DELITOS INFORMÁTICOS

Trabajo realizado por:

Melvin Leonardo Landaverde Contreras
mlandav@yahoo.com
Joaquín Galileo Soto Campos
jg_soto@yahoo.com
Jorge Marcelo Torres Lipe
chelo_lipe@yahoo.com
Universidad de El Salvador

Octubre de 2000

Índice general

1. 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.

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».

Debido a lo anterior se desarrolla el presente documento que contiene una investigación sobre la temática de los delitos informáticos, de manera que al final pueda establecerse una relación con la auditoría informática.

Para lograr una investigación completa de la temática se establece la conceptualización respectiva del tema, generalidades asociadas al fenómeno, estadísticas mundiales sobre delitos informáticos, el efecto de éstos en diferentes áreas, como poder minimizar la amenaza de los delitos a través de la seguridad, aspectos de legislación informática, y por último se busca unificar la investigación realizada para poder establecer el papel de la auditoría informática frente a los delitos informáticos.

Al final del documento se establecen las conclusiones pertinentes al estudio, en las que se busca destacar situaciones relevantes, comentarios, análisis, etc.

2. Objetivos

General

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

Específicos.

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

3. Alcances y Limitaciones

Alcances

Esta investigación sólo tomará en cuenta el estudio y análisis de la información referente al problema del Delito Informático, tomando en consideración aquellos elementos que aporten criterios con los cuales se puedan realizar juicios valorativos respecto al papel que juega la Auditoria Informática ante éste tipo de hechos.

Limitaciones

La principal limitante para realizar ésta investigación es la débil infraestructura legal que posee nuestro país con respecto a la identificación y ataque a éste tipo de Delitos, no obstante se poseen los criterios suficientes sobre la base de la experiencia de otras naciones para el adecuado análisis e interpretación de éste tipo de actos delictivos.

4. Conceptualización y generalidades.

Conceptualización

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

Muchos estudiosos del Derecho Penal han intentado formular una noción de delito que sirviese para todos los tiempos y en todos los países. Esto no ha sido posible dada la íntima conexión que existe entre la vida social y la jurídica de cada pueblo y cada siglo, aquella condiciona a ésta.

Según el ilustre penalista CUELLO CALON, los elementos integrantes del delito son:

El delito es un acto humano, es una acción (acción u omisión)

Dicho acto humano ha de ser antijurídico, debe lesionar o poner en peligro un interés jurídicamente protegido.

Debe corresponder a un tipo legal (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 por una pena.

Por tanto, un delito es: una acción antijurídica realizada por un ser humano, tipificado, culpable y sancionado por una pena.

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

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

culpables en que se tienen a las computadoras como instrumento o fin (concepto típico)». Por su parte, el tratadista penal italiano Carlos SARZANA, sostiene que los delitos informáticos son «cualquier comportamiento criminal en que la computadora está involucrada como material, objeto o mero símbolo».

Algunas consideraciones.

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

La informática esta hoy presente en casi todos los campos de la vida moderna. Con mayor o menor rapidez todas las ramas del saber humano se rinden ante los progresos tecnológicos, y comienzan a utilizar los sistemas de Información para ejecutar tareas que en otros tiempos realizaban manualmente.

El progreso cada día más importante y sostenido de los sistemas computacionales permite hoy procesar y poner a disposición de la sociedad una cantidad creciente de información de toda naturaleza, al alcance concreto de millones de interesados y de usuarios. Las más diversas esferas del conocimiento humano, en lo científico, en lo técnico, en lo profesional y en lo personal están siendo incorporadas a sistemas informáticos que, en la práctica cotidiana, de hecho sin limitaciones, entrega con facilidad a quien lo desee un conjunto de datos que hasta hace unos años sólo podían ubicarse luego de largas búsquedas y selecciones en que el

hombre jugaba un papel determinante y las máquinas existentes tenían el rango de equipos auxiliares para imprimir los resultados. En la actualidad, en cambio, ese enorme caudal de conocimiento puede obtenerse, además, en segundos o minutos, transmitirse incluso documentalmente y llegar al receptor mediante sistemas sencillos de operar, confiables y capaces de responder casi toda la gama de interrogantes que se planteen a los archivos informáticos.

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

Este es el panorama de este nuevo fenómeno científico tecnológico en las sociedades modernas. Por ello ha llegado a sostenerse que la Informática es hoy una forma de Poder Social. Las facultades que el fenómeno pone a disposición de Gobiernos y de particulares, con rapidez y ahorro consiguiente de tiempo y energía, configuran un cuadro de realidades de aplicación y de posibilidades de juegos lícito e ilícito, en donde es necesario el derecho para regular los múltiples efectos de una situación, nueva y de tantas potencialidades en el medio social.

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

Esta marcha de las aplicaciones de la informática no sólo tiene un lado ventajoso sino que plantea también problemas de significativa importancia para el funcionamiento y la se-

guridad de los sistemas informáticos en los negocios, la administración, la defensa y la sociedad.

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

De acuerdo con la definición elaborada por un grupo de expertos, invitados por la OCDE a París en mayo de 1983, el término delitos relacionados con las computadoras se define como cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático de datos y/o transmisiones de datos. La amplitud de este concepto es ventajosa, puesto que permite el uso de las mismas hipótesis de trabajo para toda clase de estudios penales, criminólogos, económicos, preventivos o legales.

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

El espectacular desarrollo de la tecnología informática ha abierto las puertas a nuevas posibilidades de delincuencia antes impensables. La manipulación fraudulenta de los ordenadores con ánimo de lucro, la destrucción de programas o datos y el acceso y la utilización indebida de la información que puede afectar la esfera de la privacidad, son algunos de los procedimientos relacionados con el procesamiento

electrónico de datos mediante los cuales es posible obtener grandes beneficios económicos o causar importantes daños materiales o morales. Pero no sólo la cuantía de los perjuicios así ocasionados es a menudo infinitamente superior a la que es usual en la delincuencia tradicional, sino que también son mucho más elevadas las posibilidades de que no lleguen a descubrirse. Se trata de una delincuencia de especialistas capaces muchas veces de borrar toda huella de los hechos.

En este sentido, la informática puede ser el objeto del ataque o el medio para cometer otros delitos. La informática reúne unas características que la convierten en un medio idóneo para la comisión de muy distintas modalidades delictivas, en especial de carácter patrimonial (estafas, apropiaciones indebidas, etc.). La idoneidad proviene, básicamente, de la gran cantidad de datos que se acumulan, con la consiguiente facilidad de acceso a ellos y la relativamente fácil manipulación de esos datos.

La importancia reciente de los sistemas de datos, por su gran incidencia en la marcha de las empresas, tanto públicas como privadas, los ha transformado en un objeto cuyo ataque provoca un perjuicio enorme, que va mucho más allá del valor material de los objetos destruidos. A ello se une que estos ataques son relativamente fáciles de realizar, con resultados altamente satisfactorios y al mismo tiempo procuran a los autores una probabilidad bastante alta de alcanzar los objetivos sin ser descubiertos.

Características de los delitos

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

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

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

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

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

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

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

Son muy sofisticados y relativamente frecuentes en el ámbito militar.

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

Tienden a proliferar cada vez más, por lo que requieren una urgente regulación. Por el momento siguen siendo ilícitos impunes de manera manifiesta ante la ley.

Sistemas y empresas con mayor riesgo.

Evidentemente el artículo que resulta más atractivo robar es el dinero o algo de valor. Por lo tanto, los sistemas que pueden estar más expuestos a fraude son los que tratan pagos, como los de nómina, ventas, o compras. En ellos es donde es más fácil convertir transacciones fraudulentas en dinero y sacarlo de la empresa.

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

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

- Tratan grandes volúmenes de datos e interviene poco personal, lo que impide verificar todas las partidas.
- Se sobrecargan los registros magnéticos, perdiéndose la evidencia auditable o la secuencia de acontecimientos.
- A veces los registros magnéticos son transitorios y a menos que se realicen pruebas dentro de un período de tiempo corto, podrían perderse los detalles de lo que sucedió, quedando sólo los efectos.
- Los sistemas son impersonales, aparecen en un formato ilegible y están controlados parcialmente por personas cuya principal preocupación son los aspectos técnicos del equipo y del sistema y que no comprenden, o no les afecta, el significado de los datos que manipulan.
- En el diseño de un sistema importante es difícil asegurar que se han previsto todas las situaciones posibles y es probable que en las previsiones que se hayan hecho queden huecos sin cubrir. Los siste-

mas tienden a ser algo rígidos y no siempre se diseñan o modifican al ritmo con que se producen los acontecimientos; esto puede llegar a ser otra fuente de «agujeros».

- Sólo parte del personal de proceso de datos conoce todas las implicaciones del sistema y el centro de cálculo puede llegar a ser un centro de información. Al mismo tiempo, el centro de cálculo procesará muchos aspectos similares de las transacciones.
- En el centro de cálculo hay un personal muy inteligente, que trabaja por iniciativa propia la mayoría del tiempo y podría resultar difícil implantar unos niveles normales de control y supervisión.
- El error y el fraude son difíciles de equiparar. A menudo, los errores no son iguales al fraude. Cuando surgen discrepancias, no se imagina que se ha producido un fraude, y la investigación puede abandonarse antes de llegar a esa conclusión. Se tiende a empezar buscando errores de programación y del sistema. Si falla esta operación, se buscan fallos técnicos y operativos. Sólo cuando todas estas averiguaciones han dado resultados negativos, acaba pensándose en que la causa podría ser un fraude.

Delitos en perspectiva

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

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

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

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

5. Tipificación de los delitos informáticos

Clasificación Según la Actividad Informática

Sabotaje informático

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

Conductas dirigidas a causar daños físicos

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

Conductas dirigidas a causar daños lógicos

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

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

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

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

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

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

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

Fraude a través de computadoras

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

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

Ulrich Sieber, cita como ejemplo de esta modalidad el siguiente caso tomado de la jurisprudencia alemana:

Una empleada de un banco del sur de Alemania transfirió, en febrero de 1983, un millón trescientos mil marcos alemanes a la cuenta de una amiga –cómplice en la maniobra– mediante el simple mecanismo de imputar el crédito en una terminal de computadora del banco. La operación fue realizada a primera hora de la mañana y su falsedad podría haber sido detectada por el sistema de seguridad del banco al mediodía. Sin embargo, la rápida transmisión del crédito a través de sistemas informáticos conectados en línea (on line), hizo posible que la amiga de la empleada retirara, en otra sucursal del banco, un millón doscientos ochenta mil marcos unos minutos después de realizada la operación informática.

En segundo lugar, es posible interferir en el correcto procesamiento de la información, alterando el programa o secuencia lógica con el que trabaja el ordenador. Esta modalidad puede ser cometida tanto al modificar los programas originales, como al adicionar al sistema programas especiales que introduce el autor.

A diferencia de las manipulaciones del input que, incluso, pueden ser realizadas por personas sin conocimientos especiales de informática, esta modalidad es más específicamente informática y requiere conocimientos técnicos especiales.

Sieber cita como ejemplo el siguiente caso, tomado de la jurisprudencia alemana:

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

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

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

Una característica general de este tipo de fraudes, interesante para el análisis jurídico, es que, en la mayoría de los casos detectados, la conducta delictiva es repetida varias veces en el tiempo. Lo que sucede es que, una vez que el autor descubre o genera una laguna o falla en el sistema, tiene la posibilidad de repetir, cuantas veces quiera, la comisión del hecho. Incluso, en los casos de «manipulación del programa», la reiteración puede ser automática, realizada por el mismo sistema sin ninguna participación del autor y

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

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

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

Ejemplos

El autor, empleado del Citibank, tenía acceso a las terminales de computación de la institución bancaria. Aprovechando esta circunstancia utilizó, en varias oportunidades, las terminales de los cajeros, cuando ellos se retiraban, para transferir, a través del sistema informático, fondos de distintas cuentas a su cuenta personal.

Posteriormente, retiró el dinero en otra de las sucursales del banco.

En primera instancia el Juez calificó los hechos como constitutivos del delito de hurto en forma reiterada. La Fiscalía de Cámara solicitó el cambio de calificación, considerando que los hechos constituían el delito de estafa.

La Cámara del crimen resolvió:

«... y contestando a la teoría fiscal, entiendo que le asiste razón al Dr. Galli en cuanto sostiene que estamos en presencia del tipo penal de hurto y no de estafa. Ello es así porque el apoderamiento lo hace el procesado y no le entrega el banco por medio de un error, requisito indispensable para poder hablar de estafa. El apoderamiento lo hace el procesado directamente, manejando el sistema de computación. De manera que no hay diferencia con la maniobra normal del cajero, que en un descuido se apodera del dinero que maneja en caja y la maniobra en estudio en donde el apoderamiento del dinero se hace mediante el manejo de la computadora...»

Como el lector advertirá, la resolución adolece de los problemas de adecuación típica a que hacíamos referencias más arriba.

En realidad, el cajero no realizó la conducta de apoderamiento que exige el tipo penal del hurto ya que recibió el dinero de manos del cajero. En el caso de que se considere que el apoderamiento se produjo en el momento en el que el autor transfirió los fondos a su cuenta, el escollo de adecuación típica insalvable deriva de la falta de la «cosa mueble» como objeto del apoderamiento exigido por el tipo penal.

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 y el «animus defraudandi» 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.

«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.

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.

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.

Blanqueo de dinero: Se espera que el comercio electrónico sea el nuevo lugar de transferencia electrónica de mercancías o dinero para lavar las ganancias que deja el delito, sobre todo si se pueden ocultar transacciones.

Copia ilegal de software y espionaje informático.

Se engloban las conductas dirigidas a obtener datos, en forma ilegítima, de un sistema de información. Es común el apoderamiento de datos de investigaciones, listas de clientes, balances, etc. En muchos casos el objeto del apodera-

miento es el mismo programa de computación (software) que suele tener un importante valor económico.

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

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

Uso ilegítimo de sistemas informáticos ajenos.

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

Acceso no autorizado: La corriente reguladora sostiene que el uso ilegítimo de passwords y la entrada en un sistema informático sin la autorización del propietario debe quedar tipificado como un delito, puesto que el bien jurídico que acostumbra a protegerse con la contraseña es lo suficientemente importante para que el daño producido sea grave.

Delitos informáticos contra la privacidad.

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

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

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

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

Las circunstancias de la víctima: menor de edad o incapaz.

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

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

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.

Clasificación Según el Instrumento, Medio o Fin u Objetivo

Asimismo, TELLEZ VALDEZ clasifica a estos delitos, de acuerdo a dos criterios:

Como instrumento o medio.

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

Falsificación de documentos vía computarizada (tarjetas de crédito, cheques, etc.)

Variación de los activos y pasivos en la situación contable de las empresas.

Planeamiento y simulación de delitos convencionales (robo, homicidio, fraude, etc.)

Lectura, sustracción o copiado de información confidencial.

Modificación de datos tanto en la entrada como en la salida.

Aprovechamiento indebido o violación de un código para penetrar a un sistema introduciendo instrucciones inapropiadas.

Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa.

Uso no autorizado de programas de computo.

Introducción de instrucciones que provocan «interrupciones» en la lógica interna de los programas.

Alteración en el funcionamiento de los sistemas, a través de los virus informáticos.

Obtención de información residual impresa en papel luego de la ejecución de trabajos.

Acceso a áreas informatizadas en forma no autorizada.

Intervención en las líneas de comunicación de datos o teleproceso.

Como fin u objetivo.

En esta categoría, se enmarcan las conductas criminales que van dirigidas contra las computadoras, accesorios o programas como entidad física, como por ejemplo:

Programación de instrucciones que producen un bloqueo total al sistema.

Destrucción de programas por cualquier método.

Daño a la memoria.

Atentado físico contra la máquina o sus accesorios.

Sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centros neurálgicos computarizados.

Secuestro de soportes magnéticos entre los que figure información valiosa con fines de chantaje (pago de rescate, etc.).

Clasificación según Actividades Delictivas Graves

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

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.

Tanto el FBI como el Fiscal General de los Estados Unidos han alertado sobre la necesidad de medidas que permitan interceptar y descifrar los mensajes encriptados que utilizan los narcotraficantes para ponerse en contacto con los cárteles.

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.

Otros delitos: Las mismas ventajas que encuentran en la Internet los narcotraficantes pueden ser aprovechadas para la planificación de otros delitos como el tráfico de armas, proselitismo de sectas, propaganda de grupos extremistas, y cualquier otro delito que pueda ser trasladado de la vida real al ciberespacio o al revés.

Infracciones que no Constituyen Delitos Informáticos

Usos comerciales no éticos: Algunas empresas no han podido escapar a la tentación de aprovechar la red para hacer una oferta a gran escala de sus productos, llevando a cabo «mailings electrónicos» al colectivo de usuarios de un

gateway, un nodo o un territorio determinado. Ello, aunque no constituye una infracción, es mal recibido por los usuarios de Internet, poco acostumbrados, hasta fechas recientes, a un uso comercial de la red.

Actos parasitarios: Algunos usuarios incapaces de integrarse en grupos de discusión o foros de debate online, se dedican a obstaculizar las comunicaciones ajenas, interrumpiendo conversaciones de forma repetida, enviando mensajes con insultos personales, etc.

También se deben tomar en cuenta las obscenidades que se realizan a través de la Internet.

6. Estadísticas Sobre Delitos Informáticos.

Desde hace cinco años, en los Estados Unidos existe una institución que realiza un estudio anual sobre la Seguridad Informática y los crímenes cometidos a través de las computadoras.

Esta entidad es El Instituto de Seguridad de Computadoras (CSI), quien anunció recientemente los resultados de su quinto estudio anual denominado «Estudio de Seguridad y Delitos Informáticos» realizado a un total de 273 Instituciones principalmente grandes Corporaciones y Agencias del Gobierno.

Este Estudio de Seguridad y Delitos Informáticos es dirigido por CSI con la participación Agencia Federal de Investigación (FBI) de San Francisco, División de delitos informáticos. El objetivo de este esfuerzo es levantar el nivel de conocimiento de seguridad, así como ayudar a determinar el alcance de los Delitos Informáticos en los Estados Unidos de Norteamérica.

Entre lo más destacable del Estudio de Seguridad y Delitos Informáticos 2000 se puede incluir lo siguiente:

Violaciones a la seguridad informática.

Respuestas	(%)
No reportaron Violaciones de Seguridad	10%
Reportaron Violaciones de Seguridad	90%

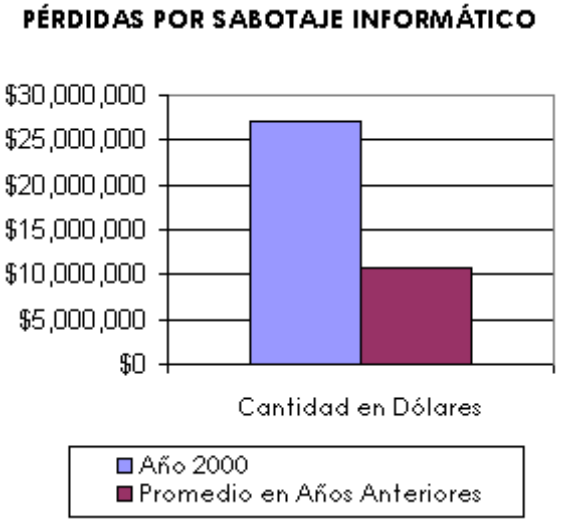
90% de los encuestados descubrió violaciones a la seguridad de las computadoras dentro de los últimos doce meses.

- 70% reportaron una variedad de serias violaciones de seguridad de las computadoras, y que el más común de estas violaciones son los virus de computadoras, robo de computadoras portátiles o abusos por parte de los empleados — por ejemplo, robo de información, fraude financiero, penetración del sistema por intrusos y sabotaje de datos o redes.

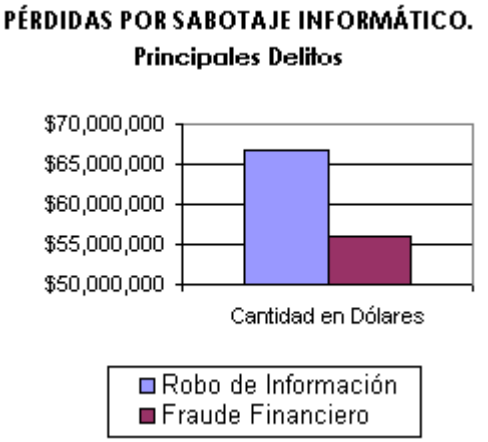
Pérdidas Financieras.

74% reconocieron pérdidas financieras debido a las violaciones de las computadoras.

- Las pérdidas financieras ascendieron a $265,589,940 (el promedio total anual durante los últimos tres años era $120,240,180).



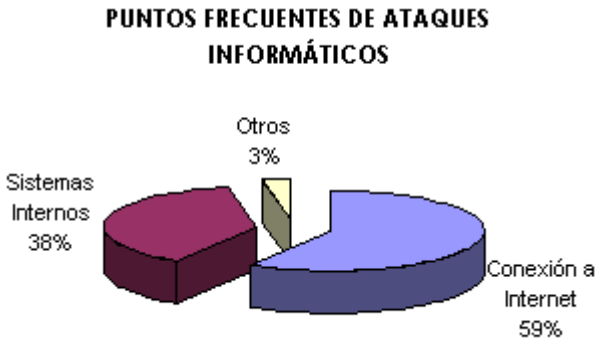
61 encuestados cuantificaron pérdidas debido al sabotaje de datos o redes para un total de $27,148,000. Las pérdidas financieras totales debido al sabotaje durante los años anteriores combinados ascendido a sólo $10,848,850.



Como en años anteriores, las pérdidas financieras más serias, ocurrieron a través de robo de información (66 encuestados reportaron $66,708,000) y el fraude financiero (53 encuestados informaron $55,996,000).

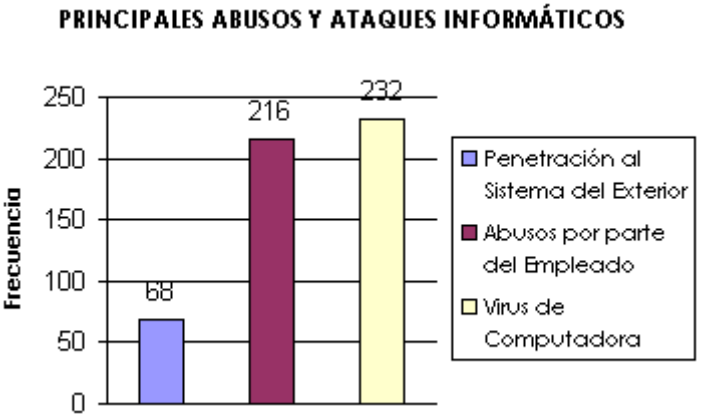
Los resultados del estudio ilustran que esa amenaza del crimen por computadoras a las grandes corporaciones y agencias del gobierno viene de ambos lados dentro y fuera de sus perímetros electrónicos, confirmando la tendencia en años anteriores.

Accesos no autorizados.



71% de los encuestados descubrieron acceso desautorizado por personas dentro de la empresa. Pero por tercer año consecutivo, la mayoría de encuestados (59%) mencionó su conexión de Internet como un punto frecuente de ataque, los que citaron sus sistemas interiores como un punto frecuente de ataque fue un 38%.

Basado en contestaciones de 643 practicantes de seguridad de computadoras en corporaciones americanas, agencias gubernamentales, instituciones financieras, instituciones médicas y universidades, los hallazgos del «Estudio de Seguridad y Delitos Informáticos 2000» confirman que la amenaza del crimen por computadoras y otras violaciones de seguridad de información continúan constantes y que el fraude financiero está ascendiendo.



Los encuestados detectaron una amplia gama a de ataques y abusos. Aquí están algunos otros ejemplos:

- 25% de encuestados descubrieron penetración al sistema del exterior.
- 79% descubrieron el abuso del empleado por acceso de Internet (por ejemplo, transmitiendo pornografía o pirateó de software, o uso inapropiado de sistemas de correo electrónico).
- 85% descubrieron virus de computadoras.
- Comercio electrónico.

Por segundo año, se realizaron una serie de preguntas acerca del comercio electrónico por Internet. Aquí están algunos de los resultados:

93% de encuestados tienen sitios de WWW.

43% maneja el comercio electrónico en sus sitios (en 1999, sólo era un 30%).

19% experimentaron accesos no autorizados o inapropiados en los últimos doce meses.

32% dijeron que ellos no sabían si hubo o no, acceso no autorizado o inapropiado.

35% reconocieron haber tenido ataques, reportando de dos a cinco incidentes.

19% reportaron diez o más incidentes.

64% reconocieron ataques reportados por vandalismo de la Web.

8% reportaron robo de información a través de transacciones.

3% reportaron fraude financiero.

Conclusión sobre el estudio csi:

Las tendencias que el estudio de CSI/FBI ha resaltado por años son alarmantes. Los «Cyber crímenes» y otros delitos de seguridad de información se han extendido y diversificado. El 90% de los encuestados reportaron ataques. Además, tales incidentes pueden producir serios daños. Las 273 organizaciones que pudieron cuantificar sus pérdidas, informaron un total de $265,589,940. Claramente, la mayoría fueron en condiciones que se apegan a prácticas legítimas, con un despliegue de tecnologías sofisticadas, y lo más importante, por personal adecuado y entrenando, practicantes de seguridad de información en el sector privado y en el gobierno.

Otras estadísticas:

- La «línea caliente» de la Internet Watch Foundation (IWF), abierta en diciembre de 1996, ha recibido, principalmente a través del correo electrónico, 781 informes sobre unos 4.300 materiales de Internet considerados ilegales por usuarios de la Red. La mayor parte de los informes enviados a la «línea caliente» (un 85%) se refirieron a pornografía infantil. Otros aludían a fraudes financieros, racismo, mensajes maliciosos y pornografía de adultos.
- Según datos recientes del Servicio Secreto de los Estados Unidos, se calcula que los consumidores pierden unos 500 millones de dólares al año debido a los piratas que les roban de las cuentas online sus números de tarjeta de crédito y de llamadas. Dichos números se pueden vender por jugosas sumas de dinero a falsificadores que utilizan programas especiales para codificarlos en bandas magnéticas de tarjetas bancarias y de crédito, señala el Manual de la ONU.
- Los delincuentes cibernéticos al acecho también usan el correo electrónico para enviar mensajes amenazantes especialmente a las mujeres. De acuerdo al libro de Barbara Jenson «Acecho cibernético: delito, represión y responsabilidad personal en el mundo online», publicado en 1996, se calcula que unas 200.000 personas acechan a alguien cada año.
- En Singapur El número de delitos cibernéticos detectados en el primer semestre del 2000, en el que se han recibido 127 denuncias, alcanza ya un 68 por ciento del total del año pasado, la policía de Singapur prevé un aumento este año en los delitos por Internet de un 38% con respecto a 1999.

- En relación con Internet y la informática, la policía de Singapur estableció en diciembre de 1999 una oficina para investigar las violaciones de los derechos de propiedad y ya ha confiscado copias piratas por valor de 9,4 millones de dólares.
- En El Salvador, existe más de un 75% de computadoras que no cuentan con licencias que amparen los programas (software) que utilizan. Esta proporción tan alta ha ocacionado que organismos Internacionales reacciones ante este tipo de delitos tal es el caso de BSA (Bussines Software Alliance).

7. Impacto de los delitos informáticos

Impacto a Nivel General

En los años recientes las redes de computadoras han crecido de manera asombrosa. Hoy en día, el número de usuarios que se comunican, hacen sus compras, pagan sus cuentas, realizan negocios y hasta consultan con sus médicos online supera los 200 millones, comparado con 26 millones en 1995.

A medida que se va ampliando la Internet, asimismo va aumentando el uso indebido de la misma. Los denominados delincuentes cibernéticos se pasean a su aire por el mundo virtual, incurriendo en delitos tales como el acceso sin autorización o «piratería informática», el fraude, el sabotaje informático, la trata de niños con fines pornográficos y el acecho.

Los delincuentes de la informática son tan diversos como sus delitos; puede tratarse de estudiantes, terroristas o figuras del crimen organizado. Estos delincuentes pueden pa-

sar desapercibidos a través de las fronteras, ocultarse tras incontables «enlaces» o simplemente desvanecerse sin dejar ningún documento de rastro. Pueden despachar directamente las comunicaciones o esconder pruebas delictivas en «paraísos informáticos» - o sea, en países que carecen de leyes o experiencia para seguirles la pista -.

Según datos recientes del Servicio Secreto de los Estados Unidos, se calcula que los consumidores pierden unos 500 millones de dólares al año debido a los piratas que les roban de las cuentas online sus números de tarjeta de crédito y de llamadas. Dichos números se pueden vender por jugosas sumas de dinero a falsificadores que utilizan programas especiales para codificarlos en bandas magnéticas de tarjetas bancarias y de crédito, señala el Manual de la ONU.

Otros delincuentes de la informática pueden sabotear las computadoras para ganarle ventaja económica a sus competidores o amenazar con daños a los sistemas con el fin de cometer extorsión. Los malhechores manipulan los datos o las operaciones, ya sea directamente o mediante los llamados «gusanos» o «virus», que pueden paralizar completamente los sistemas o borrar todos los datos del disco duro. Algunos virus dirigidos contra computadoras elegidas al azar; que originalmente pasaron de una computadora a otra por medio de disquetes «infectados»; también se están propagando últimamente por las redes, con frecuencia camuflados en mensajes electrónicos o en programas «descargados» de la red.

En 1990, se supo por primera vez en Europa de un caso en que se usó a un virus para sonsacar dinero, cuando la comunidad de investigación médica se vio amenazada con un virus que iría destruyendo datos paulatinamente si no se pagaba un rescate por la «cura».

Los delincuentes cibernéticos al acecho también usan el correo electrónico para enviar mensajes amenazantes especialmente a las mujeres. De acuerdo al libro de Barbara Jenson «Acecho cibernético: delito, represión y responsabilidad personal en el mundo online», publicado en 1996, se calcula que unas 200.000 personas acechan a alguien cada año.

Afirma la Sra. Jenson que una norteamericana fue acechada durante varios años por una persona desconocida que usaba el correo electrónico para amenazar con asesinarla, violar a su hija y exhibir la dirección de su casa en la Internet para que todos la vieran.

Los delincuentes también han utilizado el correo electrónico y los «chat rooms» o salas de tertulia de la Internet para buscar presas vulnerables. Por ejemplo, los aficionados a la pedofilia se han ganado la confianza de niños online y luego concertado citas reales con ellos para explotarlos o secuestrarlos. El Departamento de Justicia de los Estados Unidos dice que se está registrando un incremento de la pedofilia por la Internet.

Además de las incursiones por las páginas particulares de la Red, los delincuentes pueden abrir sus propios sitios para estafar a los clientes o vender mercancías y servicios prohibidos, como armas, drogas, medicamentos sin receta ni regulación y pornografía.

La CyberCop Holding Cell, un servicio de quejas online, hace poco emitió una advertencia sobre un anuncio clasificado de servicio de automóviles que apareció en la Internet. Por un precio fijo de $399, el servicio publicaría una descripción del auto del cliente en una página de la Red y garantizaban que les devolverían el dinero si el vehículo no se vendía en un plazo de 90 días.

Informa CyberCop que varios autos que se habían anunciado en la página electrónica no se vendieron en ese plazo, pero los dueños no pudieron encontrar a ninguno de los autores del servicio clasificado para que les reembolsaran el dinero. Desde entonces, el sitio en la Red de este «servicio» ha sido clausurado.

Impacto a Nivel Social

La proliferación de los delitos informáticos a hecho que nuestra sociedad sea cada vez más escéptica a la utilización de tecnologías de la información, las cuales pueden ser de mucho beneficio para la sociedad en general. Este hecho puede obstaculizar el desarrollo de nuevas formas de hacer negocios, por ejemplo el comercio electrónico puede verse afectado por la falta de apoyo de la sociedad en general.

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.

También se observa que las empresas que poseen activos informáticos importantes, son cada vez más celosas y exigentes en la contratación de personal para trabajar en éstas áreas, pudiendo afectar en forma positiva o negativa a la sociedad laboral de nuestros tiempos.

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 recur-

sos 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.

La falta de cultura informática puede impedir de parte de la sociedad la lucha contra los delitos informáticos, por lo que el componente educacional es un factor clave en la minimización de esta problemática.

Impacto en la Esfera Judicial

Captura de delincuentes cibernéticos

A medida que aumenta la delincuencia electrónica, numerosos países han promulgado leyes declarando ilegales nuevas prácticas como la piratería informática, o han actualizado leyes obsoletas para que delitos tradicionales, incluidos el fraude, el vandalismo o el sabotaje, se consideren ilegales en el mundo virtual.

Singapur, por ejemplo, enmendó recientemente su Ley sobre el Uso Indebido de las Computadoras. Ahora son más severos los castigos impuestos a todo el que interfiera con las «computadoras protegidas» —es decir, las que están conectadas con la seguridad nacional, la banca, las finanzas y los servicios públicos y de urgencia— así como a los transgresores por entrada, modificación, uso o intercepción de material computadorizado sin autorización.

Hay países que cuentan con grupos especializados en seguir la pista a los delincuentes cibernéticos. Uno de los más antiguos es la Oficina de Investigaciones Especiales de la Fuerza Aérea de los Estados Unidos, creada en 1978. Otro es el de Investigadores de la Internet, de Australia, integrado

por oficiales de la ley y peritos con avanzados conocimientos de informática. El grupo australiano recoge pruebas y las pasa a las agencias gubernamentales de represión pertinentes en el estado donde se originó el delito.

Pese a estos y otros esfuerzos, las autoridades aún afrentan graves problemas en materia de informática. El principal de ellos es la facilidad con que se traspasan las fronteras, por lo que la investigación, enjuiciamiento y condena de los transgresores se convierte en un dolor de cabeza jurisdiccional y jurídico. Además, una vez capturados, los oficiales tienen que escoger entre extraditarlos para que se les siga juicio en otro lugar o transferir las pruebas —y a veces los testigos— al lugar donde se cometieron los delitos.

En 1992, los piratas de un país europeo atacaron un centro de computadoras de California. La investigación policial se vio obstaculizada por la doble tipificación penal —la carencia de leyes similares en los dos países que prohibían ese comportamiento— y esto impidió la cooperación oficial, según informa el Departamento de Justicia de los Estados Unidos. Con el tiempo, la policía del país de los piratas se ofreció a ayudar, pero poco después la piratería terminó, se perdió el rastro y se cerró el caso.

Asimismo, en 1996 el Servicio de Investigación Penal y la Agencia Federal de Investigación (FBI) de los Estados Unidos le siguió la pista a otro pirata hasta un país sudamericano. El pirata informático estaba robando archivos de claves y alterando los registros en computadoras militares, universitarias y otros sistemas privados, muchos de los cuales contenían investigación sobre satélites, radiación e ingeniería energética.

Los oficiales del país sudamericano requisaron el apartamento del pirata e incautaron su equipo de computadora,

aduciendo posibles violaciones de las leyes nacionales. Sin embargo, los dos países no habían firmado acuerdos de extradición por delitos de informática sino por delitos de carácter más tradicional. Finalmente se resolvió la situación sólo porque el pirata accedió a negociar su caso, lo que condujo a que se declarara culpable en los Estados Unidos.

Destrucción u ocultación de pruebas

Otro grave obstáculo al enjuiciamiento por delitos cibernéticos es el hecho de que los delincuentes pueden destruir fácilmente las pruebas cambiándolas, borrándolas o trasladándolas. Si los agentes del orden operan con más lentitud que los delincuentes, se pierde gran parte de las pruebas; o puede ser que los datos estén cifrados, una forma cada vez más popular de proteger tanto a los particulares como a las empresas en las redes de computadoras.

Tal vez la criptografía estorbe en las investigaciones penales, pero los derechos humanos podrían ser vulnerados si los encargados de hacer cumplir la ley adquieren demasiado poder técnico. Las empresas electrónicas sostienen que el derecho a la intimidad es esencial para fomentar la confianza del consumidor en el mercado de la Internet, y los grupos defensores de los derechos humanos desean que se proteja el cúmulo de datos personales archivados actualmente en ficheros electrónicos.

Las empresas también recalcan que la información podría caer en malas manos, especialmente en países con problemas de corrupción, si los gobiernos tienen acceso a los mensajes en código. «Si los gobiernos tienen la clave para descifrar los mensajes en código, esto significa que personas no autorizadas —que no son del gobierno— pueden obtenerlas y utilizarlas», dice el gerente general de una

importante compañía norteamericana de ingeniería de seguridad.

Impacto en la Identificación de Delitos a Nivel Mundial.

Las dificultades que enfrentan las autoridades en todo el mundo ponen de manifiesto la necesidad apremiante de una cooperación mundial para modernizar las leyes nacionales, las técnicas de investigación, la asesoría jurídica y las leyes de extradición para poder alcanzar a los delincuentes. Ya se han iniciado algunos esfuerzos al respecto.

En el Manual de las Naciones Unidas de 1977 se insta a los Estados a que coordinen sus leyes y cooperen en la solución de ese problema. El Grupo de Trabajo Europeo sobre delitos en la tecnología de la informática ha publicado un Manual sobre el delito por computadora, en el que se enumeran las leyes pertinentes en los diversos países y se exponen técnicas de investigación, al igual que las formas de buscar y guardar el material electrónico en condiciones de seguridad.

El Instituto Europeo de Investigación Antivirus colabora con las universidades, la industria y los medios de comunicación y con expertos técnicos en seguridad y asesores jurídicos de los gobiernos, agentes del orden y organizaciones encargadas de proteger la intimidad a fin de combatir los virus de las computadoras o «caballos de Troya». También se ocupa de luchar contra el fraude electrónico y la explotación de datos personales.

En 1997, los países del Grupo de los Ocho aprobaron una estrategia innovadora en la guerra contra el delito de «tecnología de punta». El Grupo acordó que establecería modos de determinar rápidamente la proveniencia de los ataques

por computadora e identificar a los piratas, usar enlaces por vídeo para entrevistar a los testigos a través de las fronteras y ayudarse mutuamente con capacitación y equipo. También decidió que se uniría a las fuerzas de la industria con miras a crear instituciones para resguardar las tecnologías de computadoras, desarrollar sistemas de información para identificar casos de uso indebido de las redes, perseguir a los infractores y recabar pruebas.

El Grupo de los Ocho ha dispuesto ahora centros de coordinación abiertos 24 horas al día, siete días a la semana para los encargados de hacer cumplir la ley. Estos centros apoyan las investigaciones de otros Estados mediante el suministro de información vital o ayuda en asuntos jurídicos, tales como entrevistas a testigos o recolección de pruebas consistentes en datos electrónicos.

Un obstáculo mayor opuesto a la adopción de una estrategia del tipo Grupo de los Ocho a nivel internacional es que algunos países no tienen la experiencia técnica ni las leyes que permitirían a los agentes actuar con rapidez en la búsqueda de pruebas en sitios electrónicos —antes de que se pierdan— o transferirlas al lugar donde se esté enjuiciando a los infractores.

Casos de Impacto de los Delitos Informáticos

Zinn, Herbert, Shadowhack.

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 16 y 17 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 publico 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.

Smith, David.

Programador de 30 años, 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 años de cárcel.

Por el momento y a la espera de la decisión que hubiese tomado el juez, David Smith esta en libertad bajo fianza de 10.000 dólares. Melissa en su «corta vida» había conseguido contaminar a más de 100,000 ordenadores 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 campaña de información, que alcanzo 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 aún 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, que han venido apareciendo últimamente como Happy99 o Papa.

Poulsen Kevin, Dark Dante.

Diciembre de 1992 Kevin Poulsen, un pirata infame que alguna vez utilizo el alias de «Dark Dante» en las redes de computadoras es acusado de robar órdenes de tarea relacionadas con un ejercicio de la fuerza aérea militar america-

na. Se acusa 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 años, 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.

Holland, Wau y Wenery, Steffen.

De visita en la NASA «Las dos de la madrugada, Hannover, ciudad Alemana, estaba en silencio. La primavera llegaba a su fin, y dentro del cuarto cerrado el calor ahogaba. Hacía rato que Wau Holland y Steffen Wernery permanecían sentados frente a la pantalla de una computadora, casi inmóviles, inmersos en una nube de humo cambiando ideas en susurros. - Desde acá tenemos que poder llegar. –murmuró Wau. - Mse. Hay que averiguar cómo –contestó Steffen. -

Probemos algunos. Siempre eligen nombres relacionados con la astronomía, ¿No? - Tengo un mapa estelar: usémoslo. Con el libro sobre la mesa, teclearon uno a uno y por orden, los nombres de las diferentes constelaciones.

- «Acceso Denegado» –leyó Wau-; maldición, tampoco es este - Quizá nos esté faltando alguna indicación. Calma.

Pensemos. «set» y «host» son imprescindibles...

-obvio; además, es la fórmula. Probemos de nuevo ¿Cuál sigue? - Las constelaciones se terminaron. Podemos intentar con las estrellas. A ver... ¿Castor, una de las dos más brillantes de Géminis? - Set Host Castor deletreó Wau mientras tecleaba.

Cuando la computadora comenzó a ronronear, Wau Holland y Steffen Wernery supieron que habían logrado su objetivo. Segundos más tarde la pantalla mostraba un mensaje: «Bienvenidos a las instalaciones VAX del cuartel general, de la NASA». Wau sintió un sacudón y atinó a escribir en su cuaderno: «Lo logramos, por fin... Sólo hay algo seguro, la infinita inseguridad de la seguridad».

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 ordenador. Cuando advertimos que los técnicos nos habían 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».

- El juego puede costar muchas vidas...- ¡Ni media vida! La red en que entramos no guarda información ultrasecreta; en este momento tiene 1,600 subscriptores y 4,000 clientes flotantes.

Con esos datos, Steffen anulaba la intención de presentarlos como sujetos peligrosos para el resto de la humanidad». (Hackers, la guerrilla informática - Raquel Roberti).

Murphy Ian, Captain Zap.

En julio de 1981 Ian Murphy, un muchacho de 23 años que se autodenominaba «Captain Zap», gana notoriedad cuando entra a los sistemas en la Casa Blanca, el Pentágono, BellSouth Corp. TRW y deliberadamente deja su currículum.

En 1981, no había 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 ordenes de mercancías, archivos y documentos del gobierno. «Nosotros usamos los a la Casa Blanca para hacer llamadas a líneas de bromas en Alemania y curiosear archivos militares clasificados» Explico Murphy. «El violar 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 ½ años de prueba.

Morris Robert.

En noviembre de 1988, Morris lanzo un programa «gusano» diseñado por el mismo para navegar en Internet, buscando debilidades en sistemas de seguridad, y que pudiera correrse y multiplicarse por sí solo. La expansión exponencial de

este programa causó el consumo de los recursos de muchisimas computadoras y que más de 6000 sistemas resultaron dañados o fueron seriamente perjudicados. Eliminar al gusano de sus computadoras causo a las víctimas muchos días de productividad perdidos, y millone s de dolares. Se creo 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.

8. Seguridad contra los delitos informáticos.

Seguridad en Internet

Hoy en día, muchos usuarios no confían en la seguridad del Internet. En 1996, IDC Research realizó una encuesta en donde el 90% de los usuarios expresó gran interés sobre la seguridad del Internet, pues temen que alguien pueda conseguir el número de su tarjeta de crédito mediante el uso de la Red.

Ellos temen que otros descubran su código de acceso de la cuenta del banco y entonces transferir fondos a la cuenta del hurtador. Las agencias de gobierno y los bancos tienen gran preocupación en dar información confidencial a personas no autorizadas. Las corporaciones también se preocupan en dar información a los empleados, quienes no están autorizados al acceso de esa información o quien trata de curiosear sobre una persona o empleado. Las organizacio-

nes se preocupan que sus competidores tengan conocimiento sobre información patentada que pueda dañarlos.

Aunque los consumidores tienden a agrupar sus intereses juntos por debajo del término de la seguridad general, hay realmente varias partes de la seguridad que confunden. La Seguridad significa guardar «algo seguro «. «Algo» puede ser un objeto, tal como un secreto, mensaje, aplicación, archivo, sistema o una comunicación interactiva. «Seguro» los medios son protegidos desde el acceso, el uso o alteración no autorizada.

Para guardar objetos seguros, es necesario lo siguiente:

- La autenticación (promesa de identidad), es decir la prevención de suplantaciones, que se garantice que quien firma un mensaje es realmente quien dice ser.
- La autorización (se da permiso a una persona o grupo de personas de poder realizar ciertas funciones, al resto se le niega el permiso y se les sanciona si las realizan).
- La privacidad o confidencialidad, es el más obvio de los aspecto y se refiere a que la información solo puede ser conocida por individuos autorizados. Existen infinidad de posibles ataques contra la privacidad, especialmente en la comunicación de los datos. La transmisión a través de un medio presenta múltiples oportunidades para ser interceptada y copiada: las líneas «pinchadas» la intercepción o recepción electromagnética no autorizada o la simple intrusión directa en los equipos donde la información está físicamente almacenada.
- La integridad de datos, La integridad se refiere a la seguridad de que una información no ha sido alterada, borrada, reordenada, copiada, etc., bien duran-

te el proceso de transmisión o en su propio equipo de origen. Es un riesgo común que el atacante al no poder descifrar un paquete de información y, sabiendo que es importante, simplemente lo intercepte y lo borre.

- La disponibilidad de la información, se refiere a la seguridad que la información pueda ser recuperada en el momento que se necesite, esto es, evitar su pérdida o bloqueo, bien sea por ataque doloso, mala operación accidental o situaciones fortuitas o de fuerza mayor.
- No rechazo (la protección contra alguien que niega que ellos originaron la comunicación o datos).
- Controles de acceso, esto es quien tiene autorización y quien no para acceder a una pieza de información determinada.

Son los requerimientos básicos para la seguridad, que deben proveerse de una manera confiable. Los requerimientos cambian ligeramente, dependiendo de lo que se está asegurado. La importancia de lo que se está asegurando y el riesgo potencial involucra en dejar uno de estos requerimientos o tener que forzar niveles más altos de seguridad. Estos no son simplemente requerimientos para el mundo de la red, sino también para el mundo físico.

En la tabla siguiente se presenta una relación de los intereses que se deben proteger y sus requerimientos relacionados:

Intereses	Requerimientos
Fraude	Autenticación
Acceso no Autorizado	Autorización
Curiosear	Privacidad

Alteración de Mensaje	Integridad de Datos
Desconocido	No - Rechazo

Estos intereses no son exclusivos de Internet. La autenticación y el asegurar los objetos es una parte de nuestra vida diaria. La comprensión de los elementos de seguridad y como ellos trabajan en el mundo físico, puede ayudar para explicar cómo estos requerimientos se encuentran en el mundo de la red y dónde se sitúan las dificultades.

Medidas de seguridad de la red.

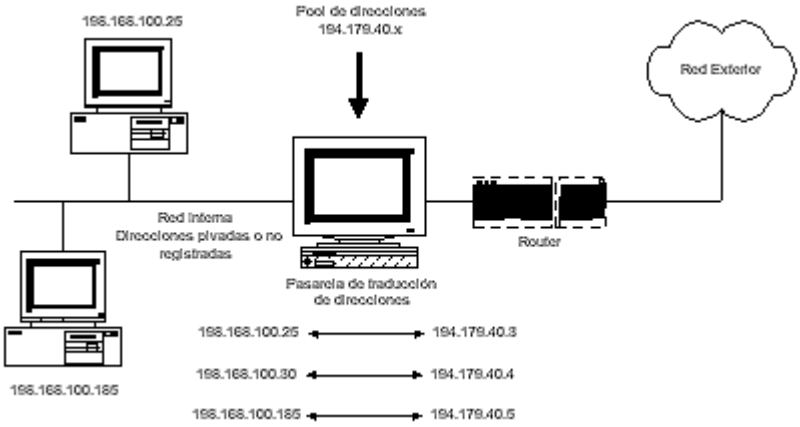
Existen numerosas técnicas para proteger la integridad de los sistemas. Lo primero que se debe hacer es diseñar una política de seguridad. En ella, definir quiénes tienen acceso a las diferentes partes de la red, poner protecciones con contraseñas adecuadas a todas las cuentas, y preocuparse de hacerlas cambiar periódicamente (Evitar las passwords «por defecto» o demasiado obvias).

Firewalls.

Existen muchas y muy potentes herramientas de cara a la seguridad de una red informática. Una de las maneras drásticas de no tener invasores es la de poner murallas. Los mecanismos más usados para la protección de la red interna de otras externas son los firewalls o cortafuegos. Estos tienen muchas aplicaciones, entre las más usadas está:

Packet filter (filtro de paquetes). Se basa en el tratamiento de los paquetes IP a los que aplica unas reglas de filtrado que le permiten discriminar el tráfico según nuestras indicaciones.

Normalmente se implementa mediante un router. Al tratar paquetes IP, los filtros que podremos establecer serán a nivel de direcciones IP, tanto fuente como destino.



Cortafuegos filtro de paquetes ejemplarizado en un router.

La lista de filtros se aplican secuencialmente, de forma que la primera regla que el paquete cumpla marcará la acción a realizar (descartarlo o dejarlo pasar). La aplicación de las listas de filtros se puede hacer en el momento de entrada del paquete o bien en el de salida o en ambos.

La protección centralizada es la ventaja más importante del filtrado de paquetes. Con un único enrutador con filtrado de paquetes situado estratégicamente puede protegerse toda una red.

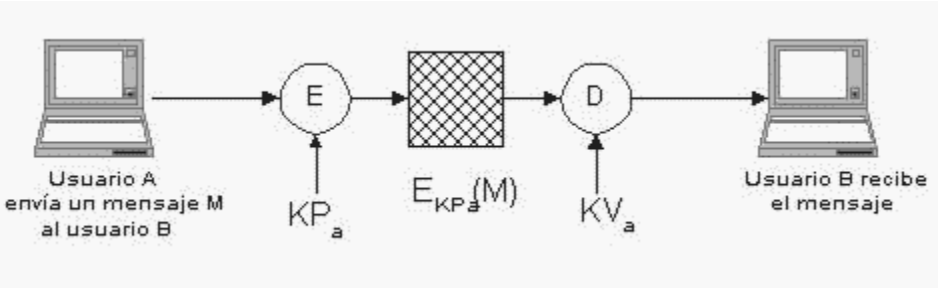
Firma digital.

El cifrado con clave pública permite generar firmas digitales que hacen posible certificar la procedencia de un mensaje, en otras palabras, asegurar que proviene de quien dice. De esta forma se puede evitar que alguien suplante a un usuario y envíe mensajes falsos a otro usuario, por la imposibilidad de falsificar la firma. Además, garantizan la integridad del mensaje, es decir, que no ha sido alterado durante la transmisión. La firma se puede aplicar a un mensaje completo o puede ser algo añadido al mensaje.

Las firmas son especialmente útiles cuando la información debe atravesar redes sobre las que no se tiene control directo y, en consecuencia, no existe posibilidad de verificar de otra forma la procedencia de los mensajes.

Existen varios métodos para hacer uso de la firma digital, uno de ellos es el siguiente: «quien envía el mensaje lo codifica con su clave privada. Para descifrarlo, sólo puede hacerse con la clave pública correspondiente a dicha persona o institución. Si efectivamente con dicha clave se descifra es señal de que quien dice que envió el mensaje, realmente lo hizo».

Firma digital formada encriptando con la clave privada del emisor:



Firma Digital y Autentificación

E: Encriptar / D: Desencriptar.

KP : Encriptación utilizando la Clave Privada.

KV : Encriptación utilizando la Clave Pública.

M : Mensaje.

Seguridad en WWW.

¿Es posible hacer un formulario seguro?

Para hacer un formulario se debe tener un servidor seguro.

En primer lugar los formularios pueden tener «agujeros» a través de los que un hacker hábil, incluso poco hábil, puede «colar» comandos.

La red es totalmente pública y abierta, los paquetes pasan por máquinas de las que no se tiene conocimiento y a las

que puede tener acceso la gente que le guste husmear el tráfico de la red. Si es así (y no tienen que ser necesariamente hackers malintencionados, algunos proveedores de servicio lo hacen) sólo se puede recurrir a encriptar el tráfico por medio, en WWW, de servidores y clientes seguros.

Política de seguridad.

Proveer acceso a los servicios de la red de una empresa y proveer acceso al mundo exterior a través de la organización, da al personal e institución muchos beneficios. Sin embargo, a mayor acceso que se provea, mayor es el peligro de que alguien explote lo que resulta del incremento de vulnerabilidad.

De hecho, cada vez que se añade un nuevo sistema, acceso de red o aplicación se agregan vulnerabilidades potenciales y aumenta la mayor dificultad y complejidad de la protección. Sin embargo, si se está dispuesto a enfrentar realmente los riesgos, es posible cosechar los beneficios de mayor acceso mientras se minimizan los obstáculos. Para lograr esto, se necesitará un plan complejo, así como los recursos para ejecutarlo. También se debe tener un conocimiento detallado de los riesgos que pueden ocurrir en todos los lugares posibles, así como las medidas que pueden ser tomadas para protegerlos.

En algunos aspectos, esto puede parecer una carga abrumadora, y podría muy bien serlo, especialmente en organizaciones pequeñas que no tienen personal experto en todos los temas. Alguien podría estar tentado para contratar un consultor de seguridad y hacerlo con él; aunque esto puede ser una buena manera para outsourcing, todavía necesita saber lo suficiente y observar la honestidad del consultor.

Después de todo, se le va a confiar a ellos los bienes más importantes de la organización.

Para asegurar una red adecuadamente, no solamente se necesita un profundo entendimiento de las características técnicas de los protocolos de red, sistemas operativos y aplicaciones que son accesadas, sino también lo concerniente al planeamiento. El plan es el primer paso y es la base para asegurar que todas las bases sean cubiertas.

¿Por qué se necesita una política de seguridad?

La imagen que frecuentemente viene a la mente cuando se discute sobre seguridad está la del gran firewall que permanece al resguardo de la apertura de su red, defendiendo de ataques de malévolos hackers. Aunque un firewall jugará un papel crucial, es sólo una herramienta que debe ser parte de una estrategia más comprensiva y que será necesaria a fin de proteger responsablemente los datos de la red. Por una parte, sabiendo cómo configurar un firewall para permitir las comunicaciones que se quiere que ingresen, mientras salvaguarda otros datos, es un hueso muy duro de roer.

Aún cuando se tenga las habilidades y experiencia necesaria para configurar el firewall correctamente, será difícil conocer la administración de riesgos que está dispuesto a tomar con los datos y determinar la cantidad de inconveniencias a resistir para protegerlos. También se debe considerar cómo asegurar los hosts que están siendo accesados. Incluso con la protección de firewall, no hay garantía que no se pueda desarrollar alguna vulnerabilidad. Y es muy probable que haya un dispositivo en peligro. Los modems, por ejemplo, pueden proveer un punto de acceso a su red que completamente sobrepase su firewall. De hecho, un firewall puede aumentar la probabilidad que alguien establecerá un

módem para el acceso al Internet mediante otro ISP (ISP - Internet Service Providers, cualquier empresa o institución que provea de conexión a Internet), por las restricciones que el firewall puede imponer sobre ellos (algo para recordar cuando se empieza a configurar su firewall). Se puede proveer restricciones o «protección,» que puede resultar ser innecesario una vez que las consecuencias se entienden claramente como un caso de negocio. Por otra parte, los riesgos pueden justificar el incremento de restricciones, resultando incómodo. Pero, a menos que el usuario esté prevenido de estos peligros y entienda claramente las consecuencias para añadir el riesgo, no hay mucho que hacer.

Los temas legales también surgen. ¿Qué obligaciones legales tiene para proteger su información?. Si usted está en una compañía de publicidad puede tener algunas responsabilidades definitivas al respecto.

Asegurar sus datos involucra algo más que conectarse en un firewall con una interface competente. Lo que se necesita es un plan comprensivo de defensa. Y se necesita comunicar este plan en una manera que pueda ser significativo para la gerencia y usuarios finales. Esto requiere educación y capacitación, conjuntamente con la explicación, claramente detallada, de las consecuencias de las violaciones. A esto se le llama una «política de seguridad» y es el primer paso para asegurar responsablemente la red. La política puede incluir instalar un firewall, pero no necesariamente se debe diseñar su política de seguridad alrededor de las limitaciones del firewall.

Elaborar la política de seguridad no es una tarea trivial. Ello no solamente requiere que el personal técnico comprenda todas las vulnerabilidades que están involucradas, también requiere que ellos se comuniquen efectivamente con la gerencia. La gerencia debe decidir finalmente cuánto de riesgo debe

ser tomado con el activo de la compañía, y cuánto se debería gastar en ambos, en dólares e inconvenientes, a fin de minimizar los riesgos. Es responsabilidad del personal técnico asegurar que la gerencia comprenda las implicaciones de añadir acceso a la red y a las aplicaciones sobre la red, de tal manera que la gerencia tenga la suficiente información para la toma de decisiones. Si la política de seguridad no viene desde el inicio, será difícil imponer incluso medidas de seguridad mínimas. Por ejemplo, si los empleados pueden llegar a alterarse si ellos imprevistamente tienen que abastecer logins y contraseñas donde antes no lo hacían, o están prohibidos particulares tipos de acceso a Internet. Es mejor trabajar con estos temas antes de tiempo y poner la política por escrito. Las políticas pueden entonces ser comunicadas a los empleados por la gerencia. De otra forma, los empleados no lo tomarán en serio, o se tendrán batallas de políticas constantes dentro de la compañía con respecto a este punto. No solamente con estas batallas tendrán un impacto negativo sobre la productividad, es menos probable que la decisión tomada racionalmente pueda ser capaz de prevalecer en la vehemencia de las guerras políticas.

El desarrollo de una política de seguridad comprende la identificación de los activos organizativos, evaluación de amenazas potenciales, la evaluación del riesgo, implementación de las herramientas y tecnologías disponibles para hacer frente a los riesgos, y el desarrollo de una política de uso. Debe crearse un procedimiento de auditoria que revise el uso de la red y servidores de forma periódica.

Identificación de los activos organizativos: Consiste en la creación de una lista de todas las cosas que precisen protección.

Por ejemplo:

- Hardware: ordenadores y equipos de telecomunicación
- Software: programas fuente, utilidades, programas de diagnóstico, sistemas operativos, programas de comunicaciones.
- Datos: copias de seguridad, registros de auditoria, bases de datos.

Valoración del riesgo:

Conlleva la determinación de lo que se necesita proteger. No es más que el proceso de examinar todos los riesgos, y valorarlos por niveles de seguridad.

Definición de una política de uso aceptable:

Las herramientas y aplicaciones forman la base técnica de la política de seguridad, pero la política de uso aceptable debe considerar otros aspectos:

- ¿Quién tiene permiso para usar los recursos?
- ¿Quién esta autorizado a conceder acceso y a aprobar los usos?
- ¿Quién tiene privilegios de administración del sistema?
- ¿Qué hacer con la información confidencial?
- ¿Cuáles son los derechos y responsabilidades de los usuarios?

Por ejemplo, al definir los derechos y responsabilidades de los usuarios:

- Si los usuarios están restringidos, y cuáles son sus restricciones.
- Si los usuarios pueden compartir cuentas o dejar que otros usuarios utilicen sus cuentas.
- Cómo deberían mantener sus contraseñas los usuarios.
- Con qué frecuencia deben cambiar sus contraseñas.
- Si se facilitan copias de seguridad o los usuarios deben realizar las suyas.

9. Legislación sobre delitos informáticos

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.

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 es de acuerdo al interés protegido, como sucede en los delitos convencionales sino de acuerdo al sujeto activo que los comete. Entre las características en común que poseen ambos delitos tenemos que:

«El sujeto activo del delito es una persona 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.

En síntesis, es destacable que la delincuencia informática se apoya en el delito instrumentado por el uso de la computadora a través de redes telemáticas y la interconexión de la computadora, aunque no es el único medio. Las ventajas y las necesidades del flujo nacional e internacional de datos, que aumenta de modo creciente aún en países latinoamericanos, conlleva también a la posibilidad creciente de estos delitos; por eso puede señalarse que la criminalidad informática constituye un reto considerable tanto para los sectores afectados de la infraestructura crítica de un país, como para los legisladores, las autoridades policiales encargadas de las investigaciones y los funcionarios judiciales.

Legislación - Contexto Internacional

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

Dado lo anterior a continuación se mencionan algunos aspectos relacionados con la ley en los diferentes países, así como con los delitos informáticos que persigue.

» Estados Unidos.

Este país adoptó en 1994 el Acta Federal de Abuso Computacional que modificó al Acta de Fraude y Abuso Computacional de 1986.

Con la finalidad de eliminar los argumentos hipertécnicos acerca de qué es y que no es un virus, un gusano, un caballo de Troya y en que difieren de los virus, la nueva acta proscribe la transmisión de un programa, información, códigos o comandos que causan daños a la computadora, a los sistemas informáticos, a las redes, información, datos o programas. La nueva ley es un adelanto porque está directamente en contra de los actos de transmisión de virus.

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

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

ponde a la necesidad de dar validez a documentos informáticos -mensajes electrónicos y contratos establecidos mediante Internet- entre empresas (para el B2B) y entre empresas y consumidores (para el B2C).

» Alemania.

Este país sancionó en 1986 la Ley contra la Criminalidad Económica, que contempla los siguientes delitos:

- Espionaje de datos.
- Estafa informática.
- Alteración de datos.
- Sabotaje informático.

» Austria.

La Ley de reforma del Código Penal, sancionada el 22 de Diciembre de 1987, sanciona a aquellos que con dolo causen un perjuicio patrimonial a un tercero influyendo en el resultado de una elaboración de datos automática a través de la confección del programa, por la introducción, cancelación o alteración de datos o por actuar sobre el curso del procesamiento de datos. Además contempla sanciones para quienes comenten este hecho utilizando su profesión de especialistas en sistemas.

» Gran Bretaña.

Debido a un caso de hacking en 1991, comenzó a regir en este país la Computer Misuse Act (Ley de Abusos Informáticos). Mediante esta ley el intento, exitoso o no, de alterar datos informáticos es penado con hasta cinco años de prisión o multas. Esta ley tiene un apartado que específica la modificación de datos sin autorización.

» Holanda.

El 1º de Marzo de 1993 entró en vigencia la Ley de Delitos Informáticos, en la cual se penaliza los siguientes delitos:

- El hacking.
- El preacking (utilización de servicios de telecomunicaciones evitando el pago total o parcial de dicho servicio).
- La ingeniería social (arte de convencer a la gente de entregar información que en circunstancias normales no entregaría).
- La distribución de virus.

» Francia.

En enero de 1988, este país dictó la Ley relativa al fraude informático, en la que se consideran aspectos como:

- Intromisión fraudulenta que suprima o modifique datos.
- Conducta intencional en la violación de derechos a terceros que haya impedido o alterado el funcionamiento de un sistema de procesamiento automatizado de datos.
- Conducta intencional en la violación de derechos a terceros, en forma directa o indirecta, en la introducción de datos en un sistema de procesamiento automatizado o la supresión o modificación de los datos que éste contiene, o sus modos de procesamiento o de transmisión.
- Supresión o modificación de datos contenidos en el sistema, o bien en la alteración del funcionamiento del sistema (sabotaje).

» España.

En el Nuevo Código Penal de España, se establece que al que causare daños en propiedad ajena, se le aplicará pena de prisión o multa. En lo referente a:

- La realización por cualquier medio de destrucción, alteración, inutilización o cualquier otro daño en los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.
- El nuevo Código Penal de España sanciona en forma detallada esta categoría delictual (Violación de secretos/Espionaje/Divulgación), aplicando pena de prisión y multa.
- En materia de estafas electrónicas, el nuevo Código Penal de España, solo tipifica las estafas con ánimo de lucro valiéndose de alguna manipulación informática, sin detallar las penas a aplicar en el caso de la comisión del delito.

» Chile.

Chile fue el primer país latinoamericano en sancionar una Ley contra delitos informáticos, la cual entró en vigencia el 7 de junio de 1993. Esta ley se refiere a los siguientes delitos:

- La destrucción o inutilización de los de los datos contenidos dentro de una computadora es castigada con penas de prisión. Asimismo, dentro de esas consideraciones se encuentran los virus.
- Conducta maliciosa tendiente a la destrucción o inutilización de un sistema de tratamiento de información o de sus partes componentes o que dicha conducta impida, obstaculice o modifique su funcionamiento.

- Conducta maliciosa que altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información.

Legislación - Contexto Nacional

En el contexto nacional se pueden encontrar legislaturas que castiguen algunos de los tipos de delitos informáticos, para lo cual se deben citar:

- El código procesal penal.
- La Ley de Fomento y Protección de la Propiedad Intelectual.

» Código Procesal Penal.

Dentro de esta ley se contemplan algunos artículos que guardan relación con los delitos informáticos, específicamente con los siguientes:

La difusión, exhibición, explotación de pornografía infantil por medios informáticos (Art. 172 y 173).

Estafa agravada, realizar manipulación que interfiera el resultado de un procesamiento o transmisión de datos (Art. 216 Num.5).

Delitos relativos a la propiedad intelectual (Art. 226 y 227).

Además en dicho código se establece que la realización de estos delitos puede significar para los delincuentes penas de prisión que van desde los 6 meses hasta los 8 años (dependiendo del tipo de delito). Referido a esto es necesario menciona que en nuestro país desgraciadamente no se cuenta con la capacidad instalada para controlar este tipo de

acciones delictivas; por lo que la ley aunque escrita esta lejos de ser cumplida.

» La Ley de Fomento y Protección de la Propiedad Intelectual.

Al revisar el contenido de la dicha ley y relacionarlo con la informática, haciendo mayor énfasis en la protección contra los delitos informáticos, se pueden establecer dos áreas de alcance:

La protección de la propiedad intelectual.

La sustracción de información clasificada.

La protección de la propiedad intelectual.

La propiedad intelectual comprende la propiedad en las siguientes áreas: Literaria, Artística, Industrial y Científica (donde se sitúa la informática). El derecho de propiedad exclusivo se conoce como 'derecho de autor', en este sentido cualquier tipo de violación dará lugar a reparación del daño e indemnización de perjuicios.

Dentro de las categorías de obras científicas protegidas por esta ley se pueden mencionar los programas de ordenador y en general cualquier obra con carácter de creación intelectual o personal, es decir, original.

La sustracción de información clasificada.

Se considera secreto industrial o comercial, toda información que guarde un apersona con carácter confidencial, que le signifique obtener o mantener una ventaja competitiva o económica frente a terceros, en la realización de activida-

des económicas y respecto de la cual haya adoptado los medios o sistemas razonables para preservar su confidencialidad y el acceso restringido a la misma.

Ahora bien, para la protección de la información secreta, la ley establece que toda persona que con motivo de su trabajo, empleo, cargo, puesto, desempeño de su profesión o relación de negocios tenga acceso a un secreto a un secreto industrial o comercial del cual se le haya prevenido sobre su confidencialidad, deberá abstenerse de utilizarlo para fines comerciales propios o de revelarlo sin causa justificada y sin consentimiento de la persona que guarde dicho secreto, o de su usuario autorizado, en caso contrario será responsable de los daños y perjuicios ocasionados. También será responsable el que por medio ilícito obtenga información que contemple un secreto industrial o comercial.

» Efectos de la inexistencia de legislatura informática.

La inexistencia de una ley informática imposibilita que la persecución y castigo de los autores de delitos informáticos sea efectiva. Aunado a esto las autoridades (PNC, Fiscalía, Corte de Cuentas, Órgano Judicial) no poseen el nivel de experticia requerido en estas áreas ni la capacidad instalada para desarrollar actividades de investigación, persecución y recopilación de pruebas digitales y electrónicas. Por lo que todo tipo de acción contra los delincuentes informáticos quedaría prácticamente en las manos de la organización que descubre un delito y el tipo de penalización sería más administrativa que de otro tipo (si el delito proviene de fuentes internas).

» Esfuerzos en legislación informática.

En nuestro país debido a factores como el auge del comercio electrónico a nivel mundial, la aprobación de la firma digital

en E.U., etc. se esta trabajando en la estructuración de una ley que le brinde un marco legal a las prácticas del comercio electrónico (las transacciones por Internet) en nuestro país. Dicho esfuerzo esta siendo realizado de manera conjunta por el Ministerio de Economía y la Secretaria Técnica de la Presidencia, y se espera que participen en dicha estructuración diferentes asociaciones y gremiales (Cámara de Comercio, DIELCO, ASI, etc.) para que sea realmente funcional y efectiva.

10. Auditor versus delitos informaticos

Es importante establecer claramente cual es el papel que juega el auditor informático en relación con la detección y minimización de la ocurrencia de delitos informáticos dentro de la organización a que presta sus servicios. Para lograr establecer dicho rol se debe examinar la actuación del auditor frente a la ocurrencia de delitos, estrategias para evitarlos, recomendaciones adecuadas, conocimientos requeridos, en fin una serie de elementos que definen de manera inequívoca el aporte que éste brinda en el manejo de los casos de delitos informáticos.

Rol del Auditor Informático

El rol del auditor informático solamente está basado en la verificación de controles, evaluación del riesgo de fraudes y el diseño y desarrollo de exámenes que sean apropiados a la naturaleza de la auditoría asignada, y que deben razonablemente detectar:

- Irregularidades que puedan tener un impacto sobre el área auditada o sobre toda la organización.

- Debilidades en los controles internos que podrían resultar en la falta de prevención o detección de irregularidades.

Detección de delitos

Puesto que la auditoria es una verificación de que las cosas se estén realizando de la manera planificada, que todas las actividades se realicen adecuadamente, que los controles sean cumplidos, etc.; entonces el auditor informático al detectar irregularidades en el transcurso de la auditoria informática que le indiquen la ocurrencia de un delito informático, deberá realizar los siguiente:

Determinar si se considera la situación un delito realmente;

Establecer pruebas claras y precisas;

Determinar los vacíos de la seguridad existentes y que permitieron el delito;

Informar a la autoridad correspondiente dentro de la organización;

Informar a autoridades regulatorias cuando es un requerimiento legal.

Es importante mencionar que el auditor deberá manejar con discreción tal situación y con el mayor profesionalismo posible; evitando su divulgación al público o a empleados que no tienen nada que ver. Puesto que de no manejarse adecuadamente el delito, podría tener efectos negativos en la organización, como los siguientes:

- Se puede generar una desconfianza de los empleados hacia el sistema;
- Se pueden generar más delitos al mostrar las debilidades encontradas;
- Se puede perder la confianza de los clientes, proveedores e inversionistas hacia la empresa;
- Se pueden perder empleados clave de la administración, aún cuando no estén involucrados en la irregularidad debido a que la confianza en la administración y el futuro de la organización puede estar en riesgo.

Resultados de la auditoria

Si por medio de la auditoria informática realizada se han detectado la ocurrencia de delitos, el auditor deberá sugerir acciones especificas a seguir para resolver el vacío de seguridad, para que el grupo de la unidad informática pueda actuar. Dichas acciones, expresadas en forma de recomendación pueden ser como las siguientes:

- Recomendaciones referentes a la revisión total del proceso involucrado;
- Inclusión de controles adicionales;
- Establecimiento de planes de contingencia efectivos;
- Adquisición de herramientas de control, etc.

Además de brindar recomendaciones, el auditor informático deberá ayudar a la empresa en el establecimiento de estrategias contra la ocurrencia de delitos, entre las que pueden destacarse:

- Adquisición de herramientas computacionales de alto desempeño;
- Controles sofisticados;
- Procedimientos estándares bien establecidos y probados.
- Revisiones continuas; cuya frecuencia dependerá del grado de importancia para la empresa de las TI; así como de las herramientas y controles existentes.

Si bien es cierto las recomendaciones dadas por el auditor, las estrategias implementadas por la organización minimizan el grado de amenaza que representa los delitos informáticos, es importante tomar en cuenta que aún cuando todos los procesos de auditoría estén debidamente diseñados y se cuente con las herramientas adecuadas, no se puede garantizar que las irregularidades puedan ser detectadas. Por lo que la verificaciones la información y de la TI juegan un papel importante en la detección de los delitos informáticos.

Perfil del Auditor Informático

El auditor informático como encargado de la verificación y certificación de la informática dentro de las organizaciones, deberá contar con un perfil que le permita poder desempeñar su trabajo con la calidad y la efectividad esperada. Para ello a continuación se establecen algunos elementos con que deberá contar:

» Conocimientos generales.

- Todo tipo de conocimientos tecnológicos, de forma actualizada y especializada respecto a las plataformas existentes en la organización;

- Normas estándares para la auditoría interna;
- Políticas organizacionales sobre la información y las tecnologías de la información.
- Características de la organización respecto a la ética, estructura organizacional, tipo de supervisión existente, compensaciones monetarias a los empleados, extensión de la presión laboral sobre los empleados, historia de la organización, cambios recientes en la administración, operaciones o sistemas, la industria o ambiente competitivo en la cual se desempeña la organización, etc.
- Aspectos legales;

» Herramientas.

- Herramientas de control y verificación de la seguridad;
- Herramientas de monitoreo de actividades, etc.

» Técnicas.

- Técnicas de Evaluación de riesgos;
- Muestreo;
- Cálculo pos operación;
- Monitoreo de actividades;
- Recopilación de grandes cantidades de información;
- Verificación de desviaciones en el comportamiento de la data;
- Análisis e interpretación de la evidencia, etc.

Auditor Externo Versus Auditor Interno

La responsabilidad del auditor externo para detectar irregularidades o fraude se establece en el prefacio de las normas

y estándares de auditoría. En este prefacio se indica que aunque el cometido de los auditores externos no exige normalmente la búsqueda específica de fraudes, la auditoría deberá planificarse de forma que existan unas expectativas razonables de detectar irregularidades materiales o fraude.

Si el auditor externo detecta algún tipo de delito deberá presentar un informe detallado sobre la situación y aportar elementos de juicio adicionales durante las investigaciones criminales posteriores. El auditor externo solamente puede emitir opiniones basado en la información recabada y normalmente no estará involucrado directamente en la búsqueda de pruebas; a menos que su contrato sea extendido a otro tipo de actividades normalmente fuera de su alcance.

El cometido y responsabilidad de los auditores internos vienen definidos por la dirección de la empresa a la que pertenecen. En la mayoría de ellas, se considera que la detección de delitos informáticos forma parte del cometido de los auditores internos.

Auditorias Eficientes

En la mayoría de las empresas existe la obligación de mantener en todo momento unos registros contables adecuados y el auditor tendrá que informar si no fuera así.

Lo más probable es que el estudio completo de la seguridad y la planificación de emergencia de los sistemas mecanizados se incluyan entre las atribuciones de la mayoría de los departamentos de auditoría interna. Por ello cuando se realice un análisis de seguridad informática y de planificación de emergencia, el auditor:

- Examinará sistemáticamente todos los riesgos que intervengan y acotarán las pérdidas probables en cada caso.
- Considerará las maneras de aumentar la seguridad para reducir los riesgos.
- Recomendará todas las acciones necesarias de protección encaminadas a reducir el riesgo de que se produzca una interrupción, en caso de que se produzca.
- Cuando corresponda, estudiará la cobertura de seguros de la empresa.

Cuando se hable de eficiencia, los auditores tendrán que tener en cuenta las bases de referencia del grupo de auditoria, que considera lo siguiente:

- A que nivel informan los auditores.
- El apoyo que la dirección presta a los auditores.
- El respeto que tenga la unidad informática hacia el grupo de auditoría.
- La competencia técnica del equipo de auditoría.
- La eficiencia de la unidad informática, en la que se incluyen más factores de protección y seguridad.

Si, durante el curso de auditoría, los auditores tuvieran razones para pensar que las disposiciones de seguridad de la empresa y los planes de emergencia no son los adecuados, deberán reflejar sus opiniones a la Alta Dirección, a través del informe de auditoria.

Si sospechase de fraude, el auditor deberá avisar a la alta dirección para que se pongan en contacto con su asesor jurídico, o con la policía, sin levantar las sospechas del personal o los clientes que estuviesen involucrados. El auditor

deberá asegurar también que los originales de los documentos que pudieran utilizarse como prueba están custodiados y a salvo y que ninguna persona que sea sospechosa de fraude tenga acceso a ellos.

11. 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 éstos 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, 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 responsabilidad del auditor informático no abarca el dar solución al impacto de los delitos o en implementar cambios; sino más bien su responsabilidad recae en la verificación de controles, evaluación de riesgos, así como en el establecimiento de recomendaciones que ayuden a las organizaciones a minimizar las amenazas que presentan los delitos informáticos.
- 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.

12. Referencias.

Algunos sitios consultados por Internet

http://members.nbci.com/segutot/delitos.htm

http://www.fas.org/irp/congress/1996_hr/s960605l.htm

http://digitaldesign.bariloche.net.ar/xiijovenab/ComDerPen%20-%20DelitosInfor.htm

http://www.npa.go.jp/hightech/antai_repo/ereport.htm

http://www.monografias.com/trabajos/legisdelinf/legisdelinf.shtml

http://www.govnews.org/mhonarc/gov/us/fed/congress/gao/reports/_msg00533.html

http://www.dtj.com.ar/publicaciones.htm

http://margay.fder.uba.ar/centro/juridicas/Juridica11/salt.html

http://www.gocsi.com/

http://www.ecomder.com.ar

http://www.bilbaoweb.com/hackuma/guidel1.htm

http://arnal.es/free/noticias/free2_08.html#T12

http://www.bilbaoweb.com/hackuma/guidel1.htm

http://www.inei.gob.pe/cpi/bancopub/cpi008.htm

http://margay.fder.uba.ar/centro/juridicas/Juridica11/salt.html

http://www.monografias.com/trabajos/legisdelinf/legisdelinf.shtml

http://www.onnet.es/04001001.htm

http://legal.infosel.com/Legal/EnLinea/Articulos/articulo/0001/