UNIVERSIDAD MAYOR DE SAN ANDRES
FACULTAD DE CIENCIAS PURAS Y NATURALES
CARRERA DE INFORMATICA

TESIS DE GRADO

MODIFICACION DEL CODIGO PENAL A TRAVES DE LA INCORPORACIÓN DE NUEVOS TIPOS PENALES RESPECTO A DELITOS INFORMATICOS

PARA OPTAR AL TITULO DE LICENCIATURA EN INFORMÁTICA

MENCIÓN: INGENIERIA DE SISTEMAS INFORMATICOS

POSTULANTE : IDALIA ISABEL MOLINA LÓPEZ

TUTOR : LIC. GERMAN HUANCA TICONA

REVISOR : LIC. ALDO RAMIRO VALDEZ ALVARADO

LA PAZ – BOLIVIA

2011

DEDICATORIA

A Dios nuestro señor, quien me dio fuerzas para seguir adelante y poder concluir con este trabajo.

A la virgencita de Copacabana porque con su manto ilumino mi mente para seguir sin desmayar.

A mis padres Eusebio y Felicidad quienes siempre confiaron en mí, me brindaron amor, cariño, paciencia y confianza, ellos que me dieron un buen ejemplo de humildad y fuerza para que nunca caiga y pueda salir adelante y culminar con lo que me había propuesto.

A mi princesa Yadhira que me tuvo paciencia durante toda la etapa de elaboración de mí tesis y quien también me motivo para terminar este trabajo.

A mis hermanos Bismarck, Weimar, Cinthia y mi cuñada querida Norma, por los consejos y apoyo que me brindaron.

A mi mama Zinda que me brindo mucho apoyo y colaboración en el desarrollo del presente trabajo.

A todos mis familiares: tíos (Lidia, Gualberto), primos y sobrinos por darme ese apoyo y ese cariño tan incondicional.

Gracias.

AGRADECIMIENTOS

A Dios nuestro creador, por darme la oportunidad de vivir esta etapa de mi vida, y no dejar que desmaye en los momentos más difíciles que se me presento.

Al Lic. Germán Huanca Ticona, mi tutor, por su colaboración, apoyo y concejos que me dio para poder culminar este trabajo de tesis.

Al Lic. Aldo Ramiro Valdez Alvarado, mi revisor, por las sugerencias, correcciones y el tiempo dedicado a mi tesis, quien me brindo su apoyo constantemente.

A la Dra. Norma López Benito, quien me colaboró en el aspecto legal, por compartir todos sus conocimientos referentes al tema y por brindarme todo su tiempo.

A cada uno de los docentes de la Carrera de Informática, por haber plasmado en mi todo ese conocimiento que ellos tienen, asiendo de todos los estudiantes hombres de bien.

A los administrativos y bibliotecarios (don Fernando, don Daniel, etc.) por brindarme su amistad, cordialidad y calidez de persona que les caracteriza.

RESUMEN

El creciente y significativo avance que ha generado el desarrollo, difusión y uso generalizado de la informática y su impacto en la sociedad boliviana, despierta con la explosiva incorporación del Internet, que de modo inexorable está presente en todos los ámbitos del quehacer humano, revolucionando los patrones de comportamiento y por ende las relaciones sociales.

La diversificación y globalización de los mercados, así como el desarrollo de toda una serie de normativas liberalizadoras en sectores de amplia influencia como las telecomunicaciones, ha posibilitado al entorno empresarial corno a particulares en general, hacer uso de modernos servicios en una estrategia centrada en costo-beneficio via Internet tanto de publicidad a nivel global, con el uso de páginas web, obtención de comunicación efectiva, dinámica e instantánea y a escala mundial con el uso de direcciones electrónicas, así como la aplicación cada vez más frecuente del comercio electrónico tiendas virtuales y empleo de contratos informáticos entre personas naturales y jurídicas.

Así la disciplina del Derecho se halla hoy en una instancia histórica en la que debe responder a estos nuevos y complejos problemas a los que se enfrenta. Por otra parte, la inexistencia de una legislación penal adecuada, posibilita al mismo tiempo, la impunidad y desprotección jurídica de la sociedad en general, pos todo esto es que en la presente tesis de realizara el estudio de la modificación al código penal atraves de la incorporación de nuevos tipos penales respecto a delitos informáticos.

El Derecho Penal, en este sentido, tendrá legitimación para privar a de libertad al agente, solo en cuanto sea respetado el Principio de Legalidad, limitador del poder punitivo Estatal, debiendo previamente ser determinada la acción criminosa como comportamiento ilícito y ser legalmente reprimida a través de legislación penal.

INDICE DE CONTENIDO

ANEXOS

CAPITULO I
MARCO PRELIMINAR

CAPÍTULO I

MARCO PRELIMINAR

1.1 Presentación

La presente investigación tiene por objeto brindar una visión global de la situación de los delitos informáticos en Bolivia en cuanto a su regulación, iniciativas de investigación, tecnología y formación de los especialistas que investigan dichos delitos, así como también identificar los desafíos y brechas que deben ser superados por Bolivia para el tratamiento de los mismos.

Se abordará el marco conceptual de los delitos y la criminalidad informática, así como también las leyes relacionadas que se encuentran establecidas en la legislación Boliviana.

Se explican las iniciativas que convergen como propuestas iníciales y recomendaciones externas para el tratamiento de los delitos informáticos, Igualmente se dará una vista de cómo están actuando países de Latinoamérica en tanto a sus regulaciones establecidas para el manejo de dichos actos ilícitos relacionados con la informática.

Se observará los retos a nivel de formación, limitaciones tecnológicas, el marco legal que en Bolivia debe superar para hacer frente a estas conductas delictivas que hacen uso de las nuevas tecnologías.

Si bien los tipos penales de la estafa, sabotaje y fraude informático constituyen hechos punibles ya presentes en algunas legislaciones foráneas desde hace más de dos décadas, es cierto que en nuestro país aún se carece de normas

que regulen ciertas conductas que tienen estrecha relación con las nuevas tecnologías de la información, delitos cuya investigación necesita de precisión y que demanda una interpretación adecuada de sus elementos, adicionando que son una computadora, un celular o cualquier dispositivo "con memoria", el objeto que puede convertirse en la huella que revele los detalles de un delito, es entonces por esa tecnodependencia a estos artefactos en la vida cotidiana, en procesos administrativos y de gestión, los que han marcado la necesidad de incluir estos medios informáticos como elementos de carácter probatorio, toda vez que los mismos pueden ser portadores de pruebas con manifestaciones de voluntad consentimiento u otros hechos de relevancia jurídica.

Este tema es en verdad abrumador por lo que se hizo necesario hacer una adecuada delimitación del mismo, ya que la interacción hombre-máquina no sólo ha abierto las puertas de la comunicación, sino que ha propiciado además nuevas formas de realización de ilícitos penales y la aparición de nuevas figuras delictivas que no encuentran precedentes en los ordenamientos jurídicos tradicionales. Es decir, que hasta la fecha nuestro Código Penal únicamente cuenta con dos tipos penales que regulan los delitos informáticos, sin considerar que con el avance de la tecnología también se han incrementado los delitos informáticos, un claro ejemplo es el fraude informático, el sabotaje, el espionaje (con los hackers, que se han infiltrado en los archivos secretos de la Banca, en temas económicos, y de seguridad nacional como es el caso de la CIA u otros organismos de seguridad estatal), tipos penales que ya se han insertado no únicamente dentro de la normativa penal de los países desarrollados sino también en la normativa de países vecinos como son Perú, Ecuador, Chile y México quienes ya han incorporado dentro de su normativa penal estos nuevos tipos penales que sancionan este tipo de conductas.

Lamentablemente en Bolivia el Código Penal en sus artículos 363 bis y 363 ter, regula únicamente la manipulación informática y alteración, acceso y uso indebido de datos, imponiendo sanciones demasiado benevolentes y nada drásticas ni ejemplarizadoras. En este sentido, el presente trabajo propone la incorporación dentro del Código Penal estas figuras, adecuándolas a la idiosincrasia boliviana, y lógicamente desde un punto de vista informático, ya que muchas veces los legisladores al desconocer una ciencia trazan lineamientos generales ignorando en muchos casos temas importantes que hacen a la informática en si.

1.2 Antecedentes.

El siglo XX se ha distinguido por la revolución tecnológica, actualmente los sistemas informáticos están presentes en casi todos los campos de la vida moderna, actividades personales, comerciales, etc., el progreso de la informática nos da la posibilidad de procesar u poner a disposición información de diversa naturaleza al alcance de millones de usuarios, viéndose facilitado por el uso del Internet.

El auge de las comunicaciones y el surgimiento de las redes informáticas, ha conducido a que existan nuevas formas de interrelación con los demás así como el e-mail, chat, foros, paginas sociales, etc., que otorga grandes beneficios, sin embargo también ofrece el aspecto negativo, cuando personas inescrupulosas, utilizan estos medios tecnológicos para delinquir, es así que conductas antisociales tradicionales se manifiestan en conductas antisociales no tradicionales, planteando problemas en cuanto al funcionamiento y seguridad de los sistemas informáticos, toda vez que la informática reúne características que la convierten en un medio idóneo para la comisión de distintas modalidades delictivas, la manipulación fraudulenta de los operadores con ánimo de lucro, la destrucción de programas o datos, el acceso y la

utilización indebida de la información que puede afectar la esfera de la privacidad.

Por ello y ante la ausencia de normas penales que sancionen estas conductas, se ha visto la necesidad de una regulación jurídica específica, ya que la delincuencia informática se comete en el ciberespacio, no reconoce fronteras nacionales convencionales, puede perpetrarse desde cualquier lugar y contra cualquier usuario del mundo, por lo que se requiere de respuestas prontas, ya que la delincuencia informática como un fenómeno de la era de la tecnología se caracteriza por su carácter trasnacional, la dificultad de descubrimiento e impunidad. Cabe resaltar que entre las conductas cometidas por delincuentes informáticos tenemos el fraude, y sabotaje entre otros a través de sistemas informáticos, en la economía actual la información es una parte vital, más aún ante el creciente desarrollo del comercio on line, pero ante la inseguridad de los usuarios on line, su consiguiente impacto en la actividad empresarial se da por que no existe una protección jurídica adecuada, idónea a la realidad social y tecnológica en que vivimos, sumado al carácter especial de las conductas que no admiten encuadrarse dentro de figuras convencionales siendo necesaria la creación de nuevas figuras penales tomando en cuenta la validez de la información contenida en los bancos de datos y el perjuicio que pudieran ocasionar.

Tal es así, que en los países con un desarrollo tecnológico mas avanzado que el boliviano, se ha trabajado bastante en la regulación de este tipo de conductas no solo dentro de la normativa penal sino también en legislación especial, tomando en cuenta el caso de Ecuador y México, quienes han realizado estudios sobre la comisión de los delitos informáticos, y que en la biblioteca virtual de la Universidad Autónoma de México UNAM, muchos de los estudiantes tanto de pre como de post grado han venido desarrollado investigaciones que se reflejan en tesis , que en muchos casos ha servido como

base para la incorporación de estos ilícitos en la normativa mexicana. Asimismo el Ecuador también ha trabajado ampliamente en este tema, ya cuenta con una normativa especial que regula el sabotaje, la estafa y el fraude informático. Por otra parte organismos internacionales como la ONU, la OCDE, la Convención de Europa, por la importancia del tratamiento urgente de esta delincuencia tecnificada y la amenaza latente para la economía de los países y de la sociedad en su conjunto, asimismo las posiciones de diversos países referente a estos nuevos ilícitos, han posibilitado que estos organismos internacionales clasifiquen estos delitos, brindándonos un amplio marco referencial que permita incorporar algunos de estos tipos penales en nuestra legislación.

En el caso de Bolivia, pese ha haber realizado una pesquisa minuciosa, no se han podido encontrar estudios serios que confluyan en la modificación del Código Penal para la incorporación de estos ilícitos, por lo que la presente propuesta se constituiría en la pionera sobre este tema, desde el punto de vista informático, basándonos lógicamente en las experiencias Ecuatorianas y Mexicanas.

Tesis de grado "legislación para la seguridad del comercio en internet": El autor Augusto Ricardo Camacho Meneses ha realizado este trabajo el año 1997 en la Universidad Mayor de San Andres, quien estableció la importancia de la implantación de leyes que regulan la actividad comercial en internet, entre las propuestas que contiene esta tesis cabe destacar:

a) Incentivar la seguridad por una legislatura
b) Establecer la necesidad de globalizar la solución dejando de lado las soluciones aisladas
c) Establecer los puntos actualmente susceptibles a ser vulnerados por delincuentes en Internet.

d) Disminuir los delitos informaticos que se comenten en internet
e) Implementar la complementación de los métodos tecnológicos de seguridad que da la tecnología con la seguridad que ofrece la legislación
f) Establecer la actitud que debe tomar el gobierno en la problemática del surgimiento de nuevos medios de comunicación como internet.

Cabe resaltar que la mayoría de los trabajos de investigación se han realizado desde el punto de vista jurídico y no desde el punto de vista informatico, un claro ejemplo es Atipicidad relativa en los delitos de falsedad, hurto, estafa y daño informáticos el trabajo de tesis de grado presentada por Maria Clara Fernández de Soto de la Escuela de Derecho de la Universidad Sergio Arboleda, en Santa Marta Colombia en la gestión 2001, otro claro ejemplo "Tipificación de los delitos informáticos y electrónicos en la Legislación Mexicana cuya autoria recae en Pamela Trillo Minutti del Departmento de Derecho de la Universidad de las Américas Puebla, "Presupuestos para la Punibilidad del Hacking", LIMA de la LUZ, María. Universidad San Marcos de Lima, Julio 2001.

1.3 Definicion del problema.

1.3.1 Problema Central

¿De qué manera es necesaria la modificación del Código Penal con la incorporación de tipos penales que se refieran a las nuevas conductas delincuenciales informáticas o simplemente será necesaria la modificación de algunos artículos adecuándolos su comisión a través de medios informáticos?

1.3.2 Problemas Secundarios

- Logra la legislación boliviana vigente responder al evidente aumento de la delincuencia informática.
- La legislación vigente ha logrado penalizar a los autores de la comisión de delitos informaticos.
- Existirá óbice alguno en las investigaciones criminales, que la legislación penal vigente no tenga sanciones para los delitos informáticos o delitos comunes cometidos a través del ciberespacio.

1.4 Justificacion del Tema.

A pesar del inimaginable crecimiento de la tecnología dentro del cotidiano vivir del boliviano, y con dicho crecimiento las conductas delictivas también han evolucionado, puesto que actualmente las personas ya no precisan delinquir en directo contacto con su victima, sino que ahora se delinque a través de la computadora y con todas las ventajas que el mundo de la cibernética ofrece. Ahora los delitos son mucho más complejos al momento de determinar la autoria de dichos crímenes, ya que estos delitos vencen las fronteras nacionales y de idioma.

Este crecimiento hace imperiosa la necesidad de modificar el Código Penal, puesto que si revisamos esta norma claramente podremos evidenciar que la norma sustantiva penal únicamente penaliza y sanciona dos conductas, prescindiendo y quedándose retrasada, pues no contempla dentro de su estructura estas nuevas formas.

No es posible que en pleno siglo XXI, conocido como la era de las nuevas tecnologías legislativamente sigamos relegados y sin contar con normativa que permita castigar estas conductas, que no simplemente dañan la economía

nacional, sino también personal asimismo la intimidad de las personas se ha visto muchas veces vulnerada y violada, ya que ahora el 89% de la población de alguna manerase esta incolucrada con el uso de las nuevas tecnologías de la información.

1.4.1 Justificacion Social.

Cabe hacer énfasis en que varios delitos informáticos atacan a las propias tecnologías de la información y las comunicaciones, como los servidores y los sitios Web, con virus informáticos de alcance mundial que causan considerables perjuicios a las redes comerciales y de consumidores.

Esta propuesta tendrá un alto impacto social, ya que se ha visto la necesidad de sancionar las conductas que ya han ocasionado grandes perjuicios a la sociedad, ya que la comisión de los ilícitos informáticos se han incrementado en temas como el acceso a cuentas bancarias personales, a través de la clonación de tarjetas de debito y crédito, el hackeo de información personal privada, vulnerándose de esta manera el derecho a la intimidad personal que se encuentra constitucionalmente protegida.

1.4.2 Justificación Económica.

La presente investigación tendrá un alto beneficio económico, teniendo en cuenta que se podrá sancionar de manera más efectiva a los delincuentes informáticos, y se podrá prevenir estos ilícitos, ya que el precedente de una sanción ejemplarizadora incidirá en que los delincuentes informaticos piensen dos veces antes de cometer un crimen de esta naturaleza. Evitandose de esta manera las cuantiosas

pérdidas económicas ocasionadas por las estafas, las clonaciones de tarjetas y documentos, y el hackeo de los sistemas de información bancario y de Estado.

1.4.3 Justificación Técnica.

Al respecto solo se puede indicar que se va a trabajar sobre la legislación actual, es decir sobre el Código Penal en vigencia, puesto que de manera general ya contempla los delitos informaticos, y lo que resta realizar es la incorporación y modificación de algunos tipos penales que observen sanciones especificas a estos delitos de orden público.

- El vandalismo electrónico y la falsificación profesional.
- El robo o fraude, por ejemplo, ataques de piratería contra bancos o sistemas financieros y fraude mediante transferencias electrónicas de fondos.
- Las computadoras se utilizan para facilitar una amplia variedad de ventas telefónicas e inversiones fraudulentas mediante prácticas engañosas.
- La "pesca" (phishing) o la inundación de mensajes supuestamente de origen conocido (spam spoofing) es la construcción de mensajes de correo electrónico con páginas Web correspondientes diseñadas para aparecer como sitios de consumidores existentes. Se distribuyen millones de estos mensajes fraudulentos de correo electrónico, que se anuncian como provenientes de bancos, subastas en línea u otros sitios legítimos para engañar a los usuarios a fin de que comuniquen datos financieros, datos personales o contraseñas.

- La difusión de material ilícito y nocivo. Durante los últimos años, la Internet ha sido utilizada para fines comerciales por la "industria del entretenimiento para adultos" legítima. Sin embargo, la Internet se utiliza ahora cada vez más para distribuir material considerado legalmente obsceno en varios países. Otro motivo de preocupación es la pornografía infantil. Desde fines de los años 80, ha venido aumentando su distribución a través de una variedad de redes informáticas, utilizando una variedad de servicios de Internet, incluidos los sitios Web. Una cierta proporción de la distribución de pornografía infantil se ha vinculado a la delincuencia organizada transnacional.
- Además de la utilización de la Internet para difundir propaganda y materiales que fomentan el odio y la xenofobia, hay indicios de que la Internet se ha utilizado para facilitar la financiación del terrorismo y la distribución de propaganda terrorista.

Por ello la presente propuesta, pretende la modificación del Código Penal con la incorporación de nuevos tipos penales que sancionen las conductas delictivas referentes a la informática, que conlleva realizar todo el trámite para ser presentada como un proyecto de ley, es decir que la factibilidad de esta propuesta es lato, ya que con la nueva Constitución Política del Estado, cualquier ciudadano, a través de la iniciativa ciudadana, puede presentar un proyecto de ley, referente al tema que mejor le parezca, en este caso, la proponente deberá trabajar en su incorporación dentro del orden del día de una sesión de Asamblea Legislativa, para que la misma luego siga su curso hasta su aprobación por el ejecutivo y finalmente su promulgación.

1.5 Objetivos

1.5.1 Objetivo General.

Proponer la modificación del Código Penal a través de la incorporación de nuevos tipos penales que sancionen las conductas ilícitas relacionadas a delitos informáticos y a los delitos comunes, cuya comisión se realiza a través del ciberespacio.

1.5.2 Objetivos Específicos.

- Determinar si la existencia de vacíos jurídicos referentes a los delitos informáticos inciden en el incremento de los ilícitos informáticos.
- Verificar si los dos tipos penales existentes en el actual Código Penal sancionan efectivamente a los delincuentes informáticos.
- Demostrar que la incorporación de nuevos tipos penales informáticos, es necesaria para brindar mayor seguridad a la población y disminuya la comisión de delitos informáticos.
- Demostrar que la incorporación de estos delitos informáticos dentro del Codigo Penal boliviano es una necesidad priomordial requerida por el consumidor cibernético.

1.6 Hipótesis

La modificación del Código Penal Boliviano, con la incorporación de tipos penales específicos para la penalización de los delitos informáticos incrementará la seguridad de las operaciones que se realicen a través de los medios informaticos y el ciberespacio, tipificando las conductas consideradas como delitivas y que se cometan por la internet.

1.7 Alcances y Aportes

1.7.1 Alcances

El alcance principal de la presente investigación será modificar el Código Penal actual con la incorporación de tipos penales especificamente que penalicen las conductas delictivas que se realicen con o a través del ciberespacio y las nuevas tecnologías de la información. El cual será remitido y revisado por la Asamblea Legislativa del Estado Plurinacional de Bolivia.

1.7.2 Aportes

El aporte de la presente investigación conllevara que su aplicación será a nivel nacional, ya que si esta modificación se promulga, su cumplimiento sería obligatorio y tendría un importante impacto social, puesto que si bien hasta ahora los administradores de justicia no contaban con los instrumentos legales necesarios para sancionar las conductas delictivas de esta naturaleza.

1.8 Metodologias Empleadas

La metodología a aplicarse en el desarrollo del presente trabajo es el método científico inductivo, tomando en cuenta las etapas de observación, comprobación y emisión de conclusiones. Las tecnicas de evaluación serán las siguientes:

Técnicas de indagación del estado actual de los delitos informaticos, o delitos comunes cometidos a través de nuevas tecnologías de la información.

Técnicas de acumulación de los datos.

Técnicas de evaluación de los datos.

Técnicas de discusión de los resultados.

CAPITULO II
MARCO REFERENCIA

CAPITULO II

MARCO TEÓRICO Y LEGISLACION EN BOLIVIA

2.1. Nace una nueva forma de criminalidad

Dado que es profusa la literatura sobre los denominados delitos informáticos, es menester encarar desde el punto de vista criminológica, el estudio sobre la perpetración de conductas que, sucedidas o no a través de la red, pueden llegar a constituir ilícitos penales, de existir una legislación que así los contemple.

Con relación a este tópico, a juzgar por los estereotipos que van apareciendo, que colocan a los sujetos autores de los ilícitos cometidos a través de la informática y en especial de Internet como una especie de "delincuentes" y por las connotaciones que toman algunas maniobras que causan daños varios en ese medio, es evidente que se está ante una nueva forma de criminalidad.

El continuo avance de la tecnología en el mundo globalizado está provocando un fenómeno de poder que desborda a los poderes políticos locales y no resulta fácil hallar paliativo a conflictos como éste en el que las acciones criminales trascienden tales límites.

2.1.1. Sus Causas

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

a) Familiares:

El nivel social al que pertenecen los sujetos que pueblan el mundo de la informática, por lo general es de medio a alto por cuanto provienen de una

extracción que les pudo proporcionar estas herramientas para alcanzar las metas que la cultura social les estaba proponiendo.

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

b) Sociales:

La tendencia al agrupamiento o formación de "grupos económicos" en continua expansión y la globalización de la economía son factores que dieron luz al crecimiento de la informática y paralelamente la aparición de Internet con las ventajas que ello les ofrecía, en una palabra el progreso tecnológico de las comunicaciones permitieron transacciones que, en segundos conllevaron a un mayor poder económico y político extranacional. Desde que surge la informática es notorio que todo aquél que desconoce el manejo de una computadora cae en la obsolencia. En las sociedades de información actual desde muy pequeños se les introduce al mundo de la informática. Pero todos tienen las condiciones de ser perito en el tema ya que el aprendizaje del manejo de esta tecnología de ciertas características técnicas y la capacidad de agilidad mental, las adquieren desde niños.

2.1.2 Sus Objetivos

Los objetivos de la nueva criminalidad es obtener beneficios, económicos, "poder" y otros que consiguen las personas que están involucradas en el manipuleo de la información de dichas personas.

La asunción desinhibida de riesgos y las débiles consecuencias jurídicas hacen que los delitos informáticos sean cometidos con mayor frecuencia y de esta forma los objetivos criminales sean conseguidos sin mucho esfuerzo o

planificación. En Bolivia por falta o existencia de vacíos jurídicos se comenten una serie de delitos sin que se realice sanción alguna.

2.2 Delitos informáticos

2.2.1 Delitos

Según la teoría dogmática *el delito es una conducta típica (acción u omisión), antijurídica y culpable, añadiéndose frecuentemente que, además, sea punible*. Sus elementos son, entonces, la tipicidad (la adecuación de un hecho determinado con la descripción que de él hace un tipo legal), la antijuricidad (la contravención de ese hecho típico con todo el ordenamiento jurídico) y la culpabilidad (el reproche que se hace al sujeto porque pudo actuar conforme a las exigencias del ordenamiento jurídico) esencialmente.

2.2.2 Los delitos informáticos

El progreso tecnológico que ha experimentado la sociedad, supone una evolución en las formas de infringir la ley, dando lugar, tanto a las diversificaciones de los delitos tradicionales como la aparición de nuevos actos ilícitos. Esta situación ha motivado un debate en torno a la necesidad de diferenciar o no los delitos informáticos del resto y de definir su tratamiento dentro del marco legal.

María de la Luz Lima, indica que "el delito electrónico en un sentido amplio es cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin", y que en un sentido estricto, el delito informático, es "cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin"[1]

[1] María de la Luz Lima, Delitos Electrónicos Pág. 100, Ediciones Porrua - México 1984.

Julio Téllez Valdés conceptualiza al delito informático en forma típica y atípica, entendiendo que en la forma típica son "las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin"[2] y la forma atípica "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin".

El Convenio de Cyber-delincuencia del Consejo de Europa, define a los delitos informáticos como "los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas redes y datos"[3]

Conviene destacar entonces, que diferentes autores y organismos han manifestado diferentes apreciaciones para señalar las conductas ilícitas en las que se utiliza la computadora, esto es "delitos informáticos", "delitos electrónicos", "delitos relacionados con la computadora", "crímenes por computadora", "delincuencia relacionada con el computador". Tal como podemos notar en las definiciones establecidas por autores anteriores, no existe una definición de carácter universal propia de delito informático, sin embargo, debemos resaltar que han sido los esfuerzos de especialistas que se han ocupado del tema y han expuesto conceptos prácticos y modernos atendiendo entornos nacionales concretos, pudiendo encasillar parte de los temas en esta área de la criminalística. Es preciso señalar que la última definición brindada por el Convenio de Cyber-delincuencia del Consejo de Europa anota especial cuidado en los pilares de la seguridad de la información: la confidencialidad, integridad y disponibilidad.

---

[2] Julio Téllez Valdés, Derecho Informático, 2da Edición, Mc Graw Hill – México 1996.

[3] CONSEJO de Europa. Estados Miembros del Consejo de Europa y otros Estados. Actualizada: Budapest 2008. [Fecha de consulta: 29 septiembre 2011]. Disponible en: http://www.coe.int

El delito informático involucra acciones criminales que en primera instancia los países han tratado de poner en figuras típicas, tales como: robo, fraudes, falsificaciones, estafa, sabotaje, entre otros, por ello, es primordial mencionar que el uso indebido de las computadoras es lo que ha creado la necesidad imperante de establecer regulaciones por parte de la legislación.

Podemos decir ahora, que el verdadero concepto de DELITO INFORMATICO, es el siguiente: ***"es toda conducta que revista características delictivas, es decir sea típica, antijurídica, y culpable, y atente contra el soporte lógico o Software de un sistema de procesamiento de información, sea un programa o dato relevante".***

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

El *"delito electrónico " "en un sentido amplio es cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en un sentido estricto, el delito informático, es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin". El delito informático* en forma típica y atípica, entendiendo por la primera a *" las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin"* y por las segundas *"actitudes ilícitas en que se tienen a las computadoras como instrumento o fin"*.

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

2.2.3 Características de los delitos informáticos.

De acuerdo a las características que menciona en su libro Derecho Informático el Dr. Julio Téllez Valdés, en donde se podrá observar el modo de operar de estos ilícitos:

- "Son conductas criminógenas de cuello blanco (white collar crimes), en tanto que sólo determinado número de personas con ciertos conocimientos (en este caso técnicos) pueden llegar a cometerlas.

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

- Son acciones de oportunidad, en cuanto 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 los realizan.

- Ofrecen facilidades 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.

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

- Ofrecen facilidades para su comisión a los menores de edad.

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

- Por el momento siguen siendo ilícitos impunes de esta manera se manifiesta ante la ley"[4].

2.2.4 Tipos de delitos informáticos

Muchos autores y organismos han clasificados de diferentes maneras los tipos de delitos informáticos, entre estas tenemos los siguientes, que llegan tener consenso entre los diferentes especialistas:

- **Reconocidos por las Naciones Unidas[5]**

  - Fraudes mediante la manipulación de computadoras (programas, datos de entrada y salida, repetición automática de procesos)

  - Falsificaciones informáticas (Alteración y falsificación de documentos)

  - Daños o modificaciones de programas o datos computarizados (sabotaje y virus)

  - Accesos no autorizados a servicios y sistemas informáticos (piratas, reproducción no autorizada)

- **Abogados especializados en delitos informáticos [6]**

  - Fraudes mediante la manipulación de computadoras:

    1. Delitos contra elementos físicos – hardware (robo y estafa)

[4] Valdés Téllez Julio, Derecho Informático, 2da Edición, Mc Graw Hill – México 1996
[5] Organización de Naciones Unidas
[6] http://informatica-juridica.com

2. Delitos contra elementos lógicos (daños, accesos ilícitos a sistemas, acceso ilícito a datos y protección de programa)

- Delitos cometidos a través de sistemas informáticos:

1. Estafas.
2. Apoderamiento de dinero por tarjetas de cajero.
3. Uso de correo con finalidad criminal
4. Utilización de Internet como medio criminalidad

2.2.5 Clasificación de los delitos informáticos

Los "Delitos Informáticos" o "cybercrímenes", son aquellas conductas que atentan contra la propiedad privada y la seguridad de las personas en el uso de los recursos informáticos. Estas conductas en la mayoría de los casos poseen un tratamiento internacional específico, tales como el fraude informático, robo de software, sabotaje y vandalismo de datos, alteración, acceso y uso indebido de datos informáticos, manipulación informática y parasitismo informático.

a) Espionaje informático:

El Espionaje informático el agente de la conducta fisgonea los datos computarizados en busca de informaciones sigilosas que posean valor económico. Tal operación se efectiviza por los programas denominados "spywares".

Para Marco Antônio Zanellato, "estos programas espiones envían informaciones del computador del usuario de la red para desconocidos. Hasta lo que es digitado en su teclado puede ser monitoreado por ellos. Algunos tienen un mecanismo que hace una conexión con el servidor del

usuario siempre que él estuviera conectado on-line. Otros envían informaciones vía e-mail. Como los softwares espiones "roban"informaciones del PC (personal computer) del usuario.

El espionaje informático se ve favorecida por el hecho de que las informaciones se encuentran archivadas en un espacio mínimo y pueden ser transferidas muy fácilmente a otro soporte similar lógico. Este puede ser utilizado para producir considerables pérdidas a una empresa u organización, o ser utilizado con fines políticos de tal manera que pudiera atentar contra la seguridad exterior del Estado.

b) Fraudes Informáticos

El fraude informático es apreciado como aquella conducta consistente en la manipulación de datos, alteración o procesamiento de datos falsos contenidos en el sistema informático, realizada con el propósito de obtener un beneficio económico. Entre estos se encuentran el Fraude por manipulación de un computador contra un procesamiento de datos.

A su vez tenemos el uso de datos engañosos "data diddling". Fraude mediante el cual se hace referencia a las distintas formas de alteración de datos contenidos en el computador antes o durante su proceso informático. Se puede cometer también este delito mediante el uso de "trojan hourses" y a través de la técnica del salami "rounding down" la cual permite sustraer mediante redondeo, pequeñas cantidades de activos financieros de diversas cuentas bancarias para situar su monto total, que puede ascender a cantidades considerables, en la cuenta del delincuente informático o "hacker".

El fraude informático se puede dar a nivel input, o materia corporal del hardware, que implica violar la integridad física del propio computador.

Esta relacionado con la alteración de datos, introducción de datos falsos al ordenador.

Otro de los fraudes se da a nivel de tratamiento. Esto es modificar los programas en el soporte lógico del ordenador sin alterar los datos electrónicos existentes. Puede igualmente interferir en el correcto procesamiento de la información, alterando solo el programa original o adicionando al sistema programas especiales que induce el propio agente. Otro de los fraude se puede dar a nivel de los output que esta relacionado con el falseamiento de los resultados obtenidos por el ordenador.

c) El sabotaje informático empresarial

Consiste con el acto de inutilizar, destruir, alterar o suprimir datos, programas e información computarizada, tiene sus inicios en los laboratorios del Instituto de Masachusetts en 1960, cuando fue creado por primera vez un dispositivo informático destructivo mediante la utilización del lenguaje Assambler. Su modus operandi es a través de bombas lógicas o cronológicas, bombas de software, virus polimorfos, gusanos, cáncer rutinario, virus de sector de arranque, Un ejemplar representativo de este virus es el "virus Navidad' que estalla cada 25 de diciembre en el computador infectado. En gran parte el sabotaje informático Empresarial es realizado por sujetos denominados "Crackers" y en menor proporción por los "Preackers y Phonopreackers", los cuales analizan las fallas del sistema y seleccionan el tipo de información que se desea destruir o inutilizar, considerándolo objetivo de ataque.

Entre los dispositivos informáticos más destructivos utilizados para cometer sabotaje informático podemos mencionar:

- **Bombas lógicas:**

Este dispositivo informático de actividad destructiva del dispositivo comienza actuar mucho después de haber sido colocada en el soporte lógico del ordenador a través de una señal o tiempo determinado. Exemplo: Programar el dispositivo para dos días después de su colocación en el ordenador.

- **Virus polimorfos:**

Son dispositivos informáticos destructivos de difícil detección pues cambian su código binario. Frecuentemente utilizado para dañar sistemas informáticos.

- **Robo de servicios o hurto de tiempo:**

Es el supuesto de Apropiación de Informaciones "scavenging", que implica la sustracción de datos que han sido abandonados por los legítimos usuarios de servicios informáticos como residuo de determinadas operaciones.

- **Intrusión de sistemas:**

Consiste en la invasión de un sistema informático, sin autorización del propietario, con el uso ilegítimo de passwords u otros. Es un tipo de acceso remoto, del cual puede resultar la obtención ilegal de informaciones visando o no la destrucción de estas.

- **El Parasitismo Informático:**

"Piggybacking". Aludido a conductas que tienen por objeto el acceso ilícito a los programas informáticos para utilizarlos en beneficio del

delincuente. Esta conducta suele asociarse a la figura de la suplantación de personalidad (Impersonation) que se refiere a toda la tipología de conductas en las que los delincuentes sustituyen a los legítimos usuarios de servicios informáticos.

Ej. Uso ilícito de tarjetas de crédito. El estudio realizado por Krauss y MacGaharf adquirió bastante notoriedad, pues en dicho análisis se simbolizan las probabilidades de Crimen Informático = P (CI), en función de tres variables.

Deshonestidad = D (inclinación al delito del personal informático) Oportunidad = O (falta de medidas de seguridad en los equipos computarizados)

Motivación = M (referido a los conflictos personales o laborales que pudieran incitar a delinquir a los empleados informáticos).

En dicha investigación se asignó a cada variable un valor de O a 10, estableciendo las siguientes ecuaciones:

Personal informático de máxima deshonestidad; D = 4

Carencia de cualquier medida de seguridad informática; 0=8

Motivos poderosos en el personal para atentar contra los sistemas informáticos: M = 5.

En función de ello, el índice de probabilidad resultante de este supuesto ofrecería el siguiente resultado;

$$P (CI) = 4 \times 8 \times 5/1.000 = 0.16$$

2.2.6 La investigación tecnológica de los delitos informáticos

a) La evidencia digital

De acuerdo a la conceptualización de Eoghan Casey, "la evidencia digital es un tipo de evidencia física. Esta construida de campos magnéticos y pulsos electrónicos que pueden ser recolectados y analizados con herramientas y técnicas especiales"7.

Miguel López Delgado, define la evidencia digital como "el conjunto de datos en formato binario, esto comprende los ficheros, su contenido o referencia a estos (metadatos) que se encuentran en los soportes físicos o lógicos del sistema vulnerado o atacado"[8]. Según Jeimy J. Cano M., "la evidencia digital es la materia prima para los investigadores, donde la tecnología informática es parte fundamental del proceso"[9].

La evidencia digital posee, entre otros, los siguientes elementos que la hacen un constante desafío para aquellos que la identifican y analizan en la búsqueda de la verdad: Es volátil, es anónima, es duplicable, es alterable y modificable, es eliminable. Estas características advierten sobre la exigente labor que se requiere por parte de los especialistas en temas de informática forense, tanto en procedimientos, como en técnicas y herramientas tecnológicas para obtener, custodiar, revisar, analizar y presentar la evidencia presente en una escena del delito.

---

[7] Eoghan Casey E, Digital Evidence and Computer Crimen, Página 9, 2da Edición, Edit Elsevier Ltda, 2004

[8] Miguel López Delgado, Análisis Forense Digital, Página 5, 2da Edición, 2007

[9] Jeimy J. Cano M, Introducción a la Informática Forense, Revista Sistemas N° 96, Publicado por Asociación Colombiana de Ingeniero de Sistemas (ACIS), 2006, http://www.acis.org.co/

b) La informática forense

El FBI, conceptualiza la informática forense "como la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y almacenados en un medio computacional"[10]. Este mismo organismo ha desarrollado programas que permiten examinar evidencia computacional.

Gerberth Adín Ramírez, "identifica los objetivos de la informática forense con el fin de: perseguir y procesar judicialmente a los criminales; crear y aplicar políticas para prevenir posibles ataques y de existir antecedentes evitar casos similares; compensar daños causados por los criminales o intrusos"[11].

Esta ciencia relativamente nueva se aplica tanto para las investigaciones de delitos tradicionales tales como: fraudes financieros, narcotráfico, terrorismo, etc.; como para aquellos que están estrechamente relacionas con las tecnologías de la información y las comunicaciones, entre los que se tienen la piratería de software, distribución pornográfica infantil, tráfico de bases de datos, etc. La investigación forense sigue los siguientes pasos en su afán de identificar el delito:

[10] FBI, Computer Evidence Examinations at the FBI, 2nd International Law Enforcement Conference on Computer Evidence, 1995, http://www.fbi.gov/

[11] Gerberth Adín Ramírez, Informática Forense, Página 4, Publicación Universidad San Carlos de Guatemala, 2008.

Pasos a realizar en la investigación forence
Fuente: Miguel López Delgado

➢ Identificación de incidentes

Consiste en asegurar la integridad de la evidencia original, sin modificaciones ni alteraciones manteniendo los requerimientos legales. Se deben establecer los procesos que se están ejecutando en el equipo Identificando procesos extraños o actividades pocos usuales conociendo la actividad normal del sistema.

➢ Recopilación de evidencias digitales

Si La recopilación de la evidencia digital requiere de una investigación forense detallada. En este proceso se debe tomar en cuenta los siguientes aspectos:

- No restablecer el sistema a su estado normal, para las evidencias que aún se encuentren en la "escena del delito".
- El especialista debe iniciar con el proceso de recopilación de las evidencias que permitan determinar los métodos de entrada, actividades de los intrusos, identidad y origen, duración del evento o incidente, siempre precautelando evitar alterar las evidencias durante el proceso de recolección.

- Necesario contar con un registro para procesar cada unos de los pasos realizados y características o información de los hallazgos encontrados, es imprescindible tratar de obtener la mayor cantidad de información posible con el acompañamiento de una persona imparcial.

- Durante esta fase, el especialista debe utilizar una técnica o metodología de recolección de evidencias reconocidas que puedan ser reproducidas o replicadas, bajo el mismo contexto del escenario presente.

➢ **Preservación de la evidencia digital**

Cuando se inicia un proceso judicial contra los atacantes del sistema, es necesario documentar en forma precisa y clara la evidencia. Para estas, se recomienda la obtención de copias exactas de la evidencia obtenida utilizando mecanismos de comprobación de integridad de cada copia, las cuales deben ser documentadas y agregadas en el etiquetamiento realizado.

El segundo factor es establecer una Cadena de Custodia, donde se distribuyen responsabilidades y controles de cada una de las personas que manipulen la evidencia digital, preparando un documento en el que se lleve el registro (nombres, fechas, custodios, lugar de almacenaje, transporte, entre otros.), y los datos personales.

➢ **Análisis de la evidencia**

Luego de que ya se ha realizado los procesos de identificación, recopilación y preservación de las evidencias digitales, el siguiente paso es el Análisis Forense, que consiste en reconstruir con todos los datos disponibles, la línea de tiempo en que se realizó el ataque. Dicho análisis

debe responder a interrogantes de cómo, quienes, bajo que circunstancia, objetivos y que daños se han causado.

- **Documentación y presentación de los resultados**

Para la presentación de los resultados el investigador debe considerar básicamente los siguientes formularios:

- Formulario de identificación de equipos y componentes.
- Formulario de obtención o recolección de evidencias.
- Formulario para el control de custodia de evidencias.
- Formulario de incidencias tipificadas.

En esta etapa, se procede con el desarrollo de los informes técnicos o periciales que deban contener una declaración detallada del análisis realizado, en el cual se debe describir la metodología, las técnicas, y los hallazgos encontrados. El informe pericial contendrá lo siguiente:

- La descripción detallada de lo que se ha reconocido o examinado.
- La determinación del tiempo probable transcurrido entre el momento en que se cometió la infracción y el de la práctica del reconocimiento.
- El pronóstico sobre la evolución del daño, según la naturaleza de la pericia.
- Las conclusiones finales, el procedimiento utilizado para llegar a ellas y los motivos en que se fundamentan.
- La fecha del informe, la firma y rubrica del perito.

Es imprescindible destacar que existen en el mercado soluciones de software que permiten realizar el análisis forense de evidencias digitales entre los cuales se destacan los siguientes:

SOFTWARE	SISTEMA OPERATIVO	FUNCIONES/HERRAMIENTAS
WINHEX	Window	**Informática forense, recuperación de archivos, peritaje informático, procesamiento de datos de bajo nivel y seguridad informática.**
HELIX Live Foresics	Linux	**Respuesta a Incidentes y herramientas forenses.**
ENCASE	**Windows, Linux, AIX, Solaris, OS X**	**Manejo de evidencias y herramientas forenses**

Tabla 1. Software para análisis forences de evidencia digital
Fuente: Elaboración Propia

c) La auditoria informática

Es la investigación que se utiliza generalmente para la prevención y detección de fraudes de una manera especializada. Consiste en el uso de técnicas de investigación criminalística, integradas con la contabilidad, conocimientos jurídicos procesales donde intervienen contadores, auditores, abogados, investigadores informáticos y otros.

2.3 Privacidad en Internet

2.3.1 Internet

Internet es una red internacional de computadoras interconectadas, habilitando a millones de usuarios a comunicarse entre sí y acceder a un enorme caudal de información proveniente de cualquier parte del mundo. Sus tres principales características son la interactividad, la libre elección de contenidos y la ausencia de una autoridad de control.

Asimismo, esta inmensa red no es una empresa u organización acotada, sino un recurso tecnológico que comparten los proveedores de acceso a la red, los que brindan aplicaciones específicas como por ejemplo, e-mails, diseño de páginas Web, e-commerce, etc. Es dable resaltar que esta inmensa red, que hoy nos avasalla tiene como todo avance tecnológico cosas a favor y en contra.

Su expansión exponencial (sin límites imaginables) genera intereses industriales y comerciales que favorecer la libertad de expresión y la educación de la población. Es cierto que el Internet puede ser utilizado para múltiples fines tanto comerciales, educativos, culturales, políticos, etc. Así mismo también puede ser utilizado con fines delincuenciales.

2.3.2 Problemas de territorialidad.

En la actualidad no existe un lugar geográfico, en que haya llegado la red. Por tanto es importante entender que para abordar el problema de la delincuencia se debe ubicar en un lugar físico o país donde esté instalado un servidor computacional. Hoy todos los países del mundo acceden al ciberespacio obteniendo incalculables contenidos. Esto se da gracias a varios ISP o proveedores de conectividad que lo posibilitan mundialmente.

Una idea es esencial: Internet es una red telemática pública y abierta, descansa en su "no regulación" o "desregulación local", lo que implica que no se puede censurar desde un Estado determinado, una realidad virtual que normativamente y en teoría sólo podría llegar a regularse mediante un tratado internacional, siempre y cuando existan criterios uniformes respecto a la forma de hacerlo.

2.3.3 Limitantes de jurisdicción.

Internet no respeta límites geográficos y no reconoce fronteras o jurisdicciones estatales. Los canales de la red traspasan todas las fronteras geográficas y políticas, en consecuencia, por ahora existe incertidumbre respecto a la ley aplicable a actos que carecen de localización física precisa.

2.3.4 Privacidad

La privacidad es el interés que tienen los individuos para sostener un espacio personal, libre de interferencias con otras personas y organizaciones. Entre los temas relacionados con la privacidad podemos mencionar los siguientes: privacidad de información, privacidad en Internet, privacidad de personas, privacidad del comportamiento personal, privacidad de comunicación personal y privacidad de datos personales.

La privacidad en Internet se puede subdividir en cuatro materias de estudio:

- **El Correo Electrónico (email)** Los mensajes de correo viajan por la red a través de decenas de servidores de correo distintos pudiendo dejar copia de estos mensajes en cada uno de ellos.

- **La Criptografía:** La Criptografía consiste en alterar los datos de un mensaje con una clave (en caso informático, formada por un conjunto de números) de tal manera que queda ilegible, y el proceso inverso

para recuperar el mensaje original sólo puede realizarse recombinando el mensaje alterado con esa clave.

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

- **El Anonimato:** La procedencia de un mensaje de correo electrónico, con determinados medios, fácilmente rastreables. En determinadas situaciones, puede que la gente necesite que su correo electrónico sea enviado de forma anónimo, sin poder saberse quién emitió el mensaje.

2.4 Acceso a las redes sin autorización

Los que acceden a las redes sin autorización no siempre son los hackers o brillantes estudiantes o graduados en ciencias de la computación, sentados en sus laboratorios en un lugar remoto del mundo. La mayoría de las violaciones a la seguridad son hechas desde las organizaciones. Estas se pueden caracterizar en las siguientes categorías:

2.4.1 Persona dentro de una organización:

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

2.4.2 Personas fuera de la organización:

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

Un buen sistema para fiscalizar la seguridad informática debe considerar todas las categorías anteriormente señaladas. Estos riesgos se controlan con los denominados firewalls o paredes de fuegos.

Al instalar unos buenos cortafuegos o firewall se puede eliminar las amenazas a la seguridad del sistema. Estos actúan como un escudo o barrera entre la red interna y el exterior y proveen un nivel de seguridad más allá de la protección por contraseñas o passwords.

Ahora debemos ver los sujetos involucrados en la comisión de estos delitos:

Sujeto activo:

Las personas que cometen los delitos informáticos son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes, estos son, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y puede ocurrir que por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible.

Con el tiempo se ha podido comprobar que los autores de los delitos informáticos son muy diversos y que la diferencia entre sí es la naturaleza de los delitos cometidos. De esta forma, la persona que "entra" en un sistema informático sin intenciones delictivas es muy diferente del empleado de una institución financiera que desvía fondos de las cuentas de sus clientes.

Sin embargo, teniendo en cuenta las características de las personas que cometen los delitos informáticos, doctrinarios en la materia los han catalogado como "delitos de cuello blanco", termino introducido por primera vez por EDWIN SUTHERLAND.

Sujeto pasivo

Tenemos que distinguir que sujeto pasivo ó víctima del delito es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo, y en el caso de los delitos informáticos las víctimas pueden ser individuos,

instituciones, gobiernos, etc., que usan sistemas automatizados de información, generalmente conectados a otros.

El sujeto pasivo del delito que nos ocupa, es sumamente importante, ya que mediante él podemos conocer los diferentes ilícitos que cometen los delincuentes informáticos, debido a que muchos de los delitos son descubiertos por el modus operandi de los sujetos activos.

Por lo que ha sido imposible conocer la verdadera magnitud de los delitos informáticos, ya que la mayor parte de los delitos no son descubierto o no son denunciados a las autoridades responsables y si a esto se le suma la falta de leyes que protejan a las víctimas de estos delitos, la falta de preparación por parte de las autoridades para comprender, investigar y aplicar el tratamiento jurídico adecuado a esta problemática, el temor por parte de las empresas de denunciar este tipo de ilícitos por el desprestigio que esto pudiera ocasionar a su empresa y las consecuentes pérdidas económicas, entre otros más, trae como consecuencia pérdidas económicas, entre otros más, trae como consecuencia que las estadísticas sobre este tipo de conductas se mantenga bajo la llama de cifra negra u oculta.

Por todo esto se reconoce que para conseguir una previsión efectiva de la criminalidad informática se requiere, en primer lugar, un análisis objetivo de las necesidades de protección y de las fuentes de peligro.

Una protección eficaz contra la criminalidad informática presupone ante todo que las víctimas potenciales conozcan las correspondientes técnicas de manipulación, así como sus formas de encubrimiento.

Además, se debe destacar que los organismos internacionales han adoptado resoluciones similares en el sentido de que educando a la comunidad de víctimas y estimulando la denuncia de los delitos se promovería la confianza

pública en la capacidad de los encargados de hacer cumplir la ley y de las autoridades judiciales para destacar, investigar y prevenir los delitos informáticos.

Otros Delitos:

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

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

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

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

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

Estafas electrónicas: La proliferación de las compras telemáticas permite que aumenten también los casos de estafa. Se trataría en este caso de una dinámica comisiva que cumpliría todos los requisitos del delito de estafa, ya que además del engaño 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.

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

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

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

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.

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.

La pornografía es uno de los pilares centrales del tema del presente trabajo. Su correcta definición es esencial, por cuanto de ella se desprenderá el alcance exacto de la restricción de acceso a la información que eventualmente se establezca para los menores que navegan por Internet.

Una definición demasiado amplia o vaga, podría redundar en una frustración del derecho de los menores a informarse y educarse. Pero, por otra parte, su acotamiento excesivo, podría significar la adopción de normas que resulten ineficientes para el cumplimiento del real objetivo de las mismas.

La pornografía puede definirse como el carácter obsceno de una obra literaria. Ello nos remite a la definición de lo obsceno, obsceno es aquello que es lascivo, ofensivo o contrario al pudor (impúdico). Tanto un concepto como el otro pueden ser catalogados como conceptos evolutivos o dinámicos ya que la definición de sus contenidos varía con el tiempo; lo obsceno, varía con los cambios que la sociedad ha tenido respecto a los valores y las virtudes. Y el concepto de obra literaria, también ha ido evolucionando, con el surgimiento de nuevas formas de expresión del arte. Es por ello que ambos conceptos son evolutivos, por oposición a lo estático.

Siguiendo la línea de la presente definición, en cuanto a concepto evolutivo y dinámico, se podría hablar de una definición de "pornografía actual", que va más allá de la mera acepción que aparece en los diccionarios, en un artículo que ha sido extractado de publicaciones efectuadas por INTERPOL, la Unidad de Investigación de la Delincuencia en Tecnologías de Información del Cuerpo Nacional del Reino Unido de España y de la actividad desarrollada por la

División Inteligencia Criminal Informática de la Policía Federal Argentina, se expresa que el concepto de "pornografía" puede resumirse en dos funciones principales: "producir excitación erótico-sexual" y, "actuar como forma de liberación ante sociedades represivas de la sexualidad", pues nadie puede negar que hace treinta años atrás, existía una cierta represión frente a todo lo referido al sexo y sus formas de manifestación; pero en la actualidad, nadie puede afirmar que se esté reprimiendo la sexualidad, ya que los quioscos de diarios, los video clubs, los sex - shops, las salas X, y las cadenas televisivas no andan con vueltas a la hora de ofrecer material sexual. Tanto es así que se hizo necesario aprobar leyes para protección de los menores, que recogen entre otras cuestiones preservar el desarrollo físico, mental y moral de los mismos y la emisión de programas que atenten contra las cuestiones antes nombradas, como ser que contengan escenas de pornografía o violencia gratuita.

Pero diversas formas de "pornografía actual" se han alejado peligrosamente de su concepto original "erótico- sexual", para pasar a acercarse a la "criminalidad sexual", nos referimos en este caso a videos y revistas, con muchísima más fuerza en esta época de la informática todo el increíble cúmulo de material pornográfico que existe en Internet cuyos mensajes van dirigidos a estimular la consecución de conductas delictivas, y lo que es más grave aún el perjuicio que pueden ocasionar tales materiales a los menores, lo cual nos tiene que llevar indefectiblemente a la reflexión y a lanzarnos a la búsqueda de soluciones, para evitar graves daños en nuestros niños.

2.5 El perfil del delincuente informático

Con el aporte de la obra criminológica del sociólogo norteamericano Sutherland, en las corrientes estructuralistas, se pone de manifiesto la relación clase social - delito

en términos de características según el estatus social, de comisión delictiva y de reacción social.

Los criminales informáticos o vándalos electrónicos en su generalidad son de sexo masculino, de 18 a 30 años de edad, con características de ser un empleado de confianza en la empresa en la que desenvuelve sus funciones, posee necesariamente conocimientos técnicos en computación.

Estos agentes, responden a motivaciones dispares, generalmente el animus delicti es motivado por razones de carácter lucrativo, por la popularidad que representa este actuar en la sociedad moderna o por simple diversión "hackers", o por la intención de que su actuar puede responder al deseo de destruir o dañar un sistema informático, desestabilizando el normal desenvolvimiento en la institución o empresa "crackers". Ambos causan perjuicios al sistema informático, lo que varia es la intencionalidad en su comisión.

Estos agentes poseen varias características semejantes a los delincuentes de cuello blanco ya que ambos sujetos activos poseen un cierto estatus socioeconómico, no pudiendo explicarse su comisión por mala situación económica o pobreza, ni por carencia de recreación, o por baja educación, ni por poca inteligencia.

La comisión de estas formas de delinquir, ofrecen al "delincuente informático" facilidades de tiempo y espacio para la consumación del hecho, ya que no existe la necesidad de presencia física.

2.5.1 Impacto de los delitos informáticos

a) 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.

Los delincuentes de la informática son tan diversos como sus delitos; que muestran un porcentaje de gran importancia, puede tratarse de estudiantes, terroristas o figuras del crimen organizado, (ver anexo A). Estos delincuentes pueden pasar desapercibidos a través de las fronteras, ocultarse tras incontables "enlaces" o simplemente desvanecerse sin dejar ningún documento de rastro.

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.

b) Impacto a Nivel Social

La proliferación de los delitos informáticos ha 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.

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

c) Impacto en la Esfera Judicial

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.

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.

2.6 Legislación sobre delitos informáticos

2.6.1 Panorama general

La legislación sobre protección de los sistemas informáticos ha de perseguir acercarse lo más posible a los distintos medios de protección ya existentes,

creando una nueva regulación sólo en aquellos aspectos en los que, basándose en las peculiaridades del objeto de protección, sea imprescindible.

Si se tiene en cuenta que los sistemas informáticos, pueden entregar datos e informaciones sobre miles de personas, naturales y jurídicas, en aspectos tan fundamentales para el normal desarrollo y funcionamiento de diversas actividades como bancarias, financieras, tributarias, previsionales y de identificación de las personas.

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.

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 por qué 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.

2.6.2 Análisis legislativo

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

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

ilegal de tales accesos, la difusión de virus o la interceptación de mensajes informáticos.

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

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

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 lo 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.

2.6.3 Panorama mundial

Un ejemplo clarificador es lo que ocurrió con el famoso gusano de Internet que lanzó Robert Morris Jr. en noviembre de 1988 y que acabó bloqueando más de 6000 ordenadores: De no existir en ese momento el Acta sobre Fraude y Abuso Informático en Estados Unidos, es más que dudoso que se le hubiese podido juzgar.

Hay que recordar también que las compañías de seguros, de varios países, ofrecen cobertura concreta contra este tipo de delitos. Sólo en Estados Unidos se calcula que se generan perjuicios económicos, por los delitos informáticos, que superan los 10.000 millones de dólares o más de 5.000 millones de libras esterlinas en el Reino Unido. También hay que recordar que hasta la propia Dirección General de Policía en España, al igual que muchos otros países, ha tenido que crear un Grupo dedicado en exclusiva a los delitos informáticos.

Casi el 90% de los delitos informáticos que investiga el FBI en Estados Unidos tienen que ver con Internet. Esto nos enlaza directamente con los problemas de inexistencia de fronteras que aparecen constantemente cuando tratamos estos delitos: ¿Cuál es la ley a aplicar en multitud de casos? La solución pasa por una coordinación internacional, tanto a la hora de investigar como a la hora de aplicar unas leyes que deben contar con un núcleo común. Es decir, hay que unificar criterios: difícil será actuar contra un delito que sí lo es en un país y no en otro. En este sentido está trabajando, por ejemplo, la Unión Europea. Es cierto, de todas formas, que un delito informático puede ser simplemente un delito clásico en un nuevo envoltorio. Lo que ocurre es que no sólo es eso. Además el avance que está sufriendo Internet en número de usuarios, que parece que vaya a colapsarse en cualquier momento, y en broma se hable ya del ciberespacio, hace que haya que actuar rápidamente ante los posibles delitos que puedan cometerse a través de ella: con el aumento de la ciberpoblación, aumentan los posibles delincuentes y los posibles objetivos.

En el nuevo Código Penal español (aprobado por Ley-Orgánica 10/1995, de 23 de noviembre / BOE número 281, de 24 de noviembre de 1995) hay varios artículos íntimamente relacionados con el tema que estamos tratando (ver anexo C)

2.6.4 Legislación en otros países

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

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

2.7 Las naciones unidas y los delitos informáticos

El Manual de las Naciones Unidas para la Prevención y Control de Delitos Informáticos señala que cuando el problema se eleva a la escena internacional, se magnifican los problemas y las insuficiencias, por cuanto, los delitos informáticos constituyen una forma de crimen trasnacional y su combate requiere de una eficaz cooperación 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:

a) Falta de acuerdos globales acerca de que tipo de conductas deben constituir delitos informáticos.

b) Ausencia de acuerdos globales en la definición de dichas conductas delictivas.

c) Falta de especialización en las policías, fiscales y otros funcionarios judiciales en el campo de los delitos informáticos.

d) Falta de armonización entre las diferentes leyes procesales nacionales acerca de la investigación de los delitos informáticos.

e) Carácter trasnacional de muchos delitos cometidos mediante el uso de las computadoras.

f) Ausencia de tratados de extradición, de acuerdos de ayuda mutua y de mecanismos sincronizados que permitan la puesta en vigor de la cooperación internacional.

2.8 Legislación Boliviana

En Bolivia, en el año de 1989, se consideró el análisis y tratamiento sobre Legislación Informática concerniente a contratación de bienes y servicios informáticos, flujo de información computarizada, modernización del aparato productivo nacional mediante la investigación científico- tecnológica en el país y la incorporación de nuevos delitos emergentes del uso y abuso de la informática.

Este conjunto de acciones tendientes a desarrollar de manera integral la informática, se tradujo en el trabajo de especialistas y sectores involucrados, representantes en el campo industrial, profesionales abogados y especialistas informáticos, iniciándose la elaboración del Proyecto de Ley Nacional de Informática, concluido en febrero de 1991.

Asimismo, el Código Penal Boliviano, texto ordenado según ley No 1768 de 1997, incorpora en el Título X un capítulo destinado a los Delitos Informáticos. Ambos

cuerpos legales tratan de manera general los nuevos delitos emergentes del uso de la informática.

La Ley No 1768, no obstante de no estar exenta de la problemática actual, al abordar en el Capítulo XI la tipificación y penalización de delitos informáticos, no contempla la descripción de estas conductas delictivas detalladas anteriormente.

Por consiguiente, la atipicidad de las mismas en nuestro ordenamiento jurídico penal vigente imposibilita una calificación jurídico-legal que individualice a la mismas, llegando a existir una alta cifra de criminalidad e impunidad, haciéndose imposible sancionar como delitos, hechos no descriptos en la legislación penal con motivo de una extensión extralegal del ilícito penal ya que se estaría violando el principio de legalidad expreso en la máxima "Nullum crime sine lege" Así mismo resulta imposible extender el concepto de bienes muebles e inmuebles a bienes incorporales como ser los datos, programas e información computarizada.

Con el surgimiento de la INTERNET, la nueva era trae nuevas relaciones jurídicas con nuevos conflictos y una serie considerable de nuevas controversias. En el mundo entero, el Derecho se viene transformando para conseguir ejercer el control social de esas innovaciones, modificando las estructuras legislativas, adecuándose a las nuevas y polémicas cuestiones.

En las últimas décadas, hay una preocupación en reformar las legislaciones visando la tipificación de nuevas figuras delictivas. Tal el caso de Bolivia, donde se percibe el interés en proteger al individuo frente la vulnerabilidad existente en los bienes informáticos de los sistemas computarizados. La legislación penal contempla sólo la tipificación de la manipulación informática, la alteración, acceso y uso indebido de datos informáticos. No menciona nada sobre sabotaje informático empresarial, espionaje informático, parasitismo informático y otras figuras como fraude informático, consideradas en el estudio(ver anexo E).

No existe otra salida que la búsqueda eficaz de mecanismos que aseguren una defensa de los derechos y garantías del ciudadano mediante la individualización de la conducta, descrita en el tipo penal respectivo, así como su respectiva penalización. Ya que de otra forma, segundo las palabras proféticas de Bertold Brecht "tal vez, con el tiempo, descubrid todo aquello que se puede descubrir, no en tanto vuestro adelanto no será más que una progresión, dejando la humanidad siempre cada vez más atrás. La distancia entre vos y ella puede, un día, hacerse tan profunda que vuestro grito de triunfo delante de alguna nueva conquista podría recibir como respuesta un grito universal de pavor".

CAPITULO III
MARCO APLICATIVO

CAPITULO III

MARCO APLICATIVO

3.1 Axiomatización

La penalización de los delitos informáticos en Bolivia es difícil, debido a que no se cuenta con una cultura operativa y procedimental para manejar adecuadamente estos delitos. La mayoría de la población boliviana desconoce las normas vigentes y comete el delito por desconocimiento. Esta situación impulsa a los interesados a trabajar no solamente para perfeccionar la ley vigente sino fundamentalmente para difundir de modo que la mayoría de la población pueda conocer y poner en práctica su aplicación.

Es importante crear en Bolivia una cultura de conocimiento sobre los delitos informáticos. Solamente así se podrá establecer una sociedad capaz de cumplir con las penalizaciones sobre el delito informático. El delito es un síntoma del problema. Para resolver se debe atacar a la esencia del problema, esto es establecer una cultura de respeto a la propiedad ajena. Establecer una cultura de cambio implica promover procesos educativos capaces de informar y desarrollar actitudes de cumplimiento de la ley.

3.2 Procedimientos para modificar el Código Penal de delito informático

A la luz del análisis del problema se puede ver vacíos en la penalización de los delitos informáticos. Por tanto se hace necesario modificar el actual código contra este tipo de delitos. Para realizar este proceso es necesario establecer en el país un sumario de los delitos que se cometen y que no son abarcados por la ley.

3.2.1 Delitos informáticos no penalizados

El actual Código Penal, Ley 1768, artículos 363 bis y 363 ter establecen normas de penalización muy genéricos que no especifican en detalle los delitos (ver anexo E). Este hecho hace que muchos de los delitos sean difícilmente tipificados y menos comprobados. Por esta razón es fundamental establecer los tipos de delito que con frecuencia se cometen en el contexto actual y futuro, ya que con el avance de la tecnología van apareciendo nuevos delitos dentro del campo informático. Entre los delitos más importantes que se ha podido observar dentro de nuestra sociedad, esto, através de una serie de encuestas que se realizo podemos citar los siguientes:

h) Manipulación de los datos de entrada.

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

i) La manipulación de programas.

Este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas. Un método común utilizado por las personas que tiene conocimientos especializados en programación informática es el denominado Caballo de Troya, que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo.

j) Manipulación de los datos de salida.

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

k) Falsificaciones informáticas.

Son delitos que están relacionados con la alteración de los datos o documentos almacenados en forma computarizada.

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

l) Daños o modificaciones de programas o datos computarizados.

Está relacionado con el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema. Los sabotajes informáticos pueden realizarse mediante la infección con virus, gusanos y otros al sistema.

m) Acceso no autorizado a servicios y sistemas informáticos.

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

Los piratas informáticos o hackers son delincuentes que acceder a la importación mediante la red. Puede aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema. A menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sistema.

n) Reproducción no autorizada de programas informáticos de protección legal.

La reproducción no autorizada de programas informáticos puede entrañar una pérdida económica sustancial para los propietarios legítimos. Algunas jurisdicciones han tipificado como delito esta clase de actividad y la han sometido a sanciones penales. El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones modernas.

Todos estos delitos deben estar claramente penalizados en las normas legales de cada país. Solamente de esta forma se podrá viabilizar una ley mas objetiva y real en su aplicación, de lo contrario es imposible penalizar muchas de las conductas delincuenciales a nivel informático.

Bolivia en la actualidad no cuenta con una ley para penalizar los delitos informáticos. El sistema penal boliviano solamente contempla algunos artículos relacionados con el problema. Sin embargo en el actual contexto de uso creciente de la tecnología informática en el país se necesita de una ley que prevenga y norme los delitos que

muchas veces son involuntarios por falta de información y reglamentos adecuadamente establecidos. Por tanto, normar los delitos informáticos en Bolivia es una necesidad urgente.

3.2.2 Revisión o reconsideración de la ley existente

Luego de visualizar claramente los delitos mas frecuentes cometidos en el contexto, el segundo paso es analizar la ley y los artículos vigentes con relación a su penalización. Esta acción implica un proceso interdisciplinario donde deben participar profesionales de derecho, informáticos, sociólogos e incluso educadores. Ya que la solución al problema necesariamente debe partir de un enfoque integral y sistémico.

a) LEGISLACIÓN NACIONAL

CAPITULO XI

DELITOS INFORMÁTICOS

Art 363ºbis.-(MANIPULACIÓN INFORMATICA). El que con la intención de obtener un beneficio indebido para sí o un tercero, manipule un procesamiento o transferencia de datos informáticos que conduzca a un resultado incorrecto o evite un proceso tal cuyo resultado habría sido correcto,ocasionando de esta manera una transferencia patrimonial en perjuicio de tercero, será sancionado de esta manera una transferencia patrimonial en perjuicio de tercero, será sancionado con reclusión de uno a cinco años y con multa de sesenta a doscientos días.

Art. 363º ter.- (ALTERACIÓN, ACCESO Y USO INDEBIDO DE DATOS INFORMATICOS). El que sin estar autorizado se apodere, acceda, utilice, modifique, suprima o inutilice, datos almacenados en una computadora o en cualquier soporte informático, ocasionando perjuicio al titular de la información,

será sancionado con prestación de trabajo hasta un año o multa hasta doscientos días.

b) LEGISLACION INTERNACIONAL

Delitos informáticos: Aplicación Chile

Chile fue el primer país latinoamericano en sancionar la ley contra delitos informáticos en donde se legisla aspecto que conciernen a la información y a la informática, a continuación la siguiente tabla lista las leyes, decretos y normas que han incorporado ésta figuras bajo el contexto legal.

AÑO	LEY / DECRETO/ACUERDO	ORDENANZA
1970	Ley 17336 (Inicial)	Ley de Propiedad Intelectual (incluye programas de computadora. a través de la Ley 18957 - 1990)
1993	Ley 19223	Ley de Delitos Informáticos. Figuras penales relativas a la informática
1999	Decreto 81/99	Uso de la Firma Digital y Documentos Electrónicos en la Administración del Estado
1999 2002	Ley 19628 Ley 19812	Protección de la vida privada. Protección de datos de carácter personal.
2002	Ley 19799	Ley de Firma Electrónica. Documentos Electrónicos, Firma Electrónica y Servicios de Certificación de Firma Digital
2003	NCH 2777	Código de práctica para la Gestión de la Seguridad de la Información
2004	Ley 19927	Pornografía Infantil

Tabla 2. Legislación en Chile – Informática e Información.
Fuente: Elaboración Propia

La Ley 19223, establece figuras penales sobre los delitos informáticos en los que se incluyen los siguientes tipos de actos ilícitos de acuerdo a lo que establecen sus articulados:

1) Sabotaje.

2) Espionaje informático.

3) Destrucción maliciosa de la información.

4) Divulgación de información no autorizada.

Para la investigación de los delitos informáticos, Chile cuenta con la Brigada Investigadora del Ciber Crimen, que pertenece como Unidad departamental a la Policía de Investigaciones de Chile, cuya creación fue en el año 2000, a pesar de contar con la Ley desde 1993, que se especializa en los delitos cometidos vía Internet, tales como amenazas, estafas, falsificación, pornografía infantil en Internet, entre otros.

Las actividades que cumplen los departamentos de la brigada, están dadas de acuerdo a lo siguiente:

1) Investigación de Pornografía Infantil:- Orientada a las investigaciones en Internet, en lo que concierne a la mantención, distribución y creación de material pornográfico infantil, además identificar comunidades y movimientos relacionados con este tipo de delitos.

2) Agrupación de Delitos Financieros e Investigaciones Especiales en Internet:- Investigación de los delitos financieros con apoyo de alta tecnología, se especializa entre otros, en la clonación de tarjetas de crédito y debito, traspasos no autorizados vía web. Además de todas las investigaciones de carácter especial, tales como, amenazas vía internet, Infracción a la Ley 19.223, Infracción a la Ley de propiedad Intelectual e industrial.

3) El Grupo de Análisis Informático:- Busca, recupera, y analiza información y evidencias, de los equipos que son atacados o utilizados para la comisión de diversos delitos.

La Policía de Investigaciones de Chile mantiene también, bajo su estructura orgánica como unidad departamental a la Jefatura Nacional de Criminalística, el cual cuenta con laboratorios especializados por secciones de operación, las ramas de criminalística tales como: balística, huellografía y dactiloscopia, planimetría, contabilidad, fotografía, mecánica, física, química, infoingenieria entre otras.

La sección de infoingenieria utiliza métodos, técnicas y conocimientos científicos avanzados para la investigación de delitos en los que se han utilizado medios informáticos o tecnologías para la comisión de actos ilícitos, así como también de delitos informáticos, siendo ellos los encargados de efectuar los peritajes informáticos desde las evaluaciones o levantamiento de evidencias hasta la aplicación de métodos avanzados en sus laboratorios especializados.

En lo que se refiere a estadísticas de los delitos informáticos, la policía de investigaciones de Chile expresa que los delitos más significativos, son los de destrucción de información y el robo de información, además se ha establecido que los ataques superan los 20000 diarios, pero solo se denuncian menos de 1000 anuales.

Vale destacar además que Chile, cuenta con el Código de Práctica para la Gestión de la Seguridad de la Información (NCH 2777), norma oficial chilena, que está basada en las especificaciones que brinda la Norma ISO 27001, la norma fue creada por el Instituto Nacional de Normalización (INN), el cual contribuye fomentando el uso de metodologías y normas técnicas en entidades públicas y privada, lo que conlleva a implantar conciencia de seguridad a varios niveles de las empresas chilenas.

Delitos informáticos: Aplicación Argentina

Argentina es uno de los países que a nivel de legislación ha desarrollado el tema sobre los delitos informáticos y los ha presentado en debate desde el año 2006, logrando en Junio del 2008 que La Cámara de Senadores del Congreso Nacional apruebe la Ley 26388 en la que se penalizan los delitos electrónicos y tecnológicos. La siguiente tabla muestra las leyes y decretos que mantiene Argentina y que contemplan especificaciones de informática e información:

AÑO	LEY / DECRETO/ ACUERDO	ORDENANZA
1933	Ley 11723	Régimen Legal de Propiedad Intelectual.
1996	Ley 24766	Ley de Confidencialidad.
1998	Ley 25036	Ley de Propiedad Intelectual (Modificación de la Ley 11723)
2000	Ley 25326	Habeas Data (Modificada en el 2008)
2001	Ley 25506	Firma Digital
2002	Decreto 2628/	Reglamentación de Firma Digital
2004	Ley 25891	Servicio y Comunicaciones Móviles
2005	Ley 26032	Difusión de Información
2008	Ley 26388	Delitos Informáticos.

Tabla 3. Legislación en Argentina – Informática e información.
Fuente: Elaboración Propia

La Ley 26388, dio paso a que se incorpore importantes cambios en el Código Penal Argentino sobre el uso de las tecnologías de la información, en la cual se sanciona:

1) Pornografía infantil.

2) Destrucción maliciosa y accesos no autorizados a la información y sistemas de información.

3) Intercepción e interrupción de las comunicaciones electrónicas y de telecomunicaciones.

4) Divulgación de información no autorizada.

Desde el año 2001 la justicia argentina, conformó un equipo de peritos expertos en delitos informáticos, los mismos que asisten a las cámaras y juzgados del país, en los casos en los que se encuentran computadoras u otro tipo de dispositivos informáticos involucrados, sin embargo, también se da la figura de otro tipo de peritos entre los que se encuentran los peritos oficiales, de oficio y de parte, que pasan por un proceso de acreditación establecido de acuerdo a la jurisdicción por ser un país federal y poseer poderes judiciales descentralizados por provincias.

1) Peritos oficiales o judiciales:- Son aquellos que pertenecen a algún organismo oficial como la policía federal o gendarmería (Ministerio de Justicia, Seguridad)

2) Peritos de parte:- Son aquello que son proveídos, como su nombre lo indica por una de las partes contratados por abogados en un caso litigioso.

3) Peritos de oficio o dirimentes:- También reconocidos como tercero en discordia y son llamados a evaluar informes previos de otros peritos, o cuando los informes presentados guardan una discordancia.

Es preciso destacar que a pesar de que Argentina, implantó la Ley de Delitos Informáticos recientemente, se han dado una serie de casos que han sido sancionados de acuerdo a las disposiciones del Código Penal, bajo el ámbito de haber cometido infracciones en otro tipos de delitos como la propiedad intelectual y la pornografía infantil, sin embargo al haberse aprobado recientemente la Ley de Delitos Informáticos, en Argentina, y más aún su reciente aplicación, no se cuentan con estadísticas oficiales y precisas sobre este tipo de delitos.

Delitos informáticos: Aplicación Colombia

Colombia ha implementado iniciativas que le permiten en diferentes espacios, establecer mecanismos que le permiten controlar los delitos relacionados con las tecnologías. En el campo jurídico, Colombia mantiene las siguientes leyes decretos y acuerdos, relacionados con la informática y la información:

AÑO	LEY / DECRETO/ ACUERDO	ORDENANZA
1985	Ley 57	Transparencia y Acceso a la Información Gubernamental
1999	Ley 527	Información en forma de mensaje de datos
2000	Decreto 1747	Entidades de Certificación, los Certificados y las Firmas Digitales
2000	Resolución 26930	Estándares para la autorización y funcionamiento de las entidades de certificación y sus auditores.
2001	Ley 679	Explotación, la Pornografía y el Turismo Sexual con Menores de Edad
2003	Decreto 2170	Certificación y Firmas Digitales
2004	Proyecto de Ley 154	Reglamento del Derecho a la Información
2006	Acuerdo PSAA06-3334	Reglamentación de medios electrónicos e informáticos en la justicia.
2009	Ley 1273	Ley de la protección de la información y de los datos

Tabla 4. Legislación en Colombia – Informática e información.
Fuente: Elaboración Propia

Colombia ha tenido un desarrollo particular con respecto a la investigación de delitos de índole informático, factores como el narcotráfico, lavado de dinero, falsificación y terrorismo, ha incentivado que este país implemente unidades de investigación que les colabore en los procesos de indagación de actos

ilícitos en los que se utilizan medios tecnológicos o que afectan sistemas de tecnología o de información.

La Ley1273, aprobada en enero del 2009, crea un nuevo bien jurídico tutelado, el cual se denomina "protección de la información y de los datos", en la sociedad colombiana, en la que se penalizan y sancionan los siguientes actos:

LEY 1273	
Atentados contra la confidencialidad, integridad y disponibilidad de los datos y de los sistemas informáticos:	
Acceso abusivo a un sistema informático	48 A 96 meses de prisión 100 a 1000 salarios mínimos legales mensuales vigentes
Obstaculización ilegítima de sistema informático o red de telecomunicaciones	48 A 96 meses de prisión 100 a 1000 salarios mínimos legales mensuales vigentes, siempre y cuando no constituya delito sancionado con una pena mayor
Interceptación de datos informáticos	36 a72 meses de prisión
Daño informático	48 A 96 meses de prisión 100 a 1000 salarios mínimos legales mensuales vigentes
Uso de software malicioso	48 A 96 meses de prisión 100 a 1000 salarios mínimos legales mensuales vigentes
Violación de datos personales	48 A 96 meses de prisión 100 a 1000 salarios mínimos legales mensuales vigentes
Suplantación de sitios web para capturar datos personales	48 A 96 meses de prisión 100 a 1000 salarios mínimos legales mensuales vigentes, siempre y cuando no constituya delito sancionado con una pena mayor
Circunstancias de agravación punitiva	Aumento de la mitad a las tres cuartas parte de las penas imponibles.
Atentados informáticos y otras infracciones: 1) Hurto por medios informáticos y semejantes 2) Transferencia no consentida de activos	

Tabla 5. Ley de Delitos Informáticos de Colombia – Ley 1273.
Fuente: Elaboración Propia

Podemos observar que las sanciones establecidas se orientan específicamente a preservar aspectos que se delinean con la seguridad de la información en la que se trata de salvaguardar la confidencialidad, integridad y disponibilidad de los datos y los sistemas informáticos.

Colombia ha sido uno de los países que ha recibido la ayuda de los Estado Unidos para la persecución de actos criminales, y la rama de investigación de naturaleza informática.

Colombia mantiene el Grupo Investigativo de Delitos Informáticos (GRIDI) como parte de la Dirección de Investigación Criminal, que investiga las conductas delictivas que se derivan del uso de la tecnología y las telecomunicaciones, éste organismo se sustenta con el apoyo de equipos de informática forense y personal profesional capacitado que atienden incidentes informáticos presentes durante una investigación judicial.

Los grupos de investigación de delitos informáticos se encuentran equipados con laboratorios de Cómputo Forense, en las ciudades de Bogotá, Medellín, Bucaramanga, Cali y Barranquilla, los cuales permiten el análisis de la información digital.

Los organismos oficiales han declarado que los delitos relacionados con la informática en Colombia han tenido un incremento significativo en el año 2007, ya que durante el transcurso del año 2006 se encausaron 433 procesos que corresponden a los delitos informáticos, las cifras oficiales brindadas por la DIJIN (Dirección Central de Policía Judicial), del mes de Enero a Septiembre del 2007, mencionan la denuncia de 630 casos, sin considerar aquellos que se llevan por la Fiscalía y el DAS (Departamento Administrativo de Seguridad), el trafico de bases de datos, fraude electrónico, falsificación o clonación de tarjetas, entre otro, han tenido un costo aproximado de 349 millones de pesos colombianos para las personas naturales y alrededor de 6.6 billones de pesos colombianos para las empresas.

LEGISLACION COMPARADA			
BOLIVIA	**CHILE**	**ARGENTINA**	**COLOMBIA**
Art 363ºbis.- (MANIPULACIÓN INFORMATICA). El que con la intención de obtener un beneficio indebido para sí o un tercero, manipule un procesamiento o transferencia de datos informáticos que conduzca a un resultado incorrecto o evite un proceso tal cuyo resultado habría sido correcto, ocasionando de esta manera una transferencia patrimonial en perjuicio de tercero, será sancionado de esta manera una transferencia patrimonial en perjuicio de tercero, será sancionado con reclusión de uno a cinco años y con multa de sesenta a doscientos días. Art. 363º ter.- (ALTERACIÓN, ACCESO Y USO INDEBIDO DE DATOS INFORMATICOS). El que sin estar autorizado se apodere, acceda, utilice, modifique, suprima o inutilice, datos almacenados en una computadora o en cualquier soporte informático, ocasionando perjuicio al titular de la información, será sancionado con prestación de trabajo hasta un año o multa hasta doscientos días.	Ley 17336 (Inicial).- Ley de Propiedad Intelectual (incluye programas de computadora, a través de la Ley 18957 - 1990) Ley 19223.- Ley de Delitos Informáticos. Figuras penales relativas a la informática Decreto 81/99.- Uso de la Firma Digital y Documentos Electrónicos en la Administración del Estado Ley 19628 y Ley 19812.- Protección de la vida privada. Protección de datos de carácter personal. Ley 19799.- Ley de Firma Electrónica. Documentos Electrónicos, Firma Electrónica y Servicios de Certificación de Firma Digital NCH 2777.- Código de práctica para la Gestión de la Seguridad de la Información Ley 19927.- Pornografía Infantil	Ley 11723.- Régimen Legal de Propiedad Intelectual. Ley 24766.- Ley de Confidencialidad. Ley 25036.- Ley de Propiedad Intelectual (Modificación de la Ley 11723) Ley 25326.- Habeas Data (Modificada en el 2008) Ley 25506.- Firma Digital Decreto 2628/ Reglamentación de Firma Digital Ley 25891.- Servicio y Comunicaciones Móviles Ley 26032.- Difusión de Información Ley 26388.- Delitos Informáticos.	Ley 57.- Transparencia y Acceso a la Información Gubernamental Ley 527.- Información en forma de mensaje de datos. Decreto 1747.- Entidades de Certificación, los Certificados y las Firmas Digitales Resolución 26930.- Estándares para la autorización y funcionamiento de las entidades de certificación y sus auditores. Ley 679.- Explotación, la Pornografía y el Turismo Sexual con Menores de Edad. Decreto 2170.- Certificación y Firmas Digitales Proyecto de Ley 154.- Reglamento del Derecho a la Información Acuerdo PSAA06-3334.- Reglamentación de medios electrónicos e informáticos en la justicia. Ley 1273.- Ley de la protección de la información y de los datos.

3.3. Modificación de la Ley

Luego del estudio de los delitos más frecuentes y contextualizados se debe dar paso a la modificación de la ley con la participación de juristas y profesionales especializados en el campo informático. Solamente de esta forma la legislación boliviana podrá responder al evidente aumento de la delincuencia informática.

La ley que llene estos vacios sobre la problemática de controlar los delitos informáticos debe reflejar la siguiente propuesta:

3.3.1 PROPUESTA DE INCORPORACIÓN SOBRE DELITOS INFORMÁTICOS EN EL CODIGO PENAL DE BOLIVIA

TITULO I

DISPOSICIONES GENERALES.

CAPITULO I

ARTÍCULO 1.- (FINALIDADES) Tiene los siguientes fines:

a) Establecer los mecanismos institucionales y recursos financieros necesarios para promover, administrar y estimular las políticas y estrategias en esta materia.

b) Promover y jerarquizar la formación de recursos humanos a nivel nacional para fortalecer conocimientos en el área de informática.

c) Apoyar la modernización del aparato productivo nacional a través de un mejor manejo de la información con conocimiento de tecnologías informáticas.

d) Procurar el aprovechamiento racional y eficiente de los recursos informáticos existentes en el país.

e) Sentar las bases para promover y fortalecer la investigación y desarrollo en el campo de la informática.

f) Estimular producción nacional de bienes y servicios informáticos de manera que se logre un grado de autonomía en el campo de la informática, compatible con la situación del país en cuanto a tecnología y gestión.

g) Implantar normas que regulen y sancione la práctica de los Delitos Informáticos, en todos los establecimientos y empresas a nivel nacional.

ARTICULO 2.- (AMBITO DE APLICACIÓN)

a) Es necesario un estudio cuidadoso de planes programas educativos en las universidades e instituciones, con el fin de corregir posibles deficiencias o desviaciones, proponiendo políticas adecuadas y aumentar conocimientos a nivel técnico y satisfacer las necesidades futuras del país.

b) Su aplicación será a todos los establecimientos, y lugares implicados en los delitos.

c) Las normas establecidas en ésta ley serán aplicadas a los delincuentes que cometan estos delitos informáticos sean estos nacionales o extranjeros en todo el territorio nacional.

CAPITULO II

ARTICULO 3.- DISPOSICIONES FUNDAMENTALES

a) Los delitos informáticos, su investigación deberán ser estudiado por un experto en delitos informaticos, atravez del cual se podrá detectar el delito.

b) La explicación precisa de los pasos a seguir para la obtención de pruebas en el delito informatico ocasionado, se deberá dar a conocer a la entidad victimizada.
c) El especialista en delitos informaticos antes de realizar el análisis para determinar el delito tendrá que dar un informe atravez de la observación, que contemple la causa por la que se cometió el delito.
d) La institución o centro de investigación de la FELCC deberá dar toda la información necesaria, a toda la población para no ser victimas de dichos ilícitos penales.

ARTICULO 4.- RESPONSABILIDAD DE LAS PARTES.

a) El profesional en delitos informaticos, en caso de encontrar evidencias de que se cometió un ilícito, y no da a conocer, se convertirá en complice del delincuente informatico, teniendo que ser este tambien castigado.

CAPITULO III

ARTICULO 5.-(MANIPULACIÓN DE LOS DATOS DE ENTRADA).- El que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera y/o acceda a él, será castigado con presidio de dos a 6 años.

Si el delito fuera ocasionado por un servidor público, la pena se agravará en un tercio

ARTICULO 6.-(MANIPULACIÓN DE PROGRAMAS).- El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información, será castigado de dos a seis años.

Si el delito fuera ocasionado por un servidor público, la pena agravara en un tercio.

ARTICULO 7.- (MANIPULACIÓN DE DATOS DE SALIDA).- Será reprimida con pena de prisión de seis meses a dos años, la persona que, para descubrir los

secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere, accese, modifique, altere, suprima, intercepte, interfiera, utilice, difunda o desvíe de su destino, mensajes, datos e imágenes contenidas en soportes: electrónicos, informáticos, magnéticos y telemáticos.

ARTICULO 8.- (FALSIFICACIONES INFORMÁTICAS).- El que, a través de cualquier medio, cree, modifique o elimine un documento que se encuentre incorporado a un sistema que utilice tecnologías de información; o cree, modifique o elimine datos del mismo; o incorpore a dicho sistema un documento inexistente, será penado con prisión de tres a seis años y una multa, de acuerdo a lo especificado por el juez.

Cuando el agente hubiere actuado con el fin de procurar para sí o para otro algún tipo de beneficio, la pena se aumentará entre un tercio y la mitad

El aumento será de la mitad a dos tercios si del hecho resultare un perjuicio para otro.

ARTICULO 9.- (DAÑOS Y MODIFICACIONES DE PROGRAMAS O DATOS INFORMÁTICOS).- El que destruya, dañe, modifique o realice cualquier acto que altere el funcionamiento o inutilice un sistema que utilice tecnologías de información o cualquiera de los componentes que lo conforman, será penado con prisión de cuatro a ocho años y una multa.

Incurrirá en la misma pena quien destruya, dañe, modifique o inutilice los datos o la información contenida en cualquier sistema que utilice tecnologías de información o en cualquiera de sus componentes.

La pena será de cinco a diez años de prisión y multa de quinientas a mil unidades tributarias, si los efectos indicados en el presente artículo se realizaren mediante la creación, introducción o transmisión, por cualquier medio, de un virus o programa análogo.

ARTICULO 11.- (ACCESO NO AUTORIZADO A SERVICIOS Y SISTEMAS INFORMÁTICOS).- El que por cualquier medio se apodere, utilice, modifique o elimine, sin el consentimiento de su dueño, la data o información personales de otro

o sobre las cuales tenga interés legítimo, que estén incorporadas en un computador o sistema que utilice tecnologías de información, será penado con prisión de dos a seis años.

La pena se incrementará de un tercio a la mitad si como consecuencia de los hechos anteriores resultare un perjuicio para el titular de la data o información o para un tercero.

ARTICULO 12.- (REPRODUCCIÓN NO AUTORIZADA DE PROGRAMAS INFORMÁTICOS DE PROTECCIÓN LEGAL).- El que sin autorización de su propietario y con el fin de obtener algún provecho económico, reproduzca, modifique, copie, distribuya o divulgue un software u otra obra del intelecto que haya obtenido mediante el acceso a cualquier sistema que utilice tecnologías de información, será sancionado con prisión de uno a cinco años.

CAPITULO IV

ARTICULO 13.- (REGLAMENTOS).-

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

Destrucción de datos: Los daños causados en la red mediante la introducción de virus, bombas lógicas, etc.

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

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

Estafas electrónicas: A través de compras realizadas haciendo uso de la red.

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

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

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

Terrorismo: Mensajes anónimos aprovechados por grupos terroristas para remitirse consignas y planes de actuación a nivel internacional.

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

3.3.3. Difusión de la ley

Toda ley a ser implementada debe ser difundida para el conocimiento de la población. Esta difusión debe realizase por diferentes medio de comunicación, especialmente por vía virtual.

3.4. Medidas de prevención general de los delitos informáticos

Dentro de las medidas preventivas en la informática necesita el apoyo de leyes adecuadamente contextualizadas y aplicables. Este proceso necesita de instrumentos y sistemas computarizados, medios que ofrezcan mayor seguridad a sus usuarios, a través de las siguientes medidas:

- La implementación de un registro de control de computadoras y software.
- La creación de un registro de especialistas en computación a través de la fundación de una institución que avale su trabajo a nivel técnico. Los

profesionales pueden ser técnicos, analistas en sistemas, Licenciados en informática e ingenieros en sistemas.

- La efectivización o realización de Auditorías computarizadas.

3.4.1. Registro de control de computadoras

La necesidad, en términos generales de una Política Nacional en materia de informática, ha promovido la formación en la Honorable Cámara de Diputados de la comisión de informática, la que elaboró un ante-proyecto denominado: "Ley nacional de Informática", que ha sido puesto en consideración en dicha cámara para su conocimiento y en consulta de especialista en informática de instituciones públicas, privadas y personas en general que tengan interés en ella. Se ha celebrado en La Paz una mesa redonda sobre Legislación en Informática, algunas de cuyas propuestas y conclusiones guardan estrecha e intima relación con medidas de prevención de la delincuencia informática que se pergeñaban en el momento de iniciar esta investigación de grado, entre las que destacan: la necesidad de un control y diagnóstico permanente y periódico de recursos informáticos de Bolivia, es decir, satisfacer la necesidad nacional de registrar y mantener información dinámica de los recursos de hardware, software y de las instituciones relacionadas o comprendidas dentro el área de la Informática.

Para la realización positiva de esto es indispensable la conformación del: "Registro Nacional de Proveedores" y de la: "Asociación Nacional de Proveedores". El primero tiene la finalidad de asentar e inscribir a las personas naturales y/o jurídicas ligadas a la actividad de importación de hardware y la segunda de agrupar a estas personas en una institución orgánica y responsable.

La importación legal de hardware tiene la ventaja de garantizar la seguridad del software.

3.4.2. Registro de los especialistas en computación

En Bolivia y en el momento actual, no existe registro alguno en el que las personas especializadas en computación sean (técnicos medios, superiores, licenciados o masters) estén inscritos y asisten su grado jerárquico de especialidad.

Si bien es el ser humano, en términos generales, quien comete delito, uno de los rasgos característicos de la delincuencia informática es el referido al sujeto activo del delito, puesto que para cometer delito informático es preciso poseer conocimientos especializados y profundos en la materia; sin estos conocimientos es inimaginable siquiera que una persona ajena a la informática pueda cometerlos. Por esto es necesario crear un registro nacional de Especialistas en informática donde en principio se debe adoptar a través de las carreras de Informática de las Universidades Bolivianas, un sistema de enseñanza que desarrolle un modelo único, al que deben regirse todos los institutos de información en Informática. Los egresados de estos institutos deberían rendir pruebas de suficiencia o de grado en las universidades, para de que esta manera sean estas las únicas autorizadas para la certificación de nivel técnico o superior.

Una vez cumplidos estos requisitos por los titulados para habilitarse al ejercicio de su carrera, deben inscribirse en el Registro Único Nacional de Especialistas en Informática y para que esta medida se constituya en una medida preventiva de la delincuencia informática es preciso sentar en dicho registro, al margen de los datos sobre los estudios realizados también lo datos personales actuales a efectos de facilitar la ubicación e identificación y , en caso de comisión de delitos, facilitar el resarcimiento de los posibles daños y perjuicios.

3.4.3. Creación de Auditorías de Sistemas

En la actualidad en nuestro país, no existe una auditoria de sistemas que garanticen la lícita utilización de programas; no hay quien revise estos programas.

Internamente se podría modificar el programa para cometer ciertos delitos. Ninguna tecnología es infalible o imposible de manipular, eso facilita que personas con conocimiento en informática, puedan modificar los programas en favor suyo, y lograr ventajas personales.

A causa de ello, los expertos en seguridad sugieren la frecuente la práctica auditorías de las cuentas y los programas que manejan todas las transacciones financieras, además de programas de protección. Es así que en Estados Unidos "varias compañías" han escrito programas de auditoría, que controlan todas las transacciones que se procesan en las computadoras, verificando las irregularidades en los manejos que se efectúan".

3.5. Medidas punitivas o de prevención especial

Las propuestas de prevención general planteadas deben ser reforzadas por medidas penales que tipifiquen conductas y señalen sanciones a partir de una Ley adecuadamente contextualizado. Esta ley por su importancia y actualidad debe ser elaborada, discutida y promulgada con la participación de todos los involucrados en el problema. Se debe tomar en cuenta que la sanción penal cumple dos funciones: La prevención general y la especial.

3.6 Validacion de la tesis

3.6.1 Validacion teorica.

Es indispensable la aprobación de leyes que regulen este tipo de procedimientos debido a que la ley positiva de nuestro país no toma en cuenta este tema en la propia Constitución Política del Estado base lógica de toda normativa.

Los avances tecnologicos en varias áreas que posibilitaron la delincuencia informatica, es imprescindible que se ajuste a las exigencias cambiantes de la realidad, de lo contrario se convertiría en algo obsoleto, y que no responde a la realidad social. La incorporación de los tipos penales ya vistos,debe cumplir con todo los requisitos exigidos por la normativa para su efectivización del mismo.

Por otra parte quedo demostrado que nuestra legislación en ninguna de las normas positivas vigentes, hace mención e este tipo de delitos, por lo tanto, es necesario crear una ley que reglamente, estas actividades primero, para proteger a las parte intervinientes,

Por ultimo, la norma jurídica que regule la practica de los delitos informaticos no debe ser tomada como el ultimo bastión en la evolución jurídica, pues los avances tecnologicos que se dieron en el periodo de desarrollo de esta tesis dieron otro paso hacia delante en la informatica.

Por todo lo expuesto, queda **PROVADA NUESTRA HIPOTESIS, por cuanto es necesario,** "La modificación del Código Penal Boliviano, con la incorporación de tipos penales específicos para la penalización de los delitos informáticos."

CAPITULO IV
CONCLUSIONES Y RECOMENDACIONES

CAPITULO IV

CONCLUCIONES Y RECOMENDACIONES

Conclusiones

Luego de haber realizado un análisis muy profundo, revisar la legislación comparada e indagar en el plano legislativo y sociocultural nacional, se ha logrado arribar a la conclusión de que los vacios jurídicos existentes en principio han incrementado la comisión de delitos informáticos ya sea por la escasa tipificación de estos dentro la norma penal o la insuficiente punibilidad a la cual se somete a los delincuentes informáticos.

Asimismo se ha demostrado, que la incorporación de nuevos tipos penales referidos a los delitos informáticos, tomando en cuenta las recomendaciones efectuadas por los Organismos Internacionales que ya trabajaron en el tratamiento de los delitos informáticos y su adecuado escarmiento.

Finalmente, demostrada la hipótesis planteada se concluye que se ha evidenciado que la incorporación de nuevos tipos penales respecto a los delitos informáticos, garantiza la seguridad en los sistemas informáticos, protegerá a los cibernautas y la información, ya que a partir de ellos se trabajara en la redacción de políticas de seguridad dirigidas a asegurar la integridad, disponibilidad y confidencialidad de los sistemas informáticos tanto del hardware y el software.

Recomendaciones

1. Desde el punto de vista social es conveniente educar y enseñar a la población sobre el uso correcto de las herramientas informáticas, las conductas prohibidas, no solo con el afán de protegerse, sino de no convertirse en un agente de dispersión que pueda contribuir a propagar por ejemplo un virus.
2. No es prudente que una sola persona conozca sobre la seguridad de la empresa o institución, para que no tenga la opción de violar la seguridad del sistema.
3. Es imprescindible que la unidad de investigación de la delincuencia en tecnologías de la información este conformada por personal especializado, con una capacitación permanente, siendo insuficiente los métodos clásicos de criminalística por el modus operandi de los delincuentes informáticos.
4. Se sugiere la creación de una nueva mención dentro del pensum de la carrera de informatica, pues es necesaria la formación de profesionales expertos en diversas areas de investigación sobre los delitos informáticos (informática forense, evidencia digital, peritos informaticos, etc),

GLOSARIO DE TERMINOS

A

Actos ilícitos: acto contrario a derecho. La causa ilícita, por otra parte, es aquella que se opone a las leyes o a la moral.

Análisis Forense: Se refiere a la recopilación de evidencias bajo notario que puedan servir como prueba judicial.

Atipicidad: es la consecuencia máxima del sometimiento del derecho penal al principio de legalidad.

C

Cyberdelincuencia: Toda esta revolución tecnológica, se ha convertido en un campo fructífero para la ciberdelincuencia. Fraudes, Robo de Identidad, Malwares (Trojanos, Spywares, etc), existen muchos tipos de amenazas que se han extendido a lo largo de la red.

Cyberespacio: Conjunto o realidad virtual donde se agrupan usuarios, páginas web, chats, y demás servicios de Internet y otras redes.

Código penal: conjunto unitario y sistematizado de las normas jurídicas punitivas de un Estado.

Comercio on line: Significa hacer negocios online o vender y comprar productos y servicios a través de escaparates Web.

Crackers: Se utiliza para referirse a las personas que *rompen* algún sistema de seguridad. Los crackers pueden estar motivados por una multitud de razones, incluyendo fines de lucro, protesta, o por el desafío.

D

Delito informático: O crimen electrónico, es el término genérico para aquellas operaciones ilícitas realizadas por medio de Internet o que tienen como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet.

Delincuencia Informática: todo delito que implique la utilización de las tecnologías informáticas.

F

Firewall: Cortafuegos, es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado.

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

H

Hackers: En la actualidad se usa de forma corriente para referirse mayormente a los criminales informáticos, gente que invade computadoras, usando programas escritos por otros, y que tiene muy poco conocimiento sobre cómo funcionan.

L

Lucro: Es la **ganancia o provecho que se obtiene de algo**

P

Pesquisa: averiguar, investigar.

Punibilidad: Situación en que se encuentra quien, por haber cometido una infracción delictiva, se hace acreedor a un castigo.

Phishing: es un término informático que denomina un tipo de delito encuadrado dentro del ámbito de las estafas cibernéticas, y que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta.

Preackers y Phonopreackers: los cuales analizan las fallas del sistema y seleccionan el tipo de información que se desea destruir o inutilizar, considerándolo objetivo de ataque.

S

Spam: Correo basura o mensaje basura a los mensajes no solicitados, no deseados o de remitente no conocido, habitualmente de tipo publicitario.

Spyware: Es un software que recopila información de un ordenador y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del ordenador.

Spoofing: Es una técnica usada para infiltrarse en una red Ethernet conmutada (basada en switch y no en hubs).

T

Tipos penales: El tipo penal es un instrumento legal, lógicamente necesario y de naturaleza predominantemente descriptiva.

Transnacional: Que se extiende a través de varias naciones

Trojan hourses: En informática, se denomina troyano o caballo de Troya a un software malicioso que se presenta al usuario como un programa aparentemente legítimo e inofensivo pero al ejecutarlo ocasiona daños.

Técnica del salami: Consiste en introducir al programa unas instrucciones para que remita a una determinada cuenta los céntimos de dinero de muchas cuentas corrientes.

Bibliografia

1. Del Peso Navarro, Emilio. Peritajes Informáticos, 2da Ed., Díaz de Santos S.A, 2001. p. 10
2. Diario el Telégrafo. Transparencia en la Información Pública. Ed. 45119, 27/10/2008. p. 4, 5.
3. Eoghan, Casey E. Digital Evidence and Computer Crimen, 2 Ed., Elsevier Ltda, 2004 . p. 9.
4. Lima, María de la Luz. Delitos Electrónicos. Ed. Porrua, México, 1984. 100 p.
5. López Delgado, Miguel. Análisis Forense Digital. 2 Ed, 2007. p. 10-23.
6. López Delgado, Miguel. Análisis Forense Digital. 2 Ed., 2007. p. 5.
7. Ramírez, Gerberth Adín. Informática Forense. Publicación Universidad San Carlos de Guatemala, 2008. p. 2, 4.
8. Riofrío, Juan Carlos. La Prueba Electrónica. TEMIS S.A., 2004
9. Sarzana, Carlo. Criminalitá e Tecnología en Computer Crime Rasaggna Penitenziaria e Criminalitá. Roma, 1979.
10. Sosa, Montiel. Criminalística. Tomo III, Ed. Limusa, 1997. p. 86
11. Téllez Valdés, Julio. Derecho Informático. 2. Ed., Mc Graw Hill, México, 1996.

Paginas web consultadas

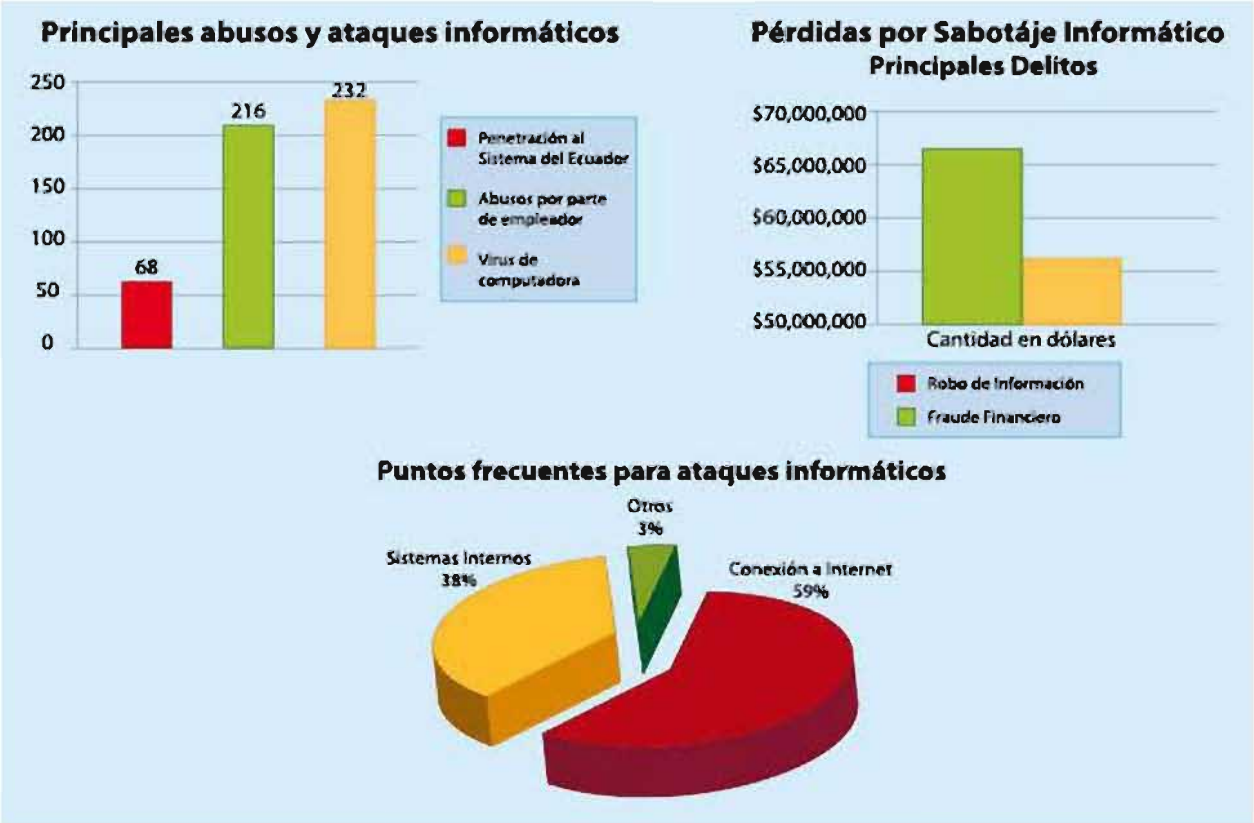
1. CONSEJO de Europa. Estados Miembros del Consejo de Europa y otros Estados. Actualizada: Budapest 2008. [Fecha de consulta: 29 septiembre 2011]. Disponible en: http://www.coe.int
2. CERT, Informe de Vulnerabilidades, 2007, http://www.cert.org/
3. CSI. Computer Crime & Security Survey, 2007, http://www.gocsi.com/
4. Jeimy J. Cano M, Introducción a la Informática Forense, Revista Sistemas N° 96, Publicado por Asociación Colombiana de Ingeniero de Sistemas (ACIS), 2006, http://www.acis.org.co/

5. FBI, Computer Evidence Examinations at the FBI, 2nd International Law Enforcement Conference on Computer Evidence, 1995, http://www.fbi.gov/
6. Pedro Miguel Lollet R, Auditoria Forense, Publicado por ACGAF, http://auditoriaforense.net/
7. Ley Modelo sobre Comercio Electrónico, CNUDMI – Comisión de las Naciones Unidas para el Derecho Mercantil Internacional, 1996 complementada por la Comisión en 1998. http://www.uncitral.org/
8. Ley Modelo sobre Firmas Electrónicas, CNUDMI – Comisión de las Naciones Unidas para el Derecho Mercantil Internacional, 2001, http://www.uncitral.org/
9. Grupo Faro, Acción Colectiva para el Bienestar Público, Cumplimiento de la Ley Lotaip, 2007, http://www.grupofaro.org/
10. Business Software Alliance BSA, 5ta Estudio Anual Global de la Pirateria de Software por BSA e IDC, 2007, http://global.bsa.org/idcglobalstudy2007/
11. Jeimy J. Cano M, Consideraciones sobre el Estado del arte del Peritaje Informático en Latinoamérica, Revista de Derecho Comunicaciones y Nuevas Tecnologías, Universidad de los Andes, 2007, http://derechoytics.uniandes.edu.co/
12. Phil Williams, Crimen Organizado y Cibernético, Centro de Enseñanza en Seguridad de la Internet de la Universidad Carnegie Mellon, http://www.pitt.edu/
13. Plan de Seguridad Ciudadana y Modernización de la Policía Judicial, http://www.policiaecuador.gov.ec/publico/img_policia/rendicion.pdf
14. Plan Operativo de creación de la Unidad de Delitos Informáticos del Ministerio Público, http://www.oas.org/juridico/spanish/cyb_ecu_plan_operativo.pdf
15. Grupo de Expertos Intergubernamentales en Materia de Delitos Cibernéticos, http://www.oas.org/juridico/spanish/cybersp.htm
16. DIJIN (Dirección Central de Policía Judicial, http://www.dijin.gov.co/

ANEXOS

ANEXO A

Cuadros estadísticos sobre fraudes informáticos, su origen y nivel de pérdidas en dólares a nivel mundial.



Fuente: www.inei.co

Anexo B

TRABAJO DE GABINETE

En el punto precedente, demostramos claramente que nuestra investigación desarrollada probó fehacientemente que es necesario crear una Ley para la modificación del Código Penal Boliviano, con la incorporación de tipos penales específicos para la penalización de los delitos informáticos con los cuadros y gráficos siguientes:

Las encuestas realizadas se efectuaron a varias personas, que alguna vez fueron victimas de algunos delitos informaticos (estudiantes, empresas, etc), por cuanto consideramos debe ser tomada como una información altamente sustentada y con un carácter de especialidad por que las personas que fueron consultadas precisan una solución a este problema que perjudica de gran magnitud a toda empresa o persona victima.

Violaciones a la seguridad informática.

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

Fuente: elaboración Propia

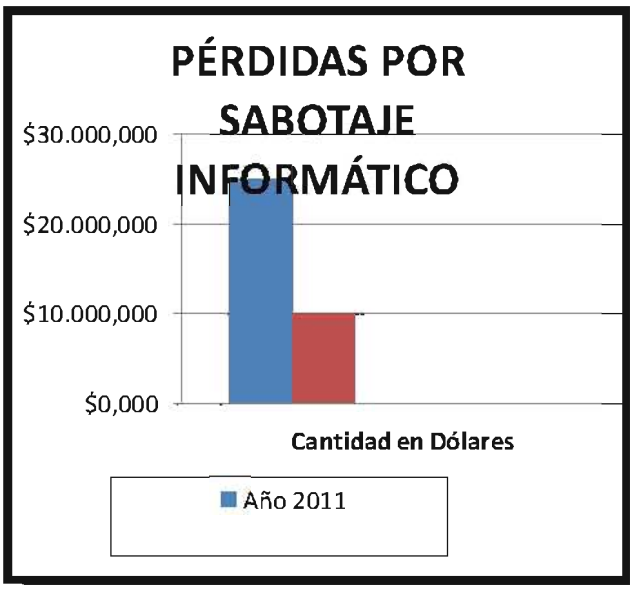
90% de los encuestados descubrió violaciones a la seguridad de las computadoras dentro de los últimos doce meses.

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.

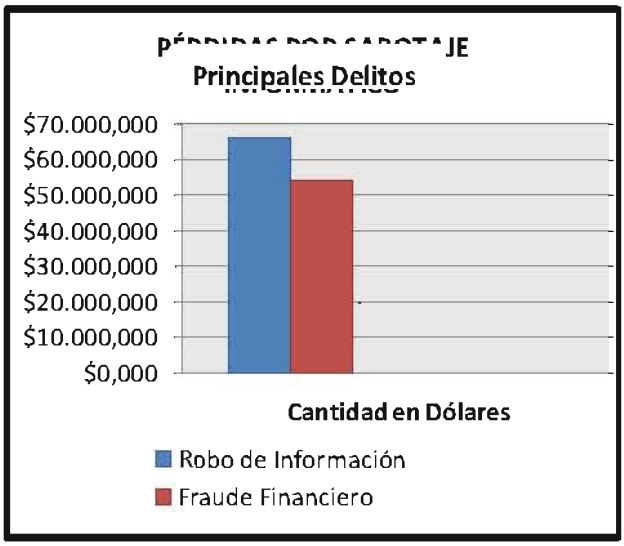
Las pérdidas financieras ascendieron a $265,589,940 (el promedio total anual durante los últimos tres años era $120,240,180).



Fuente: Elaboración Propia

6l encuestados cuantificaron pérdidas debido al sabotaje de datos o redes para un total de $27,148,000. Las pérdidas financieras totales debido al comúnmente llamado

sabotaje informatico durante los años anteriores combinados ascendido a sólo $10,848,850.



Fuente: Elaboración Propia

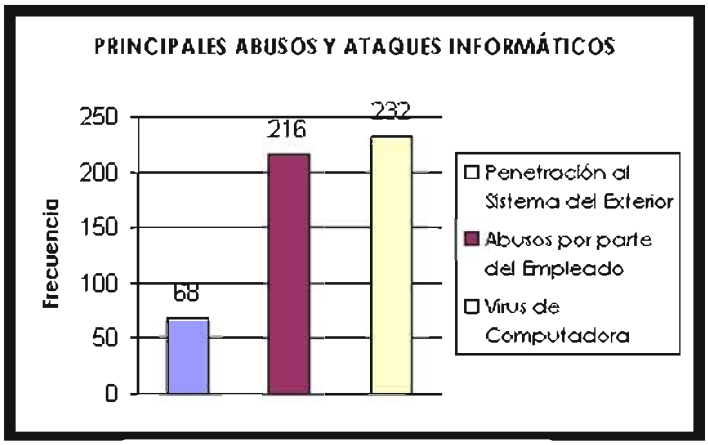
Como en años anteriores, las pérdidas financieras más serias, ocurrieron a través de robo de información (66 encuestados reportaron $66,708,000) y el fraude financiero (53 encuestados informaron $55,996,000).

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

Accesos no autorizados.

Fuente: Elaboración Propia

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%.
en corporaciones, 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.



Fuente: Elaboración Propia

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:

1. 93% de encuestados tienen sitios de WWW.
2. 43% maneja el comercio electrónico en sus sitios (en 1999, sólo era un 30%).
3. 19% experimentaron accesos no autorizados o inapropiados en los últimos doce meses.
4. 32% dijeron que ellos no sabían si hubo o no, acceso no autorizado o inapropiado.
5. 35% reconocieron haber tenido ataques, reportando de dos a cinco incidentes.
6. 19% reportaron diez o más incidentes.
7. 64% reconocieron ataques reportados por vandalismo de la Web.
8. 8% reportaron robo de información a través de transacciones.
9. 3% reportaron fraude financiero.

Anexo C

Tratados Internacionales

En los últimos años se ha perfilado en el ámbito internacional un cierto consenso en las valoraciones político-jurídicas de los problemas derivados del mal uso que se hace de las computadoras, lo cual ha dado lugar a que, en algunos casos, se modifiquen los derechos penales nacionales.

El GATT, se transformó en lo que hoy conocemos como la Organización Mundial de Comercio (OMC), por consecuencia todos los acuerdos que se suscribieron en el marco del GATT, siguen estando vigentes. En el Art. 61 se establece que para los casos de falsificación dolosa de marcas de fábrica o de comercio o de piratería lesiva del derecho de autor a escala comercial se establecerán procedimientos y sanciones penales además de que "Los recursos disponibles comprenderán la pena de prisión y/o la imposición de sanciones pecuniarias suficientemente disuasorias"

- El convenio de Berna
- La convención sobre la Propiedad Intelectual de Estocolmo
- La Convención para la Protección y Producción de Fonogramas de 1971
- La Convención Relativa a la Distribución de Programas y Señales

En 1983 la Organización de Cooperación y Desarrollo Económico (OCDE) inició un estudio de la posibilidad de aplicar y armonizar en el plano internacional las leyes penales, a fin de luchar contra el problema del uso indebido de los programas de computación. Las posibles implicaciones económicas de la delincuencia informática tienen carácter internacional e incluso transnacional, cuyo principal problema es la falta de una legislación unificada que, facilita la comisión de los delitos. En 1986 la OCDE público un informe titulado Delitos de informática: análisis de la normativa jurídica, donde se reseñaban las normas legislativas vigentes y las propuestas de reforma en diversos Estados miembros y se recomendaba una lista mínima de ejemplos de uso indebido que los países podrían prohibir y sancionar en leyes penales.

En 1992 elaboró un conjunto de normas para la seguridad de los sistemas de información, con intención de ofrecer las bases para que los Estados y el sector privado pudieran erigir un marco de seguridad para los sistemas informáticos. En 1990 la Organización de las Naciones Unidas (ONU) en el Octavo Congreso sobre Prevención del Delito y Justicia Penal, celebrado en La Habana, Cuba, se dijo que la delincuencia relacionada con la informática era consecuencia del mayor empleo del proceso de datos en las economías y burocracias de los distintos países y que por ello se había difundido la comisión de actos delictivos. La ONU ha publicado una descripción de "Tipos de Delitos Informáticos", que se transcribe al final de ésta sección. En 1992 La Asociación Internacional de Derecho Penal durante el coloquio celebrado en Wurzburgo en 1992, adoptó diversas recomendaciones respecto a los delitos informáticos, entre ellas que, en la medida que el derecho Penal no sea suficiente, deberá promoverse la modificación de la definición de los delitos existentes o la creación de otros nuevos, si no basta con la adopción de otras medidas como por ejemplo el "principio de subsidiariedad".

Hay otros Convenios no ratificados aún por nuestro País, realizados por la Organización Mundial de la Propiedad Intelectual (OMPI), de la que nuestro país es parte integrante a partir del 8/10/1980. En Noviembre de 1997 se realizaron las II Jornadas Internacionales sobre el Delito Cibernético en Mérida España, donde se desarrollaron temas tales como:

- Aplicaciones en la Administración de las Tecnologías Informáticas / cibernéticas
- Blanqueo de capitales, contrabando y narcotráfico
- Hacia una policía Europea en la persecución del delito Cibernético.
- Internet: a la búsqueda de un entorno seguro.
- Marco legal y Deontológico de la Informática.

ANEXO D

a) Alemania

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

- ✓ Espionaje de datos (202 a)
- ✓ Estafa informática (263 a)
- ✓ Falsificación de datos probatorios(269) junto a modificaciones complementarias del resto de falsedades documentales como el engaño en el tráfico jurídico mediante la elaboración de datos, falsedad ideológica, uso de documentos falsos(270, 271, 273)
- ✓ Alteración de datos (303 a) es ilícito cancelar, inutilizar o alterar datos inclusive la tentativa es punible.
- ✓ Sabotaje informático (303 b. Destrucción de elaboración de datos de especial significado por medio de destrucción, deterioro, inutilización, eliminación o alteración de un sistema de datos. También es punible la tentativa.
- ✓ Utilización abusiva de cheques o tarjetas de crédito (266b).

Por lo que se refiere a la estafa informática, la formulación de un nuevo tipo penal tuvo como dificultad principal el hallar un equivalente análogo al triple requisito de acción engañosa, causa del error y disposición patrimonial, en el engaño del computador, así como en garantizar las posibilidades de control de la nueva expresión legal, quedando en la redacción que el perjuicio patrimonial que se comete consiste en influir en el resultado de una elaboración de datos

por medio de una realización incorrecta del programa, a través de la utilización de datos incorrectos o incompletos, mediante la utilización no autorizada de datos, o a través de una intervención ilícita.

Sobre el particular, cabe mencionar que esta solución en forma parcialmente abreviada fue también adoptada en los Países Escandinavos y en Austria. En opinión de estudiosos de la materia, el legislador alemán ha introducido un número relativamente alto de nuevos preceptos penales, pero no ha llegado tan lejos como los Estados Unidos. De esta forma, dicen que no sólo ha renunciado a tipificar la mera penetración no autorizada en sistemas ajenos de computadoras, sino que tampoco ha castigado el uso no autorizado de equipos de procesos de datos, aunque tenga lugar de forma cualificada. En el caso de Alemania, se ha señalado que a la hora de introducir nuevos preceptos penales para la represión de la llamada criminalidad informática el gobierno tuvo que reflexionar acerca de dónde radicaban las verdaderas dificultades para la aplicación del Derecho penal tradicional a comportamientos dañosos en los que desempeña un papel esencial la introducción del proceso electrónico de datos, así como acerca de qué bienes jurídicos merecedores de protección penal resultaban así lesionados. Fue entonces cuando se comprobó que, por una parte, en la medida en que las instalaciones de tratamiento electrónico de datos son utilizadas para la comisión de hechos delictivos, en especial en el ámbito económico, pueden conferir a éstos una nueva dimensión, pero que en realidad tan sólo constituyen un nuevo modus operandi, que no ofrece problemas para la aplicación de determinados tipos. Por otra parte, sin embargo, la protección fragmentaria de determinados bienes jurídicos ha puesto de relieve que éstos no pueden ser protegidos suficientemente por el Derecho vigente contra nuevas formas de agresión que pasan por la utilización abusiva de instalaciones informáticas. En otro orden de ideas, las diversas formas de aparición de la criminalidad informática propician además, la aparición de

nuevas lesiones de bienes jurídicos merecedoras de pena, en especial en la medida en que el objeto de la acción puedan ser datos almacenados o transmitidos o se trate del daño a sistemas informáticos. El tipo de daños protege cosas corporales contra menoscabos de sus sustancias o función de alteraciones de su forma de aparición.

b) Austria

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

a. Destrucción de datos (126). En este artículo se regulan no sólo los datos personales sino también los no personales y los programas.
b. Estafa informática (148). En este artículo se sanciona a aquellos que con dolo causen un perjuicio patrimonial a un tercero influyendo en el resultado de una elaboración de datos automática a través de la confección del programa, por la introducción, cancelación o alteración de datos o por actuar sobre el curso del procesamiento de datos. Además contempla sanciones para quienes cometen este hecho utilizando su profesión.

c) Francia

a. Ley número 88-19 de 5 de enero de 1988 sobre el fraude informático.
b. Acceso fraudulento a un sistema de elaboración de datos(462-2).- En este artículo se sanciona tanto el acceso al sistema como al que se mantenga en él y aumenta la sanción correspondiente si de ese acceso resulta la supresión o modificación de los datos contenidos en el sistema o resulta la alteración del funcionamiento del sistema.

c. Sabotaje informático (462-3).- En este artículo se sanciona a quien impida o falsee el funcionamiento de un sistema de tratamiento automático de datos.
d. Destrucción de datos (462-4).- En este artículo se sanciona a quien intencionadamente y con menosprecio de los derechos de los demás introduzca datos en un sistema de tratamiento automático de datos o suprima o modifique los datos que este contiene o los modos de tratamiento o de transmisión.
e. Falsificación de documentos informatizados (462-5).- En este artículo se sanciona a quien de cualquier modo falsifique documentos informatizados con intención de causar un perjuicio a otro.
f. Uso de documentos informatizados falsos (462-6) En este artículo se sanciona a quien conscientemente haga uso de documentos falsos haciendo referencia al artículo 462-5.

d) Estados Unidos

Consideramos importante mencionar la adopción en los Estados Unidos en 1994 del Acta Federal de Abuso Computacional (18 U.S.C. Sec.1030) que modificó al Acta de Fraude y Abuso Computacional de 1986. Con la finalidad de eliminar los argumentos hipertécnicos acerca de qué es y que no es un virus, un gusano, un caballo de Toya, etcétera y en que difieren de los virus, la nueva acta proscribe la transmisión de un programa, información, códigos o comandos que causan daños a la computadora, al sistema informáticos, a las redes, información, datos o programas (18 U.S.C.: Sec. 1030 (a) (5) (A). La nueva ley es un adelanto porque está directamente en contra de los actos de transmisión de virus. El Acta de 1994 diferencia el tratamiento a aquellos que de manera temeraria lanzan ataques de virus de aquellos que lo realizan con

la intención de hacer estragos. El acta define dos niveles para el tratamiento de quienes crean virus estableciendo para aquellos que intencionalmente causan un daño por la transmisión de un virus, el castigo de hasta 10 años en prisión federal más una multa y para aquellos que lo transmiten sólo de manera imprudente la sanción fluctúa entre una multa y un año en prisión.

Nos llama la atención que el Acta de 1994 aclara que el creador de un virus no escudarse en el hecho que no conocía que con su actuar iba a causar daño a alguien o que él solo quería enviar un mensaje. En opinión de los legisladores estadounidenses, la nueva ley constituye un acercamiento más responsable al creciente problema de los virus informáticos, específicamente no definiendo a los virus sino describiendo el acto para dar cabida en un futuro a la nueva era de ataques tecnológicos a los sistemas informáticos en cualquier forma en que se realicen. Diferenciando los niveles de delitos, la nueva ley da lugar a que se contemple qué se debe entender como acto delictivo. En el Estado de California, en 1992 se adoptó la Ley de Privacidad en la que se contemplan los delitos informáticos pero en menor grado que los delitos relacionados con la intimidad que constituyen el objetivo principal de esta Ley. Se considera importante destacar las enmiendas realizadas a la Sección 502 del Código Penal relativas a los delitos informáticos en la que, entre otros, se amplían los sujetos susceptibles de verse afectados por estos delitos, la creación de sanciones pecuniarias de $10, 000 por cada persona afectada y hasta $50,000 el acceso imprudente a una base de datos, etcétera.

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

bases de datos y que la protección legal de todos sus tipos y formas es vital para la protección de la intimidad de los individuos así como para el bienestar de las instituciones financieras, de negocios, agencias gubernamentales y otras relacionadas con el estado de California que legalmente utilizan esas computadoras, sistemas y bases de datos. Es importante mencionar que en uno de los apartados de esta ley, se contempla la regulación de los virus (computer contaminant) conceptualizándolos aunque no los limita a un grupo de instrucciones informáticas comúnmente llamados virus o gusanos sino que contempla a otras instrucciones designadas a contaminar otros grupos de programas o bases de datos, modificar, destruir, copiar o transmitir datos o alterar la operación normal de las computadoras, los sistemas o las redes informáticas.

e) Holanda

El 1* de marzo de 1993 entró en vigor la Ley de los Delitos Informáticos, en la cual se penaliza el hancking, el preancking (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), y la distribución de virus.

f) Reino Unido de la Gran Bretaña e Irlanda del Norte

Debido al caso de hancking en 1991, comenzó a regir la Computer Misuse Act, Ley de los abusos informáticos. Mediante esta ley el intento, exitoso o no de alterar datos informáticos es penado con hasta cinco años de prisión o multas. Pena además la modificación de datos sin autorización donde se incluyen los virus.

g) Venezuela

En el año 2001 se promulgó la Ley Especial contra los delitos Informáticos por Asamblea Nacional de la Republica Bolivariana de Venezuela.

De los Delitos Contra los Sistemas que Utilizan Tecnologías de Información, De los Delitos Contra la Propiedad, De los delitos contra la privacidad de las personas y de las comunicaciones, De los delitos contra niños, niñas o adolescentes, De los delitos contra el orden económico, argumentados en cinco capítulos respectivamente. En las disposiciones comunes se abordan elementos importantes como las agravantes, las penas accesorias, la divulgación de la sentencia condenatoria etc entre otros elementos.

Los Estados miembros de la Unión Europea acordaron castigar con penas de uno a tres años de prisión a los responsables de delitos informáticos. Cuando quede comprobado que los ataques cibernéticos están relacionados con el crimen organizado, la pena ascenderá hasta los cinco años. Esta decisión marco se convierte en un gran avance dentro de la armonización de las legislaciones europeas para luchar contra los delitos informáticos. Estos delitos se han convertido en un quebradero de cabeza para los cuerpos de policía de los Estados miembros y, sobre todo, para los perjudicados por estos crímenes. El principio de territorialidad del derecho provoca que sea muy complicado perseguir a delincuentes informáticos que actúan desde otros países. Con este intento de unificar la legislación, las autoridades europeas podrán perseguir con una mayor efectividad a delincuentes que, hasta ahora, podían cometer sus delitos con casi total impunidad. Además, el acuerdo del Consejo de Ministros de Justicia de los Quince establece otro aspecto importante, como es la definición de los delitos que se consideran "informáticos". Los Estados miembros distinguen tres tipos de ataques cibernéticos: el acceso ilegal a sistemas informáticos, la ocupación de sistemas a través de ejemplos como el envío de mensajes que ocupan un

espacio considerable, y la difusión de virus informáticos. La intención de la Unión Europea es doble: por un lado se trata de definir el delito; por otro pretende unificar las penas, ya que el lugar de la comisión del delito es fundamental para saber el derecho aplicable, se trata además de una medida muy sensata que evita la desprotección absoluta que presentan hoy en día las empresas del Viejo Continente. Los Quince Estados Europeos disponen ahora de un plazo de más de dos años para la adaptación de esta medida a sus textos legislativos.

ANEXO E

Cincuenta delitos informáticos están sin resolver por falta de peritos en esa materia

Domingo 7 de diciembre de 2008, por Guido Rosales Uriona - GRU

Entre enero y septiembre de este año, la Fuerza Especial de Lucha Contra el Crimen (FELCC) recibió al menos 50 denuncias de delitos informáticos en el país, de las que sólo 36 están siendo investigadas, pero ninguna fue resuelta, por su complejidad y porque sólo hay dos peritos para atender ese tipo de casos. A ello se suma la falta de fiscales especializados en esa materia para conducir las indagaciones.

Entre 2003 y 2007, la fuerza anticrimen recibió 185 denuncias de manipulación informática y de alteración, acceso y uso indebido de datos en toda Bolivia, pero se desconoce si alguna de ellas fue resuelta.

Esos dos tipos de delitos están definidos en el Código Penal. La manipulación informática se refiere a modificar o borrar información en discos duros de computadoras para que una persona se beneficie económicamente; la alteración, acceso y uso indebido de datos tienen que ver con que alguien que se apodera, utiliza, altera o inutiliza datos almacenados en una computadora o en cualquier soporte informático.

El jefe de la División de Delitos Informáticos de la FELCC de La Paz, capitán Edson Claure, informó que en los primeros nueve meses de esta gestión se registraron en todo el país 50 denuncias de manipulación informática, pero ninguno de alteración, acceso y uso indebido de datos.

Sin embargo, la Dirección Nacional de Laboratorio de la Policía, que investiga esos casos, sólo da cuenta de 36 procesos que están en etapa de investigación, pero de éstos ninguno fue resuelto. Ni esta última entidad ni la División de Delitos

Informáticos saben por qué sólo 36 de las 50 denuncias recibidas están siendo indagadas.

En el caso de La Paz, 12 casos están en proceso de investigación y en tres de ellos hay importantes avances. De estos últimos, dos se refieren a páginas de pornografía infantil y por los cuales dos personas están en la cárcel a la espera de una sentencia, y uno sobre la "clonación" de una tarjeta de crédito. El resto están referidas a estafas electrónicas.

El capitán Claure aclaró que estos delitos no sólo son investigados por su división, sino que en el esclarecimiento coadyuvan la repartición de Delitos Económicos y Financieros y la de Trata y Tráfico de Personas.

En el delito de alteración, acceso y uso indebido, el autor ingresa sin autorización en bases de datos o programas informáticos mediante internet o dispositivos como CD-ROM, memorias USB o disquets para hurtar, modificar o bloquear la información.

El capitán Claure indicó que la investigación de este tipo de hechos es complicada porque los autores, los conocidos crackers (acceden a información para cometer estafas económicas) o hackers (que se dedican al robo o manipulación de datos), por lo general operan desde otros países, aunque también los hay en Bolivia, y operan desde direcciones que incluso son ajenas.

Procedimiento

Las divisiones Económicas y de Trata son las primeras en recibir las denuncias de las víctimas o instituciones afectadas por ciberdelincuentes. Estas oficinas coordinan con los investigadores de la División de Delitos Informáticos, y ésta, a su vez, con los peritos en informática forense dependientes de la Dirección Nacional de Laboratorio de la Policía.

Todos ellos investigan juntos, pero dirigidos por un fiscal.

Empero, el capitán Claure informó que el Ministerio Público no tiene fiscales especializados en la investigación de delitos informáticos, es ésa una de las razones por las que sus casos deben ser adecuados a delitos económicos.

Un efectivo de la División de casos económicos de la FELCC de La Paz reveló que no se esclareció ningún caso "por la carencia de material de trabajo, equipos, personal y peritos". En La Paz, la oficina de delitos informáticos, tiene un jefe de división y un investigador, ambos capacitados en esa rama.

El director nacional de Laboratorio de la FELCC, coronel Jorge Toro, admitió que estos delitos no se esclarecen porque para Bolivia sólo hay dos peritos en esa especialidad.

"Para el trabajo que nos dejan a nivel nacional no abastece (el personal), ya que el IDIF (Instituto de Investigaciones Forenses) no tiene este tipo de peritos".

Estos dos expertos estudiaron informática forense en Chile y trabajan en la Policía hace tres años. Para ellos, la "escena del crimen" es la computadora, el disco duro.

El ingeniero Ronald Rodríguez, uno de los peritos, informó que, de todos los casos que investiga, uno irá a juicio oral en los próximos días en La Paz. "Se trata de una falsificación de documentación en una computadora Macintosh en la que fraguaron cédulas de identidad, formularios notariales y otros documentos públicos, utilizados para ilícitos".

El capitán Claure también consideró que una de las causas por las que no se esclarecen los casos informáticos reside en que los interesados abandonan el proceso, tal como suele ocurrir con los delitos comunes.

Rodríguez comentó que uno de los casos que analiza es el del narcotraficante Mauro Vásquez, a quien se le encontraron imágenes de pornografía infantil en la computadora de su casa en el momento de ser detenido en la ciudad de Cobija, a principios de este año.

El ex jefe de la División de Delitos Económicos Financieros de la fuerza anticrimen del departamento de La Paz coronel Luis Fernando Remontt tampoco conoció de investigaciones concluidas, pero indicó que en su gestión, entre 2007 y parte de 2008, al menos tres hombres fueron enviados a la cárcel por retener tarjetas de crédito ajenas en cajeros automáticos.

El director nacional de la FELCC, coronel Fernando Figueredo, explicó que en 2009 se incrementará el número de investigadores en las divisiones de Delitos Informáticos del país, puesto que cada año sube el índice de este tipo de hechos. Para ello, con la ayuda de la GTZ (Cooperación Técnica Alemana) se capacitará a policías para que resuelvan estas denuncias en las oficinas de la fuerza anticrimen.

El Instituto de Investigaciones Forenses (IDIF), que trabaja de la mano con la FELCC en el análisis de pruebas de distintos delitos comunes, a la fecha no tiene expertos para la examinación de delitos informáticos.

El director nacional de esta entidad, Antonio Torres Balanza, dijo que para 2009 se contratará a especialistas en esa rama por la demanda de investigación.

El Código de Procedimiento Penal establece que el IDIF es el órgano de investigación científica; pero desde 2003, cuando la Policía empezó a investigar delitos informáticos, la Dirección Nacional de Laboratorio se hizo cargo del trabajo que le corresponde a ese instituto forense.

Estadísticas

Los datos de la Fuerza Especial de Lucha Contra el Crimen (FELCC) revelan que en Santa Cruz, La Paz y Cochabamba se producen más delitos informáticos desde 2003.

Desde ese año hasta 2007, la Policía registró un total de 185 fraudes electrónicos en todo el país, de éstos, 177 corresponden a manipulación informática y ocho a alteración, acceso y uso indebido de información. De la primera figura legal, 91 casos hubo en Santa Cruz, 46 en Cochabamba, 30 en La Paz, cuatro en Potosí, tres en Oruro, dos en Beni y uno en Tarija.

Sobre alteración informática, tres ocurrieron en La Paz, dos en Cochabamba, dos en Beni y uno en Santa Cruz. Entre enero y septiembre de este año hubo 50 denuncias de manipulación electrónica (27 en Santa Cruz, 12 en La Paz, nueve en Cochabamba y dos en Chuquisaca) y ninguna acerca de alteración.

La legislación queda atrás

Hace un año y medio fue presentado un proyecto de ley en el Parlamento para endurecer las sanciones a delincuentes informáticos y ampliar la legislación a nuevos delitos de esta naturaleza.

El capítulo 11 del Código Penal boliviano, en su artículo 363, tipifica dos tipos de delitos informáticos: uno sobre manipulación informática cuyo fin es obtener un beneficio económico, sancionado con reclusión de uno a cinco años y con multa de 60 a 200 días, y un delito de alteración y uso indebido de datos informáticos cuyo propósito es el apoderamiento o modificación de una base de datos en una computadora o un dispositivo informático (CD-ROM, USB, disquet y otros), que será sancionado con prestación de trabajo hasta un año o multa de hasta 200 días.

La Agencia Boliviana Para el Desarrollo de la Información elaboró un proyecto de ley que plantea cambiar estos dos tipos penales e incrementar la sanción penal e implementar nuevas figuras delictivas. Además, plantea que se incorporen la transgresión de sabotaje informático y la de falsificación y suplantación de identidad electrónica, delitos que ya figuran en legislaciones de otros países.

El Código Penal incorporó estas dos figuras hace diez años, pero entonces el desarrollo de la tecnología de la información no estaba en el nivel actual. El jefe de la División de Delitos Informáticos de la fuerza anticrimen de La Paz, capitán Edson Claure, explicó que "los delitos quedaron obsoletos en relación con la evolución agigantada de la informática y la tecnología".

Existe un proyecto de Ley de Delitos Informáticos que es analizado en la Cámara de Diputados y que fue presentado en septiembre de 2006. Tiene la finalidad de proteger de manera integral a quienes utilicen tecnologías de información; prevenir la comisión de los delitos contra ellas; sancionar la penalidad de los delitos que se cometieren contra estos sistemas o cualesquiera de sus componentes, o los que fueren cometidos por medio de tecnologías. En ese documento se define el fraude informático.

Casos detectados en Bolivia, Phishing

Los autores, quienes incluso operan desde otros países ingresan a la página web de alguna entidad financiera en la que escogen a su víctima; la contactan mediante su correo electrónico y le envían un portal falso del banco y bajo pretexto de que la institución está en un proceso de actualización le piden sus datos y el PIN.

Clonación de tarjetas

La víctima es afectada desde que asiste a un local o un centro comercial donde entrega su tarjeta de crédito para pagar sus compras o consumo, y el delincuente duplica su tarjera en un escáner sofisticado y se dan modos para seguirla y averiguar su clave, con la que después vacían su cuenta.

Sabotaje informático

Esta modalidad de fraude sucede cuando alguna persona, que puede ser ingeniero en sistemas, informático o conocedor de la internet, de forma maliciosa obstaculiza, modifica o comete culaquier otra acción que atente contra el normal funcionamiento de un sistema de información personal o de una institución.

Falsedad y amenazas

La falsificación y suplantación de identidad electrónica todavía no está en la legislación boliviana, pero consiste en que cierta persona averigua la contraseña de un correo electrónico ajeno y una vez que consigue ingresar modifica el contenido de cartas o documentos, o envía mensajes con diferentes fines a destinatarios.

Fuente: La Prensa: 07/02/2008

ANEXO F

Bolivia penalizará delitos informáticos y digitales

Comisión legislativa aprobó en grande el proyecto de ley de telecomunicaciones

La Comisión de Planificación, Política Económica y Finanzas de la Cámara de Diputados aprobó ayer, en su estación en grande, el proyecto de Ley de Telecomunicaciones, Tecnologías de Información y Comunicación, que entre otras cosas penaliza el delito informático digital en el país.

Si bien en la actualidad el Código Penal incorpora en el Título X un capítulo destinado a los delitos informáticos, no incluye la descripción de las conductas delictivas en ese orden, lo que debilita la lucha contra estos ilícitos.

Por ello, el proyecto de Ley de Telecomunicaciones plantea la modificación de los artículos 179 bis, 363 bis, 363 ter, 198, 199, 200, 300 y 301 del Código Penal. Las reformas apuntan a vigorizar las penas contra la manipulación informática, la alternación, acceso y uso indebido de datos informáticos y proteger la propiedad intelectual de las obras con soporte electrónico en la web.

Amplía a los delitos de falsedad material, falsedad ideológica y falsificación de documentos privados que sólo se refieren a instrumentos impresos en el sistema digital.

Además se sanciona la violación de la correspondencia electrónica privada y la falsificación y suplantación de identidad en la web, que en la actualidad no están tipificadas por la normativa vigente.

Asimismo, el proyecto incluye sanciones privativas que van de tres a seis años a quien cometa sabotaje informático e impida el normal funcionamiento del sistema de información o telecomunicaciones.

DETALLE

En el caso referido a la falsedad ideológica, el proyecto precisa que quien inserte declaraciones falsas en un instrumento público verdadero, será sancionado con privación de libertad de uno a seis años.
Pero la pena se agrava de dos a ocho años de privación de libertad si la persona que cometiere este hecho fuera un funcionario público.

Con relación a la falsificación y suplantación de identidad electrónica en el sistema digital, el proyecto de ley plantea una reclusión de uno a seis años para la persona que incurra en este delito.
La sanción se aplicará en el caso de que una persona altere un mensaje de datos utilizando una identificación física o digital que no le pertenezca y para quien interfiera o altere el proceso de transmisión del mensaje entre los titulares de origen y de destino.
Además se sanciona el delito contra las telecomunicaciones con una pena privativa de cinco años. En este escenario se sanciona a quienes tengan conexiones clandestinas de red, a quien desvíe el tráfico de larga distancia establecido por los operadores y a quien genere tráfico internacional en sentido inverso al normal.
El presidente de la Comisión de Planificación, Política Económica y Finanzas, Marcelo Elío, indicó que una vez aprobada la norma se pondrá en vigencia el

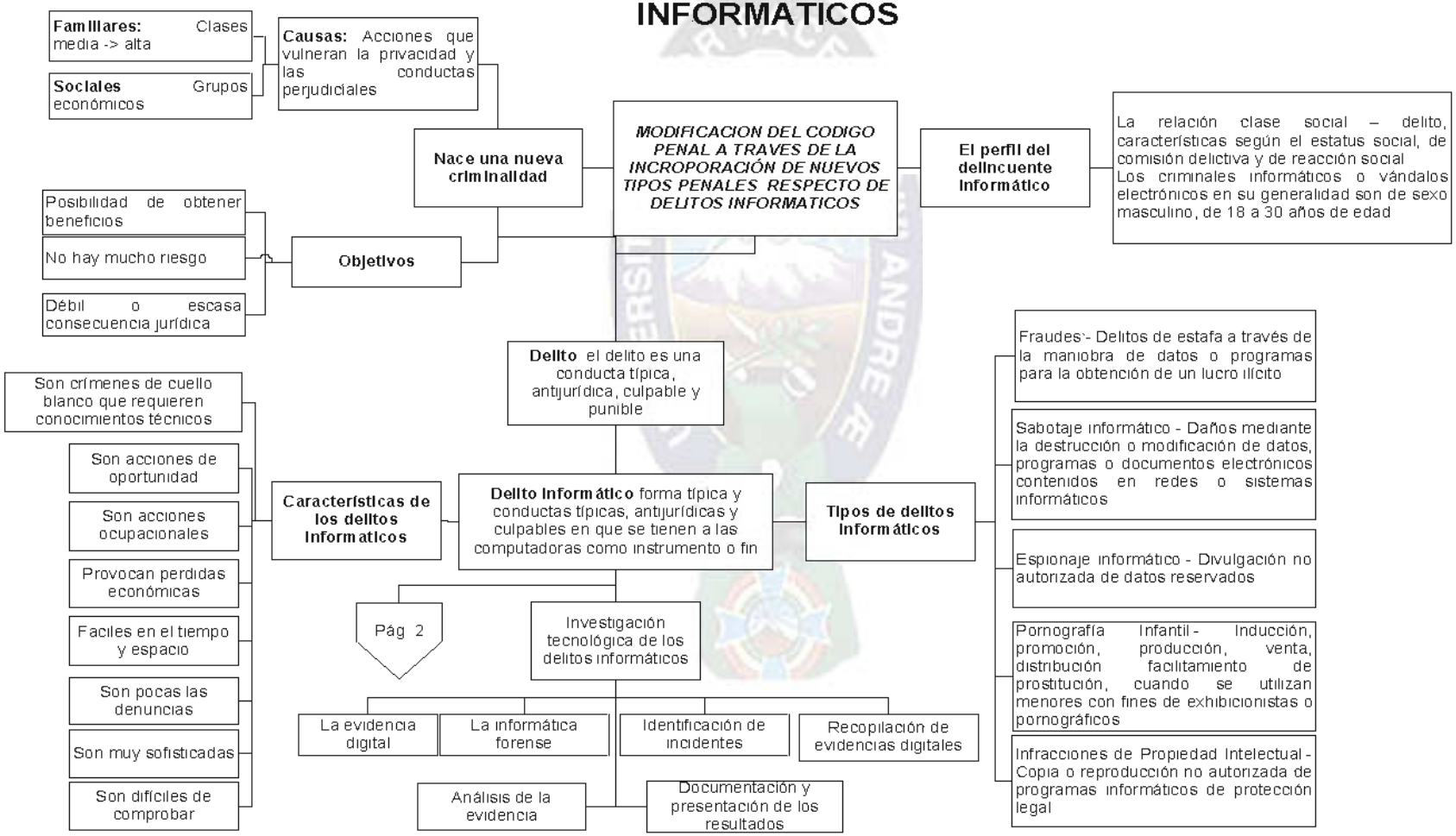
documento electrónico y la firma electrónica, lo que permitirá a Bolivia estar a un paso de la emisión de documentos mediante tecnología electrónica, como Internet o las telecomunicaciones digitales, reportó la Cámara de Diputados.

La Comisión parlamentaria aprobó ayer el proyecto en su estación en grande y el legislador anunció la apertura de un ciclo de audiencias públicas para enriquecer los contenidos de la ley.

FUENTE: periódico cambio, periódico del estado plurinacional boliviano

Anexo G

MODIFICACION DEL CODIGO PENAL A TRAVES DE LA INCORPORACIÓN DE NUEVOS TIPOS PENALES RESPECTO DE DELITOS INFORMATICOS



MODIFICACION DEL CODIGO PENAL A TRAVES DE LA INCORPORACIÓN DE NUEVOS TIPOS PENALES RESPECTO DE DELITOS INFORMATICOS