UNIVERSIDAD DE SOTAVENTO A.C.

ESTUDIOS INCORPORADOS A LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INFORMÁTICA

"IMPACTO Y PREVENCIÓN DE DELITOS INFORMÁTICOS EN LA ORGANIZACIÓN"

TESIS PROFESIONAL

QUE PARA OBTENER EL TÍTULO DE:

LICENCIADO EN INFORMÁTICA

PRESENTA:

CÉSAR GARCÍA MORALES

ASESOR DE TESIS:

LIC. RAÚL DE JESÚS OCAMPO COLÍN

Coatzacoalcos, Veracruz. **Marzo 2009.**

AGRADECIMIENTOS

Gracias a Dios

Por permitirme llegar hasta este momento tan importante de mi vida, por lograr otra meta más en mi carrera y por llenarme de dicha y bendiciones.

Gracias a mis padres y hermano

A quienes agradezco por soportarme excesivamente, por su comprensión, paciencia y apoyo sin condiciones ni medida. En todo momento los llevo conmigo y se que cuento con ellos siempre.

Gracias a cada uno de los maestros

Que participaron en mi desarrollo profesional durante mi carrera. Sin su ayuda, disposición y conocimientos no estaría en donde me encuentro ahora.

Gracias a todos mis amigos

Que estuvieron conmigo y compartimos tantas aventuras, experiencias, fiestas, desveladas, triunfos y fracasos, gracias por su confianza y lealtad. Gracias a cada uno por hacer que mi estancia en la universidad fuera súper divertida.

Índice

PROBLEMA

¿Cuáles son los efectos que producen los delitos informáticos en una organización y sus principales medidas de prevención?

HIPÓTESIS

Debido a la problemática de los delitos informáticos las organizaciones están en riesgo de perder información valiosa además de tener pérdidas económicas y genera desconfianza en ciertas personas para el uso de las herramientas informáticas.

OBJETIVOS

Objetivo General:

- Realizar una investigación acerca del fenómeno de los delitos informáticos, analizando el impacto de éstos en cualquier tipo de organización o empresa.

Objetivos Particulares:

- Conceptualizar la naturaleza de los delitos informáticos.
- Definir las características de este tipo de delitos.
- Tipificar los delitos informáticos de acuerdo a sus características principales.
- Investigar el impacto de éstos actos en la vida social y tecnológica de las personas.
- Analizar las consideraciones oportunas en el tratamiento de los delitos informáticos.
- Mencionar la legislatura que enmarca a ésta clase de delitos, y la forma en que se sancionan desde un contexto nacional.
- Presentar posibles medidas de prevención de este tipo de delitos.

JUSTIFICACIÓN

Esta tesis profesional se realiza para cubrir los requerimientos del protocolo de titulación en la facultad de Informática de la Universidad de Sotavento A.C., la cual tiene como finalidad guiar al alumno a la obtención de su titulo profesional.

MARCO TEÓRICO Y CONCEPTUAL

El delito informático implica actividades criminales que los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robos, hurtos, fraudes, falsificaciones, perjuicios, estafas, sabotajes. Sin embargo, debe destacarse que el uso de las técnicas informáticas ha creado nuevas posibilidades del uso indebido de las computadoras lo que ha creado la necesidad de regulación por parte del derecho.

Se considera que no existe una definición formal y universal de delito informático pero se han formulado conceptos respondiendo a realidades nacionales concretas: "no es labor fácil dar un concepto sobre delitos informáticos, en razón de que su misma denominación alude a una situación muy especial, ya que para hablar de "delitos" en el sentido de acciones típicas, es decir tipificadas o contempladas en textos jurídicos penales, se requiere que la expresión "delitos informáticos" esté consignada en los códigos penales, lo cual en nuestro país, al igual que en otros muchos no han sido objeto de tipificación aún." *(1)*

En 1983, la Organización e Cooperación y Desarrollo Económico (OCDE) inicio un estudio de las posibilidades de aplicar y armonizar en el plano internacional las leyes penales a fin e luchar contra el problema del uso indebido de los programas computacionales.

En 1992 la Asociación Internacional de Derecho Penal, durante el coloquio celebrado en Wurzburgo (Alemania), adoptó diversas recomendaciones respecto a los delitos informáticos, entre ellas que, en la medida que el Derecho Penal no sea suficiente, deberá promoverse la modificación de la definición de los delitos existentes o la creación de otros nuevos, si no basta con la adopción de otras medidas como por ejemplo el "principio de subsidiariedad".

(1) TÉLLES VALDEZ, Julio. Derecho Informático. 2° Edición. Mc Graw Hill. México. 1996 Pág. 103-104

Se entiende Delito como: "acción penada por las leyes por realizarse en perjuicio de algo o alguien, o por ser contraria a lo establecido por aquéllas". *(2)*

Finalmente la OCDE publicó un estudio sobre delitos informáticos y el análisis de la normativa jurídica en donde se reseñan las normas legislativas vigentes y se define Delito Informático como "cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático de datos y/o transmisiones de datos." *(3)*

"Los delitos informáticos se realizan necesariamente con la ayuda de los sistemas informáticos, pero tienen como objeto del injusto la información en sí misma". *(4)*

Adicionalmente, la OCDE elaboró un conjunto de normas para la seguridad de los sistemas de información, con la intención de ofrecer las bases para que los distintos países pudieran erigir un marco de seguridad para los sistemas informáticos.

1. En esta delincuencia se trata con especialistas capaces de efectuar el crimen y borrar toda huella de los hechos, resultando, muchas veces, imposible de deducir como es como se realizó dicho delito. La Informática reúne características que la convierten en un medio idóneo para la comisión de nuevos tipos de delitos que en gran parte del mundo ni siquiera han podido ser catalogados.
2. La legislación sobre sistemas informáticos debería perseguir acercarse lo más posible a los distintos medios de protección ya existentes, pero creando una nueva regulación basada en los aspectos del objeto a proteger: la información.

(2) MOLINER, María. Diccionario de María Moliner Edición Digital. Copyright© 1996 Novel Inc.; Copyright © 1996 María Moliner.

(3) Definición elaborada por un Grupo de Expertos, invitados por la OCDE a París en Mayo de 1993.

(4) CARRION, Hugo Daniel. Tesis "Presupuestos para la Punibilidad del Hacking". Julio 2001.

En este punto debe hacerse un punto y notar lo siguiente:

- No es la computadora la que atenta contra el hombre, es el hombre el que encontró una nueva herramienta, quizás la más poderosa hasta el momento, para delinquir.
- No es la computadora la que afecta nuestra vida privada, sino el aprovechamiento que hacen ciertos individuos de los datos que ellas contienen.
- La humanidad no está frente al peligro de la informática sino frente a individuos sin escrúpulos con aspiraciones de obtener el poder que significa el conocimiento.
- Por eso la amenaza futura será directamente proporcional a los adelantos de las tecnologías informáticas.
- La protección de los sistemas informáticos puede abordarse desde distintos perspectivas: civil, comercial o administrativa.

Lo que se deberá intentar es que ninguna de ellas sea excluyente con las demás y, todo lo contrario, lograr una protección global desde los distintos sectores para alcanzar cierta eficiencia en la defensa de estos sistemas informáticos.

Julio Téllez Valdez clasifica a los delitos informáticos en base a dos criterios:

1. Como instrumento o medio: se tienen a las conductas criminales que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito.

Ejemplos:

- Falsificación de documentos vía computarizada: tarjetas de créditos, cheques, etc.
- Variación de la situación contable.
- Planeamiento y simulación de delitos convencionales como robo, homicidio y fraude.
- Alteración el funcionamiento normal de un sistema mediante la introducción de código extraño al mismo: virus, bombas lógicas, etc.
- Intervención de líneas de comunicación de datos o teleprocesos.

2. Como fin u objetivo: se enmarcan las conductas criminales que van dirigidas en contra de la computadora, accesorios o programas como entidad física.

Ejemplos:

- Instrucciones que producen un bloqueo parcial o total del sistema.
- Destrucción de programas por cualquier método.
- Atentado físico contra la computadora, sus accesorios o sus medios de comunicación.
- Secuestro de soportes magnéticos con información valiosa, para ser utilizada con fines delictivos.

María Luz Lima, por su parte, presenta la siguiente clasificación de "delitos electrónicos" *(5)*:

1. Como Método: conductas criminales en donde los individuos utilizan métodos electrónicos para llegar a un resultado ilícito.
2. Como Medio: conductas criminales en donde para realizar un delito utilizan una computadora como medio o símbolo.
3. Como Fin: conductas criminales dirigidas contra la entidad física del objeto o máquina electrónica o su material con objeto de dañarla.

(5) LIMA de la LUZ, María. Criminalia N° 1-6 Año L. Delitos Electrónicos. Ediciones Porrua. México. Enero-Julio 1984.

Introducción

A nadie escapa la enorme influencia que ha alcanzado la informática en la vida diaria de las personas y organizaciones, y la importancia que tiene su progreso para el desarrollo de un país. Las transacciones comerciales, la comunicación, los procesos industriales, las investigaciones, la seguridad, la sanidad, etc. son todos aspectos que dependen cada día más de un adecuado desarrollo de la tecnología informática.

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.

Junto al avance de la tecnología informática y su influencia en casi todas las áreas de la vida social, ha surgido una serie de comportamientos ilícitos denominados, de manera genérica, delitos informáticos.

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

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

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.

Capitulo I

Conceptualización y generalidades.

1.1 Concepto de Fraude y Delito.

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 Intima conexión que existe entre vida social y jurídica de cada sociedad y cada siglo, ya que ambas se condicionan Íntimamente.

El articulo 110 del Código Penal dice que "Son delitos y faltas las acciones u omisiones dolosas o culposas penadas por la ley".

Esta noción de delito es especialmente formal, y no define cuáles 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 o poner 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 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 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 revelación de secretos.

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

1.2 Definición de delito informático.

El delito Informático implica actividades criminales que un primer momento los países han tratado de encuadrar 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 una concepto propio de los llamados delitos informáticos. 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 criminal en el cual la computadora ha estado involucrada como material o como objeto de la acción criminógenea, o como mero símbolo“.

“Aquel que se da con la ayuda de la informática o de 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 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 informático".

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

"Aquél que está 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 ésta, pudiendo presentar m6ltiples formas de lesión de variados bienes jurídicos"

"La realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada 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 seg6n la ley penal vigente realizados con el empleo de un equipo automático de procesamiento de datos".

"Cualquier 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 alg6n 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"

"Es cualquier acto ilegal ejecutado 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.

1.3 Terminología sobre delitos informáticos

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 con la computadora", "delincuencia informática", "criminalidad informática", "abuso informático", "computer crime".

1.4 Delitos informáticos vs. Ataques informáticos

- Delito informático. Es la conducta típica, antijurídica, culpable y punible, en que se tiene a las computadoras como instrumento o fin.
- Ataque informático. Es la conducta inapropiada que también causa daños informáticos pero no esta contemplada en la legislación.

1.5 ¿Quienes NO deben preocuparse en absoluto por los delitos informáticos?

- Los que nunca se conectan a Internet, ni tienen una computadora.
- Los que no tienen cuentas bancarias.
- Los que no usan tarjetas de crédito.
- Los que no usan celulares, teléfonos u otros medios de comunicación.
- Los que no manejan, usan trenes o aviones.
- Los que no hacen compras.
- Los que no necesitan energía eléctrica, agua, gas, etc.

1.6 Características de los delitos informáticos.

- Sólo una determinada cantidad de personas (con conocimientos técnicos por encima de lo normal) pueden llegar a cometerlos.
- Son conductas criminales del tipo "cuello blanco": no de acuerdo al interés protegido (como en los delitos convencionales) sino de acuerdo al sujeto que los comete. Generalmente este sujeto tiene cierto status socioeconómico y la comisión del delito no puede explicarse por pobreza, carencia de recursos, baja educación, poca inteligencia, ni por inestabilidad emocional.
- Son acciones ocupacionales, ya que generalmente se realizan cuando el sujeto atacado se encuentra trabajando.
- Son acciones de oportunidad, ya que se aprovecha una ocasión creada por el atacante.
- Provocan pérdidas económicas.

- Ofrecen posibilidades de tiempo y espacio.
- Son muchos los casos y pocas las denuncias, y todo ello por la falta de regulación y por miedo al descrédito de la organización atacada.
- Presentan grandes dificultades para su comprobación, por su carácter técnico.
- Tienden a proliferar, por lo se requiere su urgente regulación legal.

1.7 El Delincuente y la víctima

1.7.1 Sujeto Activo

Se llama así a las personas que cometen los delitos informáticos**.** Son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, aún cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos.

Con el tiempo se ha podido comprobar que los autores de los delitos informáticos son muy diversos y que lo que los diferencia entre sí es la naturaleza de los 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 el nivel de aptitudes no es indicador de delincuencia informática en tanto que otros aducen que los posibles delincuentes informáticos son personas listas, decididas, motivadas y dispuestas a aceptar un reto tecnológico, características que pudieran encontrarse en un empleado del sector de procesamiento de datos.

Sin embargo, teniendo en cuenta las características ya mencionadas de las personas que cometen los delitos informáticos, estudiosos en la materia los han catalogado como delitos de "cuello blanco" término introducido por primera vez por el criminólogo norteamericano Edwin Sutherland en el año de 1943.

La "cifra negra" es muy alta; no es fácil descubrirlos ni sancionarlos, en razón del poder económico de quienes lo cometen, pero los daños económicos son altísimos; existe una gran indiferencia de la opinión pública sobre los daños ocasionados a la sociedad. A los sujetos que cometen este tipo de delitos no se considera delincuentes, no se los segrega, no se los desprecia, ni se los desvaloriza; por el contrario, es considerado y se considera a sí mismo "respetable". Estos tipos de delitos, generalmente, son objeto de medidas o sanciones de carácter administrativo y no privativas de la libertad.

1.7.2 Sujeto Pasivo

Este, la víctima del delito, es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo. Las víctimas pueden ser individuos, instituciones crediticias, instituciones militares, gobiernos, etc. que usan sistemas automatizados de información, generalmente conectados a otros.

El sujeto pasivo del delito que nos ocupa, es sumamente importante para el estudio de los delitos informáticos, ya que mediante él podemos conocer los diferentes ilícitos que cometen los delincuentes informáticos.

Es imposible conocer la verdadera magnitud de los delitos informáticos, ya que la mayor parte 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; el temor por parte de las empresas de denunciar este tipo de ilícitos por el desprestigio que esto pudiera ocasionar a su empresa y las consecuentes pérdidas económicas, trae como consecuencia que las estadísticas sobre este tipo de conductas se mantenga bajo la llamada "cifra negra".

1.8 Sus causas:

Si tomamos las acciones que se producen en Internet como todas aquellas que vulneran la privacidad de determinados datos, y las conductas perjudiciales que se efectivizan utilizando el medio informático en general, vemos que su causa puede obedecer a factores:

Familiares:

El nivel social al que pertenecen los sujetos que pueblan el mundo de la informática, por lo general es de medio a alto por cuanto provienen de una extracción que les pudo proporcionar estas herramientas para alcanzar las metas que la cultura social les estaba proponiendo.

Así el acceso a esta tecnología no es propio de zonas marginales en las que, pese a los denodados esfuerzos gubernamentales de lograr llevar la computación (y el uso de Internet) hacia todos los rincones del país y del mundo, no es fácil aún encontrar a niños del Altiplano accediendo a ellos.

Sociales:

La tendencia al agrupamiento o formación de "grupos económicos" en continua expansión y la globalización de la economía son factores que dieron plafón al crecimiento de la informática y paralelamente la aparición de Internet con las ventajas que ello les ofrecía, en una palabra el progreso tecnológico de las comunicaciones permitieron transacciones que, en segundos conllevaron a un mayor poder económico y político extranacional.

Desde que surge el auge de la informática es notorio que todo aquél que desconoce el manejo de una computadora cae en la obsolencia y ya desde muy pequeños se les inculca a los niños sobre este tema que a su vez por las características técnicas que presenta requiere de ciertas condiciones de aptitud para encararlas y que facilitan la agilidad mental, de modo que va haciendo nacer en el sujeto el deseo de ser ese prototipo del ideal actual de la comunidad.

1.9 Sus Objetivos:

- La posibilidad de obtener beneficios, que pueden no ser económicos, en los que está presente el factor "poder" que involucra este manipuleo de personas y/o entes.
- La asunción desinhibida de riesgos que ello implica.
- Las débiles o escasas consecuencias jurídicas, o bien dicho la falta de impunidad de que gozan la mayoría casi siempre y que circunscriben el terreno a las simples maniobras o a "hechos" de consecuencias a veces civiles.

Capitulo II

Privacidad en Internet

Un aspecto importante de Internet, es que nadie puede poseerla ni es posible controlarla, factor que influye mucho en el grado de apertura y valor de Internet pero también deja muchos puntos a juicio del propio usuario, tanto por los emisores como para los receptores de información. La privacidad en Internet dependerá del tipo de actividad que se realice. Las actividades que se pueden suponer privadas en realidad no lo son, ya que no existe ninguna actividad en línea que garantice la absoluta privacidad. Como ejemplo, encontramos los foros, donde cualquier persona puede capturar, copiar y almacenar todo lo que se escriba; su nombre, correo electrónico e incluso información sobre su proveedor de Internet figuran en el mensaje mismo, o las listas de distribución, donde existen algunas funciones que permiten que los mensajes sean distribuidos a múltiples usuarios. Además, la cuenta con un proveedor de Internet es privada, la mayoría de estos proveedores dan a conocer públicamente información sobre sus usuarios. Otros ejemplos serían los registros de un sitio, ya que muchas personas obtienen su propio sitio en Internet, y estos registros son información pública.

La mayor parte de la gente cree que navegar por Internet es una actividad anónima, y en realidad no lo es. Prácticamente todo lo que se transmite por Internet puede archivarse, incluso los mensajes en foros o los archivos que consulta y las páginas que se visitan, mediante dispositivos como cookies, "bichos cibernéticos", los usos de la mercadotecnia y el spam y los navegadores. Los proveedores de Internet y los operadores de sitios tienen la capacidad de recopilar dicha información. Y los piratas o hackers pueden obtener acceso a su computadora, ya que un gran número de usuarios está conectado a Internet por medio de módems de cable y conexiones DSL a base de una línea telefónica. La vulnerabilidad a los ataques de hackers, se agudiza cuando los usuarios utilizan el servicio de broadband, es decir que están "siempre conectados".

Cuando los usuarios emiten información en Internet tiene los mismos derechos y obligaciones que otros autores con los derechos de copyright y sus posibles infracciones, difamaciones, etc. Si los usuarios emiten información a través de Internet deberán tener en cuenta que no se puede revisar, editar, censurar o tomar responsabilidades por cualquier tipo de información que se pueda crear, y por lo tanto

la única solución es tomar pequeñas medidas de seguridad, en una gran red donde la información corre a gran velocidad y puede alcanzar a un gran número de personas.

2.1 ¿Qué es la privacidad?

La privacidad es el interés que los individuos tienen en sostener un espacio personal, libre de interferencias con otras personas y organizaciones.

2.2 Temas relacionados con la privacidad:

- Privacidad de información
- Privacidad en Internet
- Privacidad de Personas
- Privacidad del Comportamiento Personal
- Privacidad de Comunicación Personal
- Privacidad de Datos Personales

2.2.1 Privacidad de información

Es el interés que un individuo tiene en controlar, o por lo menos influenciar, el manejo de datos de ellos mismos.

2.2.2 Privacidad en Internet

Se puede subdividir en cuatro materias de estudio:

- El correo electrónico (email)
- La criptografía
- La esteganografía
- El anonimato

El correo electrónico

Internet está formado por varios miles de redes de ordenadores pertenecientes a entidades muy diversas.

Los mensajes de correo viajan por la red a través de decenas de servidores de correo distintos pudiendo dejar copia de estos mensajes en cada uno de ellos.

La criptografía

La Criptografía consiste en alterar los datos de un mensaje con una clave (en caso informático, formada por un conjunto de números) de tal manera que queda ilegible, y el proceso inverso para recuperar el mensaje original sólo puede realizarse recombinando el mensaje alterado con esa clave.

La esteganografía:

Podemos definir a la esteganografía como un conjunto de técnicas destinadas a ocultar unos datos en otros, de tal manera que pase desapercibida su existencia.

Existen determinados ámbitos en los que el uso de criptografía para simplemente proteger datos privados puede parecer sospechoso.

El anonimato

La procedencia de un mensaje de correo electrónico, es, con determinados medios, fácilmente rastreable.

En determinadas situaciones, puede que la gente necesite que su correo electrónico sea enviado de forma anónimo, sin poder saberse quién emitió el mensaje. Esta necesidad es cubierta por los remailers anónimos.

2.2.3 Privacidad de personas

La privacidad de la persona, designada a veces como aislamiento corporal se refiere a la integridad del cuerpo del individuo.

Las ediciones incluyen la inmunización obligatoria, la transfusión de sangre sin consentimiento, la disposición obligatoria de muestras de los fluidos corporales y del tejido fino del cuerpo, y la esterilización obligatoria.

2.2.4 Privacidad del comportamiento personal

Esto se relaciona con todos los aspectos del comportamiento, pero especialmente con las materias sensibles, tales como preferencias y hábitos sexuales, actividades políticas y prácticas religiosas, en lugares privados y en públicos.

2.2.5 Privacidad de comunicación personal

Los individuos demandan un enteres en poder comunicarse entre si mismos, usando varios medios, sin vigilar lo rutinario de sus comunicaciones por otras personas u organizaciones.

2.2.6 Privacidad de datos personales

Los individuos demandan que los datos sobre si mismos no deben estar automáticamente disponibles para otros individuos y organizaciones, y que, bases de datos donde estos son poseídos por otro partido, el individuo debe poder ejercitar un grado substancial de control referente a esos datos y su uso

2.3 Monitoreo y rastreo de la actividad en Internet

¿Pueden las compañías que ofrecen servicio de Internet consultar y archivar mi actividad en línea?

Sí. Mucha gente asume que navegar por Internet es una actividad anónima. *No lo es*. Casi todo lo que se transmite por Internet puede archivarse, incluso los mensajes en foros o los archivos que consulta el subscriptor y las páginas que visita. Los

proveedores de Internet y los operadores de sitios tienen la capacidad de recopilar dicha información.

Cookies. Muchos sitios de Internet depositan en su disco duro bloques de información conocidos como *cookies,* o galletas, que contienen datos sobre su visita a una determinada página electrónica. Cuando usted regresa al sitio, la información contenida en la galleta reconocerá sus datos. El sitio entonces podrá ofrecerle productos o publicidad de acuerdo a sus intereses personales, con base en el contenido de la galleta.

La mayoría de las galletas son utilizadas sólo por el sitio que colocó dicha información en su computadora. Sin embargo, existen galletas de terceras personas que transmiten información suya a compañías de publicidad. Estos negocios comparten sus datos con otras compañías publicitarias. Su navegador de Internet le ofrece a usted la capacidad de detectar y borras galletas, incluyendo aquellas de terceras personas.

Bichos cibernéticos. Un bicho cibernético o *web bug* es una gráfica en un sitio o un mensaje electrónico "mejorado" que permite a terceras personas monitorear quién consultó el mensaje o la página. La gráfica puede ser de un tamaño fácilmente visible o casi invisible, del tamaño de un píxel. A los correos electrónicos que incluyen gráficas como páginas de Internet se les conoce como mensajes mejorados, o también son conocidos como correos estilizados o de HTML. El bicho cibernético puede confirmar cuando usted consulta un mensaje o visita una página y archivar la información, incluso la dirección IP del usuario. La dirección IP de un usuario es un número de varios dígitos que identifica a todos los aparatos conectados al Internet, como su computadora y la impresora.

Usted puede evitar los bichos cibernéticos si lee sus correos mientras está desconectado de Internet. Esta opción la ofrecen la mayoría de los programas. Otra opción es instalar un programa que detecta los bichos.

Los usos de la mercadotecnia y el *spam.* La información sobre los patrones de conducta de las personas que navegan por Internet es una valiosa y potencial fuente de ingresos para operadores de servicios de Internet y administradores de sitios. Los comerciantes pueden utilizar dicha información para desarrollar listas específicas de usuarios con gustos y comportamientos similares. Esta información también puede resultar en correos electrónicos no solicitados conocidos como spam. Asimismo, esta información puede resultar penosa para los usuarios que han consultado sitios controversiales o delicados.

Navegadores. Es importante estar al tanto de la información que transmiten a computadoras remotas los programas que usted utiliza para navegar por Internet. Los navegadores más utilizados son Firefox y Microsoft Internet Explorer.

La mayoría de los navegadores dan a conocer a los administradores de sitios información sobre su proveedor de servicio de Internet y otras páginas que usted ha visitado. Algunos navegadores, especialmente aquellos que no cuentan con las nuevas medidas de seguridad, son susceptibles de dar a conocer el correo electrónico de un usuario, teléfono y otra información contenida en su "agenda", en el caso de que el navegador también trabaje en conjunto con su correo electrónico.

Política de privacidad y sellos cibernéticos. La Comisión Federal de Comercio (Federal Trade Commission) recomienda a los administradores de todo sitio comercial que den a conocer su política de privacidad en su página de Internet. La mayoría de los sitios cuentan con información sobre sus prácticas de recaudación de información.

Monitoreo en el trabajo. Las personas con acceso al Internet en el trabajo deben estar conscientes de que los empleadores rastrean cada vez más los sitios que visitan sus empleados. Asegúrese de verificar la política de privacidad de su compañía. Recomiende que se desarrolle una en el caso de que no exista.

El acceso de las autoridades. Las autoridades pueden obtener acceso a los archivos con la información de los suscriptores con una orden judicial que demuestre que los datos son relevantes en una investigación criminal vigente. Esta ley previene

que las autoridades la utilicen para llevar a cabo "expediciones de pesca", en donde los funcionarios de gobierno esperan encontrar por accidente violaciones a la ley.

¿Pueden las compañías cibernéticas consultar información almacenada en mi computadora sin que yo me dé cuenta?

Sí. Numerosos proveedores comerciales de Internet como AOL descargan automáticamente gráficas y programas nuevos en la computadora del usuario. En estos casos se le notifica al suscriptor. Sin embargo, existen otras intrusiones no tan claras. Algunos reportajes noticiosos han documentado que algunos proveedores han admitido, tanto accidental como intencionalmente, haber entrado a los sistemas duros de computadoras personales. Las compañías por lo general justifican dichas prácticas como una manera de mejorar el servicio al cliente.

Es difícil detectar este tipo de intrusiones. Es responsabilidad suya estar consciente de este potencial abuso a la privacidad e investigar ampliamente sobre cualquier servicio antes de suscribirse. Asegúrese siempre de leer la política de privacidad y el contrato de cualquier servicio que usted pretende utilizar.

¿Pueden los piratas obtener acceso a mi computadora?

Un creciente número de usuarios está conectado al Internet por medio de módems de cable y conexiones DSL a base de una línea telefónica. La vulnerabilidad a los ataques de piratas, o *hackers,* se agudiza cuando los usuarios utilizan el servicio de *broadband,* es decir que están "siempre conectados". Aconsejamos el uso de "paredes de fuego" para monitorear la actividad en la red y limitarla sólo a las actividades autorizadas. También debe consultarse la página de Internet del proveedor para proteger su computadora desconectando programas innecesarios e instalando nuevas medidas de seguridad.

¿Cuáles son los artefactos espía y cómo puedo saber si están instalados en mi computadora?

Los artefactos espía son programas o aparatos que rastrean la actividad electrónica. Las compañías de software instalaron este tipo de programas en las computadoras para obtener más ingresos. Hay dos tipos de programas: de "monitoreo" y de "diagnóstico". El primero fue diseñado para que empleadores y padres de familia pudieran monitorear la actividad electrónica de sus subordinados e hijos, respectivamente. El servicio se utilizó para otorgar acceso a documentos por medio de contraseñas y para evitar el uso inapropiado de la red. Los programas de "diagnóstico" son utilizados por compañías de software para archivar errores y hábitos de uso para mejorar la siguiente generación del software. El usuario, sin embargo, desconoce el hecho de que este tipo de programas estén instalados en su computadora. La sección de Recursos Adicionales al final de esta guía provee información sobre cómo localizar y quitar este tipo de programas.

2.4 Consejos para salvaguardar la privacidad en Internet

- Su cuenta está tan protegida como su contraseña lo permita. Elija contraseñas que no tengan sentido utilizando una combinación de palabras mayúsculas, minúsculas, números y símbolos, como tY8%uX. No utilice la misma contraseña - o variaciones de la misma - en otros programas. Una manera de crear una contraseña fácil de recordar es utilizar la primera y última letra de su poema favorito. Utilice números y símbolos de puntuación entre las letras. "Blanca nieves y los siete enanos" sería b*ni7en$s.
- Cambie su contraseña con frecuencia. No permita que otras personas lo observen teclear su contraseña. No escriba su contraseña ni coloque dicha información en su monitor. Si debe de escribir su contraseña, tome medidas para esconder la información.
- Consulte la política de privacidad del proveedor de Internet que utilice. La mayoría de estos proveedores dan a conocer su política de privacidad en sus

sitios electrónicos o en otros tipos de documentación. Cuando esté consultando el Internet, busque las políticas de privacidad de las páginas que visite.

- Revise los ajustes de *galletas* o *cookies.* Ya pasó la época en que los navegadores escondían sus galletas sin opción para los usuarios. Hoy usted puede aceptar, rechazar o seleccionar las galletas de las páginas en las cuales usted está interesado. Tenga cuidado cuando modifique sus galletas ya que puede borrar algunas de sitios en los que usted confía. Es posible crear una función que limite las galletas de sitios que usted no conoce.
- Suponga que toda comunicación en Internet *no es privada* a menos que utilice programas decodificadores especiales (encryption programs). Sin embargo, la mayor parte de los programas decodificadores son difíciles de manejar y puede resultar problemático. Si no utiliza estos programas, recomendamos que por lo menos tome las siguientes precauciones: No dé información personal, teléfono, contraseña, dirección, número de tarjeta de crédito, de Seguro Social, información sobre su salud, fecha de nacimiento, etcétera en los cuartos de chateo, foros, correos electrónicos o biografías cibernéticas).
- Tenga cuidado con software que se carga automáticamente y que lo inscribe a su lista de usuarios. Por lo general, estos programas solicitan información personal como datos financieros y después descargan esta información en el servicio. Estos programas pudieran tener la capacidad de consultar los archivos de su computadora sin que usted se dé cuenta. Contacte a estos servicios para utilizar otros métodos de suscripción.
- Tome en cuenta que cualquier mensaje que usted teclee en Internet puede ser archivado y grabado. Es posible buscar y descubrir mensajes que alguien ha colocado en foros. Antes de teclear algo, pregúntese si le gustaría *quedar ligado* a su mensaje público, ya sea por un empleador, un familiar o un comerciante. Utilice un seudónimo o un correo electrónico anónimo cuando participe en foros públicos. Considere obtener una dirección electrónica por medio de proveedores gratis como www.hotmail.com o www.yahoo.com. Registre un correo electrónico que no lo identifique y utilícelo cuando participe en foros públicos.

- Utilizar el comando "borrar" o "delete" no significa que su correo desaparecerá ya que aún puede consultarse por medio de programas de copias de seguridad. Algunos programas pueden consultar mensajes borrados de su disco duro. Si usted desea borrar permanentemente mensajes y otros documentos de su computadora, considere utilizar programas gratuitos como los que se encuentran en http://cleanup.stevengould.org/ u otros programas generales como Norton's CleansSweep (http://www.symantec.com/sabu/ncs/) o Helix Software's Nuts & Bolts (http://www.helixsoftware.com).
- Su biografía en Internet. Si usted crea una, considere que podrá ser consultada por cualquiera. Es mejor no crear una biografía si por alguna razón usted debe de salvaguardar su identidad. Solicite a su proveedor de Internet que lo excluya de su directorio electrónico.
- Tome en cuenta que si usted publica información personal en su página de Internet, los comerciantes y otros podrán obtener su dirección, número telefónico, correo electrónico y otra información que usted provea. Si está preocupado por su privacidad, sea discreto en su página de Internet.
- Esté consciente de los peligros sociales que existen en Internet: acosos, vergüenzas, ataques verbales o ser víctima de correos spam (mensajes no solicitados). Las mujeres pueden quedar vulnerables si el nombre de su correo electrónico puede distinguirse como femenino. Considere utilizar seudónimos y direcciones electrónicas que no indiquen su sexo.
- Si sus hijos utilizan el Internet, asegúrese de enseñarles los usos apropiados para salvaguardar la privacidad. Hágales saber de los peligros de dar a conocer información sobre ellos mismos y su familia
- Utilice sólo sitios seguros cuando transmita información sensible por Internet. Asegúrese de que la transmisión sea segura cuando utilice su tarjeta de crédito en un sitio de compras. Busque un candado cerrado en la parte inferior derecha de su página. Asimismo, asegúrese de que la dirección electrónica de la página contenga una "s" después del http en la parte superior de la página.
- Esté consciente de las actividades en línea que dejan huellas electrónicas. Su proveedor de Internet puede determinar qué tipo de buscadores utiliza, qué tipos de sitios visita y la fecha, hora y duración de sus sesiones en Internet. Los

administradores de los sitios pueden monitorear sus actividades colocando galletas en su computadora. Pueden obtener más información suya si usted se registra en su sitio. Su navegador también puede transmitir información a otros sitios.

- Usted puede evitar dejar huellas al utilizar servicios de "anonimato". Aproveche las herramientas disponibles para proteger su privacidad, conocidas generalmente como tecnologías de protección a la privacidad. Aquí se ofrecen explicaciones sobre codificadores, *anonymous remailers* o correos anónimos, servicios de surfeo en el anonimato y protección de información almacenada.
- Codificación. Es un método capaz de codificar un correo electrónico o un documento de manera en que sólo las personas indicadas puedan decodificarlo y leerlo. Este método permite a los usuarios codificar información privada, transmitirla, almacenarla y difundirla sin la preocupación de que sea leída por otras personas.
- Correos anónimos. Es relativamente fácil determinar el nombre y dirección electrónica de cualquier persona que trasmite un correo electrónico o que participa en un foro público. Existe un programa llamado "anonymous remailers" que consiste en recibir un mensaje electrónico, quitar información que pudiera identificar a un usuario, y mandarlo a su destino apropiado.
- Servicios anónimos para navegar por Internet: Estos servicios combinan las funciones de "remailers", direcciones electrónicas desechables y aquellas de servidores "proxy" para esconder su identidad y transferir información entre su navegador y una página de Internet.
- Software para proteger y almacenar información. Los programas de seguridad ayudan a prevenir el acceso no autorizado a documentos dentro de su computadora. Por ejemplo, existen algunos programas que codifican todos los directorios de su computadora con diferentes contraseñas para que sólo la persona indicada pueda abrirlos. Estos programas pueden incluir "rastreadores" que archivan toda actividad en el disco duro de su computadora.

- Instalar un cortafuegos ayudara mucho evitando que un sujeto pueda entrar a nuestra computadora o bien que usen un troyano y quizá pueda robar información valiosa como numero de tarjetas de crédito o claves, etc.
- Un antivirus que en lo posible también detecte spyware servirá mucho para evitar que nos manden troyanos o spyware que envíe información confidencial aunque si tenemos un firewall es probable que este bloquee el troyano/spyware al tratar de conectarse.
- Un antispyware que ayuda a eliminar el spyware que entro a través de distintas páginas.
- Usar un explorador alternativo a Internet Explorer o bien mantenerlo actualizado completamente.
- Mantener actualizado nuestro sistema operativo es importante para evitar que a través de un fallo del mismo alguien se pueda apoderar de nuestra computadora y posteriormente de algo valioso.
- No entrar en páginas Web sospechosas de robar contraseñas o de mandar virus/spyware al PC.
- Cuando envíen un correo electrónico a varios contactos utilicen el CCO 'correo oculto' para no mostrar los contactos y parezcan como privados.

Capitulo III

Delitos y delincuentes informáticos

3.1 Tipos de delitos informáticos reconocidos por naciones unidas.

Clasificación según la actividad informática.

Delito	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 más común ya que es fácil de cometer y difícil de descubrir. Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos.
La manipulación de programas	Es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente debe tener conocimientos técnicos concretos de informática. Este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas. Un método común utilizado por las personas que 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 base de tarjetas bancarias
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.

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.
Daños o modificaciones de programas o datos computarizados.	
Sabotaje informático	Es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema. Las técnicas que permiten cometer sabotajes informáticos son:
Virus	Es una serie de claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos. Un virus puede ingresar en un sistema por conducto de una pieza legítima de soporte lógico que ha quedado infectada, así como utilizando el método del Caballo de Troya.
Gusanos	Se fabrica 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 servicios y sistemas informáticos	Por motivos diversos: desde la simple curiosidad, como en el caso de muchos piratas informáticos (hackers) hasta el sabotaje o espionaje informático.
Piratas informáticos o hackers	El acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones, recurriendo a uno de los diversos medios que se mencionan a continuación. El delincuente puede aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema. A menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sistema; esto suele suceder con frecuencia en los sistemas en los que los usuarios pueden emplear contraseñas comunes o contraseñas de mantenimiento que están en el propio sistema.

Reproducción no autorizada de programas informáticos de protección legal	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.

3.2 Otros Delitos

Por otra parte, existen diversos tipos de delitos que pueden ser cometidos y que se encuentran ligados directamente a acciones efectuadas contra los propios sistemas como son:

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

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.

"Pesca" u "olfateo" de claves secretas: Los delincuentes suelen engañar a los usuarios nuevos e incautos de la Internet para que revelen sus claves personales haciéndose pasar por agentes de la ley o empleados del proveedor del servicio. Los "sabuesos" utilizan programas para identificar claves de usuarios, que más tarde se pueden usar para esconder su verdadera identidad y cometer otras fechorías, desde el uso no autorizado de sistemas de computadoras hasta delitos financieros, vandalismo o actos de terrorismo.

Estafas electrónicas: La proliferación de las compras telemáticas permite que aumenten también los casos de estafa. Se trataría en este caso de una dinámica comisiva que cumpliría todos los requisitos del delito de estafa, ya que además del engaño existiría un engaño a la persona que compra. No obstante seguiría existiendo una laguna legal en aquellos países cuya legislación no prevea los casos en los que la operación se hace engañando al ordenador.

Estratagemas: Los estafadores utilizan diversas técnicas para ocultar computadoras que se "parecen" electrónicamente a otras para lograr acceso a algún sistema generalmente restringido y cometer delitos. El famoso pirata Kevin Mitnick se valió de estratagemas en 1996 para introducirse en la computadora de la casa de

Tsutomo Shimamura, experto en seguridad, y distribuir en la Internet valiosos útiles secretos de seguridad.

Juegos de azar: El juego electrónico de azar se ha incrementado a medida que el comercio brinda facilidades de crédito y transferencia de fondos en la Red. Los problemas ocurren en países donde ese juego es un delito o las autoridades nacionales exigen licencias. Además, no se puede garantizar un juego limpio, dadas las inconveniencias técnicas y jurisdiccionales que entraña su supervisión.

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

Por otro lado, la red Internet permite dar soporte para la comisión de otro tipo de delitos:

Espionaje: Se ha dado casos de acceso no autorizado a sistemas informáticos gubernamentales e interceptación de correo electrónico del servicio secreto de los Estados Unidos, entre otros actos que podrían ser calificados de espionaje si el destinatario final de esa información fuese un gobierno u organización extranjera. Entre los casos más famosos podemos citar el acceso al sistema informático del Pentágono y la divulgación a través de Internet de los mensajes remitidos por el servicio secreto norteamericano durante la crisis nuclear en Corea del Norte en 1994, respecto a campos de pruebas de misiles. Aunque no parece que en este caso haya existido en realidad un acto de espionaje, se ha evidenciado una vez más la vulnerabilidad de los sistemas de seguridad gubernamentales.

Espionaje industrial: También se han dado casos de accesos no autorizados a sistemas informáticos de grandes compañías, usurpando diseños industriales, fórmulas, sistemas de fabricación y know how estratégico que posteriormente ha sido aprovechado en empresas competidoras o ha sido objeto de una divulgación no autorizada.

Terrorismo: Mensajes anónimos aprovechados por grupos terroristas para remitirse consignas y planes de actuación a nivel internacional. La existencia de hosts que ocultan la identidad del remitente, convirtiendo el mensaje en anónimo ha podido ser aprovechado por grupos terroristas para remitirse consignas y planes de actuación a nivel internacional. De hecho, se han detectado mensajes con instrucciones para la fabricación de material explosivo.

Narcotráfico: Transmisión de fórmulas para la fabricación de estupefacientes, para el blanqueo de dinero y para la coordinación de entregas y recogidas.

Fraude: Ya se han hecho ofertas fraudulentas al consumidor tales como la cotización de acciones, bonos y valores o la venta de equipos de computadora en regiones donde existe el comercio electrónico.

3.3 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.

3.4 Pornografía infantil

La distribución de pornografía infantil por todo el mundo a través de la Internet está en aumento. Durante los pasados cinco años, el número de condenas por transmisión o posesión de pornografía infantil ha aumentado de 100 a 400 al año en un país norteamericano. El problema se agrava al aparecer nuevas tecnologías, como la criptografía, que sirve para esconder pornografía y demás material "ofensivo" que se transmita o archive.

3.5 Delincuentes informáticos

Es peligroso pensar que el estereotipo de los hackers o quienes violan la seguridad de los sistemas computacionales son solo brillantes estudiantes o graduados en ciencias de la computación, sentados en sus laboratorios en un lugar remoto del mundo. A pesar de que tales hackers existen, la mayoría de las violaciones a la seguridad son hechas desde dentro de las organizaciones.

Cualquiera que sea la motivación de las empresas que hacen esto, se pueden caracterizar en las siguientes categorías:

a).− Persona dentro de una organización:

Autorizados para ingresar al sistema (ejemplo: miembros legítimos de la empresa que acceden a cuentas corrientes o al departamento de personal).

No están autorizados a ingresar al sistema (ejemplo: personal contratista, aseo, eventual, etc.)

b).− Personas fuera de la organización:

Autorizadas para ingresar al sistema (ejemplo: soporte técnico, soporte remoto de organizaciones de mantenimiento de software y equipos, etc.)

No están autorizados para ingresar al sistema (ejemplo: usuarios de Internet o de acceso remoto, sin relación con la institución).

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

Hacker: Es quien intercepta dolosamente un sistema informático para dañar, apropiarse, interferir, desviar, difundir, y/o destruir información que se encuentra almacenada en computadoras pertenecientes a entidades p6blicas o privadas. El término de hacker en español significa “cortador“. Los “Hackers“, son fanáticos de la informática, generalmente jóvenes, que tan sólo con un computador personal, un módem, gran paciencia e imaginación son capaces de acceder, a través de una red p6blica de transmisión de datos, al sistema informatizado de una empresa o entidad

p6blica, 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 informáticos, o satisfacer su propia vanidad.

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

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 telefonía insuperables. Conocen a fondo los sistemas telefónicos incluso más que los propios técnicos de las compañías telefónicas.

Una de las técnicas usadas en la búsqueda de información de los Phone Phreakers es hacer trashing que consiste en escarbar en la basura de los edificios de las compañías telefónicas en busca de listas 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, escuchar 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 dolosa 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 está 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 la documentación que acompaña al mismo programa.

3.6 Técnicas de violación de sistemas informáticos

Dentro de las conductas relacionadas con el acceso no autorizado a sistemas informáticos podemos distinguir diferentes tipos:

a) Snooping: Consiste en obtener información sin modificarla, por curiosidad, con fines de espionaje o robo. Downling: “Bajar” esa información de la red.

b) Tampering o DataDiddling: Estamos acá ante casos de modificación desautorizada de datos o del software del sistema.

c) Spoofing: Es la técnica para conseguir el password de un usuario legítimo, para poder realizar actos irregulares en nombre de ese usuario.

d) Looping: En este caso el intruso utiliza el sistema para obtener información e ingresar a otro sistema. La técnica es que evapora la identidad del atacante y su ubicación.

e) Jaaming o Flooding: Son ataques que pueden activar o saturar los recursos de un sistema.

f) Phreaking: Es el acceso no autorizado a sistemas telefónicos para obtener gratuidad en el uso de las líneas, esta conducta a su vez tiene variantes, que son:

- Shoulderoperations: Consiste en la obtención del código de la víctima mientras esta lo utiliza, para aprovecharlo posteriormente.

- Call-sell operations: El sujeto presenta un código identificador de usuario que no le pertenece y carga el costo de la llamada a la víctima.

- Diverting: Penetración lícita a centrales telefónicas privadas para realizar llamadas de larga distancia que se cargan al dueño de la central.

- Acceso no autorizado a sistemas de correos de voz: Atacan a las máquinas destinadas a realizar el almacenamiento de mensajes telefónicos

g) Trashing: Obtención de información secreta o privada que se logra por revisión de la basura (material o inmaterial).

Capitulo IV

Legislación sobre delitos informáticos

4.1 Panorama general

La legislación sobre protección de los sistemas informáticos ha de perseguir acercarse lo más posible a los distintos medios de protección ya existentes, creando una nueva regulación sólo en aquellos aspectos en los que, basándose en las peculiaridades del objeto de protección, sea imprescindible.

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

No es la amenaza potencial de la computadora sobre el individuo lo que provoca desvelo, sino la utilización real por el hombre de los sistemas de información con fines de espionaje.

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

La humanidad no esta frente al peligro de la informática sino frente a la posibilidad real de que individuos o grupos sin escrúpulos, con aspiraciones de obtener el poder que la información puede conferirles, la utilicen para satisfacer sus propios intereses, a expensas de las libertades individuales y en detrimento de las personas. Asimismo, la amenaza futura será directamente proporcional a los adelantos de las tecnologías informáticas.

La protección de los sistemas informáticos puede abordarse tanto desde una

perspectiva penal como de una perspectiva civil o comercial, e incluso de derecho administrativo. Estas distintas medidas de protección no tienen porque ser excluyentes unas de otras, sino que, por el contrario, éstas deben estar estrechamente vinculadas. Por eso, dadas las características de esta problemática sólo a través de una protección global, desde los distintos sectores del ordenamiento jurídico, es posible alcanzar una cierta eficacia en la defensa de los ataques a los sistemas informáticos.

4.2 Análisis legislativo

Un análisis de las legislaciones que se han promulgado en diversos países arroja que las normas jurídicas que se han puesto en vigor están dirigidas a proteger la utilización abusiva de la información reunida y procesada mediante el uso de computadoras.

Desde hace aproximadamente diez años la mayoría de los países europeos han hecho todo lo posible para incluir dentro de la ley, la conducta punible penalmente, como el acceso ilegal a sistemas de computo o el mantenimiento ilegal de tales accesos, la difusión de virus o la interceptación de mensajes informáticos.

En la mayoría de las naciones occidentales existen normas similares a los países europeos. Todos estos enfoques están inspirados por la misma preocupación de contar con comunicaciones electrónicas, transacciones e intercambios tan confiables y seguros como sea posible.

Las personas que cometen los delitos informáticos son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, aún cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos.

Con el tiempo se ha podido comprobar que los autores de los delitos informáticos son muy diversos y que lo que los diferencia entre sí es la naturaleza de los delitos

cometidos. De esta forma, la persona que ingresa 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 el nivel de aptitudes no es indicador de delincuencia informática en tanto que otros aducen que los posibles delincuentes informáticos son personas listas, decididas, motivadas y dispuestas a aceptar un reto tecnológico, características que pudieran encontrarse en un empleado del sector de procesamiento de datos.

Sin embargo, teniendo en cuenta las características ya mencionadas de las personas que cometen los delitos informáticos, los estudiosos en la materia los han catalogado como «delitos de cuello blanco» término introducido por primera vez por el criminólogo norteamericano Edwin Sutherland en el año de 1943.

Efectivamente, este conocido criminólogo señala un sinnúmero de conductas que considera como «delitos de cuello blanco», aún 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 fábrica 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 informáticos» como la de los «delitos de cuello blanco» no son 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 de cierto status socioeconómico, su comisión no puede explicarse por pobreza ni por mala habitación, ni por carencia de recreación, ni por baja educación, ni por poca inteligencia, ni por inestabilidad emocional».

Es difícil elaborar estadísticas sobre ambos tipos de delitos. Sin embargo, la cifra 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 pública sobre los daños ocasionados a la sociedad; la sociedad no considera delincuentes a los sujetos que cometen este tipo de delitos, no los segrega, no los desprecia, ni los desvaloriza, por el contrario, el autor o autores de este tipo de delitos se considera a sí mismos «respetables» otra coincidencia que tienen estos tipos de delitos es 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 todo el mundo y, en consecuencia, existe una posibilidad muy grande de que el agresor y la víctima estén sujetos a leyes nacionales diferentes. Además, si bien los acuerdos de cooperación internacional y los tratados de extradición bilaterales intentan remediar algunas de las dificultades ocasionadas por los delitos informáticos, sus posibilidades son limitadas.

Por su parte, el «Manual de la Naciones Unidas para la Prevención y Control de Delitos Informáticos» señala que cuando el problema se eleva a la escena internacional, se magnifican los inconvenientes y las insuficiencias, por cuanto los delitos informáticos constituyen una nueva forma de crimen transnacional y su combate requiere de una eficaz co operación internacional concertada. Asimismo, la ONU resume de la siguiente manera a los problemas que rodean a la cooperación internacional en el área de los delitos informáticos:

- Falta de acuerdos globales acerca de que tipo de conductas deben constituir delitos informáticos.
- Ausencia de acuerdos globales en la definición legal de dichas conductas delictivas.
- Falta de especialización de las policías, fiscales y otros funcionarios judiciales en el campo de los delitos informáticos.
- Falta de armonización entre las diferentes leyes procesales nacionales acerca de la investigación de los delitos informáticos.
- Carácter transnacional de muchos delitos cometidos mediante el uso de computadoras.

- Ausencia de tratados de extradición, de acuerdos de ayuda mutuos y de mecanismos sincronizados que permitan la puesta en vigor de la cooperación internacional.

4.1 Legislación en México

La nueva reforma establece:

Articulo 211 BIS-1

Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de 6 meses a 2 años de prisión, y de 100 a 300 días de multa. Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrá de 3 meses a un año de prisión, y de 50 a 150 días de multa.

Articulo 211 BIS-2

Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado protegidos por algún mecanismo de seguridad, se le impondrán de un año a 4 años de prisión, y de 200 a 600 días de multa. Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado protegidos por algún mecanismo de seguridad, se le impondrá de 6 meses a 2 años de prisión, y de 100 a 300 días de multa.

Articulo 211 BIS-3

Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrá de 2 a 8 años de prisión, y de 300 a 900 días de multa. Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información que contengan, se le impondrá de uno a 4 años de prisión y de 150 a 450 días de multa.

Articulo 211 BIS-4

Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se les impondrán de 6 meses a 4 años de prisión, y de 100 a 600 días de multa. Al que sin autorización conozca o copie información contenidas en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegido por algún mecanismo de seguridad, se le impondrán de 3 meses a 2 años de prisión y de 50 a 300 días de multa.

Articulo 211 BIS-5

Al que estando autorizado para accesar a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de 6 meses a 4 años de prisión, y de 100 a 600 días de multa. Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan, se le impondrá de 3 meses a 2 años de prisión, y de 50 a 300 días de multa. Las penas previstas en este articulo se incrementan en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero.

Articulo 211 BIS-6

Para los efectos de los artículos 211 BIS-4, y 211 BIS-5 anteriores, se entiende por instituciones que integran el sistema financiero, las señaladas en el artículo 400 BIS de este código.

Articulo 211 BIS-7

Las penas previstas en este capitulo se aumentarán hasta una mitad cuando la información obtenida se utilice en provecho propio o ajeno.

Articulo 424 Ter.

Se impondrá prisión de 6 meses a 6 años y de 5 mil a 30 mil días de multa a quien venda a cualquier consumidor final en vías o en lugares públicos, en forma dolosa, con fines de especulación comercial, copias obras, fonogramas, videogramas o libros, a los que se refiere la fracción I del articulo anterior. "Si la venta se realiza en establecimientos comerciales o de manera organizada o permanente, se estará lo dispuesto en el articulo 424 BIS, de este código".

Articulo 233 BIS

Se impondrá de 2 a 6 años de prisión y multa de 100 a 10 mil días de salarios mínimos general vigente en el Distrito Federal, al que venda a cualquier consumidor final en vías o en lugares públicos, en forma dolosa y con fin de especulación comercial, objetos que ostenten falsificaciones de marcas protegidas por la Ley. "Si la venta se realiza en establecimientos comerciales o de manera organizada o permanente, se estará lo dispuesto en los artículos 233 y 224, de esta Ley".

Transitorio Cuarto

Las referencias que en el presente decreto se hagan al Código Penal para el Distrito Federal en materia del fuero Común y para toda la república en Materia de fuero Federal, se entenderán hechas al Código Penal Federal.

Capitulo V

Prevención de los delitos informáticos.

5.1 Piratería

Piratería, es copiar para utilizar o comercializar sin autorización cualquier cosa que tenga derechos de autor. En este caso se va a hablar de piratería informática; sin embargo, también lo es, por ejemplo, fotocopiar un libro, copiar un programa, teniendo además en cuenta que las editoriales son empresas mucho más modestas que las multinacionales del software.

La piratería realmente comienza con la aparición de las computadoras personales puesto que, hasta ese momento, se trabajaba únicamente en mainframes en las que se utilizaban programas hechos a medida que difícilmente podían aprovecharse de un caso particular a otro.

Las organizaciones que disponen de equipos de cómputo tienen que contar las licencias de uso de software. Deberán existir tantas licencias de uso de un producto como la cantidad de usuarios de ese producto. No sólo se trata de la compra múltiple de un mismo producto, sino que se trata de licencias o sea acuerdos contractuales entre la firma proveedora del software y la organización compradora, en donde se habilita a una cierta cantidad de usuarios para su utilización de forma conjunta y simultánea en el tiempo.

El software pirata presenta una serie de desventajas, entre ellas:

- Productividad reducida
- Alta exposición a serias represiones legales
- Poca confiabilidad debido a probables infecciones de virus
- Carencia de documentación. (Manuales, plantillas operativas, referencias adicionales, etc.)
- No da derecho a soporte técnico, ni garantía.
- Copias por lo general incompletas.

En contraposición el software original presenta las siguientes ventajas:

- Productividad total.
- Completa documentación.
- Soporte técnico.
- Garantía de todo el paquete.
- Posibilidad de actualizaciones a bajo costo.
- Acceso a beneficios adicionales (Conferencias, seminarios, exposiciones, etc.).

5.1.1 Medidas de prevención

Para poder reconocer software pirata, se deben tener en cuenta las siguientes consideraciones:

Software Original	Software Pirata
Viene en cajas impresas en alta calidad, las que tienen medidas de autenticidad, como por ejemplo stickers con un holograma de identificación.	Por lo general no se presenta de esta forma, y en el caso de venir con algún packaging, éste es de una imitación de mala calidad.
Viene entre otras cosas, todos los manuales de los productos, e información adicional.	Por lo general, carece de manuales, o estos son fotocopiados y presentados de manera incompleta.
Los juegos de CD se encuentran debidamente identificados con etiquetas preimpresas.	Los CD son grabados en algunos de marcas comerciales y son etiquetados mayormente a mano.
Las cajas contienen la/s correspondiente/s licencia/s de uso.	Carecen de la/s correspondiente/s licencia/s de uso del software.

Otros aspectos a tener en cuenta con el fin de salvaguardar los intereses de toda persona involucrada directa o indirectamente con el área de sistemas son:

- Ante cualquier duda de legitimidad respecto al software que se esta utilizando, constatar el cumplimiento de los factores especificados en el cuadro anterior.
- En el caso de comprobar el uso de software pirata, el jefe del área de sistemas tiene la obligación de elevar la denuncia correspondiente.
- A fin de evitar el compromiso civil y personal con una empresa proveedora de productos de computación que comete piratería, se debe notificar a la gerencia de la empresa el rechazo y disconformidad por escrito, del origen del software que se esta utilizando en la misma.
- Para evitar responsabilidades penales, debe negarse rotundamente a efectuar ninguna instalación que no esté respaldada por la licencia correspondiente.

5.2 Contratos informáticos

Contrato es la relación jurídica bilateral por la que "una o varias personas consienten en obligarse, respecto de otra u otras, a dar alguna cosa o prestar algún servicio". Este tipo legal básico se proyecta a los contratos informáticos con importantes peculiaridades, ya que pueden afectar al hardware y/o al software, dando lugar a una rica tipología en la que pueden distinguirse contratos de compraventa, alquiler, leasing, mantenimiento y servicios.

La complejidad "objetiva" de estos contratos procede de la inevitable conjunción del hardware y del software, en la estructura del computador (una maquina física que sólo es operativa si cuenta con un programa que le permita cumplir sus fines). De ahí, surge una importante serie de problemas ya que, en la actualidad, quien fabrica el equipo físico del computador no siempre coincide con quien crea los programas. El usuario adquiere una maquina confiando que pueda prestarle determinados servicios, pero el logro de esta finalidad depende de la adecuación entre el soporte físico y los programas.

Los contratos informáticos requieren de un tratamiento jurídico especial que superando todas las fronteras de la normativa regulatoria de los contratos civiles y comerciales, respondan a las características particulares del mercado internacional de tecnología informática, a la especificidad de su objeto y los intereses en juego, así como a su trascendencia económica para la empresa y el Estado.

Asimismo, los contratos informáticos son aquellos que se generan por la necesidad de adquirir bienes o servicios informáticos, los que adquieren cada vez mayor importancia por los efectos de la "Aldea Global". Se entiende por contratación informática cuya finalidad sea un bien o servicio informático o ambos casos, también podría decirse que es una de las prestaciones de las partes tenga por objeto un bien o servicio informático.

Se debe tener en cuenta que en la redacción de los contratos, no sólo deben participar los juristas, sino que es imprescindible que participen también los técnicos informáticos para colaborar en la elaboración de las necesarias especificaciones técnicas, ya que éstas en la contratación informática, adquieren una especial relevancia.

Generalmente los proveedores informáticos celebran contratos de adhesión con los usuarios (las cláusulas han sido previamente redactadas), los que regirán las relaciones contractuales futuras, donde hay que aceptarlos o rechazarlos en su conjunto, sin que suela haber opción a una modificación parcial.

Muchas veces el proveedor en su afán de vender ya sea un bien o un servicio exagera, a veces sin mala intención, las bondades de los mismos y a su vez el adquiriente sin la formación y el asesoramiento adecuados, y necesitado de resolver su problema, mentalmente construye una imagen ideal en la que su problema queda perfectamente resuelto con el producto que le ofrecen. Desgraciadamente esto no suele ser así y cuanto mas alejada de la realidad esté ese modelo ideal tanto mas conflictiva será la situación cuando vea que sus problemas no se resuelven tal como pensaba.

Por ello es importante determinar en forma clara y precisa lo siguiente:

1) ¿Qué se va a hacer?
2) ¿Dónde se va a hacer?
3) ¿Cuando se va a hacer?
4) ¿Cómo se va a hacer?
5) ¿Quién lo va a hacer?

5.3 Protección y desprotección de programas

Para evitar las copias ilegales de un programa se emplean diferentes técnicas tanto para impedir la copia de los disquetes como para conseguir que no se pueda trabajar en mas de una computadora por cada licencia adquirida. Otra forma de dificultar la copia ilegal, muy común en los juegos es la necesidad de introducir al comienzo una clave relacionada con un dato proporcionado y que puede encontrarse en algún manual adjunto.

Las técnicas de protección contra copia de los disquetes fueron las primeras en emplearse pero actualmente se utilizan poco, puesto que son las que plantean mayores problemas y son menos eficaces que otras. Esta protección se hacia originalmente formateando los disquetes en un modo no estándar, efectuando marcas láser, o mediante la técnica de los bits débiles, de tal forma que, empleando las herramientas que proporciona el sistema operativo, era imposible reproducir el disco en el mismo estado en que estaba.

Las protecciones anteriores suelen ir unidas a la existencia de un contador con el número de licencias adquiridas que disminuye cada vez que se instala el programa. Esto puede ser un problema, puesto que al estar limitado el número de instalaciones, si se pierde o daña alguno de los archivos de la aplicación, habría que volver a adquirir el programa.

Esta clase de protecciones no serían útiles si una vez que el programa esta instalado en el disco duro pudiera copiarse y ser llevado a otra computadora,

situación que se evitaba haciendo que el programa pida para funcionar la introducción en la unidad de disquete uno de los discos protegido contra copia, el llamado disco llave, un método que esta en desuso. Otro método es grabar cierta información en alguna zona del disco duro, por ejemplo en el último sector, que el programa consultara cada vez que se ejecute y, si no la encuentra, dejara de funcionar.

También esta la opción de almacenar codificada la localización del programa en el disco cuando se instala y cada vez que se ejecuta comprobar si sigue siendo la misma. De esta forma, si se intenta pasar a otra computadora no funcionara, puesto que es prácticamente imposible que, al volverlo a copiar, quede instalado en las mismas posiciones. Esta técnica presenta el grave inconveniente de que, si se desfragmenta el disco duro, el programa con toda probabilidad dejara de funcionar puesto que cambiara su localización. Antes de hacerlo habría que desinstalarlo, luego desfragmentar y volverlo a instalar; éste, de hecho, es un problema real que ha ocurrido con mas de un programa que utilizaba esta técnica al no avisar el fabricante de la situación.

Otro tipo de protección mas eficaz y que presenta menos problemas es el uso de un dispositivo conectado a un puerto de comunicaciones (serie o paralelo), conocido como llave y, popularmente, como “mochila“. Este método asegura que el programa protegido sólo se ejecutara en una computadora a la vez. En las primeras protecciones de este tipo el contenido de la llave era una simple memoria PROM con cierta información que el programa protegido intentaba leer al ejecutarse y si no la encontraba se interrumpía. Estas memorias eran fáciles de duplicar pero, actualmente, son mucho más complejas. Las ventajas de las mochilas sobre otros métodos son que la llave es muy difícil que se estropee, si se daña el programa instalado en el disco duro puede volverse a instalar sin problemas y que si se deterioran los disquetes del programa normalmente puede solicitarse una nueva copia al distribuidor sin tener que pueda instalar en mas de una computadora puesto que la llave garantiza que únicamente se utilizara en una de ellas a la vez. No hay ningún problema cuando se tienen que usar dos programas que requieran llave puesto que es posible conectar una sobre la otra.

5.4 Propiedad Intelectual en Internet

Una de las características de Internet es el problema que origina respecto a la aplicación de los derechos de propiedad intelectual en una red global. Internet no esta gobernada por ninguna autoridad central, ni existe organismo autorizado para rastrear copias ilegales. Los usuarios de Internet pueden copiar un trabajo y distribuirlo internacionalmente en cuestión de segundos.

El tema de la protección de los derechos intelectuales en el ámbito de Internet aun es de reciente desarrollo. Una primera consideración es la necesidad de distinguir como en las redes digitales circula información de distinto contenido o naturaleza, y que se trata de datos o documentos que pueden ser de dominio publico o que tradicionalmente han estado sujetos a las instituciones de la propiedad intelectual, del derecho de autor propiamente "copyright".

El autor de una obra original tiene facultades para reproducirla materialmente, publicarla, adaptarla, explotarla comercialmente o vindicar la paternidad, porque por el sólo hecho de crearla, en ese momento y sin solemnidad alguna la incorpora a su patrimonio.

Las redes telemáticas han "desmaterializado" las obras creadas por los autores, ya que las creaciones originales digitales o digitalizadas se reproducen, circulan y se distribuyen rápida y electrónicamente, sin que se materialicen, como se hacia anteriormente, en un soporte físico concreto o en alguna de las formas envasadas que históricamente han contenido las obras artísticas e intelectuales, haciéndose sumamente fácil que sean ilícitamente reproducidas, transformadas y copiadas con fines comerciales o "pirateadas", sin que exista diferencia alguna entre un original y una copia electrónica.

Teóricamente las leyes autorales pueden ser aplicadas a Internet, ya que las redes telemáticas simplemente son nuevas formas de reproducir en el espacio virtual,

mediante soportes magnéticos libros, cuadros, canciones, programas computacionales, etc.

Quien pone en Internet una creación intelectual tiene que entender que esta renunciando a que se le pida autorización por el uso privado de su obra, sea sólo para consultarla, sea para instalarla en una nueva pagina Web.

El factor importante en Internet es que las leyes de un país sólo pueden aplicarse por los tribunales dentro del territorio geográfico de ese mismo país.

Una copia ilegal y digital sólo podría ser controlada por la legislación y los tribunales del país en que la información esté siendo emitida o donde esté ubicado el servidor del proveedor de conectividad, mas no mas allá de sus fronteras o por los tribunales de un país extranjero.

El diseño de una página Web es una obra original del programador o la empresa que la crea, desarrolla, instala y mantiene. Se vulnerarla su propiedad intelectual si se copian elementos de una pagina Web para instalarlos en otra, conducta en a que incurren empresas menores o aficionados que ofrecen los mismos servicios que una empresa formalmente instalada pero a una tarifa muy inferior por el menor trabajo de creación desplegado.

Si la copia del diseño y la información de una página WEB se realizan dentro de las fronteras territoriales y jurídicas de un país determinado, sin lugar a dudas puede accionarse legalmente teniendo como fundamento la respectiva ley de propiedad intelectual o copyright. Lo que ocurre es que, si esa pagina Web es visitada desde un país lejano y es copiada posteriormente, el autor nunca se enterara de tal copia.

Los últimos avances de la OMPI. Importancia de los mecanismos tecnológicos. En cuanto al copyright en el ciberespacio, a fines de 1996 se realizó en Ginebra una reunión internacional de la Organización Mundial de Propiedad Intelectual (OMPI o en inglés WIPO), en la que inicialmente se esperaba avanzar en una regulación sobre los derechos de autor en Internet, idea que fracasó y no se concluyó.

La OMPI, después de constatar lo precario de la protección jurídica que el estatuto jurídico tradicional de la propiedad intelectual otorga a las obras que se comercializan y consultan en Internet, estableció la obligación que los Estados que ratifiquen y firmen la Convención de Ginebra sobre Derechos de Autor deben resguardar jurídicamente y promocionar la aplicación de medidas técnicas de seguridad de la propiedad intelectual, como es el caso de la codificación o encriptación.

Los servidores o usuarios que desean llevar a cabo un acto que esta regulado por las leyes de propiedad intelectual deben obtener la autorización del poseedor de los derechos, ya sea explícita o implícitamente.

5.5 Amenazas humanas

Una norma básica, sería verificar cada aspirante a ser nuevo empleado; aunque tampoco debemos olvidar que el hecho de que alguien entre "limpio" a la organización no implica que vaya a seguir así durante el tiempo que trabaje en la misma, y mucho menos cuando abandone su trabajo.

Para minimizar el daño que un atacante interno puede causar se pueden seguir estos principios fundamentales:

- Necesidad de conocimiento (Need to Know): comúnmente llamado mínimo privilegio. Cada usuario debe tener el mínimo privilegio que necesite para desempeñar correctamente su función, es decir, que sólo se le debe permitir que sepa lo necesario para realizar su trabajo.
- Conocimiento parcial (dual control): las actividades más delicadas dentro de la organización deben ser realizadas por dos personas competentes, de forma que si uno comete un error en las políticas de seguridad el otro pueda subsanarlo. Esto también es aplicable al caso de que si uno abandona la organización el otro pueda seguir operando el sistema mientras se realiza el reemplazo de la persona que se retiró.

- Rotación de funciones: la mayor amenaza del conocimiento parcial de tareas es la complicidad de dos responsables, de forma tal, que se pueda ocultar sendas violaciones a la seguridad. Para evitar el problema, una norma común es rotar (dentro de ciertos límites) a las personas a lo largo de diferentes responsabilidades, para establecer una vigilancia mutua.
- Separación de funciones: es necesario que definan y separen correctamente las funciones de cada persona, de forma que alguien cuya tarea es velar por la seguridad del sistema no posea la capacidad para violarla sin que nadie se percate de ello.
- Cancelación inmediata de cuenta: cuando un empleado abandona la organización se debe cancelar inmediatamente el acceso a sus antiguos recursos y cambiar las claves que el usuario conocía. Quizás este último punto sea el más difícil de implementar debido a la gran cantidad de usuarios que se deben informar de los nuevos accesos y de la movilidad de alguno de ellos.

En estos puntos se encuentran las mayores vulnerabilidades de un sistema ya que, por ejemplo, suelen encontrarse cuentas de usuario que hace años que no se utilizan, y por ende tampoco se han cambiado sus passwords.

Si bien estas normas pueden aplicarse a las organizaciones, no podrán hacerlo en instituciones como una universidad, donde la mayoría de los atacantes son alumnos y no podrá verificarse los antecedentes de miles de alumnos (y tampoco ético prohibir su acceso por ser estos dudosos). De esta forma, en las redes de Investigación y Desarrollo (I+D) de acceso público debemos ceñirnos a otros mecanismos de control y casi siempre se opta por las sanciones a todos aquellos que utilicen el centro para cometer delitos informáticos.

5.6 Propuesta para la prevención de delitos informáticos

1) **Creación de cursos, seminarios y/o talleres** de manera intensiva e inmediata para estudiantes de derecho y abogados interesados en el tema a través de institutos y centros de capacitación especializados y/o profesionales de la informática mientras se logra la inclusión en los planes de estudio a nivel licenciatura; a través de las principales autoridades educativas reguladoras de los mismos; de un tema fundamental como es el *crimen cibernético* y sus divisiones. Por lo tanto, hasta que no se tenga en concreto esta ley, el país será más fácilmente blanco de cualquier ataque cibernético a pesar de que ya se cuenta con organismos de combate al delito como la Policía Cibernética dependiente de la Secretaría de Seguridad Pública Federal cuya función es combatir cualquier delito informático pero de manera preventiva y correctiva, pues en la actualidad solamente ha actuado en forma correctiva, precisamente por la falta de una normatividad que ayude a combatir ambas acciones.

2) **Definir al sujeto activo, dentro de la creación de una ley contra los delitos informáticos (aún no existente)**; para de esa manera, poder ejercer acciones penales claras y sobretodo buscar el camino adecuado para clarificar que otra pieza fundamental como es el dato, pueda ser tomado como elemento probatorio, pues es algo intangible y difícil de comprobar. Valdría la pena consultar la manera en cómo los seis países en el mundo (Austria, Chile, Estados Unidos de América, Francia, Gran Bretaña y Holanda) que ya cuentan con una Ley contra el combate de los delitos informáticos, plantean la acción penal contra este elemento ejercido por el o los sujeto(s) activo(s) y, tienen definido claramente quiénes son los que actúan de mala fe así como la protección al hacker que labora para estas empresas.

3) **Dar mantenimiento periódicamente a los servidores a través de actualizaciones de archivos** por los administradores de los mismos para mantener integra su seguridad. Esto se menciona, con el objeto de aclarar que existen dos actores fundamentales que son el hacker y el cracker (sujetos activos), y que en la mayoría de las empresas de cualquier rama, el primero trabaja para salvaguardar los sistemas computacionales y el servidor mismo combatiendo a los virus y a los creadores de los mismos.

4) **Que los expertos en materia de informática participen activamente y de manera paralela con los legisladores** en los comités instalados para la creación de la Ley

contra los Delitos Informáticos en relación con los conceptos informáticos que surjan, explicación técnica de manera amplia sobre el funcionamiento de sistemas de cómputo y redes existentes actualmente, así como los avances tecnológicos que surjan el día de mañana y trabajar conjuntamente con las empresas públicas y privadas, en el mantenimiento de equipos de cómputo, servidores y programas para proteger los sistemas informáticos, bases de datos así como del Intranet y Extranet con que cuentan para proteger al usuario final y a ellos mismos. Actualmente, en el mundo se tiene regulado el uso de Internet mediante distintos organismos internacionales a través de la *Sociedad de Internet (ISOC)* que fija los estándares y uso adecuado del mismo mejorando su disponibilidad y expandiendo su uso a todos los rincones del mundo. Por tanto, es necesario trabajar, particularmente, con el capítulo de la *Sociedad Internet de México, A. C.* en lo que a delitos informáticos se refiere, para tomarlos en cuenta en la ley que se cree en México y no solamente en el rubro del software, pedofilia, pornografía infantil, terrorismo, entre otros que, actualmente se tiene contemplado. El Internet es un potencial enorme positivo y negativo que de no tenerse control sobre él; aún cuando México junto con diversos países trabaja en materia de regulación tecnológica; se puede convertir en lo que en informática se llama *terrorismo cibernético*, el cual, existe en el mundo desde hace tiempo y sobretodo en los últimos años y simple y llanamente hay que tener conciencia de que todos nosotros estamos expuestos a cualquier ataque al utilizar este medio electrónico. Es de interés mencionar uno de tantos casos aislados que han sucedido en nuestro país en relación con el delito informático. A mediados de este año, un sujeto activo realizó transferencias monetarias. Esta persona, finalmente fue aprehendida por las autoridades gubernamentales culpándosele de fraude bancario y no por delito informático, precisamente por la falta de esta última figura. Esto pone nuevamente de manifiesto que, además de reforzar la protección de los sistemas informáticos de manera local o al través de Internet mediante los protocolos de seguridad para ambos casos, también es necesario contar con una ley que proteja a empresas públicas o privadas, entidades gubernamentales y usuarios finales.

Conclusiones

Debido a la naturaleza virtual de los delitos informáticos, puede volverse confusa la tipificación de éstos ya que a nivel general, se poseen pocos conocimientos y experiencias en el manejo de ésta área. Desde el punto de vista de la Legislatura es difícil la clasificación de estos actos, por lo que la creación de instrumentos legales puede no tener los resultados esperados, sumado a que la constante innovación tecnológica obliga a un dinamismo en el manejo de las Leyes relacionadas con la informática.

La falta de cultura informática es un factor crítico en el impacto de los delitos informáticos en la sociedad en general, por lo que el componente educacional es un factor clave en la minimización de esta problemática.

Cada vez se requieren mayores conocimientos en tecnologías de la información, las cuales permitan tener un marco de referencia aceptable para el manejo de dichas situaciones. Nuevas formas de hacer negocios como el comercio electrónico puede que no encuentre el eco esperado en los individuos y en las empresas hacia los que va dirigido ésta tecnología, por lo que se deben crear instrumentos legales efectivos que ataquen ésta problemática, con el único fin de tener un marco legal que se utilice como soporte para el manejo de éste tipo de transacciones.

La ocurrencia de delitos informáticos en las organizaciones alrededor del mundo no debe en ningún momento impedir que éstas se beneficien de todo lo que proveen las tecnologías de información (comunicación remota, interconectividad, comercio electrónico, etc.); sino por el contrario dicha situación debe plantear un reto a los profesionales de la informática, de manera que se realicen esfuerzos encaminados a robustecer los aspectos de seguridad, controles, integridad de la información, etc. en las organizaciones.

También se observa el grado de especialización técnica que adquieren los delincuentes para cometer éste tipo de delitos, por lo que personas con conductas maliciosas cada vez más están ideando planes y proyectos para la realización de actos delictivos, tanto a nivel empresarial como a nivel global. Los constantes cambios de la tecnología hacen que para mantener un nivel parejo de seguridad, se deba actualizar permanentemente las herramientas con las que se cuenta. Como los intrusos mejoran sus armas y metodologías de penetración de forma incesante, el recambio y la revisión constantes en los mecanismos de seguridad se convierten en imprescindibles.

Aquellas personas que no poseen los conocimientos informáticos básicos, son más vulnerables a ser víctimas de un delito, que aquellos que si los poseen. En vista de lo anterior aquel porcentaje de personas que no conocen nada de informática (por lo general personas de escasos recursos económicos) pueden ser engañadas si en un momento dado poseen acceso a recursos tecnológicos y no han sido asesoradas adecuadamente para la utilización de tecnologías como la Internet, correo electrónico, etc.

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.

Nuevas formas de hacer negocios como el comercio electrónico puede que no encuentre el eco esperado en los individuos y en las empresas hacia los que va dirigido ésta tecnología, por lo que se deben crear instrumentos legales efectivos que ataquen ésta problemática, con el único fin de tener un marco legal que se utilice como soporte para el manejo de éste tipo de transacciones.

Es imprescindible contar con las herramientas tecnológicas adecuadas, y con técnicos preparados para que los delitos no queden en la letra de la ley por falta de medios para detectarlos.

Bibliografía

1. SEGU-INFO Seguridad de la información.

http://www.segu-info.com.ar/

2. La privacidad en Internet.

http://www.privacyrights.org/spanish

3. Introducción a los delitos informáticos, tipos y legislación.

http://www.delitosinformaticos.com/

4. Servicios de información de la CNN de Estados Unidos.

http://www.cnnenespanol.com

5. Fraudes por Internet Policía Cibernética

http://ciberfraudes.blogspot.com/

6. Delitos Informáticos

http://www.monografias.com/

7. Posibles sujetos de los delitos informáticos.

http://www.informatica-juridica.com/

ANEXOS

Historia de los delitos informáticos.

Casos identificados
Draper, John. Captain Crunch, en septiembre de 1970 John Draper, también conocido como Captain Crunch, descubre que el obsequio ofrecido en las cajas de cereal Captain Crunch duplica perfectamente la frecuencia de tono de 2600 Hz. de una linea de WATS, permitiéndole hacer llamadas telefónicas gratis y la gran victima era AT&T.
Gates, Bill y Allen, Paul, en sus tiempos de aprendices, estos dos hombres de Washington se dedicaban a hackear software. Grandes programadores. Empezaron en los 80 y han creado el mayor imperio de software de todo el mundo. Sus "éxitos" incluyen el SO MS-DOS, Windows, Windows 95 y Windows NT.
Mitnick Kevin, "El Cóndor", "El Chacal de la red", uno de los mayores hackers de la historia, la carrera de Mitnick, como Hacker tiene sus inicios en 1980 cuando apenas contaba 16 años y, obsesionado por las redes de computadoras, rompió la seguridad del sistema administrativo de su colegio, pero no para alterar sus notas, lo hizo "sólo para mirar". Su bautizo como infractor de la ley fue en 1981. Junto a dos amigos entró físicamente a las oficinas de COSMOS de Pacific Bell. COSMOS (Computer System for Mainframe Operations) era una base de datos utilizada por la mayor parte de las compañías telefónicas norteamericanas para controlar el registro de llamadas. Una vez dentro de las oficinas obtuvieron la lista de claves de seguridad, la combinación de las puertas de acceso de varias sucursales y manuales del sistema COSMOS.
Ha sido una de las mayores pesadillas del Departamento de justicia de los Estados Unidos. Entró virtualmente en una base de misiles y llegó a falsificar 20.000

números de tarjetas de crédito.
Al igual que el chico de la película “Juegos de Guerra“, Mitnik se introdujo en la computadora de de la Comandancia para la Defensa de Norte América, en Colorado Springs.
Pero a diferencia del muchacho de Juegos de Guerra, Mitnik se dedicó a destruir y alterar datos, incluyendo las fichas del encargado de vigilar su libertad condicional y las de otros enemigos. La compañía Digital Equipment afirmó que las incursiones de Mitnik le costaron más de cuatro millones de dólares que se fueron en la reconstrucción de los archivos y las pérdidas ocasionadas por el tiempo que las computadoras estuvieron fuera de servicio.
Uno de los Hacker más conocidos del mundo, Kevin Mitnick, que dio lugar al guión de la película “Juegos de Guerra“ y lleva en prisión desde 1995, ha conseguido un acuerdo con jueces y fiscales en vísperas del inicio de la vista, fijada para el 29 de marzo. Los términos concretos del acuerdo se desconocen, pues ninguna de las partes ha efectuado declaraciones, pero según informó, el jueves 18, “Los Angeles Times“, Mitnick, de 35 años, podría quedar en libertad dentro de un año, aunque tendría prohibido durante tres años más el acceso a computadoras y, además, se le vetarla que obtuviera rendimiento económico contando su historia en medios de comunicación.
Sobre él pesaba una condena de 25 años por fraude informático y posesión ilegal de archivos sustraídos de compañías como Motorola y Sun Microsystems. La popularidad de Mitnick, que tiene su página en http://www.kevinmitnick.com/home.html, estalló ya en los años 80, cuando fue detenido cuatro veces. Estando en libertad provisional, en 1992, realizó diversas acciones de “hacking“, y permaneció como fugitivo hasta su captura, en Carolina del Norte, en 1995.

A partir de ese momento, un buen numero de hackers de todo el mundo, deseosos de que se produjera la excarcelación de su mentor, llevaron a cabo diversas acciones de intromisión en sistemas informáticos, el más notorio de los cuales fue el asalto, en septiembre de 1998, de la página del "New York Times", que quedó inoperativo durante un par de días. Encarcelado por el Gobierno norteamericano sin juicio, Kevin Mitnick habla sido considerado por el FBI como el hacker más peligroso y escurridizo del mundo.

Murphy Ian, Captain Zap, en julio de 1981 Ian Murphy, un muchacho de 23 años que se autodenominaba "Captain Zap", ganó notoriedad cuando entró a los sistemas en la Casa Blanca, el Pentágono, BellSouth Corp. TRW y deliberadamente deja su curriculum.

En 1981, no habla leyes muy claras para prevenir el acceso no autorizado a las computadoras militares o de la casa blanca. En ese entonces Ian Murphy de 24 años de edad, conocido en el mundo del hacking como "Captain Zap", mostró la necesidad de hacer mas clara la legislación cuando en compañía de un par de amigos y usando una computadora y una línea telefónica desde su hogar viola los accesos restringidos a compañías electrónicas, y tenia acceso a órdenes de mercancías, archivos y documentos del gobierno. "Nosotros usamos a la Casa Blanca para hacer llamadas a líneas de bromas en Alemania y curiosear archivos militares clasificados"Explicó Murphy. "El violar de accesos nos resultaba muy divertido". La Banda de hackers fue finalmente puesta a disposición de la ley". Con cargos de robo de propiedad, Murphy fue multado por US $1000 y sentenciado a 2 O años de prueba.

Austin Ron y Kevin Poulsen, en 1982 dos hackers de los Ángeles, Ron Austin y Kevin Poulsen, se introdujeron en la red de intercambio de datos Arpa del Pentágono, la precursora de la actual Internet. La primera opción, en el esquema virtual que poseían, era adivinar la palabra clave de acceso al sistema. Lo lograron al cuarto intento, utilizando las letras UCB, las iniciales de la Universidad de California, en Berkeley. Aumentaron la capacidad del usuario

ordinario UCB, diseñando una subrutina para “captar“ los privilegios del súper usuario “Jim Miller“. Su “ciberpaseo“ terminó al intentar hojear unos ficheros “cebo”, preparados para mantener el mayor tiempo posible conectados a los hackers, pero no sin antes sacar algo de provecho: el manual de Unix, el sistema operativo multitarea, diseñado por los laboratorios Bell (organismo de investigación de la ATT) la mayor compra a telefónica de EE.UU.

Herbert Zinn, (expulsado de la educación media superior), y que operaba bajo el seudónimo de “Shadowhawk“, fue el primer sentenciado bajo el cargo de Fraude Computacional y Abuso en 1986. Zinn tenia 17 años cuando violo el acceso a AT&T y los sistemas del Departamento de Defensa. Fue sentenciado el 23 de enero de 1989, por la destrucción del equivalente a US $174,000 en archivos, copias de programas, los cuales estaban valuados en millones de dólares, además publicó contraseñas y instrucciones de cómo violar la seguridad de los sistemas computacionales. Zinn fue sentenciado a 9 meses de cárcel y a una fianza de US$10,000. Se estima que Zinn hubiera podido alcanzar una sentencia de 13 años de prisión y una fianza de US$800,000 si hubiera tenido 18 años en el momento del crimen.

Holland, Wau y Wenery, Steffen, el 2 de mayo de 1987, los dos hackers alemanes, de 23 y 20 años respectivamente, ingresaron sin autorización al sistema de la central de investigaciones aerospaciales más grande del mundo. Por qué lo hicieron?, preguntó meses después un periodista norteamericano.

Porque es fascinante. En este mundo se terminaron las aventuras. Ya nadie puede salir a cazar dinosaurios o a buscar oro. La única aventura posible — respondió Steffen, está en la pantalla de un computador. Cuando advertimos que los técnicos nos hablan detectado, les enviamos un telex: Tememos haber entrado en el peligroso campo del espionaje industrial, el crimen económico, el conflicto este-oeste y la seguridad de los organismos de alta tecnología. Por eso avisamos, y paramos el juego.

Morris Robert, en noviembre de 1988, Morris lanzó un programa “gusano“ diseñado por el mismo para navegar en Internet, buscando debilidades en sistemas de seguridad, y que pudiera correrse y multiplicarse por si solo. La expansión exponencial de este programa causó el consumo de los recursos de muchísimas computadoras y que más de 6000 sistemas resultaron dañados o fueron seriamente perjudicados. Eliminar al gusano de sus computadoras causó a las victimas muchos días de productividad perdidos, y millones de dólares. Se creó el CERT (Equipo de respuesta de emergencias computacionales) para combatir problemas similares en el futuro. Morris fue condenado y sentenciado a tres años de libertad condicional, 400 horas de servicio comunitario y US $10,000 de fianza, bajo el cargo de fraude computacional y abuso. La sentencia fue fuertemente criticada debido a que fue muy ligera, pero reflejaba lo inocuo de las intenciones de Morris mas que el daño causado. El gusano producido por Morris no borra ni modifica archivos en la actualidad.
Poulsen Kevin, Dark Dante, en diciembre de 1992 Kevin Poulsen, que alguna vez utilizó el alias de “Dark Dante“ en las redes de computadoras fue acusado de robar órdenes de tarea relacionadas con un ejercicio de la fuerza aérea militar americana. Se acusó a Poulsen del robo de información nacional bajo una sección del estatuto de espionaje federal y encara hasta 10 años en la cárcel.
Siguió el mismo camino que Kevin Mitnick, pero es más conocido por su habilidad para controlar el sistema telefónico de Pacific Bell. Incluso llegó a “ganar“ un Porsche en un concurso radiofónico, si su llamada fuera la 102, y así fue. Poulsen también crackeó todo tipo de sitios, pero él se interesaba por los que contenían material de defensa nacional. Esto fue lo que lo llevó a su estancia en la cárcel, 5 anos, fue liberado en 1996, supuestamente “reformado“. Que dicho sea de paso, es el mayor tiempo de estancia en la cárcel que ha comparecido un hacker.
La Macchia, David, en 1994 David La Macchia, estudiante de 20 anos del prestigioso y serio MIT (Massachusetts Institute of Technology), reconoce que ha

distribuido en Internet multitud de programas informáticos obtenidos sin licencia y por valor de 1 millón de dólares. Para ofrecerlos a los cibernautas montó su propia BBS (Bulletin Board System - sistema que ofrece servicios avanzados de mensajería, boletines y archivos). Todo un escándalo que manchó el nombre de esta mítica institución universitaria.
Levin, Vladimir, un matemático ruso de 24 anos, penetró vía Internet desde San Petersburgo en los sistemas informáticos centrales del banco Citibank en Wall Street, logró transferir a diferentes cuentas de EE.UU., Rusia, Finlandia, Alemania, Israel, Holanda y Suiza fondos por valor de 10 millones de dólares, según el FBI. Detenido en el Reino Unido a principios de 1995, Levin espera que los tribunales británicos se pronuncien sobre una demanda de extradición solicitada por EE.UU.
Mentor, El, H4G13, casi todo es posible dentro de la imaginación de los hackers. Un grupo de ellos, a los que algunos llaman corsarios, denominado H4G13, consiguió romper los códigos de seguridad de la NASA.
Kevin & Ronald, Makaveli & Tooshort, Ronald y Kevin, con los nombres de guerra Makaveli y TooShort en el ciberespacio, asaltaron las computadoras del Pentágono en Marzo del ano 1998, a la edad de 17 anos. Con sus conocimientos y con un equipo básico informático, se introdujeron en cuatro sistemas de la Marina y siete de las fuerzas aéreas, relacionados con centros digitales en Estados Unidos y Okinawa. Simplemente fueron formados por algún “experto hacker“, que se encontraba a miles de kilómetros de su pueblo natal, Cloverdale, y que se hacia llamar el “Pirata Maestro”.
Estas acciones no son novedosas en el mundo del Hacking. El mayor sueno de un recién estrenado hacker es “colarse“ en las profundidades del mayor organismo de seguridad del mundo, pero normalmente, el riesgo que entraña, y sus consecuencias legales, hace que lo hagan por computadoras de Universidades, o

de empresas que no son muy conocidas.
Smith, David, programador de 30 anos, detenido por el FBI y acusado de crear y distribuir el virus que ha bloqueado miles de cuentas de correo, “Melissa“. Entre los cargos presentados contra él, figuran el de “bloquear las comunicaciones publicas“ y de “dañar los sistemas informáticos“. Acusaciones que en caso de demostrarse en el tribunal podrían acarrearle una pena de hasta diez anos de cárcel.
Melissa había conseguido contaminar a más de 100,000 computadoras de todo el mundo, incluyendo a empresas como Microsoft, Intel, Compaq, administraciones públicas estadounidenses como la del Gobierno del Estado de Dakota del Norte y el Departamento del Tesoro.
En España su “éxito“ fue menor al desarrollarse una extensa campana de información, que alcanzó incluso a las cadenas televisivas, alertando a los usuarios de la existencia de este virus.
La detención de David Smith fue fruto de la colaboración entre los especialistas del FBI y de los técnicos del primer proveedor de servicios de conexión a Internet de los Estados Unidos, América On Line.
Los ingenieros de América On Line colaboraron activamente en la investigación al descubrir que para propagar el virus, Smith había utilizado la identidad de un usuario de su servicio de acceso. Además, como otros proveedores el impacto de Melissa había afectado de forma sustancial a buzones de una gran parte de sus catorce millones de usuarios.
Fue precisamente el modo de actuar de Melissa, que remite a los cincuenta primeros inscritos en la agenda de direcciones del cliente de correo electrónico “Outlook Express“, centenares de documentos “Office“ la clave para encontrar al

autor del virus. Los ingenieros rastrearon los primeros documentos que fueron emitidos por el creador del virus, buscando encontrar los signos de identidad que incorporan todos los documentos del programa ofimático de Microsoft “Office“ y que en más de una ocasión han despertado la alarma de organizaciones en defensa de la privacidad de los usuarios. Una vez desmontado el puzzle de los documentos y encontradas las claves se consiguió localizar al creador de Melissa. Sin embargo, la detención de Smith no significa que el virus haya dejado de actuar.
Compañías informáticas siguen alertando que aun pueden quedar miles de usuarios expuestos a sus efectos, por desconocimiento o por no haber instalado en sus equipos sistemas antivíricos que frenen la actividad de Melissa u otros virus.
Ing-Hou, Chen, Taipei, Taiwan, Abril 30 de 1999. El autor del virus “Chernobyl”, dijo a los investigadores que el creó el bug con la esperanza de humillar y vengarse de los que llamo “proveedores incompetentes de antivirus para software”, dijo la policía ahora. Pero él admitió que no esperaba que CIH causara daño alrededor del mundo. Este virus devastó cientos de miles de computadoras alrededor del mundo.
El virus Chernobyl U conocido en Taiwan como el CIH, por las iniciales de Chen, fue mostrado a la Armada China de Liberación para que lo estudiaran.
Chen creó el virus en Abril, cuando todavía era estudiante de ingeniería computacional en el Instituto Tecnológico. Chen desde su egreso ha estado bajo el mandato de Taiwan a dos años de servicio militar.
Este inusual virus destructivo; programado para funcionar el 26 de Abril, o sea el 13 aniversario del desastre nuclear de Chernobyl, trata de borrar el disco duro de la computadora y escribir garabatos dentro del sistema para que no arranque la maquina.

Casos anónimos sonados de crimen por computadora.
1988, varios hackers consiguieron entrar en las computadoras de siete universidades de Gran Bretaña, la de Londres incluida. Para resolver este crimen, la policía necesitó la ayuda técnica de un asesor informático, Robert Jones. Una vez arrestado un sospechoso, las pruebas se analizaron durante un año y medio antes de presentarlas ante el tribunal, que lo condenó a un año de prisión. Después de varias colaboraciones más, Scotland Yard propuso la creación de un centro universitario dedicado a la investigación de estos casos.
El Centro de Investigación de Delitos Informáticos, adscrito al Queen Mary & Westfield College, se creó a principios de 1996 y el abogado Ian Walden, experto en la legislación de tecnología de la información, es su director. El Centro obtiene fondos del Gobierno y se dedica a la investigación y la accesoria en el campo de los delitos informáticos, así como a impartir cursos de formación en la materia para policías, fiscales, abogados y cualquier interesado.
1989, la justicia alemana detiene a un grupo de crackers germanos que hablan copiado durante años miles de programas de acceso no legal y passwords de computadores en departamentos de la administración de EEUU. El destinatario de la información era el KGB soviético.
1993, la compañía discográfica Frank music Corporation vence en su demanda contra Compuserve, el mayor proveedor de Internet, por permitir que sus abonados copiaran mas de 500 canciones sometidas a derechos de autor. Otras 140 discográficas han denunciado a Compuserve por idéntica razón.
La revista Play Boy gana un juicio contra George Frena, que habla distribuido ilegalmente en su BBS fotos de desnudos procedentes del Web de esta publicación. En 1993 y 1994, Play Boy denunció a 12 BBS más por el mismo

motivo.
Todos estos asaltos no suelen tener consecuencias importantes, pero lo peor de todo es cuando lo efectúan los crackers o hackers de contraseñas.
1994, uno de los casos más destacados que se produjo en ese año es el que, cuando varios “piratas“ consiguieron introducirse en el sistema de seguridad de la Florida State University, violándolo y llevándose consigo varias copias de prueba de Windows 95, uno de los más potentes sistemas operativos de Microsoft, que en aquel entonces no era comercial ni publico.
Crackers americanos se hacen vía Internet desde Mallorca con 140.000 números de tarjetas de crédito telefónicas de EEUU. Usuarios de todo el mundo llaman a cuenta de las víctimas. El fraude llega a los 140 millones de dólares perdidos por compañías como Bell Atlantic, MCI o AT&T.
1995, en agosto de ese año, Adam Back (británico), Eric Young (australiano) y David Byers (sueco), demuestran en Internet como pueden violarse en cuestión de minutos los algoritmos de seguridad de Netscape Navigator, el programa de acceso a WWW más usado mundialmente. Al mes siguiente, los cyberpunks americanos David Wagner y Ian Goldberg crean un método para violarlo en sólo 25 segundos.
1996, Public Access Networks Corp., una de las grandes empresas dedicadas al suministro de acceso a la red de Estado Unidos, que controla las páginas de más de 1,000 empresas en la World Wide Web, sufrió un feroz ataque por parte de piratas informáticos. Estos llevaron a la locura a las computadoras de la empresa mediante el continuo envío de solicitudes de información adulteradas, mas de
150 por segundo.
Como ejemplo, tenemos lo que sucedió el 19 de Septiembre de ese año, cuando

la CIA sufrió los ataques de un grupo de Hackers suecos, que desmantelaron su servidor de Información en Internet, modificando el mensaje de presentación "Bienvenidos a la Agencia Central de Inteligencia" por "Bienvenidos a la Agencia Central de Estupid...". Entre la maraña de contenidos de la Web, colocaron también varias conexiones directas a otros lugares de Internet, como a las revistas Flashback o Playboy. La CIA experimentó una grave derrota.
El Grupo Antipiratería de la empresa de software Novell, informaba de la captura de un individuo que respondía al alias de "El Pirata". Con la colaboración de la Policía de Zurich, Novell consiguió atrapar a este cracker que ofrecía productos de la compañía a usuarios de Internet de forma ilegal por valor de 60.000 dólares, junto con software comercial de otros miembros de la BSA (Business Software Aliance). Se localizaron también instrucciones para realizar operaciones fraudulentas con tarjetas de crédito.
1997, en Mayo, un grupo de hackers asaltan la página de una de las películas más taquilleras de la fábrica Spilberg: Jurassic Park, cambiando durante 18 horas el logotipo del dinosaurio por otro en el que aparece un pato.
La Homepage de Microsoft fue atacada por varios hackers en junio de ese año. Estos hackers, accedieron al sistema operativo por un bug de Windows Nt 4.0, el cual era el servidor bajo el que se ejecutaba la Web de Microsoft. Hay muchas formas de dar publicidad a actos "presumiblemente ilegales", pero algunas son más ingeniosas que otras.
Price, un joven hacker que accedía gratuitamente al sistema telefónico chileno y desde ahí conseguía entrar en las computadoras del Ministerio de Defensa de los Estados Unidos. Llegó a copiar archivos que no eran materia reservada, pero si investigaciones de temas delicados. Su centro de trabajo era su casa, en Londres, y desde ahí causó uno de los mayores desastres informáticos de la

década. No trabajaba solo, por lo que intercambió todos los documentos que habla obtenido con hackers de distintos países, vía Internet. El caos fue total, llegando incluso al cierre temporal de la red norteamericana. Estos grupos tienen una forma de operar muy estricta, y la exclusión de uno de sus miembros significa la recesión total de privilegios, y la condena al ostracismo virtual. Fidelidad, confidencialidad y tenacidad son los rasgos más comunes entre los hackers.
Se publica el libro "Takedown" de Tsutomu Shimomura y John Markoff de la editorial El País-Aguilar de 464 páginas. En el se relatan la búsqueda y captura de un escurridizo hacker que domina el arte del "IP-spoofing", que consiste en producir falsos números IP para ser reconocido por otras máquinas conectadas y pasearse por su interior. Es un reportaje novelado, contado en primera persona por el experto en seguridad Tsutomu Shimomura, que fue saqueado por el hacker en plena navidad del 94 y dedicó medio año a detenerle. Lo escribió junto a John Markoff, un periodista del New York Times que habla seguido el caso.
Microsoft embargó cerca de 100,000 copias ilegales o programas falsos, CD-ROM y dispositivos hardware, procedentes de canales de distribución europeos y con un valor de más de 23 millones de dólares.
2001, En mayo se ha hecho publico roces entre los Hackers Chinos y los Estadounidenses, Hackers de ambos países se han retado a duelo en la Internet, alterando decenas de sitios si causar daños aparentes. "Los hackers pro-China atacaron hoy otros 14 sitios estadounidenses, además de los 12 que atacaron el domingo y los 4 del sábado", dice Michael Cheek, editor de los servicios de inteligencia de iDEFENSE, una importante firma de inteligencia y evaluación de riesgos de Fairfax, Virginia.
"Pero parece que los hackers pro-estadounidenses están respondiendo con fuerza", dijo. "Hasta ahora son 24 los sitios chinos en la red, incluyendo ocho

gubernamentales, que han sido atacados el lunes“, dijo Cheek a CNN.
Dice que un informe preparado por iDEFENSE a ultima hora del lunes mostrarla que entre los sitios atacados el domingo y el lunes abundan los pertenecientes al gobierno federal, algunos sitios comerciales, organizaciones privadas e instituciones de educación publica.
Un funcionario involucrado con la lucha contra los hackers confirmó la existencia de ataques adicionales efectuados el lunes, pero dijo que “los sistemas de defensa están aguantando“ y no se han denunciado daños de importancia.
La amenaza está siendo tomada seriamente por el Pentágono, que modificó su Condición de Información --el estado de sus sistemas informáticos-- de normal a alfa, que indica que la probabilidad de un ataque ha aumentado.
El Departamento de Defensa es el principal usuario de computadoras dentro del gobierno de los EE.UU. y mantiene oficinas que son asistidas por especialistas en seguridad los 365 días del año, cuya única tarea es la de mantener a raya los ataques informáticos.
El FBI habla advertido la semana pasada sobre la posibilidad de estos ataques debido a la existencia de fechas conmemorativas durante esta semana, incluyendo el Día de Trabajadores.
Un experto en seguridad informática dijo que los ataques no parecen ser nada fuera de lo común. “La alteración de sitios de Internet es un típico ataque utilizado por activistas políticos ya que provee la audiencia para exhibir un mensaje político“, dice Rob Clyde, jefe de tecnologías de Symantec, una firma que provee sistemas de seguridad. “Esto es el equivalente de pintar un mensaje con aerosol sobre el frente del edificio de una compañía“, dice. “Cada día son atacados entre 30 y 50 sitios, por lo que hasta el momento los ataques chinos no han

excedido lo normal“.
Un reporte de la firma iDEFENSE expresa que entre las páginas alteradas el domingo y el lunes se encuentran una de la Casa Blanca, dos de la Marina y dos de Institutos Nacionales de Salud. También fue atacado el sitio del Departamento de Trabajo. En la página principal se publicó un tributo al desaparecido piloto chino Wang Wei junto con su fotografía. “Todo el país está triste“ dice el texto. (Wang es el piloto chino derribado por el avión espía estadounidense. Se encuentra desaparecido y se presume que ha muerto).
De acuerdo con el Departamento de Trabajo, el ataque se limitó a la página principal y no se alteró ninguna otra página del sitio. “No hubo daños monetarios“, dijo Roy. “Si se trató de una travesura o de un intento de hacer más daño, no lo sé“. El contenido modificado estuvo disponible durante seis horas del sábado hasta que todo el sistema fue desconectado. Luego de otras cuatro horas de verificación y búsqueda de virus y posibles daños, el sitio fue puesto nuevamente en línea. Pudiendo quedar virus ocultos
El lunes 30 de abril se produjeron nuevos incidentes. En la página principal del servicio noticioso de United Press International, se publicó una bandera china con el mensaje: “iiHurra a la Gran Nación China!! iiLos EE.UU. serán totalmente responsables por el accidente!! iiOpónganse a la venta de armas a Taiwán, destruye la paz mundial!!“. La fuente de estos mensajes no pudo ser determinada.
El personal de Network Associates, una firma de seguridad de Silicon Valley, también denunció cierta actividad de intrusos durante el lunes. Vincent Gullotto, vicedirector de los laboratorios de seguridad, calificó como baja-media a la amenaza china. Destacó que los ataques consistieron en simples alteraciones de páginas, lo cual es más fácil y rápido e implica menores riesgos de ser detectado.
Sin embargo, señaló que si hubieran inyectado algún virus, este podría no activarse

hasta que el sistema sea reiniciado o se llegue a una fecha determinada.
Los ataques en favor de los Estados Unidos pueden no provenir de ese país. Uno de los hackers más notorios, conocido como PoisonBox se declaró responsable por la alteración de 238 sitios chinos desde hace cierto tiempo, e insistió en que no se trata de un ciudadano estadounidense, dijo Cheek. Los analistas creen que ha continuado con sus actividades en Taiwán y Malasia.
El Centro Nacional de Protección de Infraestructura de Información del FBI, que emitió la advertencia sobre posibles ataques, dijo no contar con ninguna información nueva. Las declaraciones del FBI también advierten sobre la existencia de un gusano llamado “Lion“ que infecta computadoras e interfiere las herramientas de servicios de varios sistemas.