuerte apogeo a nivel internacional, que contrasta con la débil preparación de las autoridades para hacerles frente. Según el FBI, el cibercrimen plantea un importante desafío para los sectores público y privado, en todos los países.

Ciberdelitos: Actividad delictiva o abusiva relacionada con los ordenadores y las redes de comunicaciones, bien porque se utilice el ordenador como herramienta del delito, bien porque sea el sistema informático (o sus datos) el objetivo del delito.

Ciberespacio: El auge de las comunicaciones entre ordenadores cuyo máximo exponente es la macrored mundial Internet ha creado un nuevo espacio virtual, poblado por millones de datos, en el que se puede navegar infinitamente en busca de información.

Cifrado: Es un método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido, de manera que sólo pueda leerlo la persona que cuente con la clave de cifrado adecuada para descodificarlo.

Comercio Electrónico: Es un concepto generalista que engloba cualquier forma de transacción comercial o de negocios que se transmite electrónicamente usando las redes de telecomunicación y utilizando como moneda de cambio el dinero electrónico.

Delincuencia Informática: Implica actividades criminales que en un primer momento los países han tratado de encuadrar en figurar típicas de carácter tradicional, tales como robos o hurto, fraudes, falsificaciones, perjuicios, estafa, sabotaje, etcétera.

Delitos de cuello blanco: Se describe delitos no violentos cometidos por empleados de negocios o del gobierno. Algunas definiciones demandan que el supuesto delincuente se encuentre en las clases socioeconómicas medias o altas, a fin de que un delito sea considerado de cuello blanco.

Delito Electrónico: El auge del Comercio Electrónico evidencia en los tiempos actuales, que constituye un instrumento cuyo crecimiento es impresionante, sobre los cuales es necesario ejercer control que resguarde el desarrollo de la actividad Comercial que allí se efectúa.

Delitos Informáticos: Crimen genérico o crimen electrónico, que agobia con operaciones ilícitas realizadas por medio de Internet o que tienen como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet. Sin embargo, las categorías que definen un delito informático son aún mayores y complejas y pueden incluir delitos tradicionales como el fraude, el robo, chantaje, falsificación y la malversación de caudales públicos en los cuales ordenadores y redes han sido utilizados. Con el desarrollo de la programación y de Internet, los delitos informáticos se han vuelto más frecuentes y sofisticados.

Descentralizada: Puede entenderse bien como proceso (desde lo centralizado) o como forma de funcionamiento de una organización. Supone transferir el poder, (y como tal, el conocimiento y los recursos) de un gobierno central hacia autoridades que no están jerárquicamente subordinadas. La relación entre entidades descéntrales son siempre horizontales no jerárquicas.

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

Estafa: Robo de dinero o de bienes que se hace con engaño. Incumplimiento de las condiciones o promesas que se habían asegurado, especialmente en una venta o en un trato.

Firmas Digitales: Sirve para demostrar la autenticidad de un mensaje digital o de un documento electrónico. Una firma digital da al destinatario seguridad en que el mensaje fue creado por el remitente, y que no fue alterado durante la transmisión. Las firmas digitales se utilizan comúnmente para la distribución de software, transacciones financieras y en otras áreas donde es importante detectar la falsificación y la manipulación.

Hackers: Es una persona que pertenece a una de estas comunidades o subculturas distintas pero no completamente independientes

Hurto: Es el apoderamiento ilegítimo de una cosa mueble, ajena en todo o en parte, realizado sin fuerza en las cosas, ni violencia o intimidación en las personas. El hurto se considerará falta o delito en función del valor económico de lo hurtado.

Infraestructura: Es la base material de la sociedad que determina la estructura social y el desarrollo y cambio social. Incluye las fuerzas productivas y las relaciones de producción. De ella depende la superestructura, es decir, el conjunto de elementos de la vida social dependientes de la infraestructura.

Infracción al copyright de bases de datos: Uso no autorizado de información almacenada en una base de datos.

Interceptación de e-mail: Lectura de un mensaje electrónico ajeno.

Jurisdicción: (del latín juris, «decir o declarar el derecho») es la potestad, derivada de la soberanía del Estado, de aplicar el Derecho en el caso concreto, resolviendo de modo definitivo e irrevocable una controversia, que es ejercida en forma exclusiva por los tribunales de justicia integrados por jueces autónomos e independientes.

Nombre de Dominio: El propósito principal de los nombres de dominio en Internet y del sistema de nombres de dominio (DNS), es traducir las direcciones IP de cada nodo activo en la red, a términos memorizables y fáciles de encontrar.

Piratería Informática: Consiste en la distribución y/o reproducción ilegales de software. Comprar software significa en realidad comprar una licencia para usar el software, y esta licencia especifica la forma legal de usar dicho software.

Resguardos: Lugar que sirve para proteger o defender ya sea información, objetos etc.

Sabotaje: Es una acción deliberada dirigida a debilitar a un enemigo mediante la subversión, la obstrucción, la interrupción o la destrucción de material. En ocasiones, el sabotaje es utilizado como una forma de ineficiencia organizada por los trabajadores para impactar negativamente al empleador o para desinhibirse de responsabilidades de daños ocurridos a terceros.

Transferencias de fondos: Engaños en la realización de este tipo de transacciones.

Vulnerabilidad: Se entiende las características de una persona o grupo desde el punto de vista de su capacidad para anticipar, sobrevivir, resistir y recuperarse del impacto de una amenaza natural, implicando una combinación de factores que determinan el grado hasta el cual la vida y la subsistencia de alguien queda en riesgo por un evento distinto e identificable de la naturaleza o de la sociedad.

Bibliografía

Bibliografía

1. AZPILCUETA HERMILIO, Tomas. **Derecho Informático**. Editorial Abeledo-Perrot Buenos Aires Argentina 1996.
2. CÁMPOLI, Gabriel Andrés. **Derecho Penal Informático en México**. Editorial INACIPE, México 2004.
3. CARRANCÁ Y TRUJILLO, Raúl y CARRANCÁ Y RIVAS, Raúl. **Derecho Penal Mexicano. (Parte general).** Vigésima tercera edición. Editorial Porrúa. México 2007.
4. CASTELLANOS TENA, Fernando. **Lineamientos elementales de Derecho Penal*. (Parte General);*** Cuadragésima séptima edición actualizada por Horacio Sánchez Sodi, primera reimpresión. Editorial Porrúa, México 2007.
5. CORREA, CARLOS M. Carlos, **Derecho Informático.** Editorial Desalma Buenos Aires Argentina 1994.
6. CUELLO CALÓN, Eugenio. **Derecho Penal. Parte General.** Décima octava edición. Editorial Nacional. México 1980.
7. 7. HASKIN, David. **Multimedia fácil.** (Traducción. Sánchez García Gabriel). Editorial Prentice Hall. México 1995.
8. JIMÉNEZ DE ASÚA, Luis. **La Ley y el Delito.** Décima primera edición, Editorial Sudamericana, Buenos Aires Argentina. Mayo 1980.
9. JIMÉNEZ DE ASÚA, Luis. **Tratado de Derecho Penal.** Tomo III, Tercera edición actualizada. Editorial Losada, S.A. Buenos Aires 1965.
10. JIMÉNEZ HUERTA, Mariano. **Derecho Penal Mexicano.** Tomo I. Quinta edición, Editorial Porrúa. México 1992.
11. LÓPEZ BETANCOURT, Eduardo. **Teoría del delito.** Décima cuarta edición. Editorial Porrúa, México 2007.
12. MALO CANACHO, Gustavo. Derecho penal mexicano. teoría general de la ley penal. Teoría general del delito. Teoría de la culpabilidad y el sujeto responsable, teoría de la pena. Sexta edición Editorial Porrúa. México 2005.

13. MÁRQUEZ PIÑERO, Rafael. Derecho Penal. Parte General. Cuarta edición. Primera reimpresión agosto 1999. Editorial Trillas. México 2006.
14. MATEOS MUÑOZ, Agustín. COMPENDIO DE ETIMOLOGÍAS GRECO-LATINAS DEL ESPAÑOL. Editorial Esfinge. Cuadragésima sexta edición. México 2007.
15. MEZGER, Edmundo. Tratado de Derecho Penal. Tomo I. Traducción de J. Arturo Rodríguez Muñoz. Editorial Revista de Derecho Privado. Madrid España 1955.
16. MONTIEL SOSA, Juventino. Criminalística. Editorial Limusa. Segunda edición México 2007.
17. MORENO MARTÍN, Arturo. Diccionario de Informático y telecomunicaciones ingles y español. Editorial Ariel Barcelona 2001.
18. MUÑOZ CONDE, Francisco. Teoría general del delito. Segunda edición. Editorial Toblandú. 2005.
19. PAVÓN VASCONCELOS, Francisco. Manual de Derecho Penal Mexicano. Décima edición debidamente corregida y puesta al día. Editorial Porrúa. México 1991.
20. PORTE PETIT CANDAUDAP, Celestino. Apuntamientos de la parte general de Derecho Penal. Vigésima edición. Editorial Porrúa. México 2003.
21. REALE, Miguel. La Teoría Tridimensional del Derecho. (Una división integral del Derecho). Traducción e introducción de Ángeles Mateos, Licenciada en Filosofía y doctora en Derecho. Editorial Tecnos. España 1997.
22. REYNOSO DÁVILA, Roberto. Teoría general del delito. Sexta edición. Editorial Porrúa. México 2006.
23. RODAO, Jesús de Marcelo. Piratas cibernéticos. cyberwars, seguridad Informática e Internet. Editorial- Ra-ma. España 2005.
24. ROJAS AMANDI, Víctor Manuel. El uso de la Internet en el derecho. Segunda Edición. Editorial Oxford, México 2001.
25. TÉLLEZ VALDÉS, Julio. Derecho Informático. Tercera Edición. Editorial Mc Graw Hill, México 2003.
26. TORRES LÓPEZ, Mario Alberto; Las leyes penales. Editorial Porrúa. Quinta Edición. México 2005.

27. VILLALOBOS, Ignacio. Derecho Penal Mexicano. Quinta edición. Editorial Porrúa. México 1990.
28. ZAFFARONI EUGENIO, Raúl. **Manual de Derecho Penal.** Segunda edición. Editorial Cárdenas. México 2007.

Medios Electrónicos

1. LA HISTORIA QUE LLEVO A CONSTRUIR LA PRIMERA COMPUTADORA.com/trabajos14/histcomput/histcomput2.shtml
2. http://es.wikipedia.org/wiki/Internet#Historia
3. CASTILLO GARCÍA, Gustavo. Internet es usada ya por *narcos* para comprar armamento: PGR La Jornada http://www.jornada.unam.mx/2005/06/13/012n1pol.php
4. GUTIÉRREZ CORTÉS, Fernando e ISLAS CARMONA, Octavio. Apuntes académicos para una historia de internet en México .www.mexicanadecomunicacion.com.mx/tables/FMB/foromex/apuntes.html.
5. TREJO GARCÍA, Elma del Carmen. Regulación jurídica de Internet. Servicio de Investigación y Análisis, subdirección de Política Exterior, Cámara de Diputados. http://www.diputados.gob.mx/cedia/sia/spe/SPE-ISS-12-06.pdf
6. Internet Socity. HISTORIA DE LA INTERNET EN MÉXICO. http://www.isocmex.org.mx/historia.html