# UNIVERSIDAD MAYOR DE SAN ANDRÉS

# FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS

# CARRERA DE DERECHO

ACREDITADA POR RESOLUCIÓN
CEUB Nº 1126/02

## MONOGRAFÍA

***Fundamentos jurídicos para la creación del departamento de la policía informática dentro de la estructura de la fuerza especial de lucha contra el crimen***


POSTULANTE:

Alan Joseph Morales Valdez
TUTOR ACADÉMICO:
Dr. Claribel Patricia Ramírez Hurtado



LA PAZ – BOLIVIA
2009

# DEDICATORIA

A DIOS TODOPODEROSO, por haberme guiado al camino del éxito y superación, con perseverancia, sapiensa, fuerza, coraje y valentía para poder afrontar los retos en los distintos ámbitos de la vida.

A mis ejemplares padres: Reynaldo Pairumani y Lilian Valdez, quienes fueron mis primeros maestros y seguirán siendo.

A los entrañables padres de mi progenitora, mi querida mama Goyita Magne de Valdez y Ernesto Valdez Luna, quienes son el regalo de Dios, que ilumina mi vida desde los primeros años de mi existencia.

A mis tíos: David, Rolando, William y Delia Valdez y en general a toda mi familia.

**Alan Joseph Morales Valdez**

# AGRADECIMIENTOS

A la Casa de Estudios Superiores, Universidad Mayor de San Andrés, por habernos brindado la excelencia Académica, capaces de responder a las necesidades de la sociedad y tener competitividad Profesional.

Muchas Gracias por ser la institución que nos ha formado profesionalmente durante los años que nos toco desempeñar como estudiantes.

A mi tutora la Dra. Claribel Ramírez, que en momentos difíciles me brindo su tiempo y conocimientos de manera desinteresada, y me impulso para llegar al epilogo del presente trabajo.

Al Dr. Edmundo López, Juez de Instrucción de civil y familia, quien me inculco la ética profesional de la misión que están encomendados a todos los que ejercen tan noble profesión como es la abogacía.

Al Dr. Juan Morales Mayta, Fiscal adscrito a la provincia Loayza, quien vio en mi una persona que tenia aquella capacidad de resolver problemas y por ello agradecerle infinitamente puesto que sus palabras las llevare en el corazón a través del tiempo.

Al Dr. Rafael Alcón, Juez de instructor Penal Cautelar, quien con humildad y su capacidad me dieron mis primeras herramientas practicas para el ejercicio de la profesión.

Al Gobierno Municipal de Luribay, quien a través del Consultorio Jurídico Popular de la U.M.S.A. me dio la oportunidad de poder ayudar en lo que humildemente me habían impartido en mi casa de estudios, y dárselo a la población de la manera mas solidaria y con el más alto nivel de responsabilidad.

A la Población de Luribay que en su conjunto me recibió con los brazos extendidos, haciéndome sentir, como en mi propio hogar.

Y finalmente a mi tía la Prof. Deysi Choque, quien me ha colaborado en la corrección del presente trabajo, con paciencia y esmero.

**Alan Joseph Morales Valdez**

# PRÓLOGO

El Postulante Alan Joseph Morales Valdez, quien ha egresado de la Facultad de Derecho y Ciencias Políticas, en la Carrera de Derecho, me ha invitado para que haga el prologo de su monografía titulada: "**FUNDAMENTOS JURÍDICOS PARA LA CREACIÓN DEL DEPARTAMENTO DE LA POLICÍA INFORMÁTICA EN LA ESTRUCTURA DE LA FUERZA ESPECIAL DE LUCHA CONTRA EL CRIMEN"**, que constituye un aporte en innovación. Tomando en cuenta que en la actualidad existe un incremento en el índice de los delitos informáticos que se dan en el contexto boliviano durante los últimos años.

El trabajo responde a una necesidad social, en específico al avance tecnológico y como puede utilizarse en la comisión de delitos.

Comienza desde aspectos de orden histórico y doctrinal que involucran ala Institución Policial boliviana y respectivamente al derecho informático. Para luego adentrarse en lo concerniente a los Delitos informáticos, realizando una descripción de manera general y llegando a una delineación concreta en el ámbito de la realidad nacional de la presencia de los delitos informáticos en Bolivia, así como ser: los más frecuentes, y el tratamiento que reciben actualmente.

Realizando un Diagnostico de lo que se quiere enfocar, el problema de eficiencia y culminando con la propuesta a un nivel administrativo con el Departamento Informático y jurídico con la propuesta de reglamento para su funcionamiento.

La propuesta de la incursión de un departamento informático policial, encargado del tratamiento para la recepción de delitos informáticos para su investigación, es importante, puesto que estos tipos penales van en

incremento en la sociedad boliviana, y la Fuerza Policial tiene que estar a la par de la tecnología, tanto para su prevención como para el tratamiento, que contiene características particulares que deben considerarse, para poder obtener resultados concretos.

De esta manera se pone a consideración, una determinada sistematización, presentando una organización que parte de un Departamento Central, del cual se desprende sub departamentos y estos en secciones, de manera que no exista confusión en la remisión de casos y puedan ser derivados conforme especialización.

A ello mencionar el proyecto de reglamento que contiene la suma para que jurídicamente pueda ser ejecutable, conteniendo los elementos básicos como ser: objeto, funciones y estructura.

Para concluir agradecer la invitación por la deferencia para prologar el presente trabajo, deseándole éxitos en su formación profesional, al postulante.

# INTRODUCCIÓN

Con el devenir del tiempo, se presentan nuevas figuras delictivas que amenazan a la sociedad, por ello es imperiosa la necesidad del Derecho regular para que exista control sobre determinadas conductas, que van apareciendo.

En la monografía que a continuación se presenta, involucra a la tecnología como potencial para la consumación de delitos, proponiendo la creación del departamento de la Policía Informática dentro de la estructura de la Fuerza Especial de Lucha Contra el Crimen, para que de manera sistémica se enfrente los delitos informáticos, que no están exentos de la realidad nacional.

Sobre la base de esta institución se propone un reglamento que se encontrará inserto en la organización administrativa de la F.E.L.C.C. que como primera fuerza contra el crimen esta llamada a enfrentarse a los nuevos retos y medios que utiliza el delincuente cibernético.

Para llegar a esta misión tendremos que:

- Identificar las características de un delincuente informático.

- Determinar que son los delitos informáticos en el ordenamiento legal boliviano.

- Identificar la importancia de esta repartición en la estructura de la FELCC,

- Determinar la existencia de información actualizada sobre la comisión de delitos informáticos en Bolivia.

- Identificar los delitos informáticos más frecuentes en Bolivia y determinar la repuesta de la Policía Nacional ante los delitos informáticos.

Y de esta forma culminando en un diagnostico, que nos de cuenta si en la actualidad se da la Eficiencia en la asunción de la respuesta ante estos casos.

El Panorama es complejo por que trasciende el radio nacional convirtiéndose incluso en un problema de orden internacional, en un mundo que se encuentra cada vez más globalizado debido entre otras a la comunicación por medios tecnológicos.

Al final tendremos que hacer un análisis conclusivo donde se dará de cuenta que el modo de operación en la consumación delictiva, varia puesto que ahora en los tiempos en que vivimos bastará un celular, un ordenador y ya no así armas letales como pistolas, para su consumación, tomando en cuenta que ahora es la era de la Revolución Informática y con ella la Información como el bien jurídico de mayor relevancia.

**Alan Joseph Morales Valdez**

# Í N D I C E



## CAPÍTULO I: DIAGNÓSTICO HISTÓRICO - TEÓRICO DE DERECHO INFORMÁTICO Y LA POLICÍA NACIONAL

## CAPÍTULO II: ELEMENTOS CONCEPTUALES APLICADOS EN EL TRABAJO



## CAPÍTULO III: MARCO JURÍDICO POSITIVO VIGENTE Y APLICABLE

## CAPÍTULO IV: DE LOS DELITOS INFORMÁTICOS

## CAPÍTULO V: DE LA POLICÍA INFORMÁTICA

**CAPITULO VI: PROYECTO DE REGLAMENTO DE LA POLICÍA INFORMÁTICA DENTRO DE LA LEY ORGÁNICA DE LA POLICÍA**

# ÍNDICE
# DE CUADROS

# CAPÍTULO I

# DIAGNÓSTICO HISTÓRICO - TEÓRICO DE DERECHO INFORMÁTICO Y LA POLICÍA NACIONAL

## 1.1 MARCO HISTÓRICO DE LA INFORMÁTICA

La informática, en el concepto amplio del término, proviene de la conjunción de las palabras información y automática. Como ciencia, procede de una serie de estudios aplicados acerca de la nueva tecnología en la innovación de máquinas al servicio del hombre, desde la utilización de pequeñas piedras para calcular, por medio de unas ranuras efectuadas en el suelo usadas para contar. A partir de este sencillo elemento de cálculo fueron apareciendo en diversos lugares otros similares, como el denominado comúnmente ábaco. “El más antiguo se remonta aproximadamente al año 3500 a.C. en el valle que se encuentra entre el Tigris y el Éufrates. En los años 2600 A.C. apareció el ábaco chino, que evolucionó rápidamente y se denominó Suan-Pan, otro elemento apareció en Japón el Soroban”. El ábaco constituyó el primer dispositivo manual de cálculo, servía para representar números en el sistema decimal y realizar operaciones con ellos, consta de un marco de madera dividido en dos partes; además lleva una varilla vertical por cada dígito, en la que en su parte inferior contiene cinco discos situados en reposo hacia abajo, y en su parte superior dos disco que en reposo están hacia arriba. Cada unidad correspondiente a uno de sus dígitos hacia mover un disco de su parte inferior hacia arriba, cuando los cinco estaban hacia arriba, estos se bajaban haciendo esta misma operación con uno de sus discos de la parte superior, si los dos discos de la parte superior estaban hacia

abajo, se subían, añadiendo una unidad en la varilla que estaba situada en la siguiente posición a la izquierda. Con este dispositivo se podía contar dependiendo del número de varillas[1]. No queriendo abarcar en exceso el punto, se presenta el siguiente resumen esquemático de la evolución informática:

| Año/Periodo | Acontecimiento |
|---|---|
| 3500 a.C. | Se inventa el ábaco (en Babilonia), primera máquina para realizar cálculos. |
| 1617 | Jhon Napier inventa sus varillas de numeración (o huesos de Napier). |
| 1621 | Invención de la regla de cálculo. |
| 1624 | Wilhelm Schickard construye la primera calculadora mecánica. |
| 1639 | Blasie Pascal inventa y fabrica una sumadora mecánica llamada la Pascalina. |
| 1673 | Gottfried Whilhelm diseña y construye una máquina mecánica para realizar cálculos aritméticos. |
| 1800 | Tarjetas perforadas de Jacquard. |
| 1854 | George Boole desarrolla el algebra que lleva su nombre: algebra booleana. |
| 1885 | Herman Hollerith construye la máquina cansadora o tabuladora, que por medio de tarjetas perforadas reducía el tiempo al realizar el censo. |
| 1894 | Leonardo Toorez Quevedo presenta máquina algebraica. |
| 1938 | Konrad Zuse construye la primera de sus computadoras: la Z1. |
| 1939 | George R. Stibitz empieza el desarrollo de la Complex |

[1] http://orio.eui.upm.es/historia_informática/ddoc/principal.htm

| | |
|---|---|
| | Calculator. |
| 1940 | Tesis de Claude Shannon sobre la teoría matemática de la comunicación. |
| 1941 | Primera computadora funcional del mundo controlada por programas la Z3 de Zuse. |
| 1942 | Atanasoff desarrolla el ABC, máquina electrónica digital para la resolución de sistemas lineales. |
| 1943 | Un equipo dirigido por Alan Turing construye el Colossus para descifrar los mensajes de Enigma. |
| 1943 | Se empieza la construcción del EINAC, por Jhon Mauchly y Jhon Eckert. |
| 1944 | Howard Hathaway Aiken termina la construcción de la Harvard Mark. |
| 1945 | Primer “bug” informático. |
| 1946 | Nace una de las primeras computadoras no diseñadas con un propósito militar: la UNIVAC. |
| 1947 | Nace la cibernética, vocablo designado por Norberto Wiener, uno de sus padres. |
| 1948 | Nace el proyecto del Manchester Mark I en donde Alan Turing, participó activamente. |
| 1949 | La compañía Mauchly y Erkert construye una pequeña computadora: la BINAC. |
| 1952 | John Von Neumann hace realidad su sueño: se pone en marcha el EDVAC. |
| 1952 | Empieza la fabricación industrial y comercialización de ordenadores. |

| | |
|---|---|
| 1956 | Conferencia de Darthmouth, en donde nace la inteligencia artificial. |
| 1960 | Nace el primer lenguaje de programación de inteligencia artificial: el LISP. |
| 1964 | IBM empieza a comercializar los 360. |
| 1968 | Robert Noyce y Gorden Moore fundan Intel Corporation. |
| 1969 | Kenneth Thompson y Dennis Ritchie crean el sistema operativo Unix, en los laboratorios AT&T. |
| 1971 | IBM crea el disquete de 8 pulgadas. |
| 1972 | Aparecen los disquetes de 5.25 pulgadas. |
| 1975 | Seymour Cray considera que el software podría ser más potente en ordenadores mono procesadores por medio del procesamiento en paralelo. Nace así el CRAY 1. |
| 1976 | Se comercializan el Altair 8800, considerado el primer ordenador personal. |
| 1977 | Bill Gates y Paul Allen fundan Microsoft. |
| 1981 | Steve Jobs y Steve Wozniac fundan la Apple Computer, Inc. |
| 1981 | Se comercializa el IBM PC. |
| 1981 | Microsoft presenta el sistema operativo MS-DOS (Microsoft Disk Operating System). |
| 1982 | Sony crea disquetes de 3.5 pulgadas. |
| 1984 | Aparece el primer clónico del IBM PC. |
| 1985 | Sony y Philips crean CD-Rom para los ordenadores. |
| 1988 | Microsoft anuncia Windows 1.0. |
| 1989 | W.H. Sim funda Creative Labs. |
| 1994 | Shor describe un algoritmo cuántico que permitirá factorizar enteros en tiempo poli nominal. |
| 1995 | Se supera el teraflop en computación en paralelo. |

## 1.2 MARCO HISTÓRICO DE LA POLICÍA NACIONAL

### 1.2.1 EL MARISCAL SUCRE, FUNDADOR DE LA INSTITUCIÓN

El Mariscal de Ayacucho, don Antonio José de Sucre, nació en la ciudad de Cumaná (Nueva Granada), el 3 de febrero de 1795. Fueron sus progenitores don Vicente Sucre y doña María de Alcalá. Cuando nuestro héroe aún se encontraba en el período de la niñez, fallecieron sus padres, uno después de otro, a causa de una epidemia que se produjo en aquella región.

Anoticiados Bolívar y Sucre de las diferentes opiniones que se estaban debatiendo en el Alto Perú, dispusieron que se organizara una Asamblea de hombres notables, para determinar cuál sería la decisión de la opinión pública. Efectuada dicha Asamblea, en la sesión del 6 de agosto de 1825, presidida por don José Mariano Serrano, se determinó por mayoría absoluta crear un nuevo Estado Americano, al que se le puso del nombre de República de Bolívar, denominación que fue cambiada por la de REPUBLICA DE BOLIVIA. Cuando su Primer Presidente, el Libertador Bolívar, se ausentó, transfirió sus poderes al vencedor de Ayacucho Antonio José de Sucre.

Durante su Gobierno, el Presidente Sucre demostró entera generosidad, desinterés y nobleza. Acogía con gran bondad a cuantos solían pedirle favores que no contraríen al derecho y al buen gobierno de la República; prefería controvertir con algunos solicitantes de favores, imponiéndose por la persuasión, el derecho, la justicia y el respeto que debía tenerse para las autoridades. Por eso se dedicó con verdadero ahínco a la organización y mejora del país y en este empeño nos toca hacer resaltar la organización de la primera Policía de la República, constituyéndose en el creador de esta Institución del orden y de la seguridad nacional.

Las medidas que pensaba ejecutar para hacer un buen gobierno, las meditaba mucho y en más de una ocasión las consultaba con hombres de saber, prefiriendo escuchar los consejos sanos que permitan el progreso de la república. Quizó declinar su mandato, pero el Congreso Nacional le pidió por unanimidad que siguiera gobernando, a lo que accedió sólo por un tiempo limitado, porque había advertido que había disparidad de criterios y descontento que se materializó en el motín militar del 18 de abril de 1828, en el que estuvieron a punto de victimario hiriéndole un brazo con un disparo.

El 1° de agosto de 1828, abandonó el Gobierno para dirigirse al Ecuador y entregó al Congreso Nacional su último mensaje a la Nación, que todos los bolivianos debemos recordar siempre con unción patriótica porque constituye un mandato histórico al manifestar: *"AÚN PEDIRÉ OTRO PREMIO A LA NACIÓN: EL DE NO DESTRUIR LA OBRA DE MI CREACIÓN; DE CONSERVAR POR ENTRE TODOS LOS PELIGROS LA INDEPENDÉNCIA DE BOLIVIA"*

### 1.2.3 SUCRE EN LA ORGANIZACIÓN DE LA REPÚBLICA

Sucre, con criterio sereno y de estadista, inicia la división política del territorio en departamentos, provincias, cantones y parroquias; señalándoles a cada uno, autoridades político-administrativas, a las que les estaba prohibido todo conocimiento judicial. De esta manera, los departamentos estarían mandados por un jefe civil con el nombre de Prefecto; las provincias, por el Gobernador; los cantones, por el Corregidor y, si en un Cantón hubieran dos parroquias, en cada una de ellas se nombrarían Alcaldes. Los Prefectos y Gobernadores, como Agentes de Gobierno, eran sólo funcionarios del poder civil y político, y la sujeción de su jerarquía era la de Prefecto a Gobierno, Gobernador a Prefecto, Corregidor a Gobernador y Alcalde a Corregidor; los dos primeros nombrados por los cantones mismos y los Alcaldes por su pueblo. Tales son la división

política y las autoridades que se asignaban a sus partes constitutivas en conformidad con el D.S. del 23 de enero de 1826.

Complementa este decreto, la orden suprema por la cual los Gobernadores debían velar por que las postas no experimenten retrasos; que las autoridades no falten a sus pueblos, y que sus cortas ausencias sean suplidas por encargados que dejen para resolver las cosas que pudieran ocurrir.

Esta parte de la administración de Sucre nos muestra sin lugar a dudas, que el Gran Mariscal de Ayacucho fue el indiscutible fundador de la República, sin que esto signifique desconocer que el Libertador fue el artífice de su independencia, el Padre de la Patria. La tarea de organizar un nuevo Estado y darle una legislación que defina las características de la República, fue ardua para Sucre, si se tiene presente que entre sus problemas estaba el de velar por la conservación del orden público y de las garantías de la ciudadanía, donde el peso de un ejército desproporcionado requería de un sistema especial de tratamiento a la intervención de estas fuerzas en su relación con el común de los pobladores a quiénes había que sustraer de su dominio y apartar de la influencia de los políticos. Entre estas medidas, se cuenta la de establecer una Policía que garantice la convivencia de esa sociedad.

### 1.2.4 RATIFICACIÓN CONSTITUCIONAL

La Constitución Política del Estado de 6 de noviembre de 1826, sancionada por el Congreso Constituyente, ratificó las medidas administrativas y políticas que había adoptado Sucre, determinando que en el régimen interior de la República, el Gobierno Superior Político Departamental residía en un Prefecto, el provincial en el Gobernador, el de los cantones en el Corregidor, y que en los pueblos cuyo número de habitantes lo exija, por cada mil haya un Juez de Paz.

A todos ellos les estaba prohibido el conocimiento judicial; pero, si la tranquilidad pública exigía la aprehensión de algún individuo, éste debía ser puesto a disposición del juez respectivo en el término de 48 horas.

El General Manuel Isidoro Belzu, asumió la Presidencia de la República el 15 de agosto de 1850, habiendo aprobado la Convención Nacional, el 20 de septiembre de 1851, la nueva Constitución Política del Estado. En el capítulo correspondiente de dicha Constitución se determina al tratar del Régimen Interior de la República que en los Departamentos, Provincias y Cantones, habría autoridades encargadas de hacer cumplir las Leyes y los Reglamentos inherentes a las funciones policiales así como que los nombramientos y duración de las mismas se determinarían por el Supremo Gobierno.

Esa Constitución del Estado suprimió los Concejos y los Juntas Municipales, las cuales habían acaparado la mayor parte de las funciones policiales. En consecuencia, el Gobierno expidió el Decreto Supremo de 22 de noviembre de 1851, determinando que los Comisarios Mayores de Policía ejerzan las funciones que los reglamentos pertinentes señalaban para los Intendentes de Policía.

### 1.2.5 LA POLICÍA ADQUIERE CARÁCTER NACIONAL 1910 –1964

Hasta aquí la Policía de Seguridad había funcionado con carácter departamental, bajo el mando directo de los Intendentes de Policía y la supervisión de los Prefectos y Comandantes Generales de los Departamentos respectivos. La Ley Reglamentaria de Policías de 11 de noviembre de 1886 dio con sus preceptos el concepto de una Institución que debía ejercer su potestad de conservar el orden público, en resguardo de las garantías personales y reales, previniendo los delitos y faltas con carácter de uniformidad para toda la República.

### 1.2.6 CREACIÓN DE LA ESCUELA DE POLICÍAS

Durante el período Presidencial del Dr. Bautista Saavedra, mediante Decreto Supremo de 20 de diciembre de 1923, se dispuso la creación de una Escuela de Policías, de manera que pudiera funcionar en cada ciudad, con destino a la instrucción y educación de alumnos, para el servicio de los Policías de la República.

Sostenía el Decreto que era de necesidad impostergable dar una base técnica y profesional a los funcionarios de Policía, para que puedan desenvolverse en su noble misión con eficacia, dentro del grado cultural que había alcanzado la República.

Decía que se creaba en la ciudad de La Paz una Escuela de Policías que comenzaría a funcionar desde el año siguiente, teniendo por objeto instruir y educar convenientemente a elementos destinados al servicio general de la República.

Dicho Decreto Supremo contenía principios para preparar alumnos, en las siguientes carreras de Policía: a) Oficiales y Suboficiales de Gendarmería; b) Agentes de Policía propiamente dichos; c) Agentes de Investigación y Pesquisa. d) Comisarios de Policía. Venciendo las materias respectivas, debían ser declarados profesionales con carácter nacional. Como requisitos se debían cumplir los siguientes: a) Tener l9 años de edad y no exceder de 25 b) Saber leer y escribir correctamente c) Poseer las cuatro operaciones de aritmética d) Hablar con propiedad el idioma nacional e) No haber sido procesado criminalmente y tener buenos antecedentes; que acrediten con su libreta de conscripción los que hubiesen prestado el servicio militar y los demás con

certificados de personas o instituciones que merezcan crédito f) Ser declarados aptos para el servicio militar.

g) Medir por lo menos 1.70 m. de estatura.

### 1.2.7 SE CREA LA DIRECCIÓN NACIONAL DE INVESTIGACIÓN CRIMINAL

Por Decreto Ley No. 07015, de 4 de enero de 1965, fue creada la Dirección Nacional de Investigación Criminal, como organismo integrado por personal civil profesional egresado de la Academia Nacional de Policías, los especializados en el exterior y capacitados en los cursos de la División de Seguridad Pública de USAID y USOM-Bolivia en cooperación con la Policía Boliviana; debiendo quedar bajo su dependencia los departamentos de Investigación Criminal, Servicio Nacional de Identificación Personal, Policía Internacional, Juzgados Policiales y demás secciones establecidas en el Reglamento Orgánico. Se establecía que la Dirección Nacional de Investigación Criminal, tenía como función específica la investigación de los actos y hechos delictivos, la acumulación de la prueba y elementos de juicio y la identificación de los delincuentes, así como cumplir con todas las actuaciones relacionadas con el levantamiento de las Diligencias de Policía Judicial que requiere la justicia para la aplicación de la Ley Penal.

En el corto tiempo de funcionamiento independiente de la Dirección Nacional de Investigación Criminal en sus niveles nacionales, departamentales, provinciales, etc., se produjeron desacuerdos con el personal uniformado, creando situaciones delicadas, tanto para la Institución como para la ciudadanía que reclamaba atención coordinada y completa de la Policía[2].

[2] MOLINA ROBERTO, MOLINA JUVENAL, CESPEDEZ JAIME, CASTAÑON CARLOS, “Historia de la Policía Nacional”, Tomos I y II, Edit. Cima, La Paz, Bolivia.

## 1.3 INTRODUCCIÓN AL DERECHO INFORMÁTICO

Los avances tecnológicos que se han dado en la actualidad, como es el caso de los instrumentos digitales, que nos permiten acceso a la información de una manera rápida y sencilla, se nos abren puertas para mezclar estos dos instrumentos y expandir de modo más simple esa información.

El problema surge en el momento que los derechos de los creadores de las obras se ven violentados, debido a que con las nuevas tecnologías facilitan la transmisión de dichas obras sin el consentimiento del autor, y en muchas ocasiones con un afán de lucro, lo cual afecta el derecho patrimonial del autor, de los herederos y de los adquirentes por cualquier título.

Es por eso que es importante crear normas en las cuales se contemple la forma en que se registrarán las publicaciones; los permisos o autorizaciones que se deberán solicitar; los medios para hacerlo, y ante qué autoridad deberán realizarse, los delitos en que se puede incurrir, y las sanciones aplicables.

### 1.3.1 EL DERECHO INFORMÁTICO

El derecho informático, ha sido analizado desde diversas perspectivas.
Por un lado el Derecho Informático se define como un conjunto de principios y normas que regulan los efectos jurídicos nacidos de la interrelación entre el Derecho y la informática. Por otro lado hay definiciones que establecen que es una rama del derecho especializado en el tema de la informática, sus usos, sus aplicaciones y sus implicaciones legales.

El término "Derecho Informático" (Rechtinformatik) fue acuñado por el Prof. Dr. Wilhelm Steinmüller, académico de la Universidad de Regensburg de Alemania,

en los años 1970.1 Sin embargo, no es un término unívoco, pues también se han buscado una serie de términos para el Derecho Informático como Derecho Telemático, Derecho de las Nuevas Tecnologías, Derecho de la Sociedad de la Información, Iuscibernética, Derecho Tecnológico, Derecho del Ciberespacio, Derecho de Internet, etc[3].

Se considera que el Derecho Informático es un punto de inflexión del Derecho, puesto que todas las áreas del derecho se han visto afectadas por la aparición de la denominada Sociedad de la Información, cambiando de este modo los procesos sociales y, por tanto, los procesos políticos y jurídicos. Es aquí donde hace su aparición el Derecho Informático, no tanto como una rama sino como un cambio.

Es el sector normativo de los sistemas, dirigido a la regulación de la informática y la telemática. Así mismo integran el Derecho Informático las proposiciones normativas, es decir, los razonamientos de los teóricos del Derecho que tienen por objeto analizar, interpretar, exponer, sistematizar o criticar el sector normativo que disciplina la informática y la telemática. Las fuentes y estructura temática del Derecho Informático afectan las ramas del Derecho Tradicionales. Estas se inscriben en el ámbito del Derecho Público: El problema de la regulación del flujo internacional de datos informatizados, que interesa al derecho internacional público; la Libertada Informática, o defensa de las libertades frente a eventuales agresiones perpetradas por las tecnologías de la información y la comunicación, objeto de especial atención por parte del Derecho Constitucional y Administrativo; o los delitos informáticos, que tienden a configurar un ámbito propio en el Derecho Penal Actual. Mientras que inciden directamente en el ámbito del Derecho Privado cuestiones, tales como: Los contratos informáticos, que pueden afectar lo mismo al hardware que al

[3] www.wikipediaderechoinfor.com

software, dando lugar a una rica tipología de los negocios en la que pueden distinguirse contratos de compraventa, alquiler, leasing, copropiedad, multicontratos de compraventa, mantenimiento y servicios; como los distintos sistemas para la protección jurídica de los objetos tradicionales de los Derechos Civiles y Mercantiles.

Ese mismo carácter inter disciplinario o "espíritu transversal", que distingue al derecho informático, ha suscitado un debate teórico: si se trata de un sector de normas dispersas pertenecientes a diferentes disciplinas jurídicas o constituye un conjunto unitario de normas (fuentes), dirigidas a regular un objeto bien delimitado, que se enfoca desde una metodología propia, en cuyo supuesto entraría una disciplina jurídica autónoma.

### 1.3.3 LA INFORMÁTICA JURÍDICA

Es una disciplina bifronte en la que se entrecruzan una metodología tecnológica con sus posibilidades y modalidades de tal aplicación.

La informática jurídica estudia el tratamiento automatizado de: las fuentes del conocimiento jurídico a través de los sistemas de documentación legislativa, jurisprudencial y doctrinal (informática jurídica documental);las fuentes de producción jurídica, a través de la elaboración informática de los factores lógico-formales que concurren en proceso legislativo y en la decisión judicial (informática jurídica decisional).

Los procesos de organización de la infraestructura o medios instrumentales con los que se gestiona el Derecho (informática jurídica de gestión)[4].

[4] LUÑO ANTONIO ENRIQUE, “Ensayo de Informática Jurídica”, Edit. Fontamar, México, 2005.

## 1.3.4 CAMPOS DE ESTUDIO DEL DERECHO INFORMÁTICO

A continuación mencionaremos puntualmente la división temática del Derecho Informático que son las siguientes:

- Acceso a la información.
- Acceso a las TICs.
- Administración de Justicia y Nuevas Tecnologías.
- Banca y Dinero Dígital.
- Censura en Internet.
- Libertad de Expresión online.
- Comercio Electrónico.
- Contratos Informáticos.
- Compras públicas mediante el uso de las NTIC.
- Correo electrónico.
- Defensa del consumidor.
- Delitos Informáticos.
- Derecho en la Era Dígital.
- Derecho de las Telecomunicaciones.
- Derecho Laboral e Informática. Teletrabajo.
- Documento Electrónico, mensajes de datos, EDI y Factura Electrónica.
- Editoriales online de Derecho.
- E-government.
- E-Learning del Derecho y Nuevas Tecnologías.
- Firma Electrónica.
- Hábeas data.
- Impuestos e Internet.
- Informática Jurídica.

- Manifestación de la Voluntad por Medios Electrónicos.
- Medidas Cautelares sobre Equipos Informáticos.
- Nombres de Dominio y Direcciones IP.
- Notas Bibliográficas y de Eventos.
- Notificación por Medios Electrónicos.
- Privacidad.
- Profesionales del Derecho en la Era Dígital.
- Propiedad Intelectual y Propiedad Industrial e Internet.
- Programas: Software Jurídico. Bases de datos y Gestión de Bufetes.
- Protección de Datos de Carácter Personal.
- Publicidad e Internet.
- Relación entre el Derecho y la Informática.
- Seguridades informáticas.
- Sociedad Civil e Internet.
- Sociedad de la Información.
- Software libre.
- Telefonía y Voz sobre IP.
- Wireless Application Prototocol (WAP).
- Derechos de autor.
- Patente de software.

### 1.3.3 LA POLICÍA NACIONAL

Es una de las instituciones más importantes dentro de la estructura de todo estado. Manuel Ossorio, señala sobre el término: “A este vocablo se le asigna como origen la voz latina política o politeia, como equivalentes del buen orden que se observaba en la guarda de las ciudades y repúblicas, cumpliéndose las leyes u ordenanzas establecidas para su mejor gobierno.

Se ha dicho que la policía es el cuerpo encargado de vigilar por el mantenimiento del orden público y la seguridad de los ciudadanos, a las órdenes de las autoridades políticas. Marcel Le Clére, en su Historie de la Pólice, señala que paralelamente con el desarrollo de las comunidades humanas, van apareciendo órganos cuya misión es el mantenimiento del orden. Al comienzo, se encuentran en un mismo magistrado los poderes políticos, militares y judiciales. Los primeros funcionarios policiales tienen un carácter hibrido: son representantes del gobierno central y a la vez auxiliar de los tribunales[5].

Por otra parte, constitucionalmente, "La policía Nacional, como fuerza, tienen la misión específica de la defensa de la sociedad y la conservación del orden público y el cumplimiento de las leyes en todo el territorio nacional. Ejerce la función policial de manera integral bajo mando único, en conformidad con su Ley Orgánica y las Leyes del Estado Boliviano[6].

En cumplimiento con este mandato constitucional, la Policía Nacional tiene un papel protagónico en la defensa de la sociedad, la conservación del orden público y el cumplimiento de las leyes. En este propósito, la institución policial requiere una continua evaluación y la organización efectiva de todos sus recursos, planteándose la identificación y clasificación de los actos jurídicos como una prioridad institucional.

## 1.3.4 FUNCIÓN DE LA POLICÍA NACIONAL

La Policía Nacional, en su quehacer diario se caracteriza por construir el instrumento directo de la Constitución Política del Estado que hace práctica la

[5] OSSORIO MANUEL:Policia de seguridad, en Diccionario Jurídico Omeba, Edit. Driskill, Buenos Aires, Argentina, 1978, Tomo XXIII.
[6] BOLIVIA, Constitución Política del Estado, Cap. II, Art. 251.

libertad interna y garantiza la función que debe el Estado dentro de la sociedad, como:

- El  sostén de la estructura jurídica del país.
- Protege los recursos naturales así como la actividad económica del país.
- Coadyuva el proceso socio-cultural en los diferentes niveles sociales.
- Precautela los valores que la cultura boliviana ha heredado y creado.
- Respalda la gran estructura del Estado.
- Es la institución fundamental en la preservación de la paz y el orden social.

Al tener como base los Objetivos Nacionales, la Policía Nacional vincula con los más prioritarios como ser:

- El bienestar.
- Integración.
- Paz social y Estabilidad institucional.
- Objetivos nacionales comprometidos con la seguridad nacional.
- Libertad.
- Integridad.
- Democracia Representativa.

### 1.3.5 LA POLICÍA NACIONAL COMO INSTITUCIÓN FUNDAMENTAL DE BOLIVIA

La Policía Nacional como Institución fundamental y principal para la Seguridad y desarrollo de Bolivia, por la caracterización misma de su razón de ser, que se debe fundamentalmente a una necesidad dentro de la realidad social, y nace bajo cuatro aspectos fundamentales:

### 1.3.5.1 La Policía Nacional como necesidad Pública

De la relación que existe entre hombres de la sociedad boliviana, emergen derecho y obligaciones, sean estos de carácter jurídico o social, los cuales habrán de ser regulados y controlados especialmente por un organismo que tenga la capacidad y competencia necesarias, además que este sea dependiente del Estado, de ahí que la Policía Nacional surge como una necesidad social, es decir, como un órgano capaz de garantizar las acciones públicas y privadas.

### 1.3.5.2 La Policía Nacional como necesidad Social

La conservación del orden público, la defensa de la sociedad, la garantía del cumplimiento de las Leyes.

Significaría que la Institución tiene el rol de un papel netamente de auxilio social; pero la connotación política en su creación por el fenómeno de dependencia, orienta sus actividades hacia el estipulado por la Ley.

Por esta razón, la Institucionalización Policial emerge por las necesidades sociales.

### 1.3.5.3 La Policía Nacional como necesidad Política

El Estado se constituye en el poder político de dominación social en la sociedad boliviana, pero fundamentalmente, para que logre mantener ese poder, necesita de organizaciones no solo represivas como las Fuerzas Armadas o a la Policía nacional, sino también requiere tener bajo control todo el aparato ideológico para que a partir de ellos tengan asegurado el dominio de la sociedad.

La Institución Policial si bien es una necesidad social, al mismo tiempo se

constituye y emerge a la realidad social como un instrumento coadyuvante de la sustentación política del Estado.

#### 1.3.5.4 La Policía Nacional como necesidad Cultural

La existencia del acervo cultural con que cuenta la sociedad boliviana, contiene valores culturales que son parte ineludible de la realidad boliviana; por ello la Institución Policial se origina como un patrimonio encargado de la preservación cultural nacional.

## 1.3.6 SU ROL EN LA ORGANIZACIÓN DEL ESTADO

“La Policía Nacional, como fuerza, tienen la misión de defender la sociedad y la conservación del orden público y el cumplimiento de las leyes en todo el territorio nacional. Ejerce la función policial de manera integral bajo mando único, en conformidad con su Ley Orgánica y las leyes del Estado”

En cumplimiento con este mandato constitucional, la Policía Nacional tiene un papel protagónico en la defensa de la sociedad, la conservación del orden público y el cumplimiento de las leyes.

Una forma de cooperar al desarrollo integral del país, a través de la actividad cotidiana de la Policía, es trabajar al lado y con la población en forma solidaria y mancomunada. Otra forma de construir el país es apoyar el fortalecimiento de la democracia, a través del desempeño de las propias atribuciones de los miembros de la Policía, en la conservación, garantía y defensa de la sociedad, el orden público, de la seguridad ciudadana y el cumplimiento de las leyes del Estado.

Estos son los tres principios fundamentales en los que se basa una labor policial ética y licita y de los que se derivan todos los demás requisitos y disposiciones específicas para una labor policial ética y licita.

El desarrollo y consolidación de espacios de relación entre sociedad civil y la Policía debe ser una tarea que se planteé de forma conjunta entre la institución policial y las organizaciones de la sociedad civil. Esta relación debe auspiciar un mutuo conocimiento y apoyo en el marco de un estado de derecho y también debe permitir tener un conocimiento profundo de la realidad del país, participar en ella y contar con opciones para dar soluciones a las violaciones de los derechos humanos, construyendo un camino efectivo para su ejercicio pleno.

### 1.3.7 RELACIÓN POLICÍA NACIONAL Y DERECHO

El sistema penal está conformado por instituciones penales, normas penales y operadores de justicia penal, todo ellos encargados de controlar a la sociedad a través de la Policía, este sistema de control si bien es una reducción del delito, permite al Estado brindar seguridad desde el sistema a la sociedad en su conjunto a través de la Policía Nacional primordialmente como institución dual que participa activamente en la denominada seguridad urbana y en la investigación de delitos.

El rol de la Policía Nacional bifronte sociedad y sistema penal ha generado diversas opiniones por parte de la sociedad (que se siente menos vigilada por esta institución) y por los operadores de justicia que perciben un trabajo formalista, rutinario, con movilidad de los investigadores, jerárquico sobrecargado de trabajo que imposibilita la prestación de un servicio de calidad en la actividad investigativa y reactiva de la Policía contra la comisión de conductas, típicas, antijurídicas y culpables.

Sin embargo, los procesos de evaluación han detectado que el problema de fondo que debe ser contrarrestado es la asunción institucional de reforma de las rutinas inquisitivas autoritarias por parte de los policías investigadores como marco de cumplimiento (el ser la practica investigativa) asumiendo la responsabilidad de generar mecanismos o correctivos de actuación enmarcados cercanos al deber ser.

La labor amplia en la que se desenvuelve la Policial Nacional enmarcada en la decisión política del Estado de formulación de la política criminal, concepto que debe ser entendido como un conjunto e instrumentos, mecanismos y decisiones del Estado tendientes a la prevención y control del delito.

Estas decisiones políticas implican que la Constitución Política del Estado, en el cual los dispositivos institucionales generan programas políticos y tecnologías de intervención en el ámbito de la prevención y control del delito a partir de las necesidades del contexto y del fenómeno criminal en un tiempo determinado. En este sentido la policía criminal se desenvuelve en dos finalidades: la represión del delito y la prevención del delito.

Reprimir el delito significa la intervención, después que el delito ha sido producido y está dirigido a castigar al sujeto que lo ha realizado. Fase en la cual la Policía a través de la Fuerza Especial de Lucha Contra el Crimen operativiza la investigación técnica y científica, con la finalidad de aportar al sistema penal indicios y pruebas para la reconstrucción de los hechos que causaron el delito. Sin embargo, cabe recalcar que esta fase solo puede ser emprendida una vez cometido el delito.

Prevenir el delito es la intervención, antes que el delito se produzca con el fin de evitar que este suceda a través de la implementación de técnicas de intervención fuera del sistema penal. La Policía Nacional a través de instancias especializadas

de prevención, patrullaje, construyendo barreras contra los potenciales agresores, esta función es orientada a la construcción de una policía.

Para cumplir estas finalidades la policía criminal pone en movimiento diversos recursos que delimitan a su vez esferas en las prácticas sociales e instituciones.

Estos recursos son: penales o extrapenales. Son recursos penales, aquellos utilizados en el marco de la prevención penal general y especial de la pena, los que funcionan posterior a la comisión del delito, es decir, son represivos (Código Penal, Código de Procedimiento Penal) y utilizados a través de las instituciones oficiales para tal efecto y son recursos extrapenales los que no se refieren a la imposición de una pena.

La política criminal en nuestro país en los últimos diez años y donde la Policía fue construida y fortalecida, se ha desarrollado a partir de la concepción de reprimir al delincuente es prevenir al delito, esta idea se cumple a partir del desarrollo y expansión de los fines del derecho penal y la pena en el ámbito de construcción de tecnologías de intervención, es decir, la sociedad en su conjunto y los dispositivos institucionales del Estado, han volcado la misión de prevención en la formulación de políticas penales represivas orientadas a llevar al ofensor a la cárcel como forma de retribución y disminución de las necesidades sociales de seguridad.

La idea de represión /prevención desde el sistema penal, ha sido desbordada debido al aumento en la comisión de delitos y por la creciente sensación de inseguridad de las personas en cuanto al miedo de ser victimas del delito, sin embargo, este desbordamiento ha sido ocasionado por una sola razón, la aplicación de la represión es tardía y reducida ante el delito que los órganos de represión solamente actúan después de que se cometió el delito.

Una vez que se comete el delito el sistema penal empieza a funcionar, la policía investiga, el fiscal acusa y el juez administra justicia, el funcionamiento del sistema penal resuelve el conflicto y averigua la verdad histórica de los hechos, pero no proviene la comisión de mas delitos, claro empleo de es estos es el equilibrio anual de comisión de delitos sobre todo los de violación, robo, lesiones y hurtos en los últimos cinco años.

Si la reacción de los órganos del sistema penal es eficaz, esta labor aporta a la seguridad de las personas, ya que hará que la sociedad en su conjunto crea en el sistema penal, en la solución del conflicto y al acceso a la justicia pronta y oportuna, por otro lado, si la labor no se ajusta a las necesidad sociales, la gente en su conjunto criticará al sistema penal.

Sin embargo, la represión no interactúa o se desenvuelve en el ámbito de la seguridad ciudadana, sino por el desenvolvimiento de los actores y funcionamiento de ella, la ayuda, colabora pero no previene la comisión de más delitos.

Elaborar políticas públicas de control y represión del delito en el ámbito normativo, implica no solo la formulación de normas positivas tendientes a sancionar los delitos, de investigar su comisión, de reprimirlos a través de políticas penitenciarias sino también está compuesta por decisiones institucionales de implementación de mecanismos, seguimientos y monitoreo del desenvolvimiento instituciones en cuanto al cumplimento de sus objetivos a través de sistemas de gestión de casos de articular con los operadores políticas que fortalezcan sus dispositivos de reacción frente al delito, definición de líneas de persecución penal redistribución de sus recursos humanos, de permanencia de los investigadores en la tramitación de casos de su conocimiento, entre otras.

Estas tecnologías de intervención están orientadas en su construcción en el marco de la Constitución Política del Estado y del respecto de los Derechos Humanos, con el objetivo de mejorar los canales de acceso a la justica, de prestación del servicio de justicia con igualdad, eficacia, transparencia, pronta y oportuna. En el marco de la prevención del delito strictu sensu, se debe entender que la seguridad urbana vinculada con la idea de prevención del delito y del uso extra penal, entendida como el miedo y pánico social con respecto al delito.

Ahora bien, producir seguridad urbana es equivalente a reducir el riesgo de ser victimatizado y/o reducir la sensación personal y colectiva de temor frente al delito. En este sentido, podemos definir la prevención del delito siguiendo a Van Dijk "…todas las políticas, medidas y técnicas, fuera de los limites de sistema de justicia penal, dirigidas a la reducción de las diversas clases de daños producidos por actos definidos como delitos por el estado".

Dentro este ámbito de prevención y seguridad urbana, la institución encargada por Ley para su promoción y regulación es la Policía Nacional junto al Viceministro de Seguridad Ciudadana, instituciones que tiene la misión de proponer políticas dirigidas a preservar la seguridad interna del Estado, es decir, el ámbito de aplicación de la seguridad urbana como prevención extra penal recae en órganos establecidos.

Estas funciones ambientales de intervención en la Policía Criminal asignadas a la Policía Nacional deben ser reasumidas y agrupadas de acuerdo a las prioridades institucionales de reconstrucción de la percepción social de confianza en la Institución Policial.

Un área importante a fortalecer sin duda, es la tramitación y reacción inmediata por parte de la Policía ante la comisión del delito o denuncia del mismo por parte de la sociedad, es decir debe fortalecerse en el corto plazo el trabajo de la

Fuerza Especial de Lucha Contra el Crimen con el objetivo de implantar mecanismo de descongestión de casos por investigador, especialización efectiva de las divisiones de investigación, la presentación de una atención oportuna al denunciante y operadores del sistema, generar mecanismo de comunicación con la fiscalía de distrito en el diseño de estrategias de investigación, definición de líneas de persecución penal.

### 1.3.8 IMPLEMENTACIÓN EN PROCESOS DE GESTIÓN

Informes de evaluación como el Informe de Línea Base para la evaluación y seguimiento, aprobado por la comisión Nacional de implementación en fecha 28 de julio de 2005, detectan que en la etapa procesal con mayores dificultades en cuanto a su cumplimiento y aplicación es la etapa preparatoria detectando los siguientes problemas:

- Ausencia de coordinación entre la policía y Ministerio Publico en la realización de las investigaciones.
- Duración excesiva de la etapa preparatoria.
- Ausencia de sistemas de reelección de información estadística.
- Baja aplicación de salidas alternativas al proceso penal.
- Ausencia de sistemas de gestión de causas a nivel institucional.
- Congestionamiento del sistema penal.
- Muchos de estos problemas refuerzan la idea de un proceso

congestionado de caos debido a la ausencia de coordinación interinstitucional entre Policías, Fiscales y Jueces en la etapa preparatoria que faciliten una resolución efectiva a los conflictos penales que son de su conocimiento.

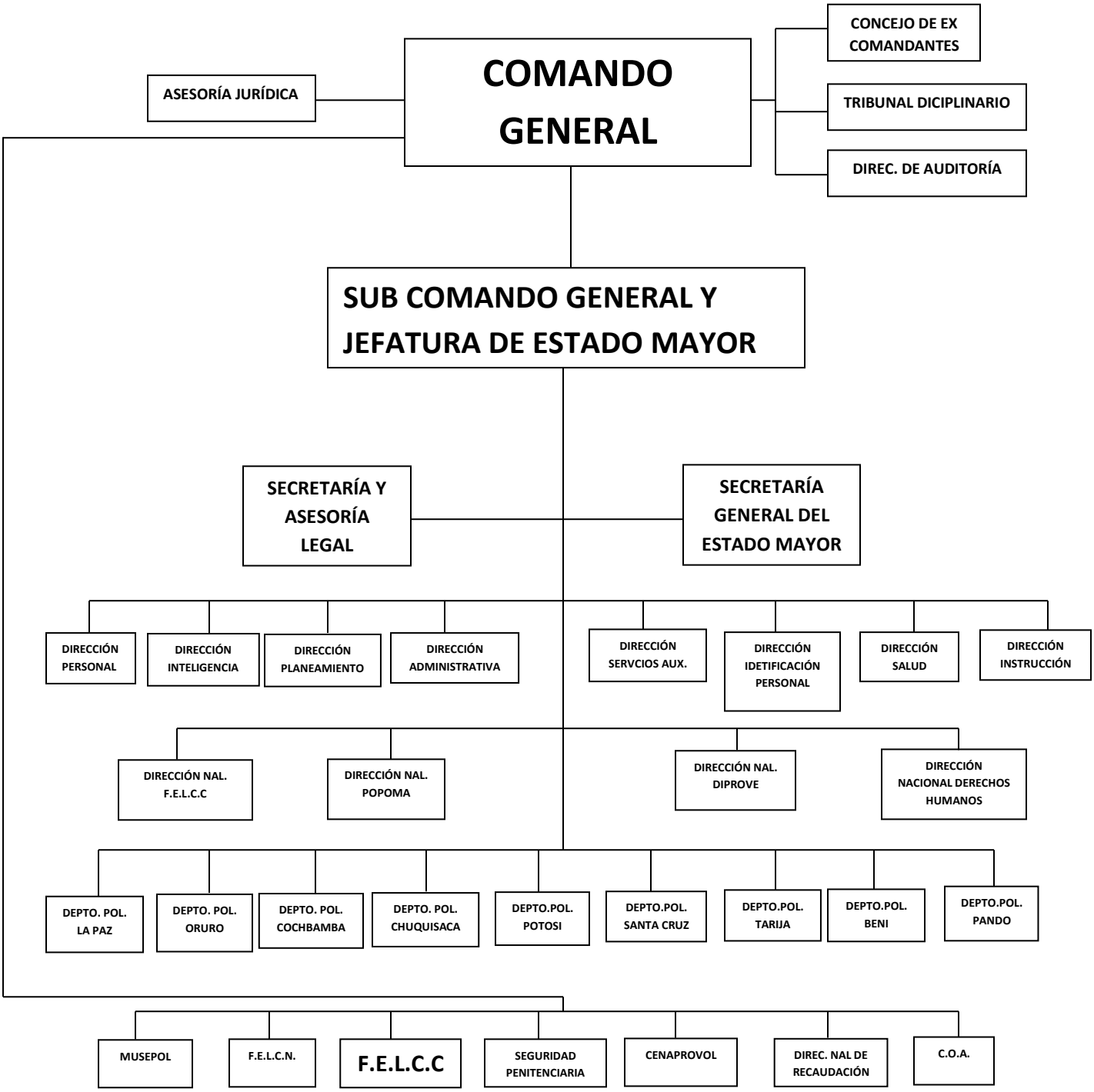
Implementar procesos de Gestión debe entenderse como la capacidad de la Policial Nacional como agente penal de administrar la distribución de casos, generar mecanismos de evaluación y seguimientos de la vida de las investigaciones con la finalidad de alcanzar resultados institucionales en el cumplimiento de sus actividades a partir del análisis de los recursos humanos y materiales.

La ausencia de procesos de gestión han ocasionado principalmente en la etapa preparatoria reafirmar el reflejo de la etapa de instrucción del sistema procesal penal anterior. Sobre la base de la necesidad institucional de implementación de sistemas de seguimiento de casos y descongestiona miento del sistema, es necesario la implementación de mecanismos que faciliten la labor del operador en la solución de casos de manera pronta y oportuna con el objetivo de corregir prácticas erróneas de la normativa procesal penal aportando a la sociedad en la generación de confianza en las instituciones penales sobre todo en la Policía Nacional.

Por tal motivo la estructura de la FELCC debe adecuarse al tratamiento oportuno de caos que saturan al sistema, por ello se requiere de la especialización por departamentos o secciones para el tratamiento de los casos que en el presente trabajo será de la implementación de la policía informática como unidad para atender delitos de exclusividad tecnológica.

## 1.3.9 ESTRUCTURA ORGÁNICA DE LA POLICÍA

Conforme su organización que se desprende de su jerarquía podemos realizar el siguiente esquema conceptual:



# CAPÍTULO II

## ELEMENTOS CONCEPTUALES APLICADOS EN EL TRABAJO

**2.1 INFORMÁTICA:** Conjunto de conocimientos científicos y de técnicas que hacen posible el tratamiento automático de la información por medio de computadoras. La informática combina los aspectos teóricos y prácticos de la ingeniería, electrónica, teoría de la información, matemáticas, lógica y comportamiento humano. Los aspectos de la informática cubren desde la programación y la arquitectura informática hasta la inteligencia artificial y la robótica[7].

**2.2 POLICÍA**: Policía, cuerpos y fuerzas que utiliza el Estado para asegurar de modo coactivo el orden, la seguridad y la salubridad públicas, así como para investigar el delito y prevenir la delincuencia[8].

Desde una perspectiva técnica, la actividad policial de la administración pública hace referencia a todas las intervenciones limitativas de las libertades y derechos de los ciudadanos, como son la imposición de prestaciones personales (por ejemplo, el servicio militar obligatorio), la expropiación forzosa, los decomisos de bienes muebles o los múltiples casos de coacción administrativa, como son aquéllos en que una persona ha obtenido la posesión de algo cuyo legítimo poseedor es la administración (y que no requerirá recurrir al juez para ejercitar los interdictos, pues la función de policía legitima sin más a la administración para llevar a cabo

[7] GARCIA-PELAYO Y GROSS, "Larousse Diccionario", Edit. Larousse, Madrid, España, 1993
[8] MICROSOFT, "Enciclopedia Encarta", Microsoft corporation, 1993 – 2005.

estas actividades coactivas) o los de imposición de deberes a los ciudadanos (declaraciones familiares para la elaboración de censos estadísticos, deberes laborales de higiene y seguridad en el trabajo, deberes de sanidad alimentaria o farmacéutica, deberes de escolarización obligatoria de la población hasta una determinada edad, entre otros). En este sentido, que es el propio del Derecho administrativo, la actividad de policía es el conjunto de medidas de coacción y represión que puede utilizar una administración pública para que el ciudadano ajuste sus actuaciones a fines de utilidad o de orden público, aunque ello suponga limitaciones a su libertad.

**2.3 INTERNET:** Interconexión de redes informáticas que permite a los ordenadores o computadoras conectadas comunicarse directamente, es decir, cada ordenador de la red puede conectarse a cualquier otro ordenador de la red. El término suele referirse a una interconexión en particular, de carácter planetario y abierto al público, que conecta redes informáticas de organismos oficiales, educativos y empresariales. También existen sistemas de redes más pequeños llamados intranets, generalmente para el uso de una única organización, que obedecen a la misma filosofía de interconexión[9].

**2.4 CORREO ELECTRÓNICO:** Sistema de envío y recepción de correo mediante el uso de un ordenador o computadora u otro dispositivo electrónico, de manera que se utilice una red de área local (LAN), Internet o conexiones inalámbricas para su transmisión y recepción. Se conoce también como e-mail, término que deriva de Electronic Mail, 'correo electrónico'; 'mensajería electrónica' es una acepción más restrictiva, que

[9] MICROSOFT, "Enciclopedia Encarta", Microsoft corporation, 1993 – 2005.

suele referirse a mensajes enviados desde dispositivos de comunicaciones, como teléfonos móviles[10].

**2.5 RED (informática):** Conjunto de técnicas, conexiones físicas y programas informáticos empleados para conectar dos o más ordenadores o computadoras. Los usuarios de una red pueden compartir ficheros, impresoras y otros recursos, enviar mensajes electrónicos y ejecutar programas en otros ordenadores[11].

**2.6 CRACKER:** Usuario y programador informático que tiene amplios conocimientos y crea código malicioso capaz de romper los sistemas de seguridad, para acceder a otros ordenadores o computadoras y así poder recabar o destruir información. En ocasiones se utiliza como sinónimo de hacker, aunque este último tiene como finalidad su propia satisfacción o vencer retos tecnológicos, sin ánimo de realizar daño u obtener información de forma ilegal[12].

**2.7 BASE DE DATOS:** Cualquier conjunto de datos organizados para su almacenamiento en la memoria de un ordenador o computadora, diseñado para facilitar su mantenimiento y acceso de una forma estándar. La información se organiza en campos y registros. Un campo se refiere a un tipo o atributo de información, y un registro, a toda la información sobre un individuo. Por ejemplo, en una base de datos que almacene información de tipo agenda, un campo será el NOMBRE, otro el NIF, otro la DIRECCIÓN..., mientras que un registro viene a ser como la ficha en la que se recogen todos los valores de los distintos campos para un individuo, esto es, su

[10] www.wikipedia/defincion.corrreoelectronico.org.htm
[11] www.wikipwdia/defincion/redinformatica.org.com
[12] MICROSOFT, "Enciclopedia Encarta", Microsoft corporation, 1993 – 2005.

nombre, NIF, dirección... Los datos pueden aparecer en forma de texto, números, gráficos, sonido o vídeo. Normalmente las bases de datos presentan la posibilidad de consultar datos, bien los de un registro o los de una serie de registros que cumplan una condición. También es frecuente que se puedan ordenar los datos o realizar operaciones sencillas, aunque para cálculos más elaborados haya que importar los datos en una hoja de cálculo. Para facilitar la introducción de los datos en la base se suelen utilizar formularios; también se pueden elaborar e imprimir informes sobre los datos almacenados[13].

**2.8 VIRTUAL:** Sistema que permite a uno o más usuarios ver, moverse y reaccionar en un mundo simulado por ordenador o computadora. Los distintos dispositivos de interfaz permiten al usuario ver, tocar y hasta manipular objetos virtuales. Los mundos virtuales y todo lo que contienen (incluyendo imágenes computarizadas de los participantes) se representan con modelos matemáticos y programas de computadora. Las simulaciones de realidad virtual difieren de otras simulaciones de computadora en la medida en que requieren dispositivos de interfaz especiales. Estos dispositivos transmiten al usuario las imágenes, el sonido y las sensaciones de los mundos simulados. También registran y envían el habla y los movimientos de los participantes a los programas de simulación. En lugar de utilizar un teclado o un ratón o mouse para comunicarse con la computadora, estos dispositivos especiales permiten al participante moverse, actuar y comunicarse con la computadora de forma parecida a como lo hace en su vida cotidiana. Este estilo natural de comunicación y la capacidad de mirar a su alrededor dan al usuario la sensación de estar inmerso en el mundo simulado[14].

[13] PACHECO KLEIN JORGE, "Introducción a los delitos informáticos en el ciberespacio" Edit. Nueva Jurídica, Buenos Aires, Argentina, 1998.
[14] www.wikipwdia/definicion/virtualinformatica.org.com.org.

**2.9 SEGURIDAD INFORMÁTICA:** Técnicas desarrolladas para proteger los equipos informáticos individuales y conectados en una red frente a daños accidentales o intencionados. Estos daños incluyen el mal funcionamiento del hardware, la pérdida física de datos y el acceso a los datos por personas no autorizadas. Diversas técnicas sencillas pueden dificultar la delincuencia informática. Por ejemplo, el acceso a información confidencial puede evitarse destruyendo la información impresa, impidiendo que otras personas puedan observar la pantalla del ordenador o computadora, manteniendo la información y los ordenadores bajo llave o retirando de las mesas los documentos sensibles. Sin embargo, impedir los delitos informáticos exige también métodos más complejos[15].

**2.10 DELITO:** "Acto típicamente antijurídico, culpable, sometido a veces a condiciones objetivas de penalidad, imputable a un hombre y sometido a una sanción penal".

**2.11 INSTITUCIÓN:** "Establecimiento o fundación de una cosa. Cosa establecida o fundada. Cada una de las organizaciones fundamentales de un Estado, como república, monarquía, feudalismo, democracia. Órganos constitucionales del poder soberano de la nación. Cada una de las materias de las diversas ramas del Derecho: Institución de la familia, del matrimonio, de la patria potestad, de las sucesiones, de la propiedad[16]".

**2.12 POBLACIÓN:**"…Cuantos hombres y mujeres, en determinado momento, componen el genero humano sobre el planeta o los habitantes de

[15] LIMA DE LA LUZ MARIA, "Delitos electrónicos", Edit. Porrúa, México, 1984.
[16] JIMENEZ DE ASUA LUIS, "Principios de Derecho Penal", Edit. Sudamericana, Buenos Aires Argentina, 1997.

un Estado, provincia u otra comarca o sitio en que se vive en estabilidad al menos relativa. También. Cualquier ciudad o pueblo[17]".

**2.13 SOCIEDAD:"…**la sociedad es un grupo en el cual están presentes todas las instituciones necesarias para la existencia social y colectiva. Dentro de este grupo que todo lo abarca se podrá encontrar la multiciplicidad de los grupos formados por los hombres en el curso de su vida colectiva[18]".

[17] OSSORIO MANUEL, "Diccionario de Ciencias Jurídicas, Políticas y Sociales, Edit. Heliasta, Buenos Aires, Argentina, 2003.

[18] OSSORIO MANUEL, ibídem: Óp. , Cit.,

# CAPÍTULO III

# MARCO JURÍDICO POSITIVO VIGENTE Y APLICABLE

## 3.1 ANTECEDENTES

Centrándonos en el plano estrictamente jurídico, el espacio donde se ubica las normas, constitucionales, leyes y otras disposiciones concretas que serán utilizadas como fundamento en la presente monografía jurídica son las siguientes:

## 3.2 CONSTITUCIÓN POLÍTICA DEL ESTADO

### SECCIÓN IV CIENCIA, TECNOLOGÍA E INVESTIGACIÓN

**3.2.1 Art.103 Parágrafo I.** Es la protección y la garantía que brinda el Estado para el desarrollo de la Ciencia, investigación y la tecnología, donde claramente se puede evidenciar que fomenta la incursión del avance de la ciencia para el progreso y beneficio satisfaciendo necesidades sociales en sentido general, por ello es que se propone la incursión de nuevas herramientas jurídicas que nos permitan lograr este objetivo, sea de esta manera la inserción de la Policía Informática dentro de la Fuerza Especial de Lucha contra el Crimen. Además comprometiéndose a destinar recursos necesarios para su implementación, que básicamente se refiere a su ejecución[19].

[19] BOLIVIA, Constitución Política del Estado, Sec. IV, Art.103, par. I, II y III.

**3.2.2 Parágrafo II.** La implementación de tecnología para el desarrollo como una política para el desarrollo.

**3.2.3 Parágrafo III.** Donde es misión fundamental primero del Estado, Universidades y sociedad en sus diferentes ámbitos fomentar la investigación conjunta para su aplicación.

## 3.3 CÓDIGO PENAL

### CAPÍTULO XI, DELITOS INFORMÁTICOS

**3.3.1 Art.363 bis.- (Manipulación Informática)** Se protege la información, de datos informáticos que afecten a un tercero, provocado de manera intencional.

**3.3.2 Art.363 ter. - (Alteración, acceso y uso indebido de datos informáticos**) Se controla el acceso de datos que se encuentren en cualquier soporte informático de manera que no se puedan manipular facialmente información que no solo pueda afectar a una sino también a varias[20].

### CAPÍTULO V APROPIACIÓN INDEBIDA

**3.3.3 Art.345.- (Apropiación Indebida**) Con relación a la manipulación de datos encuentra su subsunción en el presente trabajo.

**3.3.4 Art.346 bis.-(Agravación en caso de Víctimas)** Que señala expresamente que tanto en la consumación del uso indebido y en los delitos informáticos entre otros, si el perjuicio se daría a varias víctimas al mismo

[20] BOLIVIA, Código Penal Boliviano, Cap. XI, Art.363 bis. y 363 ter.

tiempo existe agravación de la pena, en una estafa informática podría perjudicar a múltiples acreedores de un banco[21].

**CAPÍTULO X DELITOS CONTRA EL DERECHO DE AUTOR**

**3.3.5 Art.362.- (Delitos contra la propiedad Intelectual)** Quien para sí se aproveche del patrimonio intelectual para ganar dinero será penado, una de las características de los delitos informáticos es que tienen un valor patrimonial pero son intangibles en cuanto a su posesión[22].

**3.3.6 Art. 363.- (Violación de Privilegio de Intervención)** Donde básicamente refuerza y garantiza la propiedad intelectual en la invención o descubrimiento. Nos interesa puesto que tratamos con elementos que son bienes intelectuales.

## 3.4 LEY ORGÁNICA DE LA POLICÍA NACIONAL

**CAPÍTULO III MISIÓN Y ATRIBUCIONES**

**3.4.1 Art. 7.-** En este artículo se identifican dos de las atribuciones más importantes de la Policía Nacional: la prevención de la comisión de los delitos y la investigación de aquellos que ya fueran cometidos. En este sentido, la prevención e investigación de delitos informáticos se constituye en una de las atribuciones correspondientes a la función policial[23].

[21] BOLIVIA, Código Penal Boliviano, Cap. V, Art. 345 y 346 bis.
[22] BOLIVIA, Código Penal Boliviano. Cap. X, Art. 362 y 363.
[23] BOLIVIA, Ley Orgánica de la Policía Nacional, Cap. III, Art.7.

# CAPÍTULO IV

# DE LOS DELITOS INFORMÁTICOS

## 4.1 NOCIÓN DE DELITO

Muchos estudiosos del Derecho Penal han intentado formular una noción de delito que sirviese para todos los tiempos y en todos los países. Esto no ha sido posible dada la íntima conexión que existe entre la vida social y la jurídica de cada pueblo y cada siglo, aquella condiciona a ésta. Según el ilustre penalista CUELLO CALON, los elementos integrantes del delito son: El delito es un acto humano, es una acción (acción u omisión).

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

Debe corresponder a un tipo legal (figura de delito), definido por La Ley, ha de ser un acto típico. El acto ha de ser culpable, imputable a dolo (intención) o a culpa (negligencia), y una acción es imputable cuando puede ponerse a cargo de una determinada persona. La ejecución u omisión del acto debe estar sancionada por una pena[24].

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

Se podría definir el delito informático como toda acción (acción u omisión) culpable realizada por un ser humano, que cause un perjuicio a personas sin

[24] CUELLO CALON EUGENIO, Derecho Penal, Edit. Bosch, Buenos Aires, Argentina,1985

que necesariamente se beneficie el autor o que, por el contrario, produzca un beneficio ilícito a su autor aunque no perjudique de forma directa o indirecta a la víctima, tipificado por La Ley, que se realiza en el entorno informático y está sancionado con una pena.

## 4.2 LOS DELITOS INFORMÁTICOS

Delito informático, crimen cibernético o crimen electrónico, se refiere a actividades ilícitas realizadas por medio de ordenadores o del Internet o que tienen como objetivo la destrucción y el daño de ordenadores, medios electrónicos y redes de Internet.

Sin embargo, las categorías que definen un delito informático son aún mayores y complejas y pueden incluir delitos tradicionales como el fraude, el robo, chantaje, falsificación y la malversación de caudales públicos en los cuales ordenadores y redes han sido utilizados. Con el desarrollo de la programación y de Internet, los delitos informáticos se han vuelto más frecuentes y sofisticados[25].

Existe una amplia gama de actividades delictivas que se realizan por medios informáticos: ingreso ilegal a sistemas, intercepción ilegal de redes, interferencias, daños en la información (borrado, deterioro, alteración o supresión de data), mal uso de artefactos, chantajes, fraude electrónico, ataques a sistemas, robo de bancos, ataques realizados por hackers, violación de los derechos de autor, pornografía infantil, pedofilia en Internet, violación de información confidencial y muchos otros.

[25] www.wikipedia/delitos/informaticos.htm.org.com

## 4.3 CONCEPTO DE DELITO INFORMÁTICO

Al respecto no existe unificación del concepto de Delito informático, pero como se podrán evidenciar existe un contenido que no es muy distante de una a otra acepción.

A continuación señalaremos algunos de los autores resaltantes: Jijena Leiva, define el delito informático:"….toda acción típica, antijurídica y culpable, para cuya consumación se usa la tecnología computacional o se afecta la información contenida en un sistema de tratamiento automatizado de la misma[26]".

Julio TELLEZ VALDEZ señala que los delitos informáticos son "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin (concepto típico)[27]".

Por su parte, el tratadista penal italiano Carlos SARZANA, sostiene que los delitos informáticos son "cualquier comportamiento criminal en que la computadora está involucrada como material, objeto o mero símbolo".

La Organización para la Cooperación Económica y el Desarrollo (OECD) da una definición que es considerada como abarcante y lo define como "cualquier conducta, no ética, o no autorizada, que involucra el procesamiento automático de datos y/o la transmisión de datos".

[26] LEIVA JIJENA, "Delitos informáticos", Edit. Libra, México, Monterrey, 1996.
[27] TELLEZ VALDEZ JULIO, "Derecho Informático", Edit. Mac Graw Hill, México, 2003.

## 4.4 CLASIFICACIÓN DE LOS DELITOS INFORMÁTICOS

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

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

2. Como fin u objeto: se enmarcan a las conductas criminógenas que van dirigidas en contra de la computadora, accesorios o programas como entidad física[28].

- ***María de la Luz Lima***, clasifica los delitos electrónicos en tres categorías, de acuerdo a como utilizan la tecnología electrónica:

1. Como método: cuando los individuos utilizan métodos electrónicos para llegar a un resultado ilícito.

2. Como medio: en donde para realizar un delito utilizan una computadora como medio o símbolo.

3. Como fin: conductas criminógenas dirigidas contra la entidad física del objeto o máquina electrónica o su material con objeto de dañarla[29].

[28]TELLEZ VALDEZ JULIO, Ibídem: Óp. , Cit.
[29] LIMA DE LA LUZ MARIA, "Delitos Electrónicos", Edit. Porrua, México, 1984.

## 4.5 CARACTERÍSTICAS DE LOS DELITOS INFORMÁTICOS

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

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

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

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

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

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

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

- Son muy sofisticados y relativamente frecuentes en el ámbito militar.

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

- Tienden a proliferar cada vez más, por lo que requieren una urgente regulación. Por el momento siguen siendo ilícitos impunes de manera manifiesta ante la ley[30].

## 4.8 CARACTERIZACIÓN DE LOS SUJETOS

4.8.1 **Sujeto Activo.-** No estamos hablando de delincuentes comunes. Los sujetos activos tienen las siguientes características:

- Poseen importantes conocimientos de informática.

- Ocupan lugares estratégicos en su trabajo, en los cuales se maneja información de carácter sensible (se los ha denominado delitos ocupacionales ya que se cometen por la ocupación que se tiene y el acceso al sistema).

- A pesar de las características anteriores debemos tener presente que puede tratarse de personas muy diferentes. No es lo mismo el joven que entra a un sistema informático por curiosidad, por investigar o con la motivación de violar el sistema de seguridad como desafío personal, que el empleado de una institución financiera que desvía fondos de las cuentas de sus clientes.

[30] TELLEZ VALDEZ JULIO, Ibídem: Óp. , Cit.

- Las opiniones en cuanto la tipología del delincuente informático se encuentran divididas, ya que algunos dicen que el nivel educacional a nivel informático no es inductivo, mientras que otros aducen que son personas inteligentes, motivadas y dispuestas a aceptar el desafío tecnológico.

- Estos delitos se han calificado de "cuello blanco", porque el sujeto que comete el delito es una persona de cierto status socioeconómico[31].

Pacheco Klein nos dice: "Otro estudio estimo que solo el 1% de los robos de computadora son detectados, y quizá solo un 15% de ellos sean denunciados.

Cuando los delitos informáticos son denunciados y llevados a juicio, muchos de ellos son negociados fuera del juzgado; solo alrededor del 24% van realmente a juicio, y alrededor de dos tercios de esos juicios resultan en la absolución y el archivo del expediente".

4.8.2 **Sujeto Pasivo.-** Es la persona o entidad sobre el cual recae la conducta que realiza el sujeto activo.

La mayoría de los delitos informáticos no son descubiertos, como ya dijimos, pro es importante destacar que se debe en gran parte a que los mismos no son denunciados, las empresas o bancos tienen miedo al desprestigio y a su consecuente pérdida económica[32].

## 4.9 DELITOS ESPECÍFICOS

[31] PACHECO KLEIN JORGE, "Introducción a los delitos informáticos en el ciberespacio", Edit. Porroa, México 2003.
[32] PACHECO KLEIN JORGE, Ibídem: Óp. , Cit.

### 4.9.1 **Spam**

El Spam o los correos electrónicos no solicitados para propósito comercial, es ilegal en diferentes grados. La regulación de la ley en cuanto al Spam en el mundo es relativamente nueva y por lo general impone normas que permiten la legalidad del Spam en diferentes niveles. El Spam legal debe cumplir estrictamente con ciertos requisitos como permitir que el usuario pueda escoger el no recibir dicho mensaje publicitario o ser retirado de listas de email.

### 4.9.2 **Fraude**

El fraude informático es inducir a otro a hacer o a restringirse en hacer alguna cosa de lo cual el criminal obtendrá un beneficio por lo siguiente:

- Alterar el ingreso de datos de manera ilegal. Esto requiere que el criminal posea un alto nivel de técnica y por lo mismo es común en empleados de una empresa que conocen bien las redes de información de la misma y pueden ingresar a ella para alterar datos como generar información falsa que los beneficie, crear instrucciones y procesos no autorizados o dañar los sistemas.

- Alterar, destruir, suprimir o robar data, un evento que puede ser difícil de detectar.

- Alterar o borrar archivos.

- Alterar o dar un mal uso a sistemas o softwares, alterar o reescribir códigos con propósitos fraudulentos. Estos eventos requieren de un alto nivel de conocimiento.

- Otras formas de fraude informático incluye la utilización de sistemas de computadoras para robar bancos, realizar extorsiones o robar información clasificada.

### 4.9.3 **Contenido Obsceno u Ofensivo**

El contenido de un website ó de otro medio de comunicación electrónico puede ser obsceno u ofensivo por una gran gama de razones. En ciertos casos dicho contenido puede ser ilegal. Igualmente, no existe una normatividad legal universal y la regulación judicial puede variar de país a país, aunque existen ciertos elementos comunes.

Sin embargo, en muchas ocasiones, los tribunales terminan siendo árbitros cuando algunos grupos se enfrentan a causa de contenidos que en un país no tienen problemas judiciales, pero sí en otros. Un contenido puede ser ofensivo u obsceno, pero no necesariamente por ello es ilegal.

Algunas jurisdicciones limitan ciertos discursos y prohíben explícitamente el racismo, la subversión política, la promoción de la violencia, los sediciosos y el material que incite al odio y al crimen.

### 4.9.4 **Hostigamiento / Acoso**

El hostigamiento o acoso es un contenido que se dirige de manera específica a un individuo o grupo con comentarios derogativos a causa de su sexo, raza, religión, nacionalidad, orientación sexual, etc. Esto ocurre por lo general en canales de conversación, grupos o con el envío de correos electrónicos destinados en exclusiva a ofender. Todo comentario que sea derogatorio u ofensivo es considerado como hostigamiento o acoso.

### 4.9.5 **Tráfico de Drogas**

El narcotráfico se ha beneficiado especialmente de los avances del Internet y a través de este promocionan y venden drogas ilegales a través de emails codificados y otros instrumentos tecnológicos.

Muchos narcotraficantes organizan citas en cafés Internet. Como el Internet facilita la comunicación de manera que la gente no se ve las caras, las mafias han ganado también su espacio en el mismo, haciendo que los posibles clientes se sientan más seguros con este tipo de contacto. Además, el Internet posee toda la información alternativa sobre cada droga, lo que hace que el cliente busque por sí mismo la información antes de cada compra.

### 4.9.6 **Terrorismo Virtual**

Desde 2001 el terrorismo virtual se ha convertido en uno de los novedosos delitos de los criminales informáticos los cuales deciden atacar masivamente el sistema de ordenadores de una empresa, compañía, centro de estudios, oficinas oficiales, etc. Un ejemplo de ello lo ofrece un hacker de Nueva Zelandia, Owen Thor Walker (AKILL), quien en compañía de otros hackers, dirigió un ataque en contra del sistema de ordenadores de la Universidad de Pennsylvania en 2008.

La difusión de noticias falsas en Internet (por ejemplo decir que va a explotar una bomba en el Metro), es considerado terrorismo informático y es procesable[33].

[33] "http://es.wikipedia.org/wiki/Delito_inform%C3%A1tico"

## 4.10 PANORAMA ACTUAL SISTEMAS Y EMPRESAS CON MAYOR RIESGO EN DELITOS INFORMÁTICOS

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

Los sistemas mecanizados son susceptibles de pérdidas o fraudes debido a que, tratan grandes volúmenes de datos e interviene poco personal, lo que impide verificar todas las partidas. Se sobrecargan los registros magnéticos, perdiéndose la evidencia auditable o la secuencia de acontecimientos.

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

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

En el diseño de un sistema importante es difícil asegurar que se han previsto todas las situaciones posibles y es probable que en las previsiones que se hayan hecho queden huecos sin cubrir.

Los sistemas tienden a ser algo rígidos y no siempre se diseñan o modifican al ritmo con que se producen los acontecimientos; esto puede llegar a ser otra fuente de "agujeros". Sólo parte del personal de proceso de datos conoce todas las implicaciones del sistema y el centro de cálculo puede llegar a ser un centro de información.

Al mismo tiempo, el centro de cálculo procesará muchos aspectos similares de las transacciones. En el centro de cálculo hay un personal muy inteligente, que trabaja por iniciativa propia la mayoría del tiempo y podría resultar difícil implantar unos niveles normales de control y supervisión.

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

### 4.10.1 **Delitos en Perspectiva**

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

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

Aunque depende en gran medida del tipo de organización, se puede mencionar que los Fraudes y sabotajes son los delitos de mayor incidencia en las organizaciones.

Además, aquellos que no están claramente definidos y publicados dentro de la organización como un delito (piratería, mala utilización de la información, omisión deliberada de controles, uso no autorizado de activos y/o servicios computacionales; y que en algún momento pueden generar un impacto a largo plazo).

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

## 4.11 ESTADÍSTICAS SOBRE DELITOS INFORMÁTICOS

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

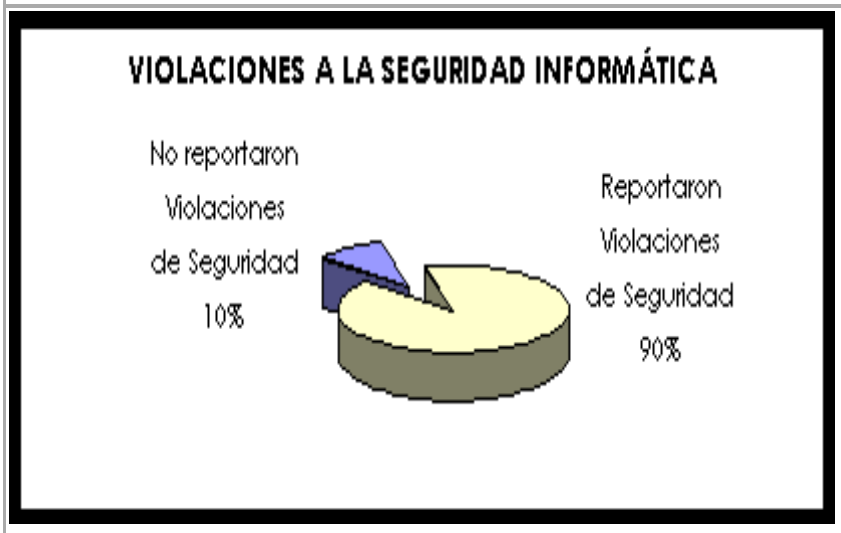
Esta entidad es El Instituto de Seguridad de Computadoras (CSI), quien anunció recientemente los resultados de su quinto estudio anual denominado "Estudio de Seguridad y Delitos Informáticos" realizado a un total de 273 Instituciones principalmente grandes Corporaciones y Agencias del Gobierno.

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

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

### 4.9.1 Violaciones a la Seguridad Informática

**CUADRO N°1: VIOLACIONES ALA SEGURIDAD INFORMÁTICA**

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

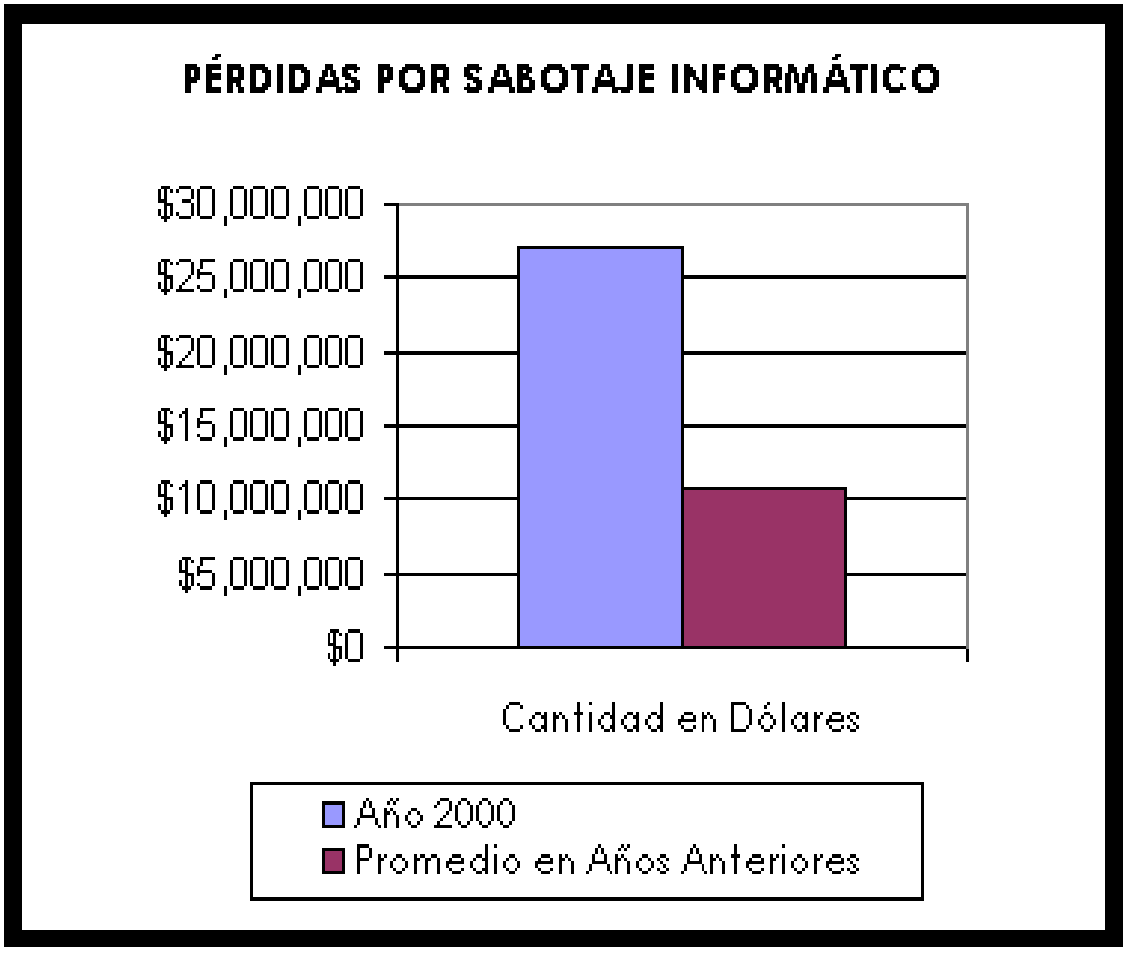
90% de los encuestados descubrió violaciones a la seguridad de las computadoras dentro de los últimos doce meses. 70% reportaron una variedad de serias violaciones de seguridad de las computadoras, y que el más común de estas violaciones son los virus de computadoras, robo de computadoras portátiles o abusos por parte de los empleados; por ejemplo, robo de

información, fraude financiero, penetración del sistema por intrusos y sabotaje de datos o redes.

### 4.9.2 Pérdidas Financieras

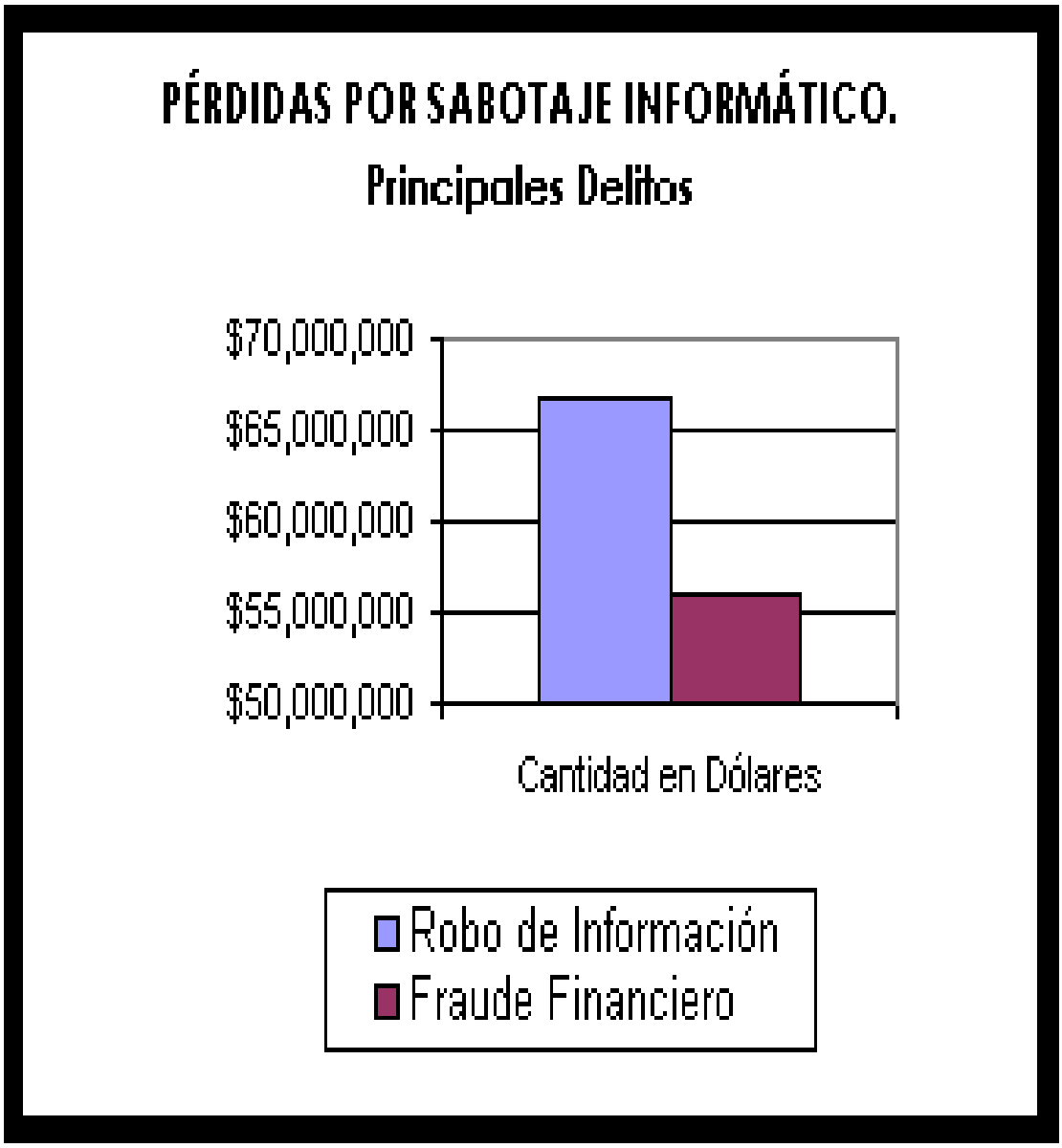
74% reconocieron pérdidas financieras debido a las violaciones de las computadoras. Las pérdidas financieras ascendieron a $265, 589,940 (el promedio total anual durante los últimos tres años era $120, 240,180).

**CUADRO N° 2: PÉRDIDAS POR SABOTAJE INFORMÁTICO**



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

**CUADRO N° 3: PÉRDIDAS POR SABOTAJE INFORMÁTICO**

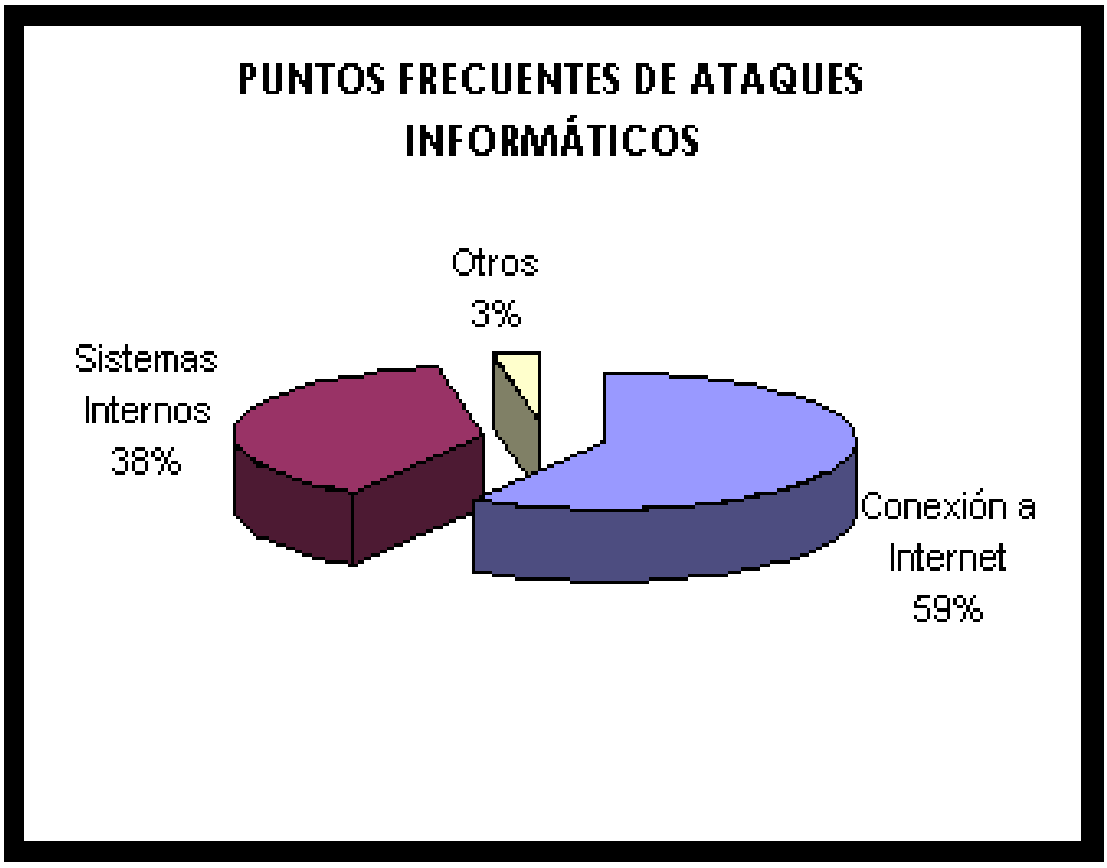


Como en años anteriores, las pérdidas financieras más serias, ocurrieron a través de robo de información (66 encuestados reportaron $66, 708,000) y el fraude financiero (53 encuestados informaron $55, 996,000).

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

### 4.9.3 Accesos No Autorizados

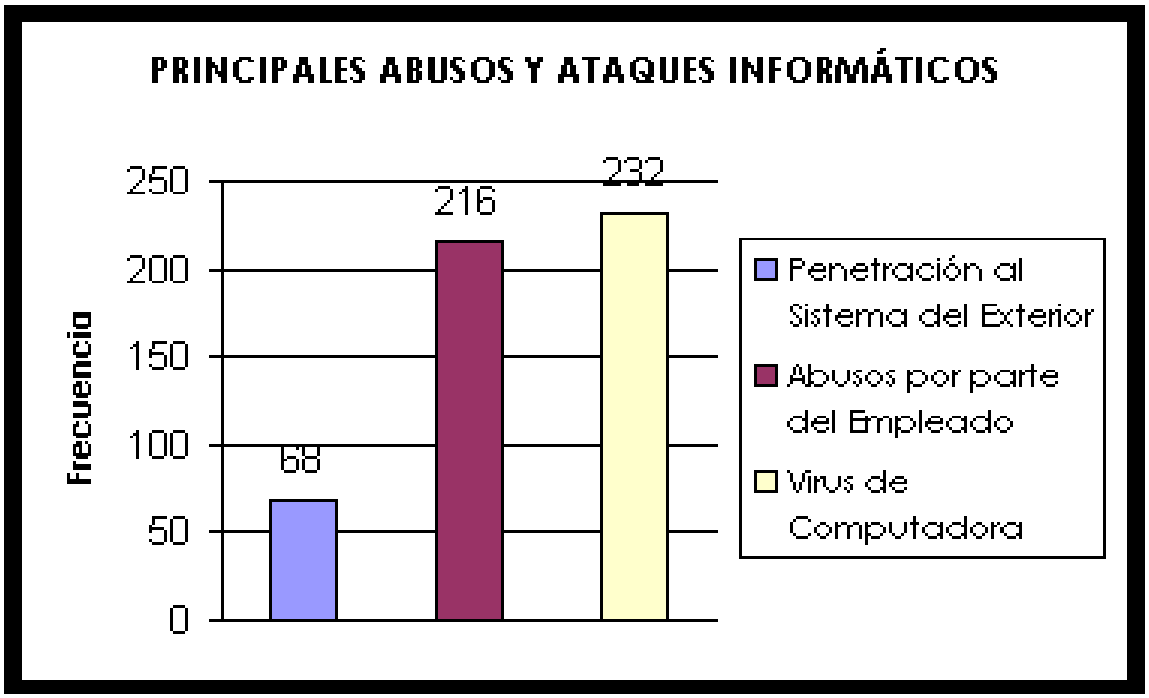
**CUADRO N°4: ACCESOS NO AUTORIZADOS**



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

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

**CUADRO N° 5: PRINCIPALES ABUSOS Y ATAQUES INFORMÁTICOS**




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.

### 4.9.4 Comercio Electrónico

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

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

### 4.9.5 Conclusión sobre el estudio CSI

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

### 4.9.6 Otras Estadísticas

La "línea caliente" de la Internet Watch Foundation (IWF), abierta en diciembre de 1996, ha recibido, principalmente a través del correo electrónico, 781 informes sobre unos 4.300 materiales de Internet considerados ilegales por usuarios de la Red. La mayor parte de los informes enviados a la "línea caliente" (un 85%) se refirieron a pornografía infantil. Otros aludían a fraudes financieros, racismo, mensajes maliciosos y pornografía de adultos.

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

Los delincuentes cibernéticos al acecho también usan el correo electrónico para enviar mensajes amenazantes especialmente a las mujeres. De acuerdo al libro de Barbará Jenson "Acecho cibernético: delito, represión y responsabilidad

personal en el mundo online", publicado en 1996, se calcula que unas 200.000 personas acechan a alguien cada año.

En Singapur El número de delitos cibernéticos detectados en el primer semestre del 2000, en el que se han recibido 127 denuncias, alcanza ya un 68 por ciento del total del año pasado, la policía de Singapur prevé un aumento este año en los delitos por Internet de un 38% con respecto a 1999. En relación con Internet y la informática, la policía de Singapur estableció en diciembre de 1999 una oficina para investigar las violaciones de los derechos de propiedad y ya ha confiscado copias piratas por valor de 9,4 millones de dólares.

En El Salvador, existe más de un 75% de computadoras que no cuentan con licencias que amparen los programas (software) que utilizan. Esta proporción tan alta ha ocasionado que organismos Internacionales reacciones ante este tipo de delitos tal es el caso de BSA (Bussines Software Alliance)[34].

## 4.10 DELITOS INFORMÁTICOS RECONOCIDOS POR LAS NACIONES UNIDAS

Los delitos informáticos conocidos por Naciones Unidas son:

- Manipulación de computadoras

- Datos de entrada. Este tipo de fraude informático conocido también como sustracción de datos es el más común ya que es fácil de cometer y difícil de descubrir. No es necesario que el infractor sea especialista en informática.

[34] http://www.monografias.delinformatic. mlandav.org.com

- Programas. El delincuente debe tener conocimientos técnicos concretos de informática. Consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas.
- Datos de salida. Se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude en los cajeros automáticos.

- Fraude efectuado por manipulación informática. Transacciones financieras repetidas que transfieren montos de una cuenta a otra.

- Falsificaciones Informáticas.

- Como objeto: Cuando se alteran datos de los documentos almacenados en forma computarizada.
- Como instrumentos: Las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial.

- Daños o modificaciones de programas o datos computarizados.

- Sabotaje informático: Es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema. Para ello se utilizan los virus (daño irreversible), gusanos (afectación parcial), bomba lógica o cronológica (destrucción o modificación de datos).

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

- Piratas informáticos o hackers: El acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones.

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

## 4.11 DERECHO COMPARADO EN LA LEGISLACIÓN DE DELITOS INFORMÁTICOS

### 4.11.1 Argentina

La Argentina sancionó el 4 de junio del 2008 la Ley 26.388 (promulgada de hecho el 24 de junio de 2008) que modifica el Código Penal a fin de incorporar al mismo diversos delitos informáticos, tales como la distribución y tenencia con fines de distribución de pornografía infantil, violación de correo electrónico, acceso ilegítimo a sistemas informáticos, daño informático y distribución de virus, daño informático agravado e interrupción de comunicaciones.

#### 4.11.1.1 Definiciones Vinculadas a la Informática

En el nuevo ordenamiento se establece que el término "documento" comprende toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión (art. 77 Código Penal).Los términos "firma" y "suscripción" comprenden la firma digital, la creación de una firma digital o firmar digitalmente (art. 77 Código Penal). Los

términos "instrumento privado" y "certificado" comprenden el documento digital firmado digitalmente (art. 77 Código Penal).

#### 4.11.1.2 Delitos contra Menores

En el nuevo ordenamiento pasan a ser considerados delitos los siguientes hechos vinculados a la informática:

Artículo 128: Será reprimido con prisión de seis (6) meses a cuatro (4) años el que produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere, por cualquier medio, toda representación de un menor de dieciocho (18) años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales, al igual que el que organizare espectáculos en vivo de representaciones sexuales explícitas en que participaren dichos menores.

Será reprimido con prisión de cuatro (4) meses a dos (2) años el que tuviere en su poder representaciones de las descriptas en el párrafo anterior con fines inequívocos de distribución o comercialización.

Será reprimido con prisión de un (1) mes a tres (3) años el que facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico a menores de catorce (14) años.

#### 4.11.1.3 Protección de la Privacidad

Artículo 153: Será reprimido con prisión de quince (15) días a seis (6) meses el que abriere o accediere indebidamente a una comunicación electrónica, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra

naturaleza, que no le esté dirigido; o se apoderare indebidamente de una comunicación electrónica, una carta, un pliego, un despacho u otro papel privado, aunque no esté cerrado; o indebidamente suprimiere o desviare de su destino una correspondencia o una comunicación electrónica que no le esté dirigida.

En la misma pena incurrirá el que indebidamente interceptare o captare comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido.

La pena será de prisión de un (1) mes a un (1) año, si el autor además comunicare a otro o publicare el contenido de la carta, escrito, despacho o comunicación electrónica.

Si el hecho lo cometiere un funcionario público que abusare de sus funciones, sufrirá además, inhabilitación especial por el doble del tiempo de la condena. Artículo 153 bis: Será reprimido con prisión de quince (15) días a seis (6) meses, si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido.

La pena será de un (1) mes a un (1) año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros. Artículo 155: Será reprimido con multa de pesos un mil quinientos ($ 1.500) a pesos cien mil, el que hallándose en posesión de una correspondencia, una comunicación electrónica, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, no destinados a la publicidad, los hiciere publicar indebidamente, si el hecho causare o pudiere causar perjuicios a terceros.

Está exento de responsabilidad penal el que hubiere obrado con el propósito inequívoco de proteger un interés público. Artículo 157: Será reprimido con prisión de un (1) mes a dos (2) años e inhabilitación especial de un (1) a cuatro (4) años, el funcionario público que revelare hechos, actuaciones, documentos o datos, que por ley deben ser secretos.

Artículo 157 bis: Será reprimido con la pena de prisión de un (1) mes a dos (2) años el que:

1. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales;

2. Ilegítimamente proporcionare o revelare a otra información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley.

3. Ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales.

4. Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de un (1) a cuatro (4) años.

#### 4.11.1.4 Delitos contra la Propiedad

Artículo 173 inciso 16: (Incurre en el delito de defraudación)...El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el

normal funcionamiento de un sistema informático o la transmisión de datos. Artículo 183 del Código Penal: (Incurre en el delito de daño).

En la misma pena incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático.

Cualquier programa destinado a causar daños. Artículo 184 del Código Penal: (Eleva la pena a tres (3) meses a cuatro (4) años de prisión, si mediare cualquiera de las circunstancias siguientes): Inciso 5: Ejecutarlo en archivos, registros, bibliotecas, museos o en puentes, caminos, paseos u otros bienes de uso público; o en tumbas, signos conmemorativos, monumentos, estatuas, cuadros u otros objetos de arte colocados en edificios o lugares públicos; o en datos, documentos, programas o sistemas informáticos públicos; Inciso 6: Ejecutarlo en sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones, de provisión o transporte de energía, de medios de transporte u otro servicio público.

#### 4.11.1.5 Delitos contra las Comunicaciones

Artículo 197: Será reprimido con prisión de seis (6) meses a dos (2) años, el que interrumpiere o entorpeciere la comunicación telegráfica, telefónica o de otra naturaleza o resistiere violentamente el restablecimiento de la comunicación interrumpida. Delitos contra la administración de justicia. Artículo 255: Será reprimido con prisión de un (1) mes a cuatro (4) años, el que sustrajere, alterare, ocultare, destruyere o inutilizare en todo o en parte objetos destinados a servir de prueba ante la autoridad competente, registros o documentos confiados a la custodia de un funcionario público o de otra persona en el interés del servicio público.

Si el autor fuere el mismo depositario, sufrirá además inhabilitación especial por doble tiempo.

Si el hecho se cometiere por imprudencia o negligencia del depositario, éste será reprimido con multa de pesos setecientos cincuenta ($ 750) a pesos doce mil quinientos ($ 12.500).

### 4.11.2 España

En España, los delitos informáticos son un hecho sancionable por el Código Penal en el que el delincuente utiliza, para su comisión, cualquier medio informático. Estos tienen la misma sanción que sus homólogos no-informáticos. Por ejemplo, se aplica la misma sanción para una intromisión en el correo electrónico que para una intromisión en el correo postal.

El Tribunal Supremo emitió una sentencia el 12 de junio 2007 (recurso Nº 2249/2006; resolución Nº 533/2007) que confirmó las penas de prisión para un caso de estafa electrónica (phising).

### 4.11.3 México

En México los delitos de revelación de secretos y acceso ilícito a sistemas y equipos de informática ya sean que estén protegidos por algún mecanismo de seguridad, se consideren propiedad del Estado o de las instituciones que integran el sistema financiero son hechos sancionables por el Código Penal Federal en el titulo noveno capítulo I y II.

El artículo 167 fr.VI del Código Penal Federal sanciona con prisión y multa al que dolosamente o con fines de lucro, interrumpa o interfiera comunicaciones alámbricas, inalámbricas o de fibra óptica, sean telegráficas, telefónicas o

satelitales, por medio de las cuales se transmitan señales de audio, de video o de datos.

La reproducción no autorizada de programas informáticos o piratería esta regulada en la Ley Federal del Derecho de Autor en el artículo 11. También existen leyes locales en el código penal del Distrito Federal y el código penal del estado de Sinaloa.

### 4.11.4 Venezuela

Concibe como bien jurídico la protección de los sistemas informáticos que contienen, procesan, resguardan y transmiten la información. Están contemplados en la Ley Especial contra los Delitos Informáticos, de 30 de octubre de 2001.
La ley tipifica cinco clases de delitos:

Contra los sistemas que utilizan tecnologías de información: acceso indebido (Art.6); sabotaje o daño a sistemas (Art.7); favorecimiento culposos del sabotaje o daño. (Art. 8); acceso indebido o sabotaje a sistemas protegidos (Art. 9); posesión de equipos o prestación de servicios de sabotaje (Art. 10); espionaje informático (Art. 11); falsificación de documentos (Art. 12).

Contra la propiedad: hurto (Art. 13); fraude (Art. 14); obtención indebida de bienes o servicios (Art. 15); manejo fraudulento de tarjetas inteligentes o instrumentos análogos (Art. 16); apropiación de tarjetas inteligentes o instrumentos análogos (Art. 17); provisión indebida de bienes o servicios (Art. 18); posesión de equipo para falsificaciones (Art. 19); Contra la privacidad de las personas y de las comunicaciones: violación de la privacidad de la data o información de carácter personal (Art. 20); violación de la privacidad de las comunicaciones (Art. 21); revelación indebida de data o información de carácter

personal (Art. 22); Contra niños y adolescentes: difusión o exhibición de material pornográfico (Art. 23); exhibición pornográfica de niños o adolescentes (Art. 24); Contra el orden económico: apropiación de propiedad intelectual (Art. 25); oferta engañosa (Art. 26).

### 4.11.5 Estados Unidos

Este país adoptó en 1994 el Acta Federal de Abuso Computacional que modificó al Acta de Fraude y Abuso Computacional de 1986. En el mes de Julio del año 2000, el Senado y la Cámara de Representantes de este país -tras un año largo de deliberaciones- establece el Acta de Firmas Electrónicas en el Comercio Global y Nacional. La ley sobre la firma digital responde a la necesidad de dar validez a documentos informáticos -mensajes electrónicos y contratos establecidos mediante Internet- entre empresas (para el B2B) y entre empresas y consumidores (para el B2C)[35].

[35] ibídem: Óp. , Cit.,www.monografias.delinformatic. mlandav.org.com

## 4.12 DELITOS INFORMÁTICOS EN BOLIVIA

### 4.12.1 ANTECEDENTES

En Bolivia ya comienzan a presentarse este tipo de delitos y se cuenta en la actualidad con más de cincuenta delitos informáticos que se encuentran sin resolver por falta de peritos en esa materia.

Entre los que figuran: Modificar programas informáticos o invadir correos electrónicos, esto es ilegal en otros países.

Con el tiempo surgen nuevos modos de fraude en Bolivia y su legislación no puede combatirlos.

El Instituto de Investigaciones Forenses de Bolivia (IDIF) prevé contratar para el 2009 especialistas en delitos informáticos porque hay demanda para ello.

### 4.12.2 RELACIÓN DE CASOS DETECTADOS EN BOLIVIA

#### 4.12.2.1 El Phishing (pesca de claves)

Se ha detectado que es frecuente el Fraude informático puesto que 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.

#### 4.12.2.2 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.

#### 4.12.2.3 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 cualquier otra acción que atente contra el normal funcionamiento de un sistema de información personal o de una institución.

#### 4.12.2.4 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.

### 4.12.3 LA POLICÍA NACIONAL Y LOS DELITOS INFORMÁTICOS

La Fuerza Especial de Lucha Contra el Crimen (FELCC) recibió al menos 50 denuncias de delitos informáticos en Bolivia, 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.

**CUADRO N° 6: DENUNCIAS RECIBIDAS E INVESTIGADAS A NIVEL NACIONAL - 2009**


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.

No obstante lo cual, 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 hasta la fecha.

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.

Estos delitos no sólo son investigados por esta división, sino que en el esclarecimiento coadyuvan la repartición de Delitos Económicos y Financieros y la de Trata y Tráfico de Personas. Un ejemplo de manipulación informática es el phishing (pesca de claves), técnica de estafa electrónica en la que un informático o conocedor de internet ingresa en la página de una entidad financiera, de la que selecciona a su víctima, y mediante correo electrónico le envía un portal falso del banco en el que pide que ingrese sus datos personales y su PIN (clave secreta) con el pretexto de actualizar la base de datos de los clientes. Una vez que el delincuente cibernético accede a la contraseña, procede a vaciar la cuenta del cliente del banco.

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. 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[36].

## 4.12.4 PROCEDIMIENTO DE RECEPCIÓN - DENUNCIAS DE DELITOS INFORMÁTICOS EN BOLIVIA

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.

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.

[36] http://www.laprensa.com.bo/noticias/07-12-08/index.php

En La Paz, la oficina de delitos informáticos, tiene un jefe de división y un investigador, ambos capacitados en esa rama[37].

## 14.12.5 TRATAMIENTO Y SITUACIÓN ACTUAL DE DELITOS INFORMÁTICOS EN BOLIVIA

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 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.

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.

[37] POLICIA NACIONAL, FELCCC, Cap. CLAURE EDSON, División de Delitos Informáticos.

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) organismo dependiente de la fiscalía General de la República, trabaja de la mano con la FELCC en el análisis de pruebas de distintos delitos comunes. A la fecha no tiene expertos para la exanimación de delitos informáticos.

El director nacional de esta entidad, Antonio Torres Balanza, dijo que para 2009 se contratarán a especialistas en esa rama por la demanda de investigación[38].

## 14.12.6 DELITOS INFORMÁTICOS EN EL MARCO JURÍDICO POSITIVO VIGENTE

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

[3838] POLICIA NACIONAL, FELCCC, Cap. CLAURE EDSON, División de Delitos Informáticos

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 el ordenamiento jurídico penal boliviano 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".

Asimismo resulta imposible extender el concepto de bienes muebles e inmuebles a bienes incorporales como ser los datos, programas e información computarizada.

Entre 2004 y 2008, 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 Boliviano.

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 Código de Procedimiento Penal establece que el IDIF es el órgano de investigación científica; pero desde el 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.

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.

Igualmente 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 pero en la actualidad se desconoce de su promulgación.

Tendría 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 cualquiera de sus componentes, o los que fueren cometidos por medio de tecnologías. En ese documento se define el fraude informático.

## 14.12.7 ESTADÍSTICAS SOBRE DELITOS INFORMÁTICOS A NIVEL NACIONAL

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.

**CUADRO N° 7: DELITOS INFORMÁTICOS EN BOLIVIA 2003 – 2009**


Desde ese año hasta mediados de 2009, 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.

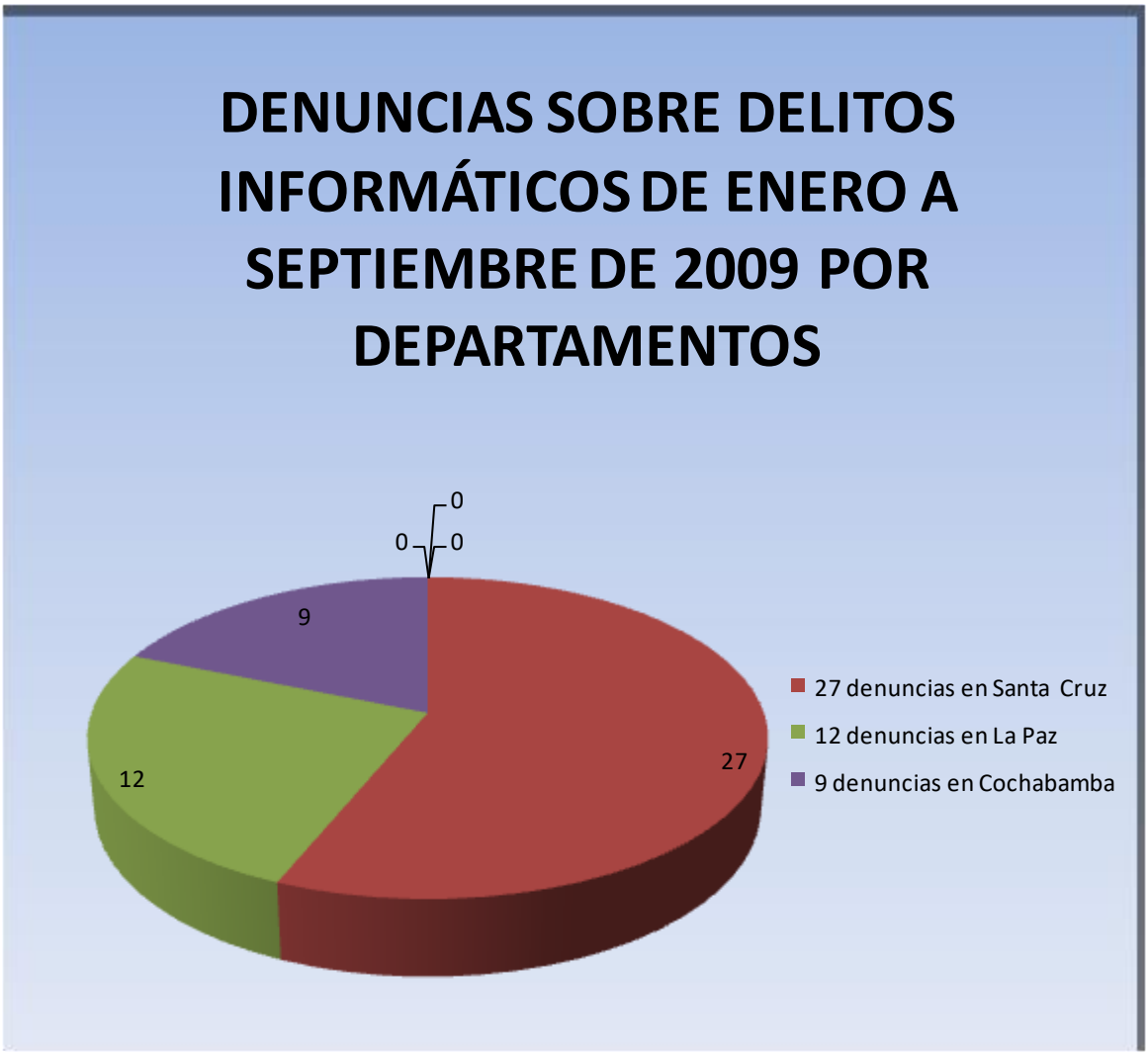
**CUADRO N° 8: DELITOS DE MANIPULACIÓN INFORMÁTICA POR DEPARTAMENTOS**


Sobre alteración informática, tres ocurrieron en La Paz, dos en Cochabamba, dos en Beni y uno en Santa Cruz.

**CUADRO N°9: DELITOS DE ALTERACIÓN Y USO INDEBIDO DE INFORMACIÓN POR DEPARTAMENTOS**


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.

**CUADRO N° 10: DENUNCIAS SOBRE DELITOS INFORMÁTICOS**




La legislación va quedando 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. Pero hasta el momento no se conoce nada concreto sobre su promulgación[39].

[39] POLICIA NACIONAL, FELCCC, Cap. CLAURE EDSON, División de Delitos Informáticos

# CAPÍTULO V

# DE LA POLICÍA INFORMÁTICA

## 5.1 GENERALIDADES

El uso generalizado de la informática en la actualidad contribuye innegablemente al avance y desarrollo de la ciencia y la sociedad.

El impacto de la informática en Bolivia conlleva cambios significativos tanto en el campo de la industria y el comercio como en la vida cotidiana de las personas individuales, cambios que se traducen en modificaciones y mejoras tanto en métodos de organización y gestión empresarial como en el mejor cuidado que pueda dar el usuario particular, generando controles más eficaces para garantizar la seguridad en el procesamiento de la información.

Al tomar en cuenta que la Policía Nacional no debe investigar solo los delitos convencionales, sino también los de reciente aparición, el presente tema de investigación fundamenta la necesidad de crear una unidad policial específica para perseguir a los autores de los denominados delitos informáticos, identificar y capturar a los sospechosos, y ponerlos a disposición de la autoridad competente para su juzgamiento y condena o absolución, ya que en la actualidad las distintas divisiones, como la División de Trata y Trafico de Personas, son colaborados por funcionarios especialistas en informática ante distintas denuncias que se presentan, pero no existe una unidad especializada de lucha contra el crimen informático.

Asimismo, se podría complementar esta labor con el control en los establecimientos financieros y otras entidades afines, que son los lugares donde se cometen con mayor frecuencia los delitos informáticos.

Finalmente, se plantea la necesidad de contar con una norma específica que regule la organización y funciones de una unidad especializada de este tipo en Bolivia, a fin de garantizar una lucha eficiente contra los delitos informáticos que se cometen en el territorio nacional.

## 5.2 FUNDAMENTACIÓN E IMPORTANCIA DE LA CREACIÓN DEL DEPARTAMENTO DE POLICÍA INFORMÁTICA

Los nuevos tiempos que vive la sociedad boliviana exigen la actualización y tecnificación de las instituciones que luchen contra la delincuencia en cualquiera de sus formas. En este sentido, la evolución de la tecnología informática es un elemento crucial a ser considerado dentro de los procesos y tendencias actuales que se viven, y el tratamiento de la Ciencia del Derecho respecto a la informática sin duda resulta fundamental para procurar la mejor relación entre individuos y colectividades con la mediación de estos recursos tecnológicos.

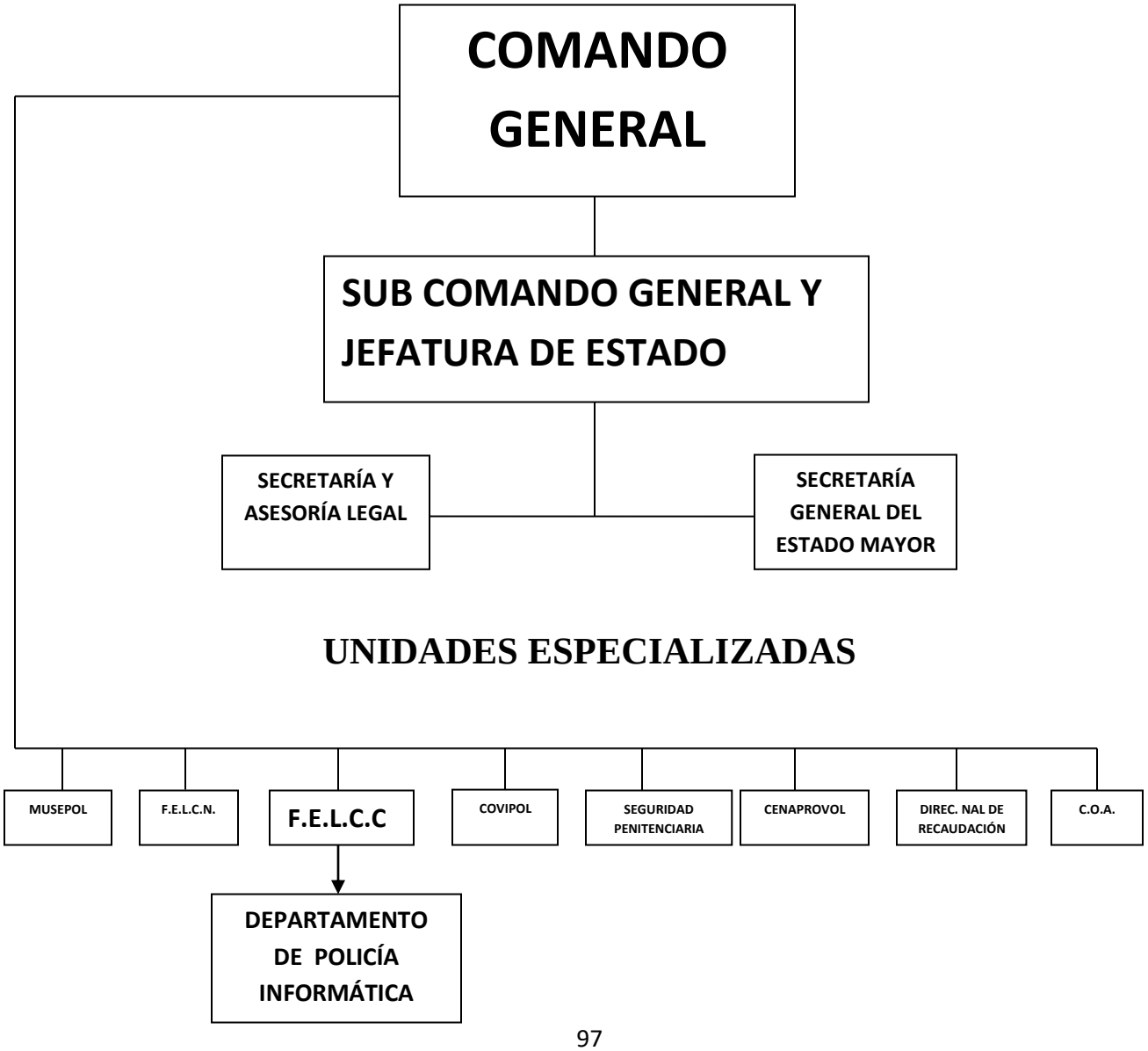
En este sentido, la identificación, persecución y captura de los diferentes delincuentes informáticos, que poco a poco irrumpen en el escenario general del país, amerita que diferentes organismos se preparen estructural, tecnológica y funcionalmente a los tiempos y desafíos que se viven en la actualidad.

Finalmente es importante mencionar, que en la actualidad existe una división dependiente de la Policía Nacional, pero que lamentablemente no cuenta con una estructura formal como departamento especializado, por lo cual tampoco

tiene funciones especificas en el ámbito de su actuación, quitándole institucionalidad y eficiencia en el conocimiento y derivamiento de estos casos.

## 5.3 LA POLICÍA INFORMÁTICA DENTRO DE LA FUERZA ESPECIAL DE LUCHA CONTRA EL CRIMEN

La Policía Nacional, es la principal entidad llamada a enfrentar los nuevos tipos de delito que se hacen presentes en la actualidad.



Por ello se plantea la incorporación de la unidad especializada del "Departamento de la Policía Informática" que depende directamente de la Fuerza Especial de Lucha Contra el Crimen para el tratamiento y la investigación del delito, bajo esta estructura de funcionamiento.

La Fuerza Especial de Lucha Contra el Crimen (F.E.L.C.C) capacitará investigadores con apoyo de la GTZ (1) En este año 2009.

## 5.4 LA POLICÍA INFORMÁTICA

Es la división especializada en la Investigación de Delitos Informáticos de Alta Tecnología dependiente de la F.E.L.C.C. y apoyo a la Justicia, está dirigida a identificar y capturar a los delincuentes informáticos.

Lo que constituye un reto para la Policía del futuro, que necesariamente deberá ponerse a la par y más aún, en cuanto a su eficacia y eficiencia en la lucha contra la delincuencia organizada.

Cumpliendo con los mandatos legales estipulados, evolucionando con la misma rapidez de la sociedad, percibiendo y adelantándose a los problemas sociales, respondiendo a las expectativas ciudadanas, para alcanzar la paz, seguridad y tranquilidad.

Es así que, ante este incremento de los delitos cometidos utilizando la tecnología y el ciberespacio, se tendría que ejecutar un Plan Estratégico, en el que se considera el patrullaje virtual en el ciberespacio.

Que demanda estar en las mismas y de ser posible, en mejores condiciones tecnológicas que los delincuentes informáticos.

También implica una gran dedicación y paciencia para detectarlos a través de minuciosos trabajos de inteligencia.

## 5 .5 OBJETIVO DE LA POLICÍA INFORMÁTICA

El órgano de ejecución de la Dirección de Investigación Criminal que tiene como objetivo, investigar, denunciar y combatir el crimen organizado transnacional (Globalizado) y hechos trascendentes a nivel nacional en el campo de los Delitos Contra la Libertad, Contra el Patrimonio, Seguridad Pública, Tranquilidad Pública, Contra la Defensa y Seguridad Nacional, Contra la Propiedad Industrial y otros, cometidos mediante el uso de la tecnología de la información y comunicación.

Aprehendiendo los indicios, evidencias y pruebas, identificando, ubicando y deteniendo a los autores con la finalidad de ponerlos a disposición de la autoridad competente.

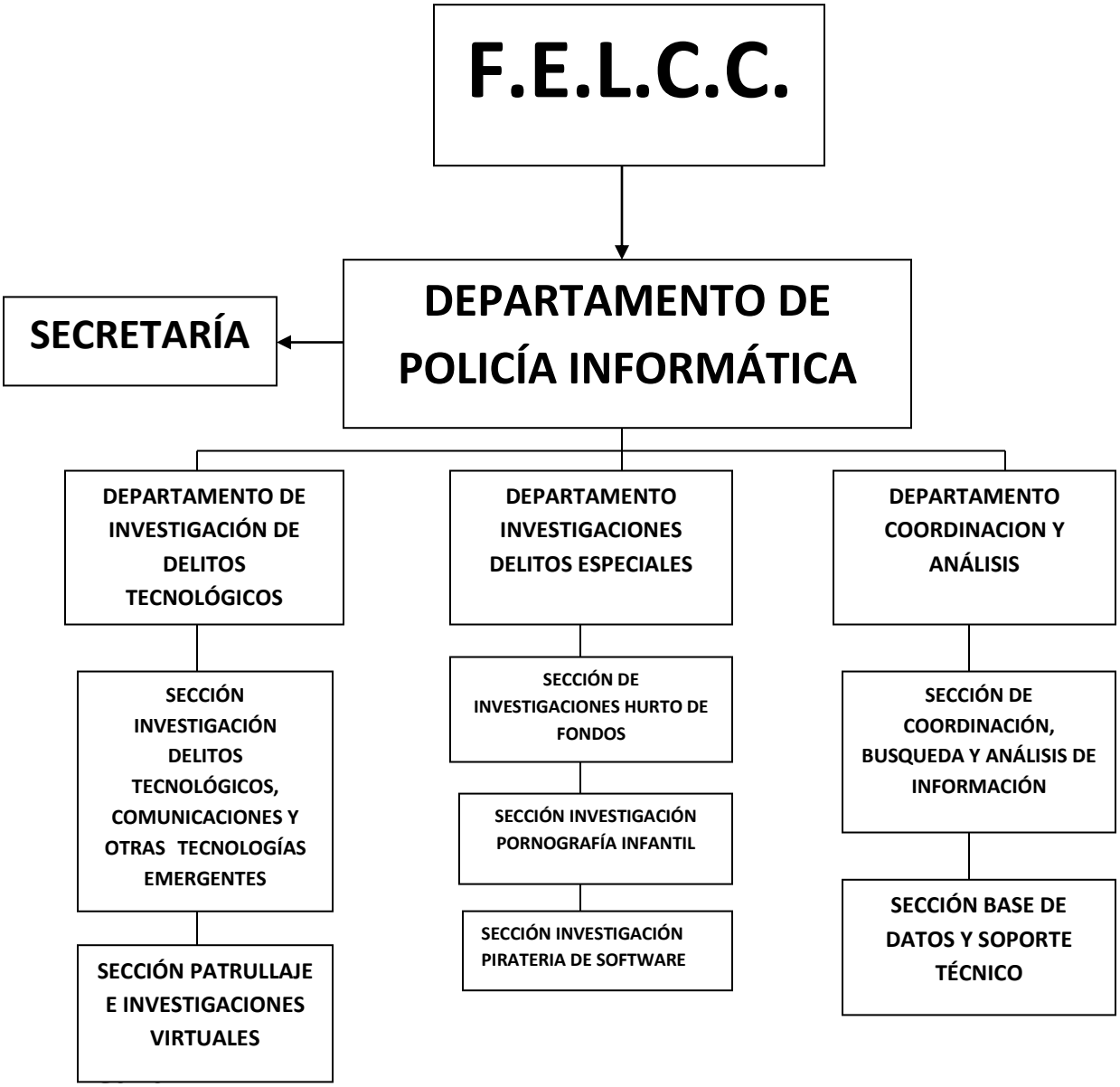
## 5.6 VISIÓN DE LA POLICÍA INFORMÁTICA

Ser reconocida nacional e internacionalmente en la investigación de delitos cometidos mediante el uso de las tecnologías de la información y comunicación.

Contar con personal altamente capacitado es decir que tenga conocimientos en derecho e informática.

## 5.7 ESTRUCTURA ORGÁNICA POLICÍA INFORMÁTICA

Para dar una verdadera eficacia institucional se presenta la siguiente composición de organización, en base a funcionalidad y especialidad:




Como se podrá observar en el esquema de organización, la policía informática depende exclusivamente de la F.E.L.C.C., de la cual se desprende en una estructura propia para que tenga mayor eficiencia.

Es así que se encuentra dividida en departamentos y estas en secciones según su especialidad. Que a continuación describiremos en qué consisten.

### 5.7.1 Secretaría

El departamento de secretaría cumple las siguientes funciones:

- Es el órgano administrativo, que recepciona y desconcentra la denuncia hacia el departamento que corresponde según la tipología del delito que se presenta.

- Además es relacionador entre distintas instituciones, judiciales, policiales, económicas o financieras entre otras. Para coadyuvar en la investigación de los casos, fortaleciendo de esta manera su propia institucionalización.

- Promueve y coordina información preventiva acerca de los peligros tecnológicos en general, plasmada desde revistas hasta la emisión de conferencias.

### 5.7.2 Departamento de Investigación de Delitos Tecnológicos

Básicamente se divide en dos secciones para su funcionalidad que son:

- **Sección de Investigación Delitos Tecnológicos, Comunicaciones y otras Tecnologías Emergentes.**

- **Sección Patrullaje e Investigaciones Virtuales.**

### 5.7.2.1 Sección de Investigación Delitos Tecnológicos, Comunicaciones y otras Tecnologías Emergentes

Sección encargada de investigar los delitos que son cometidos mediante cualquier tecnología, que puede ser desde ordenadores hasta la utilización de celulares para la comisión del delito.

Así por ejemplo se puede encargar de este tipo de delitos:

- **FRAUDE, CLONACIÓN DE TARJETAS**

LAS BANDAS DE "CLONADORES", UTILIZAN SOFISTICADOS APARATOS ELECTRÓNICOS QUE SIRVEN PARA EXTRAER LOS NÚMEROS DE LAS VERDADERAS TARJETAS DE CRÉDITO, DENOMINADO "SKIMMER".

GRABA TODA LA INFORMACIÓN DE LA BANDA MAGNETICA.


UNA VEZ EXTRAIDA LA INFORMACION, LA DESCARGAN EN UNA COMPUTADORA PORTÁTIL O UNA COMPUTADORA PERSONAL.

DESPUÉS DE ESE PROCESO, UTILIZAN OTRO APARATO LECTOR Y GRABADOR CON EL PROGRAMA Y LA TRANSFIEREN A UN PLASTICO UTILIZADO PARA LA CREACION DE TARJETAS DE CREDITO/DEBITO, CON LOS MISMOS DATOS PERSONALES DE LA TARJETA ORIGINAL.

UNA VEZ OBTENIDA LA TARJETA, LOS "CLONADORES" EFECTÚAN COMPRAS O RETIRAN ELEVADAS SUMAS DE DINERO.

Como se podrá observar no siempre se utilizan computadoras, pueden ser distintos medios tecnológicos, como ser aparatos duplicadores de series, que al solo pasar pueden registrar datos inmersos en una tarjeta de crédito, accediendo de esta manera a una cuenta económica personal, posterior a ello recién pasa a un ordenador donde se descarga la información obtenida en primera instancia. Concurriendo el uso de dos o  más tecnologías para obtener un fin ilícito.

- **ACCESO NO AUTORIZADO A BASE DEDATOS**

ES EL USO ILEGÍTIMO DE PASSWORDS Y LA ENTRADA A UN SISTEMA INFORMÁTICO DE UNA ENTIDAD PUBLICA O PRIVADA, SIN LA AUTORIZACIÓN DEL PROPIETARIO O USUARIO, CON LA FINALIDAD DE INSERTAR, BORRAR O MODIFICAR INFORMACION PRIVILEGIADA DE UNA BASE DE DATOS.

Actualmente hay que darle mayor relevancia en el medio nacional puesto que son los delitos informáticos que se comenten con mayor frecuencia, ingresando a cuentas particulares, y aun se desconoce sobre un caso en concreto sobre la violación a una base datos de una entidad financiera.

- **INTRUSIONES (HACKING , CRACKING)**


INTRUSIONES INFORMÁTICAS, DAÑOS Y VIRUS, ES DECIR, CUANDO SE CONSIGUE COMPROMETER EL FILTRO DE SEGURIDAD DE UN SISTEMA INFORMÁTICO PARA OBTENER PRIVILEGIOS NO AUTORIZADOS Y ACCEDER A ORDENADORES AJENOS.

ACTIVAS: ACCEDE A SUS ARCHIVOS O HACE QUE NO FUNCIONEN, MEDIANTE ACCESOS NO AUTORIZADOS O CON ATAQUES DE DENEGACIÓN DE SERVICIO.

PASIVAS: NO ALTERAN EL FUNCIONAMIENTO DEL ORDENADOR Y SE LIMITAN A RECOPILAR INFORMACIÓN.

ACTIVIDADES DE "CRACKING" EN LO REFERENTE A LA ELIMINACIÓN DE PROTECCIONES EN LOS PROGRAMAS ORIGINALES.

### 5.7.2.2 Sección Patrullaje e Investigaciones Virtuales

Programa policial dedicado a la ciber navegación policial, permitiendo la actuación oportuna para combatir las actividades delictivas, las nuevas modalidades y tendencias criminales del mundo virtual. A nivel nacional tiene la finalidad de observar, controlar portales bolivianos que ofrecen cualquier tipo de bienes y servicios.

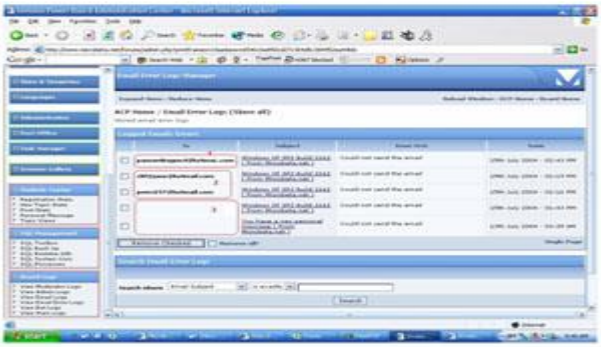
### 5.7.3 Departamento Investigaciones Delitos Especiales

Por delitos especiales, nos referirnos a la investigación de delitos específicos, como ser: hurto de fondos, la pornografía infantil y la piratería de software. Además ingresan en esta sección la aparición de nuevos figuras jurídicas delictivas presentadas a nivel informático con el transcurrir del tiempo y la evolución de la tecnología.

Así por ejemplo:

- **EXTROSION**


MODALIDAD DELICITVA EN LA QUE UNA ORGANIZACIÓN DE DELINCUENTES COMUNES, BUSCABAN A SUS POSIBLES VICTIMAS EN LA PAGINA WEB DE MILLONARIOS DEL MUNDO.



A QUIENES ENVIABAN MENSAJES DE TEXTO INTIMIDATORIOS, SIMULANDO SER EX-INTEGRANTES DE GRUPOS TERRORISTAS INTERNACIONALES.


SUGIRIENDOLES PARA QUE ENVÍEN DINERO, MEDIANTE EMPRESAS COURIER, PARA QUE SUSPUESTAMENTE LES REMITAN VIDEOS TAPES CON PRUEBAS.

- **CHANTAJE SEXUALY ECONOMICO**



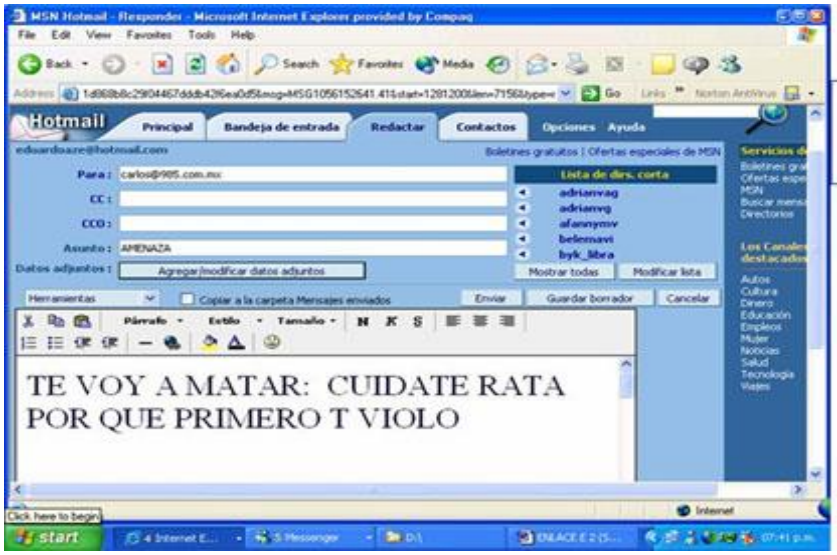




VIA CHAT O PAGINAS WEB DE SUPUESTOS PROMOTORES DE MODELOS, CAPTAN MUJERES OFRECIENDOLES PASAR CASTING O POSEN EN LA WEB CAM SEMI-DESNUDAS O DESNUDAS, A FIN DE FOTOGRAFIARLAS Y SER CONSIDERADAS PARA EVENTOS, PARA DESPUES PROCEDER VIA CORREO ELECTRÓNICO, A SOLICITARLES DINERO O FAVORES SEXUALES, A CAMBIO DE NO REMITIR DICHAS TOMAS A SUS FAMILIARES, AMIGOS O PUBLICARLAS EN PAGINAS WEB DE PORNOGRAFIA.




- **AMENAZAS POR E- MAIL**




CONSISTE EN EFECTUAR AMENAZAS, INSULTOS E INJURIAS HACIENDO USO DE SERVIDORES DE INTERNET

Este departamento de divide igualmente en secciones:

- **Sección Investigaciones Hurto de Fondos.**
- **Sección Investigación Pornografía Infantil.**
- **Sección Investigación Piratería de Software.**

### 5.7.3.1 Sección Investigaciones Hurto de Fondos

Se ha dedicado una sección particular, a este tipo de investigaciones por las características propias que tiene para su comisión. Es así que parte por el principio de discrecionalidad, puesto que podría ocasionar incertidumbre en la economía particular y general a nivel bancario por la gravidez del hecho.

Así tenemos el siguiente detalle ilustrativo:

CONSISTE EN OBTENER MEDIANTE LA MODALIDAD DEL "PHISHING", DONDE EL TIMADOR BUSCA QUE ALGUIEN "MUERDA EL ANZUELO", A REVELAR INFORMACIÓN CONFIDENCIAL PERSONALQUE PUEDE SER USADA PARA ROBARLE SU DINERO.


LUEGO DE OBTENER LA INFORMACIÓN NECESARIA PARA ACCEDER A LA CUENTA DE TU BANCO, PROCEDEN A EFECTUAR OPERACIONES FRAUDULENTAS ON-LINE, (TRANSFERENCIAS DE FONDOS A OTRAS CUENTAS, PAGOS DE SERVICIOS, ETC).

### 5.7.3.2 Sección Investigación Pornografía Infantil

Dedicada a la búsqueda de manipulación, exhibición y publicación de pornografía por internet de menores de edad.


### 5.7.3.3 Sección Investigación Piratería de Software

Es decir que investiga la reproducción total o parcial de material de programas informáticos, tomando en cuenta que actualmente existe bastante demanda de la creación de los mismos, por ingenieros bolivianos.

### 5.7.4 Departamento Coordinación y Análisis

Que se encuentra divida en dos secciones:

- **Sección de Coordinación, Búsqueda y Análisis de la Información.**
- **Sección de Base de Datos y Soporte Técnico.**

#### 5.7.4.1 Sección de Coordinación, Búsqueda y Análisis de la Información

Si bien la estructura organiza de la Policía Informática se encuentra divida, también funciona interdependientemente, este departamento se encargará, si es que existiera necesidad de un trabajo, coadyuvando a coordinar los distintos departamentos y/o secciones para la resolución de una investigación.

Puesto que también podrían suscitarse multiplicidad de delitos en la consumación de un mismo acto que involucren a dos o más secciones de cada departamento.

Con relación a la búsqueda, se da sobre la base de la información a nivel informático, y fáctico en la búsqueda de realidad histórica de los hechos. De manera que no solo realiza estudio a nivel informático, sino también de campo, en la búsqueda de personas, instituciones, etc.

Del análisis, donde se equipará a un departamento de inteligencia, que estudia la descomposición de los elementos constitutivos del tipo penal y la inserción de estrategias, entre otras.

#### 5.7.4.2 Sección de Base de Datos y Soporte Técnico

Sección que acumula la información, organizándola de manera sistemática, en soportes electrónicos y documentales.

El soporte técnico debe entenderse como la generación de tecnología, para la utilización de los departamentos o de un caso especifico en búsqueda que brinde mayor eficiencia en la resolución de los casos. Donde se encuentran especialistas en estas ramas (informático, electrónica, etc.)

## 5.8 MODO DE OPERACIÓN DE LOS DELITOS INFORMÁTICOS

En la actualidad los delincuentes que cometen Delitos Informáticos trabajan solos, sentados frente a su computador o en una cabina de internet.

Su inversión es el costo de la hora en la cabina de internet y desde ahí cometen una gran diversidad de delitos.

## 5.9 ASPECTOS RELEVANTES SOBRE 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, realizado con el propósito de obtener un beneficio económico.

Entre estos supuestos se encuentran el Fraude por manipulación de un computador contra un procesamiento de datos, el uso de datos engañosos ¨data diddling¨ y el fraude en el que se realiza la alteración de datos contenidos en el computador antes o durante su proceso informático.

El fraude informático puede cometerse mediante el uso de los caballos de Troya ¨Trojan hourses¨, el cual es un programa informático destinado a introducir rutinas o instrucciones aparentemente inicuas, para distorsionar el funcionamiento del sistema y así cometer fraudes vi Internet, como también 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¨.

Para José Luis Fernández, quien prefiere designar a todas las acciones disvaliosas ligadas a la informática como ¨Fraudes Informáticos¨, distingue de forma dicotómica las siguientes categorías: Fraudes en la materia corporal, o del hardware: Estas acciones criminosas violan la integridad física del propio computador, encontrándose fraudes en el nivel de input. Esta conducta, también llamada de manipulación del input, revelaría en la conducta del agente el ánimo de alterar datos, omitir o ingresar datos verdaderos o introducir datos

falsos en un ordenador. Fraudes a nivel de tratamiento: El delincuente informático modifica 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.
Fraudes a nivel de los output: Es el acto de falsear el resultado inicialmente correcto, obtenido por el ordenador.

En la jurisprudencia alemana se tiene conocimiento que en febrero de 1983, una empleada de Banco del Sur transfirió un millón, trescientos mil marcos a la cuenta de su cómplice a primera hora del día. Se dice que esta operación ilegal podría haber sido detectada por el sistema de seguridad del banco a las 12:30 AM. Mas la rápida transmisión del crédito a través de sistemas informáticos conectados en línea on-line, hizo posible que la cómplice de la empleada retirase el dinero en otra sucursal del banco.

## 5.10 SABOTAJE INFORMÁTICO

Entendido como el acto mediante el cual se logra inutilizar, destruir, alterar o suprimir datos, programas e información computarizada, tiene sus inicios en los laboratorios del Instituto de Massachusetts 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, una bomba cronológica puede servir como medio de extorsión para la obtención de un

desembolso pecuniario en perjuicio del titular del bien informático, si a cambio la bomba lógica es desactivada.

Estos dispositivos informáticos son también denominados de “tecno virus”, “programas criminales” o “asesinos electrónicos” pues destruyen la información en milésimas de segundo. El “animus delicti” es causar daño a bienes informáticos. En gran parte el sabotaje informático 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 de Software**

Estos programas informáticos detonan a pocos minutos de ser introducidos en una red o al ser cargados en el ordenador. No esperan ninguna condición previa para activarse ni necesitan auto duplicarse.

La diferencia entre las bombas lógicas y las de software es la necesidad de que en las bombas lógicas exista una orden especial por parte del programador para activar la misma con el fin de que explote.

- **Bombas de tiempo**

Parecidas en su estructura y funcionamiento a las bombas lógicas, las bombas de tiempo explotan en una fecha determinada. Son considerados programas ocultos destinados a activarse en una fecha memorable. Ejemplo: virus “Navidad”, el cual explota solo en fecha 25 de diciembre.

Frente a este problema destructivo, algunos usuarios deciden salir de la situación de peligro y adelantar el reloj del computador del día, simulando un 26 de Diciembre. Sin embargo, se crearon virus nuevos que actúan igualmente en esa fecha. Esta competencia entre dispositivos informáticos destructivos y antivirus así como trucos de programadores para desactivarlos o eliminarlos y usuarios por evadirlos es cada vez mayor y está en continuo crecimiento.

Y esto sucede a tal punto que en el año de 1996 existían alrededor de 10000 formas de virus informáticos.

**- Cáncer rutinario**

Se fabrica en forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse.

- **Gusanos electrónicos**

Son programas que viajan o se arrastran a través de un sistema informático interconectado borrando toda la información computarizada que encuentre a su paso, se diseminan mediante ordenadores anfitriones de la red, se cargan en la memoria de la computadora infectada introduciendo mensajes burlones, causando fallas de operación. Son también denominados “dispositivos informáticos polillas”, pues al introducirse en el ordenador destruyen la información borrándola, pudiendo auto replicarse.

Las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus; por ejemplo, un programa gusano que subsiguientemente se destruirá puede dar instrucciones a un sistema informático de una empresa comercial para que le envíe información de sus clientes deudores para posteriormente destruir esa información.

En noviembre de 1988, Robert Morris lanzó un programa “gusano” diseñado por él mismo para navegar en Internet, buscando debilidades en sistemas de seguridad informáticos, pudiendo multiplicarse y contagiar a otros computadores por sí solo. La expansión exponencial de este programa causó el consumo de los recursos de muchísimas computadoras. Más de 6.000 sistemas informáticos resultaron dañados o fueron seriamente perjudicados.

Eliminar el gusano de sus computadoras causó a las víctimas muchos días de improductividad y millones de dólares perdidos.

A causa del gran daño causado por este dispositivo informático, fue creado el Instituto CERT “Equipo de respuesta de emergencias computacionales” para combatir problemas similares en el futuro. El gusano producido por Morris no borra ni modifica archivos en la actualidad.

# CAPÍTULO VI

# PROYECTO DE REGLAMENTO DE LA POLICÍA INFORMÁTICA DENTRO DE LA LEY ORGÁNICA DE LA POLICÍA

## 6.1 UNIDAD ESPECIALIZADA

**6.1.1 Art. 1.- (OBJETO)** El departamento de la Policía Informática, es el encargado de la recepción y detección de los Delitos Informáticos, para investigar y capturar a aquel que haga uso fraudulento de las Tecnologías de la Información y la Comunicación que se encargan del estudio, desarrollo, implementación, almacenamiento y distribución de la información mediante la utilización de hardware y software, mediante técnicas especializadas, conforme a su estructura orgánica.

## 6.2 FUNCIONES DE LA POLÍCIA INFORMÁTICA

**6.2.1 Art. 2.- (DELITOS CONTRA EL PATRIMONIO)** Investigar y Denunciar la Comisión de los Delitos Contra el Patrimonio (hurto agravado) mediante la utilización de sistemas de transferencias electrónicas de fondos, de la telemática en general, o la violación del empleo de claves secretas, identificando, ubicando y capturando a los autores y cómplices, poniéndolos a disposición de la autoridad competente.

**6.2.2 Art.3.- (ALTERACIÓN DE DATOS)** Investigar y Denunciar la Comisión de los Delitos Informáticos en la modalidad de interferencia, acceso, copia

ilícita, alteración, daño o destrucción contenida en base de datos y otras que ponga en peligro la seguridad nacional, identificando, ubicando y capturando a los autores y cómplices, poniéndolos a disposición de la autoridad competente.

**6.2.3 Art.4.- (DELITOS CONTRA EL PUDOR Y LA LIBERTAD SEXUAL)** Investigar y Denunciar la Comisión de los delitos contra la libertad (ofensas al pudor público-pornografía infantil), ubicando y capturando a los autores y cómplices, poniéndolos a disposición de la autoridad competente.

**6.2.4 Art.5.- (REQUISITORIAS)** Solicitar las Requisitorias de las Personas plenamente identificadas, a quienes se les ha probado responsabilidad en la comisión de los delitos investigados.

**6.2.5 Art.6.- (REMISIONES)** Remitir a las Unidades Especializadas los Delitos que no son de su competencia y de cuya comisión se tenga conocimiento.

**6.2.6 Art. 7.- (DEFENSA NACIONAL)** Colaborar con la Defensa Interior del Territorio Nacional.

**6.2.7 Art.8.- (DEFENSA CIVIL)** Participar en las Acciones de Defensa Civil.

**6.2.8 Art. 9.- (DEFENSA ECONÓMICA)** Contribuir en el Desarrollo Socio-Económico Nacional.

**6.2.9 Art.11.- (OTRAS FUNCIONES)** Cumplir con las Funciones que le asigne el Comando Institucional (FELCC).

## 6.3 ESTRUCTURA ORGÁNICA DE LA POLÍCIA INFORMÁTICA

**6.3.1 Art. 12.- (DEPENDENCIA)** La Policía Informática es dependiente de la Fuerza Especial de Lucha Contra el Crimen, como unidad especializada técnico científica en la investigación de delitos informáticos.

**6.3.2 Art. 13.- (ORGANIZACIÓN)** Para el cumplimiento de sus funciones La Policía Informática se encuentra organizada de la siguiente manera:

**6.3.2.1 SECRETARÍA.-** Órgano administrativo, integrado por un secretario general, encargado de la recepción y derivamiento conforme la especialidad a los siguientes sub departamentos:

a) **DEPARTAMENTO DE INVESTIGACIÓN DELITOS TECNOLÓGICOS.-** Sección encargada de la investigación de delitos tecnológicos, informáticos, comunicaciones y otras tecnologías emergentes además de realizar el patrullaje virtual.

b) **DEPARTAMENTO DE INVESTIGACIÓN DE DELITOS ESPECIALES**.- Sección encargada de la investigación de hurtos de fondos o entidades financieras, pornografía infantil y piratería de software.

c) **DEPARTAMENTO DE COORDINACIÓN Y ANÁLISIS.-** Sección de la coordinación general, encargada de la base de datos en la búsqueda y análisis de información.

# CONCLUSIONES

Después de haber efectuado un análisis descriptivo de la realidad nacional con respecto al tratamiento de los delitos informáticos en la Policía Nacional, en base a estudios de gabinete y de campo, se tiene las siguientes conclusiones:

1) El Derecho, como producto cultural, es un instrumento que permanentemente está regulando las relaciones sociales, ya sea para resolver conflictos de intereses o para prevenirlos. Hoy, la transformación de la sociedad y las relaciones sociales como producto de la Revolución Tecnológica, ha dado lugar también a la creación y recreación del Derecho, dadas sus características como fenómeno social dinámico, generando como consecuencia, una Revolución Jurídica. Por ello debemos de preocuparnos en desarrollar y profundizar esta fascinante rama del Derecho Informático en sentido restringido, al presentar, nuevas instituciones como el presente trabajo, y fundamentos jurídicos que sustenten su regulación.

2) Frente a la generalización del uso de la Informática, se deben marcar límites en la conducta de los operadores a través del Derecho Penal. No se debe ir contra el principio de intervención mínima, pero, también se debe legislar acorde al principio de intervención suficiente. Considero que es necesaria, por ende, la tipificación penal del acceso no autorizado a los sistemas informáticos que en actualidad se ha vuelto insuficiente.

3) Se ha visto que uno de los aspectos que deben ser considerados por la legislación informática es la protección de los datos personales debido a la problemática que se presenta por un mal uso de las nuevas tecnologías informáticas. El uso inadecuado de la informática afecta

fundamentalmente la esfera de intimidad de la persona. Esta acción es una nueva forma de lesión a la intimidad, contra la cual se debe reaccionar inmediatamente desde el ámbito del Derecho.

4) Indudablemente, los tiempos han cambiado, nos encontramos en la era digital, ahora sí las huellas son digitales, se han cambiado las armas de fuego por los teclados, la herramienta de trabajo es una PC y se realizan autopsias en discos duros, el ciberdelincuente no está presente en el lugar del delito, puede estar a miles de kilómetros, la persecución policial es por el ciberespacio mediante el patrullaje virtual y cada día estos delincuentes evolucionan y tienen mayores conocimientos y habilidades con la tecnología y aunque no se conocen entre ellos, funcionan como una red, se corre la voz de un nuevo delito y lo ponen en práctica, ante esta realidad nos vemos en la imperiosa necesidad de que en este escenario surja una nueva raza de investigadores a los cuales denominaríamos: los Ciberpolicías.

5) Es importante que nos preparemos y más importante aún, es actualizarnos permanentemente, así como renovar los equipos y herramientas acorde al desarrollo tecnológico, que nos permitan estar en las mismas o en mejores condiciones para enfrentar con éxito el ciberdelito.

6) Estamos frente a personas que disponen de un poder potencialmente peligroso. El número de hackers aumenta debido a la relativa facilidad para serlo. Su accionar movido por razones políticas, económicas o de otra índole puede acarrear graves problemas, porque pueden disponer de unos de los bienes más preciados en la actualidad: la información.

# RECOMENDACIONES

La principal recomendación es la adecuada instauración de medidas de prevención para la población en general:

- ✓ Es necesario alertar a la población sobre estas intrusiones no autorizadas.
- ✓ El abuso de nuestra privacidad es un tema muy grave pero que poca gente conoce.
- ✓ La inmensa mayoría de las personas se mueven por Internet con una confianza muy inocente, pensando que están paseando de forma anónima, cuando en realidad está dejando todo tipo de huellas a su paso.

Para las Instituciones sean públicas o privadas cualquiera sea su naturaleza de funcionamiento son las siguientes:

- ✓ Se deben reducir los riesgos de una intrusión, mejorando permanentemente las medidas de seguridad, tanto las de detección como las de respuesta-corrección. Esto supone una actualización permanente ya que estos recursos suelen ser analizados y difundidas sus debilidades entre los hackers con mucha rapidez, convirtiéndolos en obsoletos.

# SUGERENCIAS

Como uno de los principales problemas de los delitos informáticos es la operavilidad desde cualquier punto del mundo se tiene la siguiente sugerencia:

- ✓ En un futuro no muy lejano tenga que existir algún órgano estatal o supranacional, que obtenga la cooperación de todos los usuarios para lograr una más eficiente prevención. Recabaría denuncias sobre accesos no autorizados a los sistemas, no revelando la identidad de la víctima. Sobre la base de esto elaboraría recomendaciones al usuario común, principalmente, sobre las medidas de seguridad a aplicar en su sistema informático.

En el ámbito del derecho la implementación de:

- ✓ En materia de Derecho Penal la introducción de un tipo Penal con relación a la Falsificación de Documentos Informáticos y Fraude en la Administración de Personas Jurídicas.

Debido a que el proceso de investigación tiene características particulares en la persecución de este tipo de delitos, se sugiere la incorporación de Fiscales especializados.

# BIBLIOGRAFÍA


- BOLIVIA. Ley N° 2615, octubre de 2008, Constitución Política del Estado, Edit. U.P.S., 2008, La Paz Bolivia.

- BOLIVIA. Ley N°1768 de 18 de marzo de 1997, Código Penal, Edit. U.P.S, 2001, La Paz, Bolivia.

- BOLIVIA. Ley N° 734 de 8 de abril de 1985, Ley Orgánica de la Policía Nacional, Edit. U.P.S., 2002, La Paz, Bolivia.

- BOLIVIA. Ley N°1632 de 5 de julio de 1995, Ley de Telecomunicaciones, Edit. U.P.S., 2005, La Paz, Bolivia.

- CUELLO CALON EUGENIO, Derecho Penal, Edit. Bosch, Buenos Aires, Argentina, 1985.

- GARCIA-PELAYO Y GROSS, “Larousse Diccionario”, Edit. Larousse, Madrid, España, 1993.

- JIMENEZ DE ASUA LUIS, “Principios de Derecho Penal”, Edit. Sudamericana, Buenos Aires Argentina, 1997.

- LEIVA JIJENA, “Delitos informáticos”, Edit. Libra, México, Monterrey, 1996.

- LIMA DE LA LUZ MARIA, “Delitos electrónicos”, Edit. Porrúa, México, 1984.

- LUÑO ANTONIO ENRIQUE, “Ensayo de Informática Jurídica”, Edit. Fontamar, México, 2005.

- MICROSOFT, “Enciclopedia Encarta”, Microsoft corporation, 1993 – 2005.

- MOLINA ROBERTO, MOLINA JUVENAL, CESPEDEZ JAIME,

- CASTAÑON CARLOS, “Historia de la Policía Nacional”, Tomos I y II, Edit. Cima, La Paz, Bolivia.

- OSSORIO MANUEL, “Policía de seguridad”, en Diccionario Jurídico Omeba, Edit. Driskill, Buenos Aires, Argentina, 1978, Tomo XXIII.

- OSSORIO MANUEL, “Diccionario de Ciencias Jurídicas, Políticas y Sociales”, Edit. Heliasta, Buenos Aires, Argentina, 2003.

- PACHECO KLEIN JORGE, “Introducción a los delitos informáticos en el ciberespacio”, Edit. Porroa, México 2003.

- POLICÍA NACIONAL, FELCCC, Cap. CLAURE EDSON, División de Delitos Informáticos.

- TELLEZ VALDEZ JULIO, “Derecho Informático”, Edit. Mac Graw Hill, México, 2003.

- www.wikipediaderechoinfor.com
- www.wikipedia/defincion.corrreoelectronico.org.htm

- www.wikipedia/defincion/redinformatica.org.com

- www.wikipedia/definicion/virtualinformatica.org.com.org.

- http://es.wikipedia.org/wiki/Delito_inform%C3%A1tico

- http://www.monografias.delinformatic. mlandav**.**org.com

- http://www.laprensa.com.bo/noticias/07-12-08/index.php

- http://orio.eui.upm.es/historia_informatica/ddoc/principal.htm

# ANEXOS

# Investigación judicial en los delitos informáticos

La investigación policial y judicial de la delincuencia vinculada a las TIC se caracteriza, desde el punto de vista probatorio, por que se suele lograr demostrar sus modalidades delictivas mediante las pericias que analizan los rastros que los delitos dejan en la Red. La información buscada y la cadena de transmisión de las acciones atacantes del infractor se encuentran en los sistemas informáticos, por lo que su obtención, desde una perspectiva jurídica, afecta a la privacidad y los derechos fundamentales del imputado, que exige máximas garantías constitucionales. Ésta es una delincuencia cuya prueba obliga a una intervención activa del juez instructor en su papel de juez de garantías.

La inmensidad y universalidad de contenidos en la Red, y la gran cantidad de técnicas para anonimizar, borrar, suplantar o intermediar la conducta delictiva, hacen indispensable la denuncia. El rastreo ha sido cuestionado ya en algunas investigaciones que han afectado al mundo virtual, al considerar que entrar en la Red y descubrir los iniciales vestigios del delito podría ser ilícito si no se autoriza con un mandamiento judicial, porque se vulneraría el derecho al secreto de las comunicaciones, algo que ya ha sido descartado por el Tribunal Supremo.

Donde sí hay privacidad es en los archivos con los contenidos privados. La cesión al investigador de estos datos mediante la intervención judicial posibilita la conexión del ataque informático con una ubicación geográfica y con una persona que los delincuentes pueden enmascarar, pero permiten continuar el rastro del ataque y el acceso a vestigios que aportan material imprescindible al investigador. En cuanto a la ubicación física del PC desde el que ha podido venir el ataque informático, exige la intervención del juez de instrucción, desde la óptica de la protección de la inviolabilidad domiciliaria. El clonado del disco duro es una garantía de que lo que se copia es imagen fiel de lo que se ocupa, y debe vincularse a la obtención de la fuente de prueba. Por último, la cadena de custodia es el proceso mediante el que el objeto de la pericia es transmitido sin modificación desde que se ocupa hasta que se analiza pericia.

Autor: Eloy Velasco. | Fecha: 01/06/2009

# INFORME PERICIAL

El informe pericial es el documento redactado por el perito informático, en el que se exponen las conclusiones obtenidas por el experto, tras la **investigación** de un caso de **delito informático.**

El Informe pericial debe incluir:

- Los datos del cliente.
- Los objetivos de la investigación.
- La declaración previa del **perito informático**, en la que se establecen los principios de profesionalidad, veracidad e independencia.
- Documentación sobre el proceso de adquisición de pruebas.
- Detalle de las acciones que el perito informático lleva a cabo durante la investigación.
- Resultados de la **investigación informática** y conclusiones.

La elaboración del informe consta a su vez de tres fases:

1. Fase de adquisición de las pruebas:

   Recogida de todos elementos que van a intervenir en la investigación. Es importante que el proceso de intervención de los equipos informáticos se lleve a cabo con todas las garantías para las partes. La documentación del proceso de adquisición de las pruebas es una información que debe formar parte del **informe pericial**.

2. Fase de la investigación:

   El perito informático realiza un análisis exhaustivo de los equipos informáticos, especialmente de las unidades de almacenamiento de datos en busca de todos aquellos elementos que puedan constituir prueba o evidencia electrónica en el caso en cuestión.

   Constarán en el informe todos las acciones realizadas durante la fase de investigación, como las herramientas empleadas para la adquisición de la evidencia electrónica y el detalle y resultado de los procesos efectuados sobre el dispositivo o unidad que se está analizando.

3. Fase de elaboración de la memoria.

   Tras el minucioso estudio de la información almacenada en los dispositivos, intervenidos en la fase de adquisición de pruebas, el perito

informático analiza los resultados obtenidos con el fin de extraer las conclusiones finales de la investigación.

En esta última fase, el perito informático recopila la información que ha obtenido durante todo el proceso de investigación y redacta el informe o memoria que se presentará ante los Tribunales. En algunas ocasiones, un buen **informe pericial** elaborado por Recovery Labs ha llevado a las partes a adoptar un acuerdo, sin que el juicio llegue a celebrarse.

**RECOVERY LABS © 2009 –**

# SEGURIDAD CONTRA LOS DELITOS INFORMÁTICOS

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

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

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

Para guardar objetos seguros, es necesario lo siguiente:

- La autenticación (promesa de identidad), es decir la prevención de suplantaciones, que se garantice que quien firma un mensaje es realmente quien dice ser.
- La autorización (se da permiso a una persona o grupo de personas de poder realizar ciertas funciones, al resto se le niega el permiso y se les sanciona si las realizan)

- La privacidad o confidencialidad, es el más obvio de los aspectos y se refiere a que la información solo puede ser conocida por individuos autorizados. Existen infinidad de posibles ataques contra la privacidad, especialmente en la comunicación de los datos. La transmisión a través de un medio presenta múltiples oportunidades para ser interceptada y copiada: las líneas "pinchadas" la intercepción o recepción electromagnética no autorizada o la simple intrusión directa en los equipos donde la información está físicamente almacenada.
- La integridad de datos, La integridad se refiere a la seguridad de que una información no ha sido alterada, borrada, reordenada, copiada, etc., bien durante el proceso de transmisión o en su propio equipo de origen. Es un riesgo común que el atacante al no poder descifrar un paquete de información y, sabiendo que es importante, simplemente lo intercepte y lo borre.
- La disponibilidad de la información, se refiere a la seguridad que la información pueda ser recuperada en el momento que se necesite, esto es, evitar su pérdida o bloqueo, bien sea por ataque doloso, mala operación accidental o situaciones fortuitas o de fuerza mayor.
- No rechazo (la protección contra alguien que niega que ellos originaron la comunicación o datos).
- Controles de acceso, esto es quien tiene autorización y quien no para acceder a una pieza de información determinada.

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

requerimientos para el mundo de la red, sino también para el mundo físico.

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

| Intereses | Requerimientos |
|---|---|
| Fraude | Autenticación |
| Acceso no Autorizado | Autorización |
| Curiosear | Privacidad |
| Alteración de Mensaje | Integridad de Datos |
| Desconocido | No - Rechazo |

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

**Medidas de seguridad de la red.**

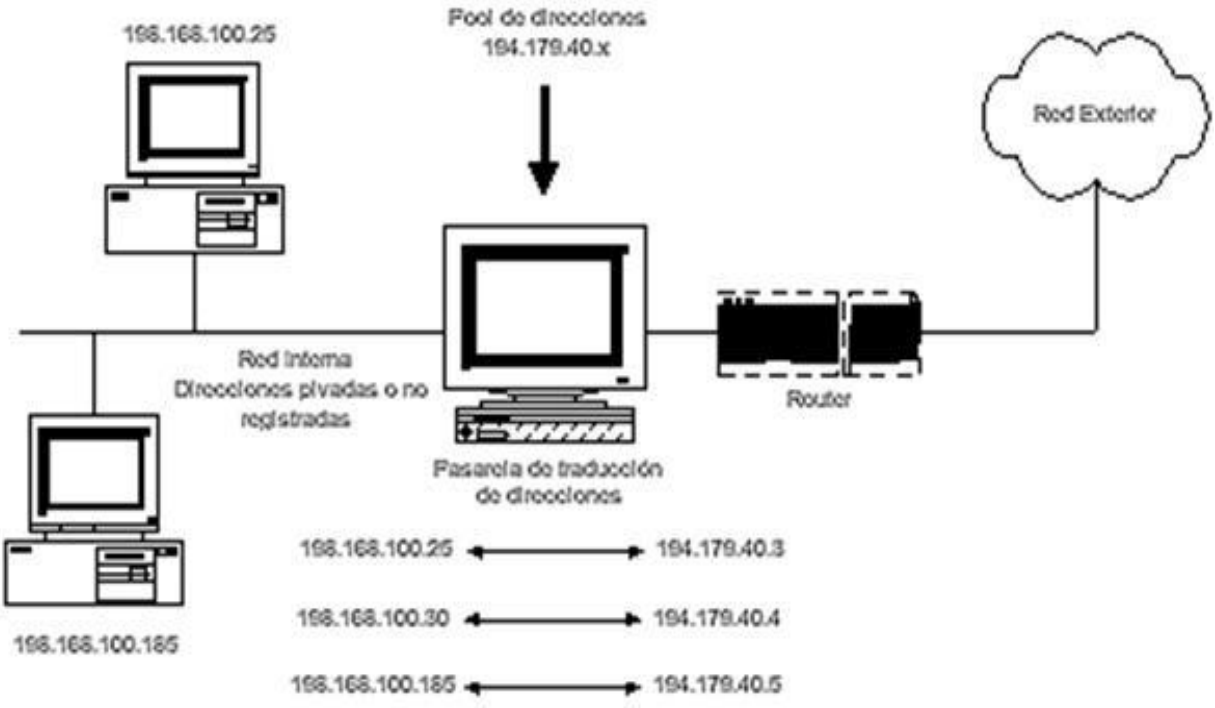
Existen numerosas técnicas para proteger la integridad de los sistemas. Lo primero que se debe hacer es diseñar una política de seguridad. En ella, definir quiénes tienen acceso a las diferentes partes de la red, poner protecciones con contraseñas adecuadas a todas las cuentas, y preocuparse de hacerlas cambiar

periódicamente (Evitar las passwords "por defecto" o demasiado obvias).

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

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

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



Cortafuegos filtro de paquetes ejemplarizado en un router.

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

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

Firma digital.

El cifrado con clave pública permite generar firmas digitales que hacen posible certificar la procedencia de un mensaje, en otras palabras, asegurar que proviene de quien dice.

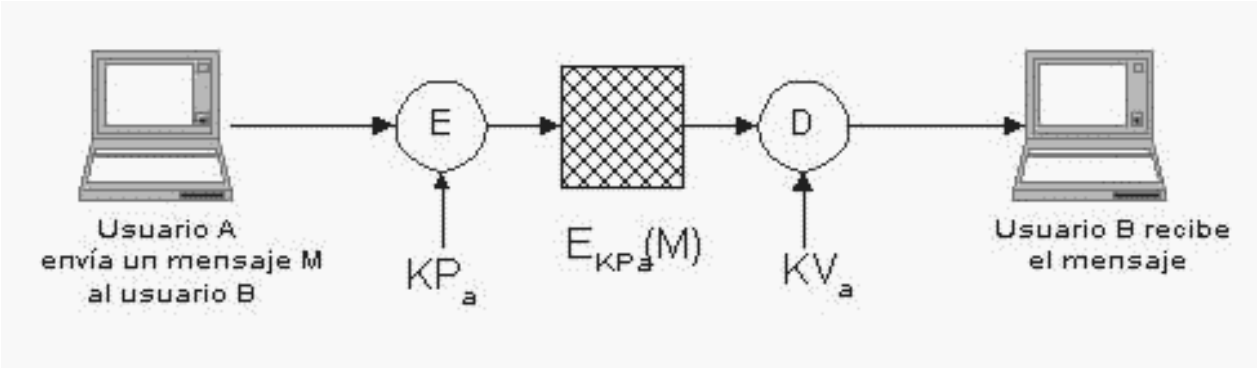
De esta forma se puede evitar que alguien suplante a un usuario y envíe mensajes falsos a otro usuario, por la imposibilidad de falsificar la firma. Además, garantizan la integridad del mensaje, es decir, que no ha sido alterado durante la transmisión. La firma se puede aplicar a un mensaje completo o puede ser algo añadido al mensaje.

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

Existen varios métodos para hacer uso de la firma digital, uno de ellos es el siguiente: "quien envía el mensaje lo codifica con su clave privada. Para descifrarlo, sólo puede hacerse con la clave pública

correspondiente a dicha persona o institución. Si efectivamente con dicha clave se descifra es señal de que quien dice que envió el mensaje, realmente lo hizo".

Firma digital formada encriptando con la clave privada del emisor:




Firma Digital y Autentificación

E: Encriptar / D: Desencriptar.

KP : Encriptación utilizando la Clave Privada.

KV : Encriptación utilizando la Clave Pública.

M : Mensaje.

Seguridad en WWW.

Para hacer un formulario se debe tener un servidor seguro.

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

La red es totalmente pública y abierta, los paquetes pasan por máquinas de las que no se tiene conocimiento y a las que puede tener acceso la gente que le guste husmear el tráfico de la red. Si es así (y no tienen que ser necesariamente hackers malintencionados, algunos proveedores de servicio lo hacen) sólo se puede recurrir a

encriptar el tráfico por medio, en WWW, de servidores y clientes seguros.

**Política de seguridad.**

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

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

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

Para asegurar una red adecuadamente, no solamente se necesita un profundo entendimiento de las características técnicas de los protocolos de red, sistemas operativos y aplicaciones que son accesadas, sino también lo concerniente al planeamiento. El plan es

el primer paso y es la base para asegurar que todas las bases sean cubiertas.

## ¿Por qué se necesita una política de seguridad?

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

Aún cuando se tenga las habilidades y experiencia necesaria para configurar el firewall correctamente, será difícil conocer la administración de riesgos que está dispuesto a tomar con los datos y determinar la cantidad de inconveniencias a resistir para protegerlos. También se debe considerar cómo asegurar los hosts que están siendo accesados. Incluso con la protección de firewall, no hay garantía que no se pueda desarrollar alguna vulnerabilidad. Y es muy probable que haya un dispositivo en peligro.

Los modems, por ejemplo, pueden proveer un punto de acceso a su red que completamente sobrepase su firewall. De hecho, un firewall puede aumentar la probabilidad que alguien establecerá un módem para el acceso al Internet mediante otro ISP (ISP - Internet Service Providers, cualquier empresa o institución que provea de conexión a Internet), por las restricciones que el firewall puede imponer sobre ellos (algo para recordar cuando se empieza a configurar su firewall).

Se puede proveer restricciones o "protección," que puede resultar ser innecesario una vez que las consecuencias se entienden claramente como un caso de negocio. Por otra parte, los riesgos pueden justificar el incremento de restricciones, resultando incómodo. Pero, a menos que el usuario esté prevenido de estos peligros y entienda claramente las consecuencias para añadir el riesgo, no hay mucho que hacer.

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

Asegurar sus datos involucra algo más que conectarse en un firewall con una interface competente. Lo que se necesita es un plan comprensivo de defensa. Y se necesita comunicar este plan en una manera que pueda ser significativo para la gerencia y usuarios finales.

Esto requiere educación y capacitación, conjuntamente con la explicación, claramente detallada, de las consecuencias de las violaciones. A esto se le llama una "política de seguridad" y es el primer paso para asegurar responsablemente la red. La política puede incluir instalar un firewall, pero no necesariamente se debe diseñar su política de seguridad alrededor de las limitaciones del firewall.

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

La gerencia debe decidir finalmente cuánto de riesgo debe ser tomado con el activo de la compañía, y cuánto se debería gastar en

ambos, en dólares e inconvenientes, a fin de minimizar los riesgos. Es responsabilidad del personal técnico asegurar que la gerencia comprenda las implicaciones de añadir acceso a la red y a las aplicaciones sobre la red, de tal manera que la gerencia tenga la suficiente información para la toma de decisiones. Si la política de seguridad no viene desde el inicio, será difícil imponer incluso medidas de seguridad mínimas.

Por ejemplo, si los empleados pueden llegar a alterarse si ellos imprevistamente tienen que abastecer logins y contraseñas donde antes no lo hacían, o están prohibidos particulares tipos de acceso a Internet. Es mejor trabajar con estos temas antes de tiempo y poner la política por escrito. Las políticas pueden entonces ser comunicadas a los empleados por la gerencia. De otra forma, los empleados no lo tomarán en serio, o se tendrán batallas de políticas constantes dentro de la compañía con respecto a este punto. No solamente con estas batallas tendrán un impacto negativo sobre la productividad, es menos probable que la decisión tomada racionalmente pueda ser capaz de prevalecer en la vehemencia de las guerras políticas.

El desarrollo de una política de seguridad comprende la identificación de los activos organizativos, evaluación de amenazas potenciales, la evaluación del riesgo, implementación de las herramientas y tecnologías disponibles para hacer frente a los riesgos, y el desarrollo de una política de uso.

Debe crearse un procedimiento de auditoria que revise el uso de la red y servidores de forma periódica.

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

Por ejemplo:

- Hardware: ordenadores y equipos de telecomunicación

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

Valoración del riesgo:

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

**Definición de una política de uso aceptable:**

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

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

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

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

**AUTOR:**
**http://www.recoverylabs.com/servicios/inv.informatica.htm**