UNIVERSIDAD MAYOR DE SAN ANDRES
FACULTAD DE CIENCIAS JURIDICAS Y POLITICAS
CARRERA DE DERECHO

Acreditada por Resolución CEUB Nº 1126/02

MONOGRAFIA
(PARA OPTAR AL GRADO DE LICENCIATURA EN DERECHO)

Tutor: Dr. MARCELO FERNANDEZ IRAOLA

Postulante: MORALES CUBA RICHARD ALCIDES

TITULO:

"FUNDAMENTOS JURIDICOS SOCIALES PARA REGLAMENTAR LA CREACION Y CAPACITACION DE LA POLICIA ESPECIALIZADA EN INFORMATICA PARA LA REPRESION Y PREVENCION DE LOS DELITOS INFORMATICOS"

La Paz –Bolivia, 19 de AGOSTO de 2011

Dedicatoria

A Dios Todopoderoso por

darme fortaleza y perseverancia.

A mis Padres Mario y Olimpia por su apoyo durante

las etapas de mi vida.

A mi Esposa e hijos

por fortalecer

mis anhelos y proyectos soñados

evitando mi desistimiento en proyectos iniciados.

Richard Alcides Morales Cuba

ÍNDICE GENERAL

CAPITULO IV: LOS DELITOS INFORMATICOS: CONCEPTOS, CARACTERISTICAS Y SUJETOS:

INTRODUCCIÓN.

El presente trabajo pretende abordar y plantear una problemática socio-jurídica emergente del aumento y desarrollo de las tecnologías en informática, que ha ido generando un inusual incremento y sofisticación en la aparición de nuevas figuras delictivas, con denominativos propios y nuevos, sus efectos delictivos se ven reflejados en la comunidad y población que hace uso de estos adelantos tecnológicos informáticos, siendo los mismos victimas día a día de estos nuevos y modernos delincuentes con la aparición del denominado "*internet o dominio web*", estos delincuentes "*cibernautas*" han ido perfeccionando sus formas y actuaciones delictivas, valiéndose de esta tecnología como el medio adecuado y propicio para cometer tipos delictivos de diferente naturaleza u "*modus operandum*", que describiremos paso a paso en este trabajo. La aparición de esta potencial tecnología está siendo utilizada como conducto y medio para quienes aprovechando las ventajas globales que ofrece la red informática cometen una serie de ilícitos penales que muchas veces no están contempladas en los ordenamientos jurídicos de países como el nuestro, es ahí donde nace la iniciativa de replantear esquemas coyunturales de lucha contra este nuevo tipo de criminales sobre bases científicas y tecnológicas, de adecuar y/o modernizar nuestra policía con adelantos tecnológicos y científicos de avanzada para alcanzar una labor eficaz y pronta en el manejo informático de la investigación de delitos, convirtiéndola en una necesidad social urgente, una nueva y reestructurada policía, con el personal calificado, con peritos expertos en la materia al servicio y esclarecimiento de los casos investigativos, actualizados constantemente en el manejo y operación de nuevas técnicas sobre todo en informática investigativa, solo así podremos estar preparados para reprimir la aparición de nuevas figuras delictivas tan sofisticadas en su realización que casi no dejan pistas algunas.

La rapidez con la que ingreso esta revolución informática a la comunidad mundial dejo en muchos casos atrasados y obsoletos a nuestros mecanismos de seguridad y control en materia de prevención de delitos, nuestra policía desprovista de los

medios, de infraestructura, de estrategias modernas, del personal capacitado y de una constante actualización en lo que se refiere al aspecto comprehensivo de conocimientos en materia investigativa informática tendientes a hacer frente a este nuevo reto, nos presenta un panorama de inseguridad y desprotección frente al actuar de estos "*modernos delincuentes cibernéticos*" que están situados en el mundo entero frente a un ordenador o computadora con el único propósito de sacar provecho y ventaja de sus conocimientos y aplicarlos en contra de una sociedad desprotegida y desprevenida para apoderarse ilegalmente en la mayoría de los casos de información valiosa u otras figuras como son: "*el saqueo de cuentas bancarias, la estafa virtual, el sabotaje, el espionaje industrial, terrorismo virtual, la pornografía infantil, el robo de identidad* " entre otras, siendo miles de víctimas hasta ahora carentes de protección jurídica y policial.

También mencionar que en el desarrollo del trabajo pretendemos rescatar los aportes que la Informática en general nos proporciona y en especial el Derecho Informático pone a nuestro alcance a través de sus conocimientos científicos para determinar a los delitos informáticos en el ordenamiento legal boliviano, estableciendo esa relación intrínseca entre el derecho y la informática proveniente del conjunto de principios y normas que regulan sus efectos jurídicos describiendo a los diferentes tipos de delitos informáticos, para posteriormente dar lugar a la propuesta e importancia de reglamentar la creación de una "*Policía Informática especializada en delitos informáticos"* en nuestro país, dotada de todos los elementos científicos y adelantos tecnológicos que existen hoy en día, del personal humano en continua capacitación y preparación como política permanente de Estado de lucha contra el crimen, teniendo la misión fundamental de frenar y disminuir el avance del "*crimen cibernético"*.

CAPITULO I
DIAGNOSTICO HISTORICO - TEORICO

1.1. AVANCE E HISTORIA DE LA RED DEL INTERNET.

La historia de Internet se remonta al temprano desarrollo de las redes de comunicación. La idea de una red de computadoras diseñada para permitir la comunicación general entre usuarios de varias computadoras sea tanto desarrollos tecnológicos como la fusión de la infraestructura de la red ya existente y los sistemas de telecomunicaciones.

Las más antiguas versiones de estas ideas aparecieron a finales de los años cincuenta. Implementaciones prácticas de estos conceptos empezaron a finales de los ochenta y a lo largo de los noventa. En la década de 1980, tecnologías que reconoceríamos como las bases de la moderna Internet, empezaron a expandirse por todo el mundo. En los noventa se introdujo la World Wide Web (WWW), que se hizo común.

La infraestructura de Internet se esparció por el mundo, para crear la moderna red mundial de computadoras que hoy conocemos. Atravesó los países occidentales e intentó una penetración en los países en desarrollo, creando un acceso mundial a información y comunicación sin precedentes, pero también una brecha digital en el acceso a esta nueva infraestructura. Internet también alteró la economía del mundo entero.

Para Thomas L. Friedman, el Internet recién empezó a gestarse a raíz de una reacción norteamericana en fecha 4 octubre 1957, luego del lanzamiento del satélite ruso Sputnik, que pesaba solamente 184 libras y tenía un tamaño más o menos como el de una pelota de basquetbol, este satélite fue enviado al espacio en un

cohete soviético que no solamente conmocionó la era espacial sino que conmocionó la era del ciberespacio.[1]

Un método de conectar computadoras, prevalente sobre los demás, se basaba en el método de la computadora central o unidad principal, que simplemente consistía en permitir a sus terminales conectarse a través de largas líneas alquiladas. Este método se usaba en los años cincuenta por el Proyecto RAND para apoyar a investigadores como Herbert Simon, en Pittsburgh (Pensilvania), cuando colaboraba a través de todo el continente con otros investigadores de Santa Mónica (California) trabajando en demostración automática de teoremas e inteligencia artificial.

Un pionero fundamental en lo que se refiere a una red mundial, J.C.R. Licklider, comprendió la necesidad de una red mundial, según consta en su documento de enero, 1960, Man-Computer Symbiosis (Simbiosis Hombre-Computadora), "*una red de muchos ordenadores, conectados mediante líneas de comunicación de banda ancha", las cuales proporcionan* "*las funciones hoy existentes de las bibliotecas junto con anticipados avances en el guardado y adquisición de información y otras funciones simbióticas*" [2]

La primera conexión ARPANET fuera de los Estados Unidos se hizo con NORSAR en Noruega en 1973, justo antes de las conexiones con Gran Bretaña. Todas estas conexiones se convirtieron en TCP/IP en 1982, al mismo tiempo que el resto de las ARPANET. En 1984 América empezó a avanzar hacia un uso más general del TCP/IP, y se convenció al CERNET para que hiciera lo mismo. El CERNET, ya convertido, permaneció aislado del resto de Internet, formando una pequeña Internet interna.

---

[1] FRIEDMAN L., Thomas, "The Lexus And The Alive Tree", Farrar Straus & Giroux, 1999.

[2] J.C.R.LICKLIDER, "Man Computer Symbiosis", http.//groups.csail.mit.edu/medg/people/psz/Licklider, html.

Al mismo tiempo que se producía el ascenso de la interconexión en Europa, se formaron conexiones hacia el ARPA y universidades australianas entre sí, basadas en varias tecnologías como X.25 y UUCPNet. Éstas estaban limitadas en sus conexiones a las redes globales, debido al coste de hacer conexiones de marcaje telefónico UUCP o X.25 individuales e internacionales. En 1990, las universidades australianas se unieron al empujón hacia los protocolos IP para unificar sus infraestructuras de redes. AARNet se formó en 1989 por el Comité del Vice-Canciller Australiano y proveyó una red basada en el protocolo IP dedicada a Australia.

En Europa, habiendo construido la JUNET (Red Universitaria canadesa) una red basada en UUCP en 1984, Japón continuó conectándose a NSFNet en 1989 e hizo de anfitrión en la reunión anual de The Internet Society, INET'92, en Kōbe. Singapur desarrolló TECHNET en 1990, y Thailandia consiguió una conexión a Internet global entre la Universidad de Chulalongkorn y UUNET en 1992.[3]

Otra versión con gran aceptación nos dice que los inicios de Internet nos remontan a los años 60. En plena guerra fría, Estados Unidos crea una red exclusivamente militar, con el objetivo de que, en el hipotético caso de un ataque ruso, se pudiera tener acceso a la información militar desde cualquier punto del país. Esta red se creó en 1969 y se llamó ARPANET. En principio, la red contaba con 4 ordenadores distribuidos entre distintas universidades del país. Dos años después, ya contaba con unos 40 ordenadores conectados. Tanto fue el crecimiento de la red que su sistema de comunicación se quedó obsoleto. Entonces dos investigadores crearon el Protocolo TCP/IP, que se convirtió en el estándar de comunicaciones dentro de las redes informáticas (actualmente seguimos utilizando dicho protocolo).[4]

[3] SEGAL, Ben, "A Short History of Internet Protocolo at CERN", (1995).

[4] INTERNET HISTORY IN ASIA, "Advanced Network Conference in Busan", 16th APAN Meetings, 2005.

ARPANET siguió creciendo y abriéndose al mundo, y cualquier persona con fines académicos o de investigación podía tener acceso a la red. Las funciones militares se desligaron de ARPANET y fueron a parar a MILNET, una nueva red creada por los Estados Unidos. La NSF (National Science Fundation) crea su propia red informática llamada NSFNET, que más tarde absorbe a ARPANET, creando así una gran red con propósitos científicos y académicos. El desarrollo de las redes fue abismal, y se crean nuevas redes de libre acceso que más tarde se unen a NSFNET, formando el embrión de lo que hoy conocemos como INTERNET.

En 1985 la Internet ya era una tecnología establecida, aunque conocida por unos pocos. El autor William Gibson hizo una revelación: el término "*ciberespacio*". En ese tiempo la red era básicamente textual, así que el autor se basó en los videojuegos. Con el tiempo la palabra "*ciberespacio*" terminó por ser sinónimo de Internet. El desarrollo de NSFNET fue tal que hacia el año 1990 ya contaba con alrededor de 100.000 servidores.

En el Centro Europeo de Investigaciones Nucleares (CERN), Tim Berners Lee dirigía la búsqueda de un sistema de almacenamiento y recuperación de datos. Berners Lee retomó la idea de Ted Nelson (un proyecto llamado "*Xanadú*") de usar hipervínculos. Robert Caillau quien cooperó con el proyecto, cuenta que en 1990 deciden ponerle un nombre al sistema y lo llamarón World Wide Web (WWW) o telaraña mundial.

La nueva fórmula permitía vincular información en forma lógica y a través de las redes. El contenido se programaba en un lenguaje de hipertexto con "*etiquetas*" que asignaban una función a cada parte del contenido. Luego, un programa de computación, un intérprete, era capaz de leer esas etiquetas para desplegar la información. Ese intérprete sería conocido como "*navegador*" o "*browser*".

En 1993 Marc Andreesen produjo la primera versión del navegador "*Mosaic*", que permitió acceder con mayor naturalidad a la WWW. La interfaz gráfica iba más allá de lo previsto y la facilidad con la que podía manejarse el programa abría la red a los legos. Poco después, Andreesen encabezó la creación del programa Netscape.

A partir de entonces, Internet comenzó a crecer más rápido que otro medio de comunicación, convirtiéndose en lo que hoy todos conocemos. Podemos definir a Internet como una "*red de redes*", es decir, una red que no sólo interconecta computadoras, sino que interconecta redes de computadoras entre sí. Una red de computadoras es un conjunto de máquinas que se comunican a través de algún medio (cable coaxial, fibra óptica, radiofrecuencia, líneas telefónicas, etc.) con el objeto de compartir recursos.[5]

De esta manera, Internet sirve de enlace entre redes más pequeñas y permite ampliar su cobertura al hacerlas parte de una " *red global* ". Esta red global tiene la característica de que utiliza un lenguaje común que garantiza la intercomunicación de los diferentes participantes; este lenguaje común o protocolo (*un protocolo es el lenguaje que utilizan las computadoras al compartir recursos*) se conoce como TCP/IP.

Aunque el uso comercial estaba prohibido, su definición exacta era subjetiva y no muy clara. Todo el mundo estaba de acuerdo en que una compañía enviando una factura a otra compañía era claramente uso comercial, pero cualquier otro asunto podía ser debatido. UUCPNet y la IPSS X.25 no tenían esas restricciones, que eventualmente verían la excepción oficial del uso de UUCPNet en conexiones ARPANET y NSFNet. A pesar de ello, algunas conexiones UUCP seguían conectándose a esas redes, puesto que los administradores hacían la vista gorda ante su funcionamiento.

Durante los finales de los años ochenta se formaron las primeras compañías Internet Service Provider (ISP). Compañías como PSINet, UUNET, Netcom, y Portal Software se formaron para ofrecer servicios a las redes de investigación regional y dar un

[5] BARAN, Paul, "The Origins of the Internet", http//www.rand.org/about/history/baran. Html, Enero de 2006.

acceso alternativo a la red, e-mail basado en UUCP y Noticias Usenet al público. El primer ISP de marcaje telefónico, world.std.com, se inauguró en 1989.

Esto causó controversia entre los usuarios conectados a través de una universidad, que no aceptaban la idea del uso no educativo de sus redes. Los ISP comerciales fueron los que eventualmente bajaron los precios lo suficiente como para que los estudiantes y otras escuelas pudieran participar en los nuevos campos de educación e investigación.

Para el año 1990, ARPANET había sido superado y reemplazado por nuevas tecnologías de red, y el proyecto se clausuró. Tras la clausura de ARPANET, en 1994, NSFNet, actualmente ANSNET (Advanced Networks and Services, Redes y Servicios Avanzados) y tras permitir el acceso de organizaciones sin ánimo de lucro, perdió su posición como base fundamental de Internet. Ambos, el gobierno y los proveedores comerciales crearon sus propias infraestructuras e interconexiones. Los NAPs regionales se convirtieron en las interconexiones primarias entre la multitud de redes y al final terminaron las restricciones comerciales.

La historia del correo electrónico se dio al considerarla como la aplicación de Internet; aunque realmente, el e-mail ya existía antes de Internet y fue una herramienta crucial en su creación. Empezó en 1965 como una aplicación de ordenadores centrales a tiempo compartido para que múltiples usuarios pudieran comunicarse.[6] La red de computadoras de ARPANET hizo una gran contribución en la evolución del correo electrónico. Existe un informe que indica transferencias de e-mail entre sistemas experimentales poco después de su creación. Ray Tomlinson inició el uso del signo @ para separar los nombres del usuario y su máquina, en 1971.[7]

[6] THE RISKS DIGEST, "Great moments in e-mail history", html//catless.ncl.ac.uk, 27 de abril de 2006.

[7] THE FIRST NETWORK EMAIL, http://openmap.bbn.com.html, 23 de diciembre de 2005.

1.2. RIESGOS EN LA RED INFORMATICA.

A medida que la Web creció, los riesgos de la actuación de delincuentes llamados cibernéticos fueron cada vez mayores la mayor parte de ellos refugiados en el anonimato, se constituyeron en una amenaza para la libertad de información que inspiraba la red desde su creación, es por eso que diferentes países fueron implementando medidas para frenar y desactivar la aparición de estos hackers informáticos, medidas que en cierta medida fueron paliando las necesidades de brindar seguridad en el manejo de la información que se hacía en la red, naturalmente el delito que se propagaba en el mundo informático no le fue ajeno a nuestro país y las consecuencias las hemos ido observando a lo largo de este último periodo que la red ingreso con su enorme potencial a los potenciales usuarios en nuestro país.

El verdadero peligro del uso de la Internet, radica en que el acceso a la información del mundo se encuentra al alcance de cualquier persona con acceso a la red, siendo que, la difamación, el contenido violento o pornográfico y su distribución son prácticamente masivos y libres en todo el mundo. En este sentido, muchos países pretendieron aplicar sus legislaciones nacionales para impedir este tipo de contenidos nocivos a la niñez y juventud, sin embargo, el desarrollo tecnológico de la Internet no permite una restricción jurídica a un hecho tecnológico avasallante como es el mismo.[8]

El hecho tecnológico que se manifiesta con el avance de la informática y los medios informáticos en constante evolución, vienen a modificar las relaciones entre los sujetos debido a la irrupción de nuevas modalidades y distintos procedimientos, más veloces y precisos que nos han conducido a no identificar necesariamente los títulos circulatorios o el contrato con el papel que lo contiene en vías de reemplazo por el

[8] ARCE JOFRE, José Alfredo, "Informática y Derecho", Edit. Bolivia Dos Mil, Pág. 24.

documento electrónico. La pregunta que cabe formularse es si el documento electrónico puede ser considerado una cosa.[9]

El intercambio de información elaborada con base en los grandes avances tecnológicos representa un gran reto para las normas de las naciones. Reto que debe ser afrontado con agilidad pero con cuidado, con el fin de facilitar la incorporación de la nueva tecnología las transacciones y procesos tradicionales, manteniendo un sistema confiable y simple.[10]

Una nueva forma de vida se estaba desarrollando, Internet era la tecnología que estaba introduciendo nuevos cambios al estilo de vida; el comercio electrónico, comúnmente llamado "*e-commerce*", se hizo presente en número considerable de negocios. La sociedad ha tenido que adaptarse a estos cambios a los cuales legisladores, abogados e instituciones nacionales e internacionales no son ajenos, manifestando una preocupación con relación a los aspectos que requieren de reglamentación.[11]

1.3. LA LIBERTAD DE EXPRESION EN INTERNET.

Uno de los rasgos fundamentales que fue adquiriendo la red informática o Internet luego de sus inicios es justamente la libertad de expresión y la libertad de información, una libertad entendida en el sentido propio del uso correcto del bagaje de información disponible, libertad desde el punto de vista de la propagación de ideas, pensamientos, teorías, opiniones, etc. sin la censura correspondiente, pero además en muchos de los casos aparejada del término gratuidad en la obtención de dicha información, libertad que pretendemos no atropellar con la propuesta de

[9] JURISPRUDENCIA ARGENTINA, "Documento Electrónico", Tomo II. Año 1999, pág. 851.

[10] LORENZETTI L., Ricardo, "Comercio Electrónico", ed. Abeledo-Perrot. Bs. As. Argentina, Pág. 70.

[11] LORENZETTI L., Ricardo, **Ob. Cit**., Pág. 42.

reglamentar la creación de una Policía Informática, pero la libertad de expresión a través del Internet debe entenderse, tanto como la posibilidad que tienen los usuarios de comunicarse entre sí, así como la de hacer circular y tener acceso a la información e ideas difundidas por otros usuarios. Esa libertad no significa una falta de regulación en casos como pornografía infantil, violación de la intimidad en el tratamiento de datos personales, estafa virtual, incremento en el fomento del terrorismo, violación de las comunicaciones personales, sabotaje informático, entre otras. La libertad de expresión vista desde el punto de vista de nuestra realidad jurídica se expresa textualmente en nuestro ordenamiento jurídico, el artículo 21 numerales 5 y 6 de la Constitución Política del Estado que la transcribimos:

CAPÍTULO TERCERO

DERECHOS CIVILES Y POLÍTICOS

SECCIÓN UNO

DERECHOS CIVILES

Artículo 21. Las bolivianas y los bolivianos tienen los siguientes derechos:

5. A expresar y difundir libremente pensamientos u opiniones por cualquier medio de comunicación, de forma oral, escrita o visual, individual o colectiva.

6. Acceder a la información, interpretarla, analizarla y comunicarla libremente, de manera individual o colectiva.[12]

Por su parte, el Pacto de San José de Costa Rica, establece una regulación muy precisa sobre la libertad de pensamiento y expresión, la cual se configura como un derecho de doble vía, que comprende por una parte: el derecho al acceso a la información y por otro el derecho a la libertad de expresión y difusión. Dicho "*derecho*

[12] CONSTITUCIÓN POLÍTICA DEL ESTADO, Gaceta Oficial de Bolivia, 7 Feb. 2009, La Paz Bolivia, Pág. 14.

de dos vías", se configura en el numeral 1º del artículo13 del Pacto de Derechos Humanos, que a la letra dice: "*toda persona tiene derecho a la libertad de pensamiento y de expresión. Éste derecho comprende la libertad de buscar, recibir y difundir información e ideas de toda índole. Sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección*".[13]

Por otro lado, el derecho a la información, libertad de pensamiento, expresión, tal cual se encuentra establecido en el referido Pacto, al igual que la generalidad de los derechos y bienes jurídicamente tutelados, se encuentra limitado en su ejercicio, estableciendo que el ejercicio de dichos derechos, no puede estar sujeto a previa censura sino a responsabilidades ulteriores, las que deben estar expresamente fijadas por la ley y ser necesarias para asegurar "*el respeto a los derechos o a la reputación de los demás y la protección de la seguridad nacional, el orden público o la salud o la moral públicas*".[14]

Dado que el derecho a la información y a la libertad de expresión, constituye un elemento esencial de los estados democráticos, las excepciones que pueda establecer la legislación al principio de la libre expresión de las ideas a través de Internet, deben ser expresamente establecidas, claras, precisas, cumpliendo una necesidad social imperativa, siendo proporcionales a tal necesidad, y debiendo tener un propósito legítimo, como la seguridad nacional, la prevención de delitos, la protección a la moral pública y de los derechos de las personas, sean o no usuarios.[15]

---

[13] CONVENCIÓN AMERICANA SOBRE DERECHOS HUMANOS, Pacto de San José de Costa Rica, 22 noviembre 1969, Ratificada mediante LEY Nº 1430, de 11 febrero 1993.

[14] ARCE JOFRE, José Alfredo, "Informática y Derecho", Edit. Bolivia Dos Mil, Pág. 22.

[15] ARCE JOFRE, José Alfredo. **Ob. Cit**., Pág. 23.

1.4. ORGANIZACIÓN E HISTORIA DE LA POLICÍA NACIONAL.

Etimológicamente el termino policía deriva del griego "POLITEIA", que significa "*ciencia de los fines y deberes del estado*". Politeia era el conjunto de instituciones que integraban la ciudad o POLIS. Igual significado tiene la voz latín "*POLITIA*".[16]

Para el vocabulario jurídico, es un "*servicio público que tiene por objeto asegurar, mantener o restablecer el orden público, ya sea previniendo la infracción de los reglamentos, de las órdenes y de los gastos apropiados, ya sea reprimiendo las violaciones del orden público mediante el empleo de la fuerza material particularmente la organización que investiga la comisión de los delitos y trata de detener a los autores, y demás responsables, para ponerlos a disposición de los tribunales competentes".*[17]

Sumergiéndonos en la historia que dio origen y organización a la actual Policía Boliviana es necesario hacer mención cuales fueron los elementos trascendentes e importantes en su creación, dentro del contexto que representa la palabra Policía remontamos a lo que dice Pedro Kramer; " *los aimaras antes de ser conquistados por los incas se encontraban gobernados por los mallcus, quienes ejercían autoridad de policía entre los aimaras, dentro las tribus era el guerrero más valiente y en otras el anciano más responsable gozaban de autoridad absoluta y vitalicia, los jefes subalternos eran los apus, y en grado inferior se encontraban los jilacatas***".**[18]

---

[16] HINOSTROZA RODRIGUEZ, Guillermo, "Fundamentos de Doctrina y Ciencia Policial", www.monografias/ciencia policial.com.

[17] OSSORIO, Manuel, "Manual y Diccionario de Ciencias Jurídicas, Políticas y Sociales", ed., Heliasta. Buenos Aires, 2004.

[18] KRAMER, Pedro, "Historia de Bolivia", Taller Tipo litográfico, La Paz, 1889.

Durante la colonia, en las capitales de las provincias los Gobernadores representaban al Rey y si tenían bajo su mando a los Corregidores y a los Intendentes, cuyas funciones policiales eran definidas, puesto que encabezaban las actividades de conservación del orden público, el resguardo de la seguridad personal y real, con elementos que los primeros tiempos estaban compuestos por piquetes de soldados de las guarniciones españolas y vecinos honorables voluntarios. Piquetes especiales de gente armada sobre la base de las fuerzas regulares con el nombre de *VIGILANTES*, recorrían durante el día las poblaciones imponiendo el cumplimiento de las ordenanzas y bandos de carácter policial y comunal.[19]

Durante la República fue el Mariscal Antonio José de Sucre (Mariscal de Ayacucho), considerado el fundador de la institución policial, quien nació en la ciudad de Cumaná (nueva Granada) el 3 febrero 1795. Fueron don Vicente Sucre y doña María de Alcalá sus progenitores, aún encontrándose en su niñez Antonio José de Sucre perdió sus padres a causa de una epidemia que se produjo en aquella región.

Durante su gobierno el presidente Sucre demostró la generosidad desinterés y nobleza de su carácter, Sucre dedicó al buen gobierno de la República la mayor parte de su tiempo imponiendo el derecho a la justicia y el respeto que debería tenerse las autoridades, por eso dedicó con verdadero ahínco el organizar y mejorar el país y este fue el empeño del entonces presidente Sucre hacer resaltar la organización de la primera policía de la República, quien a la postre se constituyó en el creador de esta institución del orden y la seguridad nacional.

La partida de nacimiento de la Policía Nacional, con la que se institucionaliza y se le fijan atribuciones propias y específicas, también corresponde a las medidas de organización política y administrativa que el Gran Mariscal de Ayacucho dictada por el gobierno de Bolivia. Esta es la Ley Reglamentaria de 24 junio de 1826, donde se crea la primera Policía de la República con carácter departamental, al disponer se

[19] MOLINA Roberto, MOLINA Juvenal, CESPEDES Jaime, CASTAÑON Carlos, “Historia de la Policía

establezca *INTENDENTE* de policía nombrado por el Gobierno, para cuidar la tranquilidad, buen orden y comodidad de sus habitantes, que esté subordinado al Prefecto del Departamento y le suceda en el mando accidentalmente.

Poco tiempo después Sucre quiso declinar su mandato, pero el Congreso Nacional le pidió por unanimidad que siguiera gobernando, accediendo a hacerlo solamente por un tiempo limitado porque había advertido que había disparidad de criterios y descontento que se materializó en el motín militar del 18 abril 1828, en el que estuvieron a punto de victimarlo hiriéndolo en un brazo.

El 1 agosto 1828, abandonó el gobierno para dirigirse al Ecuador y entregó al Congreso Nacional su último mensaje a la nación, al manifestar "*Aún pediré otro Premio a la Nación: el de no destruir la obra de mi creación; de conservar por entre todo los peligros la independencia de Bolivia*". [20]

Sucre en la organización de la República con criterio sano 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 prohibida todo conocimiento judicial, existía un jefe civil con el nombre de prefecto; las provincias gobernadas por un gobernador, los cantones por el corregidor y si en un cantón hubieran dos parroquias en cada una de ellas se nombraría alcaldes. Los prefectos y gobernadores como agentes del gobierno, eran sólo funcionarios del poder civil y político y la sujeción de su jerarquía era la del prefecto a gobierno, gobernador a prefecto, corregidor a gobernador y alcalde a corregidor; los dos primeros nombrados por los cantones mismos y los alcaldes nominados por su pueblo. Esta organización y administración del Estado que Sucre propuso 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 Bolívar fue el artífice de su independencia fue una tarea ardua para Sucre tomando en

[20] MOLINA Roberto, MOLINA Juvenal, CESPEDES Jaime, CASTAÑON Carlos, **ob. cit**., Pág. 58.

cuenta que estaba en entre uno de sus problemas la conservación del orden público y las garantías de la ciudadanía, entre estas medidas se cuenta la de establecer una policía que garantice la convivencia pacífica en sociedad.

La Constitución Política del Estado del 6 noviembre 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 corregidor y en los pueblos en cuyo número de habitantes lo exija por cada 1000 haya un Juez de Paz.

La Ley de 23 octubre 1844, autorizó al Poder Ejecutivo para que publique el Reglamento de Policía aprobado. Fue publicado, en efecto, el 10 julio de 1845, pero sólo declaró vigente sólo desde el 22 noviembre 1851, éste contenía, entre sus 185 artículos disposiciones importantes tales como: Autoridades Policiales, Policía de las Cárceles, Delitos contra la Propiedad, ornato limpieza y aseo, servicio de seguridad, etc.

Para dar una adecuada organización a la policía de La Paz, se dispone en fecha 6 mayo 1861 que la ciudad se dividirá en dos distritos, uno a cargo del Intendente de Policías y el otro del Primer Comisario; cada distrito de la ciudad atendido por seis comisarios y 30 hombres que se turnarán en el servicio cada 24 horas.[21]

1.4.1. LA POLICÍA COMO INSTITUCIÓN DE CARÁCTER NACIONAL.

Durante el gobierno de Gregorio Pacheco se promulgó el 11 noviembre 1886 la Ley Reglamentaria de la Policía de Seguridad, sus disposiciones ponen punto final a una larga serie de disposiciones dictadas con anterioridad que muchos casos eran insuficientes y contradictorias, muchas de las actuales disposiciones se inspiran en esta ley, tal es el caso de la Ley Orgánica de la Policía Nacional vigente.

[21] MOLINA Roberto, MOLINA Juvenal, CESPEDES Jaime, CASTAÑON Carlos, **ob. cit**., Pág. 118.

Hasta este momento la policía había funcionado con carácter departamental bajo el mando directo de los intendentes de la policía y la supervisión de los prefectos y comandantes generales de los departamentos respectivos. La ley reglamentaria de los policías del 11 noviembre 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 faltas y delitos con carácter uniforme para toda la República.

El gobierno de don Eliodoro Villazón, mediante Ley de 10 febrero 1910, declara de carácter nacional al servicio de Policía de Seguridad, disponiendo que el poder ejecutivo proceda a la reorganización de un plan uniforme en toda la República, creando brigadas de Policía en cada Departamento.[22]

Con el objeto de resguardar las fronteras de la República, el Inspector General de Policías había presentado un plan de organización de "*Policías Ambulantes Montadas"* en las Provincias de los Lipez y Carangas, la Resolución Suprema del 30 marzo 1914 aprobó el plan propuesto, autorizando al inspector general de policías proceder a la organización de las indicadas Policías Ambulantes Montadas en la forma y condiciones programadas.[23]

La creación de la "*Escuela de Policías"*, mediante decreto supremo del 20 diciembre de 1923 en el periodo presidencial del Doctor Bautista Saavedra, se dispuso la creación de una Escuela de Policías de manera que pudiera funcionar en cada ciudad destinado a la instrucción y educación de alumnos para formar parte del servicio de la policía de la República como una necesidad impostergable de dar una base técnica y profesional a los funcionarios de Policía.

---

[22] MOLINA Roberto, MOLINA Juvenal, CESPEDES Jaime, CASTAÑON Carlos, **ob. cit**., Pág. 227.

[23] MOLINA Roberto, MOLINA Juvenal, CESPEDES Jaime, CASTAÑON Carlos, **ob. cit**., Pág. 235.

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 requisito se deberían cumplir los siguientes: tener 19 años de edad y no exceder los 25, saber leer y escribir correctamente, poseer las cuatro operaciones de aritmética, hablar con propiedad el idioma nacional, no haber sido procesado criminalmente y tener buenos antecedentes, los que hubiesen prestado el servicio militar acreditar con su libreta de conscripción y los demás ser declarados aptos para el servicio militar y por último un tener la estatura mínima de 1.70.

Mediante el Decreto Supremo de 28 Julio 1930 se creó la Dirección General de Policías de la República dependiente del Ministerio de Gobierno, para que tome a su cargo la instrucción y dirección técnica administrativa de todas las reparticiones policiales del país. Para ello se dispuso que pasen a depender de su autoridad y mando directo la Inspección General de Policías y todas las Policías de la República, así como la División Nacional de Carabineros.[24]

Se crea la Dirección Nacional de Investigación Criminal, por decreto ley número 07015 del 4 enero 1965 fue creada la Dirección Nacional de Investigación Criminal como organismo integrado por personal civil profesionales egresados de la Academia Nacional de Policías, los especializados en el exterior, y los capacitados en los

[24] MOLINA Roberto, MOLINA Juvenal, CESPEDES Jaime, CASTAÑON Carlos, **ob. cit**., Pág. 280.

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.[25]

Es así de esta manera que la Policía Nacional Boliviana desde su creación ha ido transformando sus organismos e instituciones que la componen de acuerdo a la coyuntura política social por el cual el país atravesaba en cada época, es importante aclarar en este punto que todas transformaciones hechas al interior de la institución del orden se dieron a lo largo de los gobiernos del Estado Republicano.

También es necesario mencionar que a cada época de la historia boliviana corresponde la responsabilidad de una sociedad boliviana que exigía cambios y mejoras dentro de su policía, ese aspecto social estaba acompañado de la evolución del delito, la aparición de nuevas formas, la especialización de los delincuentes de cada época para cometer sus actos en contra del orden legal.

[25] MOLINA Roberto, MOLINA Juvenal, CESPEDES Jaime, CASTAÑON Carlos, **ob. cit**., Pág. 259.

1.5. LA INFORMÁTICA JURÍDICA, EL DERECHO INFORMATICO: SUS RELACIONES Y CAMPOS DE ESTUDIO.

1.5.1. CONCEPTOS Y DEFINICIONES.

1.5.1.1. 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 lógicos -formales que concurren en proceso legislativo y en la decisión judicial (*informática jurídica decisional*).[26]

La otra parte de esta integración terminológica, es la voz "*Informática*" que proviene del francés: "*información - automatique*" aludiendo a las máquinas destinadas al tratamiento de la información, con la facultad de almacenar, elaborar lo almacenado, seleccionarlo en el momento justo y combinarlo adecuadamente al ser consultadas. La informática es la ciencia que estudia tratamiento de la información mediante el uso de computadores, sin duda originó su crecimiento de la tecnología. Entre el derecho y la informática se podrían apreciar dos tipos de interrelaciones. Si se toma como enfoque el aspecto netamente instrumental, se está haciendo referencia a la informática jurídica. La informática jurídica que ayudada por el derecho informático hace válida esa cooperación de la informática al derecho.

La informática jurídica estudia la utilización de aparatos o elementos físicos electrónicos, como la computadora, en el derecho; es decir, la ayuda que este uso presta al desarrollo y aplicación del derecho. En otras palabras, es ver el aspecto instrumental dado a raíz de la informática en el derecho. "*Nos referimos a la informática jurídica cuando el jurista (Jueces, Secretarios, Oficiales, Mayores, Abogados en ejercicio de la profesión), utilizan la tecnología como herramienta para*

[26] LUÑO, Antonio Enrique, "Ensayo de Informática Jurídica", Edit. Fontamar, México, 2005.

procesar, automatizar y, sistematizar la información en tres clases o fuentes, que son":

- **informática jurídica documental** (almacena y clasifica los datos jurídicos para su recuperación rápida y oportuna, crea documentos con información jurídica referente a la legislación, a la audiencia y casación así como la doctrina del derecho).
- **Informática jurídica decisoria** (la que propone y adoptar soluciones apropiadas para casos concretos que se le plantean en base a criterios que previamente se le han provisto). Intervienen programa o software, que se convierten en herramientas del jurista para la toma de decisiones. Éste tipo de informática se ha extendido hacia la administración de justicia.
- **Informática jurídica de gestión** (constituye una herramienta para la gestión diaria del jurista, es el desarrollo de la sistematización diaria de información), ejemplo el sorteo informático de causas como ser el orden de llegada, el juzgado que tenga menos trabajo.[27]

1.5.1.2. EL DERECHO INFORMÁTICO.

Ha sido considerado por CARRASCOSA López como "*el conjunto de normas que regulan las acciones, procesos, productos y relaciones jurídicas surgidas en torno a la informática y sus aplicaciones*." [28]

Julio Tellez afirma que el Derecho Informático "*es el conjunto de leyes, normas y principios aplicables a los hechos y actos derivados de la informática*" [29]

---

[27] ARCE JOFRE, José Alfredo "Informática y Derecho", ed., Bolivia Dos Mil, Págs. 36-37.

[28] CARRASCOSA LOPEZ, V, "Informática y Derecho", UNED, 1992.

[29] TELLEZ VALDEZ, Julio, "Derecho Informático", ed., Mc Graw Hill, Pág. 282.

Para Arce Jofre el derecho de la informática como "*el conjunto de normas jurídicas que regulan la creación, desarrollo, uso, aplicación de la informática o los problemas que se deriven de la misma en las que exista algún bien qué es o deba ser tutelado jurídicamente por las propias normas".* Al considerar a la informática como objeto del derecho, se hace alusión al derecho de la informática o simplemente derecho informático. [30]

Para Emilio Suñe, *"es el conjunto de normas reguladoras del objeto informático o de problemas directamente relacionados con la misma"*. [31]

El derecho informático se constituye en una ciencia, que estudia la regulación normativa de la informática y su aplicación en todos los campos, esta ciencia forma parte del derecho como rama jurídica autónoma; así como el derecho es una ciencia general integrada por ciencias específicas que resultan de las ramas jurídicas autónomas, tal es el caso de la civil, penal y contencioso administrativo.

Sin duda alguna, que tanto la informática jurídica como el derecho informático constituyen conocimientos, principios, doctrinas, que catalogan a estas disciplinas como ciencias, que tienen como marco estricto a la iuscibernética y como marco amplio a la cibernética.

1.5.1.3. AUTONOMIA DEL DERECHO INFORMATICO.

Generalmente el nacimiento de una rama jurídica surge a consecuencia de cambios sociales reflejados en las soluciones normativas al transcurso de los años. Pero resulta que, en el caso de la informática no hubo ese transcurrir del tiempo en los cambios sociales, sino que el cambio fue brusco y en poco tiempo, se lograron de

[30] ARCE JOFRE, José Alfredo, "Informática y Derecho", ed., Bolivia Dos Mil, Pág. 28.

[31] SUÑE LLINAS, Emilio, "Tratado de Derecho Informático", Introducción y Protección de datos personales, Publicaciones de la Facultad de Derecho de la Universidad Complutense de Madrid, 2000.

esta manera sociedades altamente informatizadas, que sin la ayuda actual de la informática colapsarían.

No obstante, a pesar de esta situación existen países desarrollados como España en los que sí se puede hablar de una verdadera autonomía en el derecho informático, haciendo la salvedad de que esta ciencia como rama jurídica apenas nace y se está desarrollando, pero se está desarrollando como una rama jurídica autónoma.

En efecto, la informática no puede juzgarse en su simple exterioridad, como utilización de aparatos o elementos físicos electrónicos, pura y llanamente; sino que, en el modo de proceder se crean unas relaciones inter subjetivas de las personas naturales o jurídicas y de entes morales del Estado, y surgen entonces un conjunto de reglas técnicas conectadas con el Derecho, que vienen a constituir medios para la realización de sus fines, ética y legalmente permitidos; creando principios y conceptos que institucionalizan la Ciencia informática, con autonomía propia. Esos principios conforman las directrices propias de la institución informática, y viene a constituir las pautas de la interrelación nacional-universal, con normas mundiales supra nacionales y cuyo objeto será necesario recoger mediante tratados públicos que hagan posible el proceso comunicacional en sus propios fines con validez y eficacia universal.

Concluir que en el derecho informático si existe legislación específica, que protege al campo informático. Tal vez no con tanta trayectoria y evolución como la legislación que comprenden otras ramas del derecho, pero si existe en el derecho informático, legislación basada en leyes, tratados y convenios internacionales, además de los distintos proyectos que se llevan a cabo en los entes legislativos de nuestras naciones, con la finalidad del control y aplicación lícita de los instrumentos informáticos.

1.5.2. RELACION DEL DERECHO INFORMATICO CON OTRAS DISCIPLINAS.

De esta manera, tenemos a la ciencia informática y por otro lado a la ciencia del derecho; ambas disciplinas interrelacionadas funcionan más eficiente y eficazmente, por cuanto el derecho en su aplicación, es ayudado por la informática; pero resulta que ésta debe de estar estructurada por ciertas reglas y criterios que aseguren el cumplimiento y respeto de las pautas informáticas; así pues, nace el derecho informático como una ciencia que surge a raíz de la cibernética, como una ciencia que trata la relación derecho e informática desde el punto de vista del conjunto de normas, doctrina y jurisprudencia, que van a establecer, regular las acciones, procesos, aplicaciones, relaciones jurídicas, en su complejidad, de la informática.

Pero del otro lado encontramos a la informática jurídica que ayudada por el derecho informático hace válida esa cooperación de la informática al derecho.

1.5.2.1 CON EL DERECHO CONSTITUCIONAL.

La correlación entre el derecho informático y el derecho constitucional se destaca por la forma de controlar la estructura y organización estatal que se lleva a cabo por medios informáticos.

Existe un derecho a la libertad y protección informática, y garantías orgánicas como HABEAS DATA, "*garantía constitucional que asiste a toda a solicitar judicialmente la exhibición de los registros públicos o privados en los cuales están incluidos sus datos personales o de su grupo familiar, para tomar conocimiento de su exactitud; a requerir la rectificación, la supresión de datos inexactos u obsoletos o que impliquen discriminación por ejemplo: la confesión religiosa, si el registro no tiene por objeto constatar tal situación. Tiende a proteger a la persona contra calificaciones sospechosas incluidas en registros que pueden llegar a perjudicar de cualquier modo*".

1.5.2.2. CON EL DERECHO PENAL.

En materia de delitos cibernéticos o informáticos. Es el derecho penal encargado de sancionar mediante la fuerza coercitiva que posee el Estado, delegando esa función a la estructura del órgano judicial. Esta relación es muy estrecha por cuanto aquellos delitos informáticos que vulneran el bien jurídico que atentan a los derechos de las personas, estarán tutelados por el Derecho Penal.

1.5.2.3. CON LOS DERECHOS HUMANOS.

Los derechos de las personas relativas al acceso a la información, así como la libertad de expresión y pensamiento y por otro lado, a los peligros que las nuevas tecnologías han creado sobre la vulneración de los derechos a la intimidad, privacidad, etc. el derecho informático ha agregado celeridad procesal mediante sus sistemas informáticos mejorando el funcionamiento de los órganos jurisdiccionales como cuestión relevante para los derechos humanos.

1.5.2.4. CON EL DERECHO CIVIL.

En todo aquello que se refiere a la firma digital, sistemas de autentificación y autoridades de certificación, contratos electrónicos, digitalización de los actos jurídicos, sistemas de dominios, etc.

1.5.2.5. DERECHO COMERCIAL.

El comercio electrónico, marcas y patentes, nuevos instrumentos comerciales de pago electrónico, banca electrónica, oferta a distancia en la internet, etc. [32]

Hoy en día ya no es posible hacer una clara diferenciación entre telecomunicaciones e informática, razón por la cual en la actualidad se utiliza el término "*telemática"* que

[32] ARCE JOFRE, José Alfredo, "Informática y Derecho", ed., Bolivia Dos Mil, Pág.34.

se refiere conceptualmente a la conjunción de ambos términos. En Bolivia como en el resto del mundo, la telemática plantea nuevos problemas legales y regulatorios, en especial con el fenómeno de la digitalización, donde ya no se puede saber si una comunicación es voz, video, texto, etcétera. Todo se reduce a números binarios que viajan por una misma infraestructura. Es decir, que las reglas que obligan en Bolivia los operadores de telefonía de larga distancia, a constituirse en el país y cumplir las normas regulatorias internas, pueden quedar obsoletas, debido a la posibilidad técnica de proveer servicios de telecomunicaciones sin necesidad de estar en el país, cobrándolas por tarjeta de crédito y trasmitiendo sobre el protocolo de Internet (IP).[33]

1.6. LA ORGANIZACIÓN DE NACIONES UNIDAS EN MATERIA DE DELITOS INFORMATICOS.

1.6.1. LA ONU DECLARA EL ACCESO A INTERNET COMO DERECHO HUMANO.

La web ha dado la posibilidad a miles de personas en todo el mundo de comunicar sus ideas y provocar cambios en sus sociedades. Es por esto que la Asamblea General de las Naciones Unidas ha declarado el acceso a internet como un derecho humano.

"*La única y cambiante naturaleza de internet no sólo permite a los individuos ejercer su derecho de opinión y expresión, sino que también forma parte de sus derechos humanos y promueve el progreso de la sociedad en su conjunto*", Los gobiernos deben esforzarse para hacer al internet ampliamente disponible, accesible y costeable para todos. Asegurar el acceso universal del internet debe ser una

[33] ARCE JOFRE, José Alfredo, **ob. Cit**., Pág. 14.

prioridad de todos los estados, La Organización de las Naciones Unidas también señala las formas en las que el derecho al acceso a internet es violado.[34]

A pesar de las declaraciones de las Naciones Unidas, hoy en día existen aún resabios de gobiernos monárquicos y dictatoriales que todavía pretenden coartar la libertad de expresión, tal es el caso del gobierno Egipto que ha bloqueado el acceso a internet durante las revueltas sociales que terminaron con la dictadura de Hosni Mubarak. Irán también bloqueó algunas páginas de activistas que llamaban a una manifestación y muchos otros países han seguido este ejemplo. La ONU afirma que el acceso a la web debe mantenerse y es especialmente valioso "*en momentos políticos clave como elecciones, tiempos de intranquilidad social o aniversarios históricos y políticos*".

La capacidad de los gobiernos de apagar internet es un asunto que preocupa a la ONU, pues asegura que violan las libertades de expresión y de acceso a la información de los ciudadanos.

Sobre la censura en China la ONU publica que "*China tiene uno de los sistemas más extensos para controlar la información en internet, posee los mecanismos usados para regular y censurar la información en internet son cada vez más sofisticados y con controles en varias fases que se encuentran ocultos a la población*".

A diferencia de otros medios de comunicación, la accesibilidad de internet permite que cualquier persona en el mundo pueda difundir sus ideas. Sin embargo no todas las personas tienen acceso a esta tecnología.

"*El internet como un medio para ejercer el derecho a la libertad de expresión sólo puede servir a estos propósitos si los estados asumen su compromiso por desarrollar*

[34] LA RUE, Frank, Relator Especial de la ONU, Comunicado de prensa.

políticas efectivas para lograr el acceso universal", finaliza la ONU en su comunicado.

Este medio de comunicación ya es tan importante para la organización ciudadana, que Estados Unidos ha desarrollado tecnologías para restaurar la conexión a internet en un país, en caso de que deseara hacerlo.

1.6.2. TIPOS DE DELITOS INFORMÁTICOS RECONOCIDOS POR NACIONES UNIDAS.

1.6.2.1. FRAUDES COMETIDOS MEDIANTE MANIPULACIÓN DE COMPUTADORAS.

1.6.2.1.1. MANIPULACIÓN DE LOS DATOS DE ENTRADA.

Este tipo de fraude informático, conocido también como sustracción de datos, representa el delito informático más común ya que es fácil de cometer y difícil de descubrir.

Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos.

1.6.2.1.2. MANIPULACIÓN DE PROGRAMAS.

Es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente debe tener conocimientos técnicos concretos de informática. Este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas. Un método común utilizado por las personas que tienen conocimientos especializados en programación informática es el denominado Caballo de Troya, que consiste en insertar instrucciones de

computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.

1.6.2.1.3. MANIPULACIÓN DE LOS DATOS DE SALIDA.

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

1.6.2.2. FALSIFICACIONES INFORMÁTICAS

1.6.2.2.1. COMO OBJETO.

Cuando se alteran datos de los documentos almacenados en forma computarizada.

1.6.2.2.2. COMO INSTRUMENTOS.

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

1.6.2.3. DAÑOS O MODIFICACIONES DE PROGRAMAS O DATOS COMPUTARIZADOS.

1.6.2.3.1. SABOTAJE INFORMÁTICO.

Es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema. Las técnicas que permiten cometer sabotajes informáticos son:

VIRUS: Es una serie de claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos. Un virus puede ingresar en un sistema por conducto de una pieza legítima de soporte lógico que ha quedado infectada, así como utilizando el método del Caballo de Troya.

GUSANOS: Se fabrica de forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse. En términos médicos podría decirse que un "*gusano"* es un *tumor benigno*, mientras que el "*virus*" es un *tumor maligno*. Ahora bien, las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus: por ejemplo, un programa gusano que subsiguientemente se destruirá puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita.

BOMBA LÓGICA O CRONOLÓGICA: Exige conocimientos especializados ya que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro. Ahora bien, al revés de los virus o los gusanos, las bombas lógicas son difíciles de detectar antes de que exploten; por eso, de todos los dispositivos informáticos criminales, las bombas lógicas son las que poseen el máximo potencial de daño. Su detonación puede programarse para que cause el máximo de daño y para que tenga lugar mucho tiempo después de que se haya marchado el delincuente. La bomba lógica puede utilizarse también como instrumento de extorsión y se puede pedir un rescate a cambio de dar a conocer el lugar en donde se halla la bomba.

1.6.2.4. ACCESO NO AUTORIZADO A SERVICIOS Y SISTEMAS INFORMÁTICOS.

Por motivos diversos: desde la simple curiosidad, como en el caso de muchos piratas informáticos (hackers) hasta el sabotaje o espionaje informático.

1.6.2.4.1. PIRATAS INFORMÁTICOS O HACKERS.

El acceso que efectúa el *hacker* a menudo desde un lugar exterior, situado en la red de telecomunicaciones, recurriendo a uno de los diversos medios que se mencionan a continuación. El delincuente puede aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema. A menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sistema; esto suele suceder con frecuencia en los sistemas en los que los usuarios pueden emplear contraseñas comunes o contraseñas de mantenimiento que están en el propio sistema.

Son auténticos genios de la informática, entran sin permiso en ordenadores y redes ajenas, husmean, rastrean y a veces, dejan sus peculiares tarjetas de visita. Los "*Hackers*" posmodernos de la red, son la ultima avanzada de la delincuencia informática de este principio de siglo. *Hacker es aquella persona que disfruta explorando detalles de los sistemas programables y aprendiendo a usarlos al máximo, al contrario del operador común, que en general, se conforma con aprender lo básico*.

1.6.2.4.2. REPRODUCCIÓN NO AUTORIZADA DE PROGRAMAS INFORMÁTICOS DE PROTECCIÓN LEGAL.

Esta puede entrañar una pérdida económica sustancial para los propietarios legítimos. Algunas jurisdicciones han tipificado como delito esta clase de actividad y la han sometido a sanciones penales.

El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones modernas.

Al respecto, consideramos, que la reproducción no autorizada de programas informáticos es un delito informático debido a que el bien jurídico a tutelar es la propiedad intelectual. [35]

[35] ORGANIZACIÓN de las NACIONES UNIDAS, "Delitos Reconocidos", http://www.forodeseguridad.com

1.7. FUNCIÓN ACTUAL DE LA POLICÍA NACIONAL EN MATERIA DE DELITOS INFORMÁTICOS.

La función principal que actualmente cumple a Policía Nacional está claramente establecida en nuestra Constitución Política del Estado del 7 Febrero 2009, contemplada en el Capituló Segundo, Artículo 251:

I. La Policía Boliviana, como fuerza pública, tiene 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 boliviano. Ejercerá la función policial de manera integral, indivisible y bajo mando único, en conformidad con la Ley Orgánica de la Policía Boliviana y las demás leyes del Estado.

II. Como institución, no delibera ni participa en acción política partidaria pero individualmente sus miembros gozan y ejercen sus derechos ciudadanos, de acuerdo con la ley.[36]

Como podemos advertir, la Policía Boliviana, en el mandato o misión específica que le confiere la constitución, tiene como tarea fundamental defender la sociedad, esa defensa constituye el pilar fundamental de su institucionalidad al mismo tiempo implica repeler todo ataque o agresión que constituya peligro para la sociedad, pero además la conservación del orden público, implica tareas fundamentales de vigilancia y patrullaje en todo el territorio boliviano, es entonces en virtud a esa misión específica que tiene nuestra policía, la de adecuar nuevas formas de aparición del delito como un propósito institucional requiriendo una organización efectiva en todos los campos, en este caso citado entre los delitos informáticos, hacen que la policía boliviana se plantee la necesidad de crear nuevos organismos u unidades operativas con recursos generados de la implementación de políticas

[36] CONSTITUCIÓN POLÍTICA DEL ESTADO, Gaceta Oficial de Bolivia, La Paz Bolivia, 7 Febrero 2009.

estatales de seguridad ciudadana, siendo éstos recursos humanos y económicos los mecanismos que constituirán una pronta y eficaz lucha frente al delito como una prioridad institucional.

Actualmente dentro de nuestra policía boliviana, existe un departamento llamado Sección Manipulación Informática dependiente del Departamento Nacional de la Policía Técnica Científica, cuenta con una División de Laboratorio en Criminalística, Es Parte de la Jefatura de División. La Función General que desempeña esta sección es la de controlar, analizar y evaluar todas las evidencias de carácter informático que les sean asignadas, las Funciones Específicas es la de solicitar en forma oportuna los requerimientos de material y equipo necesarios para un mejor desempeño de sus tareas además de informar y verificar en forma oportuna si las muestras remitidas son insuficientes, también tienen la misión de identificar a los autores del fraude en los procesos de falsificación, manipulación, sabotajes informáticos, inversión, piratería, reproducciones no autorizadas y por último realizar análisis de inspecciones oculares de carácter informático.[37]

1.7.1. CARACTERÍSTICAS DE LA DOCTRINA POLICIAL.

La Doctrina Policial precede y sustenta los conocimientos y conceptos teóricos prácticos sobre el Orden Interno, el Orden Público y la Seguridad Ciudadana.

La doctrina policial se nutre de la historia policial, programas de acción, disciplinas básicas y auxiliares que integran la ciencia policial, la estructura axiológica y la realidad criminógena dentro de la cual se desenvuelve la institución. Comprende los principios que orientan la conducta institucional, así como el ejercicio de la función policial. Son los linderos que enmarcan dicha función. Constituidos por aquello que se considera bueno, que beneficia a la persona. Entre ellos tenemos valores de los

[37] FUERZA ESPECIAL DE LUCHA CONTRA EL CRIMEN," Manual de Organización y Funciones", págs. 73-74.

DD HH, de la cultura de paz. La práctica de los valores morales fomenta el cultivo de las virtudes, constituye la base del progreso material y espiritual de la organización.[38]

COMUNITARIA.- La doctrina policial se origina y desarrolla en la comunidad, existe y se practica, por razones de las funciones que realiza el policía, esto solo puede existir en el ámbito social donde se desenvuelve, la coexistencia social tiene en la persona humana y la sociedad una dualidad de elementos en que la doctrina enriquece su contenido y su naturaleza humanística, comunidad y policía son los elementos de la coexistencia social.

REALISTA.- Esta característica desea demostrar que el policía actúa en mundo de realidades y no sobre algo imaginario o supuesto. Tiene su génesis en la realidad social y su estructura de acuerdo a ello. Ej. Si un policía da cuenta de una investigación que ha realizado, tendrá que sustentar con hechos reales y concretos y no suposiciones.

DINÁMICA.- Es dinámica porque no se puede concebir una doctrina estática, su evolución es permanente, esta acción dinámica será en la medida cómo evolucione tanto la sociedad como las organizaciones del estado. Tiene un constante accionar en base a los conocimientos, valores y fines.

AXIOLÓGICA.- Porque requiere de valores que tiene una naturaleza metafísica y una expresión concreta, Ejemplo: los valores, la doctrina policial se basa en principios y valores morales. Se orienta hacia principios y valores éticos, principio que se admite sin necesidad de demostración.

TEOLÓGICA.- La doctrina policial es teológica porque persigue una finalidad y aspira a alcanzar un propósito ideal, que es la paz social, la tranquilidad y el bienestar de la comunidad.[39]

[38] VILLANUEVA GARAY, José. Catedrático de la ESUPOL, "Ciencia Policial, parte de las ciencias sociales".

1.8. ROL DE LA POLICÍA EN LA ORGANIZACIÓN DEL ESTADO.

El rol de nuestra policía boliviana en la organización del Estado está claramente definida en nuestra Constitución Política del Estado, otorgando a la policía la capacidad de usar la fuerza pública, uso de la fuerza coercitiva impone cumplir específicamente la conservación del orden público en defensa de la sociedad y valores, esa función policial será ejercerá de manera integral bajo un mando único en todo el territorio boliviano de conformidad con la ley Orgánica de la Policía Boliviana y demás leyes que tengan relación. Pero también otra constitución señala específicamente que la policía como institución no deberá participar en ninguna acción política partidaria que el derecho de liberar esta coartada para esta misma respetando el goce y el ejercicio de los derechos ciudadanos para sus miembros.

En el supuesto caso de un conflicto internacional que nuestro país podría atravesar nuestra constitución es clara al respecto, indicando que las fuerzas de la Policía Boliviana pasarán a depender del Comando en Jefe de las Fuerzas Armadas por el tiempo que dure el conflicto. Las funciones primarias de la institución policial en una sociedad democrática son garantizar el cumplimiento de la ley, conservar la paz social en el marco de la justicia y proteger, previniendo e investigando, la seguridad de los ciudadanos además de cumplir y someterse a la ley que pretende aplicar.

Por el contrario, las elude y transgrede recurrentemente, los hechos que se ocurren cotidianamente en torno a las funciones policiales formales reiteran, casi con empecinamiento, que la policía no previene adecuadamente el delito, tampoco garantiza los derechos ciudadanos ni contribuye a restablecer la paz social a través de la estricta aplicación de la ley. [40]

---

[39] HINOSTROZA RODRIGUEZ, Guillermo. “Fundamentos de Doctrina y Ciencia Policial”.

[40] PROGRAMA DE INVESTIGACIÓN ESTRATÉGICA EN BOLIVIA, “Policía y Democracia en Bolivia”, 2003.

1.9. ESTRUCTURA ORGÁNICA DE LA POLICÍA.

Por la naturaleza que caracteriza a la Policía Boliviana esta obedece a un mando institucional que de forma general constituye una pirámide de jerarquía, donde en la cabeza de la misma encontramos al Presidente del Estado Plurinacional de Bolivia, en ese descenso de autoridad se encuentra posteriormente el Ministro de Gobierno, y más abajo de esa jerarquía el comandante General de la Policía.

La estructura orgánica de la Policía Boliviana responde a un mando vertical en descenso en línea directa, el comandante en jefe de la Policía Boliviana es el Presidente De La República en ejercicio, quien ejerce autoridad por intermedio del Ministro Del Interior, siendo el Comando General de la Policía Nacional el órgano máximo de dirección administración y decisión a través del Comandante General y sub Comandante General.

1.10. LA POLICÍA NACIONAL COMO MECANISMO DE DEFENSA Y NECESIDAD PÚBLICA.

La policía cumple fundamentalmente una labor de prevención en el campo de la seguridad ciudadana, indudablemente que es muy difícil cumplir a cabalidad esa tarea por las limitaciones logísticas que impone la carencia de recursos, pero no imposible poder ofrecer seguridad. Es inevitable saber la reacción que pueda tener una persona en determinado momento y frente a un determinado estímulo, las presiones a las que éstas están sujetas en toda sociedad constituye muchas veces factores que desencadenaron la comisión de un delito algunas de las cuales podemos citar como son la injusticia social, el desempleo, el alcoholismo y la drogadicción, convirtiendo a unos en agresores y a otros en víctimas. Es entonces donde el rol protagónico de la policía como ente coercitivo activa el mecanismo de defensa para satisfacer, en la medida de sus posibilidades una necesidad pública de protección y seguridad. Ese clamor social de contar con una policía eficiente, cuestiona las políticas de seguridad ciudadana que los gobiernos de turno deben

encarar con soluciones urgentes, pero que en la realidad siempre ha sido un discurso pre-electoral sin ningún resultado hasta el momento.

"*Desde luego que no se puede pensar en una sociedad con altos índices de seguridad si en ella existen los males enunciados y el Estado a través de sus gobernantes e instituciones no cumplen la función de garantizar la seguridad que les tiene encomendada la Carta Magna, y en este caso no será posible que los ciudadanos se desenvuelvan en un clima de paz, tranquilidad y garantía de sus derechos*".[41]

1.10.1. SEGURIDAD CIUDADANA.

La categoría llamada Seguridad Ciudadana es una expresión del Orden Público aplicada al ámbito local, manteniendo los aspectos derivados de la Constitución Política y prevista en los Planes Nacionales. La Policía Nacional tiene por finalidad fundamental garantizar, mantener y restablecer el orden interno. Presta protección y ayuda a las personas y a la comunidad. Garantiza el cumplimiento de las leyes y la seguridad del patrimonio público y del privado. Previene, investiga y combate la delincuencia. Vigila y controla las fronteras.[42]

El crecimiento y desarrollo de las diferentes regiones del país, la migración campo - ciudad, el crecimiento desordenado de las ciudades con asentamientos alrededor de las urbes formando cinturones de miseria, trae consigo una serie de alteraciones en la conducta de las personas, quienes en procura de conseguir mejores condiciones de vida y espacios de acción recurren a conductas que se patentizan con la comisión de faltas y contravenciones, así como también delitos que generan inseguridad. En la actualidad la población del país en todos sus estratos, se ha visto

[41] MOLINA VIAÑA, Oscar, "Seguridad Ciudadana", La Paz –Bolivia, 2001, Pág. 2.

[42] COSTA FERRECCIO, Julio, "Poder y derecho de Policía".

avasallada por diferentes formas delictivas y conductas que aquejan su seguridad; la ciudadanía, habiéndose dado cuenta del peligro que significa estar bajo el acecho de malvivientes, vagos y mal entretenidos, delincuentes habituales (antisociales), pandillas, drogadictos, así como también de personas que bajo influencia icónica y de otras sustancias, cometen agresiones, asaltos, violaciones, robo de vehículos, secuestros y hasta homicidios: por lo que la ciudadanía se siente perseguida, y estresada y lo que es peor no cree estar segura ni dentro de su propia casa.[43]

El "*Orden Interno"* es una institución jurídico-política de nivel constitucional, que se manifiesta como una situación de equilibrio y de orden en todos los campos de la vida nacional (social, económico, político, etc.), que garantizan el funcionamiento y la estabilidad del Estado. El Orden Interno conduce a la Seguridad Interna del Estado.

La *Seguridad Ciudadana* es un "*conjunto de medidas sistematizadas de carácter preventivo, tendientes a eliminar o por lo menos disminuir las posibilidades de generar conflictos o violencia que produzcan víctimas inocentes y ofrecer a las personas amplias garantías de seguridad moral y física que le garanticen su vida y sus bienes. Desde luego que mediante los programas de seguridad ciudadana no se consiguen fórmulas matemáticas indiscutibles que logren seguridad absoluta pero lo que realmente se puede disminuir y evitar son los robos, atracos violaciones, timos, estafas daños a las personas y cualquier género de contravenciones o delitos que puedan dañar la integridad física y la propiedad de los ciudadanos"*.[44]

[43] MOLINA VIAÑA, Oscar. **Ob.cit.,** Pág. 5.

[44] MOLINA VIAÑA, Oscar. **Ob.cit.,** Pág. 6.

1.11. AUSENCIA DE UNA POLICÍA ESPECIALIZADA EN DELITOS INFORMÁTICOS.

En una sociedad como la nuestra donde el desarrollo de la informática y sus innovaciones tecnológicas llegaron recientemente, estas están llegando a ser parte integrante de la vida cotidiana de sus habitantes, una tecnología informática al alcance de una parte considerable de la ciudadanía que encuentra ventajas en cuanto al acceso a la información, la libertad de expresión, etc., situación que por el contrario contrasta con la ausencia de una policía especializada en delitos informáticos, una policía preparada para la misión de defensa y combate de este nuevo tipo de infracciones a la ley, dejando por tanto a una sociedad desprovista de los mecanismos de defensa y seguridad.

Si bien es cierto que nuestra Policía Boliviana cuenta a la fecha al interior de la Dirección Nacional de la Fuerza Especial de Lucha contra el Crimen una División de Laboratorio en Criminalística, conformado por una sección de Manipulación Informática, en donde la función general es de controlar analizar y evaluar todas las evidencias de carácter informático que les sean asignados además de solicitar los requerimientos de material y equipos necesarios en el desempeño de sus tareas informando y verificando, identificando autores de fraudes en proceso de falsificación manipulación sabotajes informáticos, piratería, reproducciones autorizadas, además de realizar análisis e inspecciones oculares de carácter informático. Ahora bien si está estipulado en el manual de Organización y Funciones de la Fuerza Especial de Lucha contra el Crimen, todas estas funciones en la práctica cotidiana del desempeño de la policía no concurren todos estos factores, debido a que no existe al interior de la institución el personal profesional especializado en informática, los equipos informáticos con características adecuadas a combatir el crimen informático, pero sobre todo no existe la voluntad política de nuestros gobernantes de contar y capacitar una policía en este ámbito, a consecuencia de esto vemos reflejada en la ciudadanía el abandono, la inseguridad y la desprotección frente a la comisión y aparición de este nuevo tipo de delitos. Pero también hay que agregar que gran parte

de la población boliviana desconoce el peligro que puede significar ser víctima de uno de estos delincuentes cibernéticos, ese desconocimiento va más allá inclusive de no estar empapado con el modus operandi, la terminología usada para ese tipo de casos y sobre todo el desconcierto de no saber dónde recurrir en caso de ser víctimas.

CAPITULO II

MARCO CONCEPTUAL APLICADO EN LA MONOGRAFÍA

2.1. GLOSARIO DE TÉRMINOS.

La innovación de términos descriptivos en materia de delitos informáticos, es cada vez más innovador y sobre todo la aparición de nuevas modalidades u formas de cometer ilícitos que atentan la seguridad y protección de datos y otros, da lugar a que día a día aparezcan nuevos términos que designan nuevas conductas o formas de su realización. Citemos las más relevantes:

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

Aplicación informática. Conjunto de uno o varios programas más la documentación correspondiente.

Back Up o Recuperación de Datos. Proporciona los parámetros básicos para la utilización de sistemas de recuperación de datos y Back Up de los sistemas informáticos, permitiendo recuperar la información necesaria en caso de que ésta sufra daños o se pierda.

Cracker. Aquel que rompe con la seguridad de un sistema. El término fue acuñado por Hacker en 1985, oponiéndose al mal uso de la palabra Hacker por parte de la prensa. En cambio el Preaker, es el arte y ciencia de Crakear la red telefónica para obtener beneficios personales como por ejemplo hacer llamadas de larga distancia sin el correspondiente pago. El hacker en general utilice reglas gramaticales particulares, juega y crea un lenguaje propio con la intención de confundir y diferenciarse, y con ello obtener cierto poder. Ese lenguaje puede ser universal en el hackerdown óseos de su propia autoría en un programa en particular. Utiliza frases que literalmente significan una cosa y quieren decir otra, de este modo el operador creará que está ejecutando una acción o programa, cuando en realidad ejecutará otra cosa, es decir la programación esperada por el hacker, es habitual encontrar este tipo de actitudes entre más de ayuda, archivos o spam publicitarios, entre otros.

Computadora. Máquina compuesta de elementos físicos, en su mayoría electrónicos, capaces de realizar una serie de trabajos a gran velocidad y con gran precisión, siempre que se le den las instrucciones adecuadas.

Correo Electrónico. El correo electrónico es un sistema de mensajería que funciona a través de su ordenador. Desde donde se puede enviar y recibir mensajes escritos, además de documentos adjuntos de usuarios de cualquier parte del mundo que dispongan de dirección de correo, llamada también dirección e-mail.

Conmutación Es una técnica que nos sirve para hacer un uso eficiente de los enlaces físicos en una red de computadoras.

Criptografía. Ocultación de la información mediante cifrado.

Datos. Informaciones no elaboradas y que una vez procesados (ordenados, sumados, comparados, etc.) constituyen lo que se denomina información útil.

Fraude. Es inducir a otro a hacer o a restringirse en hacer alguna cosa de lo cual el criminal obtendrá un beneficio por lo siguiente.

Hacker. El que programa con entusiasmo (al borde de la obsesión) o aquel que se divierte mas programando que haciendo teorías sobre programación.

Hardware. Conjunto de elementos materiales que componen un sistema Informático. Son el teclado, para introducir la información, la memoria que almacena la información y el programa, la unidad de proceso CPU que lleva a cabo las instrucciones contenidas en el programa, y una pantalla para ver los resultados del trabajo realizado.

Hostigamiento o acoso. Es un contenido que se dirige de manera específica a un individuo o grupo con comentarios peyorativos a causa de su sexo, raza, religión, nacionalidad, orientación sexual, hechos a través de un medio informático.

Informática. Tratamiento automático de la información.

Información. Es el conocimiento producido como resultado del procesamiento de los datos.

Internet: Red de datos ideada para transmitir imagen y voz.

Internet protocolo (IP) protocolo de Internet números. INTERNET PROTOCOL (IP) NUMBERS O IP ADRESSES (PROTOCOLO DE INTERNET, NÚMEROS): Un identificador numérico único usado para especificar anfitriones y redes. Los números IP son parte de un plan global y estandarizado para identificar computadores que estén conectados a Internet. Se expresa como cuatro números del 0 al 255, separado por puntos: 188.41.20.11. La asignación de estos números en el Caribe, las Américas, y África la hace la American Registry for Internet Numbers.

Programa. Conjunto de órdenes que se dan a una computadora para realizar un proceso determinado.

Sistema Informático. Conjunto de elementos necesarios (Computadoras, terminales, impresores, etc.) para la realización y exploración de aplicaciones informáticas.

Software. Es la parte lógica que dota al equipo físico de capacidad para realizar cualquier tipo de trabajo, tiene su origen en ideas y procesos desarrollados por el elemento humano, plasmado en un soporte determinado del hardware. Desde un punto de vista legal, el bien jurídico tutelado será la propiedad intelectual.

Soporte Lógico: Cualquiera de los elementos (tarjetas perforadas, cintas o discos magnéticos, discos ópticos) que pueden ser empleados para registrar información en un sistema informático.

Soporte Material: Es cualquier elemento corporal que se utilice para registrar toda clase de información.

Telemática. Neologismo que hace referencia a la comunicación informática, es decir la transmisión por medio de las redes de telecomunicaciones de información automatizada., En otras palabras es el término más usado para designar la unión entre las telecomunicaciones y la informática.

TCP/IP: transmisión control protocol/internet protocol: Conjunto de protocolos que hacen posible la interconexión y tráfico de la Red Internet

CAPITULO III:

MARCO JURÍDICO POSITIVO VIGENTE

3.1. DELITOS INFORMÁTICOS EN EL MARCO JURÍDICO VIGENTE.

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

Al respecto, existen dos grandes grupos de valores merecedores de amparo específico por la legislación penal boliviana.

- Por una parte, la criminalidad informática puede afectar a bienes jurídicos tradicionalmente protegidos por el ordenamiento penal, tal el caso de delitos en los que se utiliza el computador para redactar una carta difamando a personas físicas o jurídicas, o atentar contra la integridad personal, la fe pública o la seguridad nacional.
- En otros casos las conductas del agente van dirigidas a lesionar Bienes no protegidos tradicionalmente por la legislación penal, tal el caso de los Bienes Informáticos, consistentes en datos, información computarizada, archivos y programas insertos en el soporte lógico del ordenador. En este tipo de conductas disvaliosas se encuentran entre otros el fraude electrónico y el sabotaje informático.

En Bolivia, en el año de 1989, se consideró el análisis y tratamiento sobre Legislación Informática concerniente a contratación de bienes y servicios informáticos, flujo de información computarizada, modernización del aparato

productivo nacional mediante la investigación científico- tecnológica en el país y la incorporación de nuevos delitos emergentes del uso y abuso de la informática.

Asimismo, el Código Penal Boliviano 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 en amplitud la descripción de estas conductas delictivas detalladas anteriormente.

3.1.1. CÓDIGO PENAL ARTS. 363 BIS, 363 TER.

Artículo 363 bis. - (MANIPULACIÓN INFORMÁTICA). El que con la intención de obtener un beneficio indebido para sí o un tercero, manipule un procesamiento o transferencia de datos informáticos que conduzca un resultado incorrecto o evite un proceso tal cuyo resultado habría sido correcto, ocasionando de esta manera una transferencia patrimonial en perjuicio de un tercero, será sancionado con reclusión de uno (1) a cinco (5) años y con multa de sesenta (60) a doscientos (200) días.

Artículo 363 ter. — (ALTERACIÓN, ACCESO Y USO INDEBIDO DE DATOS INFORMÁTICOS). El que sin estar autorizados se apodere, acceda, utilice, modifiquen, suprima o inutilicé, datos almacenados en una computadora o en cualquier soporte informático, ocasionando perjuicio el titular de la información, será sancionado con prestación de trabajo hasta un (1) año o multa hasta doscientos (200) días.[1]

La ilicitud reflejada en esta novísima figura jurídica penaliza el procesamiento de datos mal manejados con intencionalidad que supone resultados incorrectos o podrían evitar la conclusión de un proceso correcto en cualquier transferencia patrimonial siendo un requisito esencial que se realice utilizando la informática como el medio propicio para cometer este ilícito. Esta conducta del sujeto activo se

[1] QUIROZ & LECOÑA, "Código Penal", Tercera Edición, 2011, Pág. 216.

convierte en dolosa porque existe la intencionalidad previa de buscar el resultado pero además existe la posibilidad de la agravación cuando las víctimas son múltiples y afectadas por el mismo delito y sujeto. Por consiguiente, la atipicidad de gran parte de figuras delictivas informáticas, reguladas en nuestro ordenamiento jurídico penal vigente pero reguladas en ordenamientos jurídicos similares en países extranjeros, imposibilita una calificación jurídico-legal que individualice a la mismas, llegando a existir una alta cifra de criminalidad e impunidad informática, haciéndose imposible sancionar como delitos, hechos no descritos 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*" (no hay crimen si no hay ley) .

Así mismo resulta imposible extender el concepto de bienes muebles e inmuebles a bienes incorporales como ser los datos, programas e información computarizada. En las últimas décadas, hay una preocupación en reformar las legislaciones visualizando la tipificación de nuevas figuras delictivas. Tal el caso de Bolivia, donde se percibe el interés en proteger al individuo frente la vulnerabilidad existente en los bienes informáticos de los sistemas computarizados. La legislación penal contempla sólo la tipificación de la manipulación informática, la alteración, acceso y uso indebido de datos informáticos. No menciona nada sobre sabotaje informático empresarial, espionaje informático, parasitismo informático y otras figuras como fraude informático. En nuestro país a esta fecha se está elaborando un Proyecto de: *LEY GENERAL DE TELECOMUNICACIONES, TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN*, en donde existe una normativa de *Protección al usuario***: "***El Estado garantiza el acceso a servicios de telecomunicaciones/TIC en adecuadas condiciones de elección, precio y calidad, salvaguardando, en la prestación de éstos, la vigencia de los imperativos constitucionales, en particular, el respeto a los derechos, al honor, a la intimidad, a la protección de los datos personales, al secreto*

en las comunicaciones, la protección a la juventud, a la infancia y a los grupos con necesidades especiales".[2]

3.2. CONSTITUCIÓN POLÍTICA DEL ESTADO, ARTS. 103, 106, 251, 252.

Nuestra nueva constitución política del Estado del 7 febrero 2009 dentro del capítulo sexto DE EDUCACIÓN, INTERCULTURALIDAD Y DERECHOS CULTURALES, sección IV CIENCIA, TECNOLOGÍA E INVESTIGACIÓN, habla precisamente de las garantías que otorga el Estado al desarrollo de la ciencia y la investigación científica, además de indicar que el Estado destinará recursos que sean necesarios para este propósito, por tanto el planteamiento que hacemos en el presente trabajo está basado precisamente en aquellas directrices que nuestra constitución tiene como objetivo, directrices que son claras, específicas y sobre todo en beneficio de una sociedad que requiere de protección y seguridad en este ámbito informático.

SECCIÓN IV

CIENCIA, TECNOLOGÍA E INVESTIGACIÓN

ARTÍCULO 103.

Parágrafo II. El Estado asumirá como política la implementación de estrategias para incorporar el conocimiento y aplicación de nuevas tecnologías de información y comunicación.

Parágrafo III. El estado, las universidades, las empresas productivas y de servicios públicas y privadas, y las naciones y pueblos indígena originarios campesinos,

[2] PROYECTO LEY GENERAL DE TELECOMUNICACIONES, Tecnologías de Información y Comunicación, Titulo I, Disposiciones Generales, ARTÍCULO 6.- (PRINCIPIOS).

desarrollarán y coordinarán procesos de investigación, innovación, promoción, divulgación, aplicación y transferencia de ciencia y tecnología para fortalecer la base productiva e impulsar el desarrollo integral de la sociedad, de acuerdo con la ley.

En resumen es el Estado el actor principal para la implementación de tecnologías y desarrollo de las mismas quien deberá garantizar una apropiada gestión todo en beneficio de la comunidad. Pero además el estado garantiza el libre ejercicio de la comunicación y el derecho a la información, esto significa en el caso específico de la red informática o Internet una condición implícita que es precisamente la libertad de emitir ideas opiniones, sobre diferentes aspectos que conllevan el quehacer cotidiano de los ciudadanos.

ARTÍCULO 106.

Parágrafo II. El Estado garantiza a las bolivianas y los bolivianos el derecho a la libertad de expresión, de opinión y de información, a la rectificación y a la réplica, y el derecho a emitir libremente las ideas por cualquier medio de difusión, sin censura previa.[3]

Entonces planteamos que existen las garantías suficientes que el Estado brinda para la implementación de nuevas tecnologías y estrategias incorporando el conocimiento y la ciencia en beneficio de la sociedad como es la nuestra, no cabe duda que existe la normativa jurídica positiva que respalda tal afirmación, es donde es necesario precisar en base a la inseguridad jurídica que habíamos planteado respecto a los delitos informáticos, allanar el camino para crear un organismo policial al interior de la estructura orgánica de la fuerza pública y combate a dicho fenómeno delincuencial, policía que al estar provista como manda la norma de todos aquellos elementos tanto físicos como personales a la par de los nuevos adelantos técnicos científicos, precisamente el planteamiento de la creación de este órgano policial está

[3] CONSTITUCIÓN POLÍTICA DEL ESTADO, "Gaceta Oficial de Bolivia", 7 Febrero 2009, Págs. 40-41.

acompañado de propuestas en base a la normativa constitucional reflejadas en los artículos:

CAPÍTULO SEGUNDO

POLICÍA BOLIVIANA

ARTICULÓ 251.

Parágrafo I. La Policía Boliviana, como Fuerza Pública, tiene 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 boliviano. Ejercerá la función policial de manera integral, indivisible y bajo mando único, en conformidad con la Ley Orgánica de la Policía Boliviana y las demás leyes del Estado.

ARTÍCULO 252. Las Fuerzas de la Policía Boliviana dependen de la Presidenta o del Presidente del Estado por intermedio de la privada Ministra o Ministro de gobierno.[4]

3.3. LEY ORGÁNICA DE LA POLICIA ARTS. 8, 10, 41, 43.

La Ley Orgánica de la Policía Boliviana, se refiere fundamentalmente a que esta es una institución del Estado que cumple funciones de carácter público, preventivos y de auxilio, todo esto fundado en valores sociales de seguridad, de justicia preservando el ordenamiento jurídico vigente garantizando y asegurando el normal desenvolvimiento de todas las actividades del conjunto de la sociedad.

La Policía Boliviana fija su desenvolvimiento por la Constitución Política del Estado, la Ley Orgánica de la Policía y sus reglamentos, esta tiene a su cargo la totalidad de la actividad policial, en ese marco estaríamos siguiendo en contra la normativa al tratar de crear una policía informática paralela a la oficial que las leyes prevén, la

institución del orden depende del Presidente del Estado, quien ejerce autoridad por intermedio del Ministro del Interior. Pero veamos lo que indica la Ley Orgánica de la Policía Boliviana.

LEY ORGÁNICA DE LA POLICÍA BOLIVIANA

TÍTULO II

Organización y Funciones Capítulo I. Organización

ARTÍCULO 8. La Policía Nacional es una institución técnico científica, organizada según los principios de administración, integración de funciones, jerarquía y atribuciones propias para esta clase de actividades.

ARTÍCULO 10. El Comando General creará o suprimirá las unidades de los organismos operativos de la administración desconcentrada, de acuerdo a las necesidades del servicio.

ARTÍCULO 41. Organismos Operativos de Línea, sobre los servicios que en coordinación permanente se encargan de la ejecución y conocimiento de las funciones policiales señaladas en el capítulo III, artículo 7º. De la presente ley, para el logro de los objetivos institucionales.

ARTÍCULO 43. Las Unidades de Criminalística son las encargadas de investigar delitos, identificar y aprehender a los autores, coautores y cómplices y remitirlos a disposición de las autoridades competentes.[5]

La norma es clara y específica en lo que se refiere a la creación al interior de la policía de nuevos organismos operativos, es el Comandante General de la Policía, encargado de la creación o supresión de unidades de acuerdo a los requerimientos

de la sociedad, también cualquier organismo operativo que tenga relación con el aspecto delictivo y la criminalística estará comprendido y coadyuvará a sus funciones a la unidad de criminalística llamada también Fuerza Especial de Lucha contra el Crimen, quienes son las encargadas de la investigación, de la aprehensión, de la identificación de todos quienes atenten la normativa jurídica.

En conclusión podemos afirmar que la normativa existe en lo que se refiere a la creación de un nuevo órgano policial y las condiciones para la misma también son específicas por cuanto la policía boliviana es parte del Estado.

CAPITULO IV

LOS DELITOS INFORMATICOS: CONCEPTOS, CARACTERISTICAS Y SUJETOS:

4.1. CONCEPTO DE DELITO.

Los estudiosos del Derecho Penal han intentado formular una noción de delito que sirviese para todos los tiempos y para todos los países, lógicamente esto es imposible ya que pretender la conexión entre la vida social y jurídica de cada pueblo en diferentes siglos nunca ha sido la misma, evolucionando las formas y mecanismos de cometer nuevos delitos, siendo el delito enteramente un acto humano, por representar una exteriorización de la voluntad.

Jaime Moscoso, se refiere al mismo: "*el delito es una acción típica, antijurídica y culpable, sancionada con penas o medidas de seguridad*". Pero subsisten las discrepancias, hay analistas que excluyen de esta definición su referencia la pena y a la medida de seguridad, pues, bastaría citar los caracteres del acto delictivo (acción típica, antijurídica y culpable). La conducta humana para ser regulada por el derecho tiene que exteriorizarse de algún modo, los pensamientos, intenciones y deseos que no se manifiestan son irrelevantes para el derecho penal y quedan fuera de sus conminaciones: Cogitationis poenam neno patitur (por sus pensamientos nadie sufre la pena) [1]

Para Jiménez de Asúa, se entiende delito "*el acto típicamente antijurídico, culpable sometido a veces a condiciones objetivas de penalidad, imputable a un hombre sometido una sanción penal*". En consecuencia, según este mismo autor, las características del delito serían: actividad, adecuación típica antijuricidad, imputabilidad, culpabilidad, penalidad y en ciertos casos condición objetiva de punibilidad.

[1] MOSCOSO DELGADO, Jaime, "Introducción al Derecho", Librería Editorial Juventud, Pág. 522.

Nuestro ordenamiento jurídico penal al respecto no hace precisiones conceptuales referidas al delito, simplemente hace la enumeración de delitos contra la normativa en el libro segundo parte especial.

Para Carrara, delito es "*la infracción de la ley del Estado, promulgada para seguridad de los ciudadanos, resultante de un acto externo del hombre, positivo o negativo, moralmente imputable y políticamente dañoso*".

Osorio en su diccionario jurídico, cita a Soler quien define como "*una acción típicamente antijurídica culpable y adecuada una figura legal conforme a las condiciones objetivas de esta*", por lo cual sus elementos sustantivos son: la acción, la antijuricidad, la culpabilidad y la adecuación a una figura.[2]

El delito vendría constituirse como un hecho ilícito de negación al derecho, llamamos hecho ilícito a la conducta contraria a la prescrita por una norma jurídica o, lo que es lo mismo, a la conducta prohibida por dicha norma. Hay, pues, una relación estrecha entre la noción de hecho ilícito y la de obligación jurídica. El hecho ilícito es lo opuesto a una conducta obligatoria y hay una obligación jurídica de abstenerse de todo acto ilícito.[3]

4.2. CONCEPTO DE DELITO INFORMATICO Y SUS CARACTERÍSTICAS.

ROMEO CASABONA, se refiere a la definición propuesta por el Departamento de Justicia Norteamericana, según la cual "*delito informático es cualquier acto ilegal en relación con el cual el conocimiento de la tecnología informática es esencial para su comisión, investigación y persecución"*.[4]

---

[2] OSSORIO, Manuel, **Ob.cit.,** Edición 2004.

[3] KELSEN, Hans, "Teoría Pura del Derecho", ed., Unión Ltda., Santa Fe Bogotá, Pág. 76.

[4] ROMEO CASABONA, Carlos María, "Poder y Informático y Seguridad Jurídica", Madrid, 1988.

"*Delito informático*", crimen genérico o crimen electrónico, acción que agobia con operaciones ilícitas realizadas por medio de Internet o que tienen como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet. Sin embargo, las categorías que definen un delito informático son aún mayores y complejas y pueden incluir delitos tradicionales como el fraude, el robo, chantaje, falsificación y la malversación de caudales públicos en los cuales ordenadores y redes han sido utilizados. Con el desarrollo de la programación y de Internet, los delitos informáticos se han vuelto más frecuentes y sofisticados.[5]

El delito informático incluye una amplia variedad de categorías de crímenes. Generalmente este puede ser dividido en dos grupos:

- Crímenes que tienen como objetivo redes de computadoras, por ejemplo, con la instalación de códigos, gusanos y archivos maliciosos, Spam, ataque masivos a servidores de Internet y generación de virus.
- Crímenes realizados por medio de ordenadores y de Internet, por ejemplo, espionaje, fraude y robo, pornografía infantil, pedofilia, etc. Un ejemplo común es cuando una persona comienza a robar información de websites o causa daños a redes o servidores. Estas actividades pueden ser absolutamente virtuales, porque la información se encuentra en forma digital y el daño aunque real no tiene consecuencias físicas distintas a los daños causados sobre los ordenadores o servidores.
- Un ordenador puede ser fuente de evidencia y, aunque el ordenador no haya sido directamente utilizado para cometer el crimen, es un excelente artefacto que guarda los registros, especialmente en su posibilidad de codificar los datos. Esto ha hecho que los datos codificados de un ordenador o servidor tengan el valor absoluto de evidencia ante cualquier corte del mundo.

[5] http://www. delitos informaticos.com/HTML.

Con la expresión *delito informático* se define a todo ilícito penal llevado a cabo a través de medios informáticos y que está íntimamente ligado a los bienes jurídicos relacionados con las tecnologías de la información o que tiene como fin estos bienes. Cuando se presenta los siguientes casos:

- Manipulación en los datos e informaciones contenidas en los archivos o soportes físicos informáticos ajenos.
- Acceso a los datos y/o utilización de los mismos por quien no está autorizado para ello.
- Introducción de programas o rutinas en otras computadoras para destruir información, datos o programas.
- Utilización de la computadora y/o los programas de otra persona, sin autorización, con el fin de obtener beneficios propios y en perjuicio de otro.
- Agresión a la privacidad mediante la utilización y procesamiento de datos personales con fin distinto al autorizado.

Entre sus características tenemos:

- Rapidez y acercamiento, en tiempo y espacio. Programación de retardos, accesos remotos, etc.
- Facilidad para encubrir el hecho. (El mismo programa después de realizar el ilícito cambia la rutina dejando el archivo en su estado original).
- Facilidad para borrar las pruebas.[6]

Existen diversas clasificaciones, pero entre las más aceptadas está la de Julio Téllez Valdez, que clasifica los delitos informáticos en base a dos criterios. [7]

---

[6] GIL ALBARRAN, Guillermo Edward, "Derecho Informático", ed., Megabyte Primera Edición, 2007, Págs. 484-485.

[7] TÉLLEZ VALDÉZ, Julio, " Derecho informático", ed., Mac Graw Hill, México, 2003.

- **Como instrumento o medio**: en esta categoría se encuentran las conductas criminales que se valen de las computadoras como método, como medio o símbolo de en la Comisión de ilícito, por ejemplo.
    - Falsificación de documentos vía computarizada (tarjetas de crédito, cheques, etcétera)
    - Variación de los activos y pasivos en la situación contable de las empresas.
    - Planeamiento y simulación de delitos convencionales (robo, homicidio, fraude, etc.)
    - Lectura, sustracción o copiado de información confidencial.
    - Modificación de datos tanto en la entrada como en la salida.
    - Aprovechamiento indebido violación del código para penetrar un sistema.
    - Introduciendo instrucciones inapropiadas.
    - Variación en cuanto al destino de pequeñas cantidades de dinero es una cuenta bancaria apócrifa.
    - Uso no autorizado de programas de cómputo.
    - Introducción de instrucciones que provocan interrupciones en la lógica interna de los programas.
    - Alteraciones del funcionamiento de los sistemas, a través de los virus informáticos.
    - Obtención de la información residual impresa en papel luego de la ejecución de trabajos.
    - Acceso a áreas informatizadas en forma no autorizada.
    - Intervención en las líneas de comunicación de datos o el proceso.
- **Como fin u objetivo:** en esta categoría, se enmarcan las conductas criminales que van dirigidas contra las computadoras, accesorios o programas como entidad física, ejemplo:

    - Programación de instrucciones que producen un bloqueo total al sistema.

- Destrucción de programas por cualquier método.
- Daño a la memoria.
- Atentado físico contra la máquina o sus accesorios.
- Sabotaje político terrorismo en que se destruya o surja un apoderamiento de los centros neurálgicos computarizados.

Para DAVARA RODRIGUEZ, no parece adecuado hablar de delito informático y a que, como tal, no existe, si atendemos a la necesidad de una tipificación en la legislación penal para que pueda existir un delito.[8]

4.3. SUJETOS ACTIVOS Y PASIVOS EN EL DELITO INFORMATICO

4.3.1. SUJETO ACTIVO.

Las personas que cometen los delitos informáticos son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, los sujetos activos tienen facilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentra en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de sistemas informatizados, aún cuando en muchos de los casos, no desarrollan actividades laborales que faciliten la comisión de este tipo de delitos.[9]

Aquí, se considera que a pesar de que los delitos informáticos no poseen todas las características de los delitos "de cuello blanco", si coinciden en un número importante de ellas, aunque es necesario señalar que estas aseveraciones pueden y deben ser objeto de un estudio más profundo.

4.3.2. SUJETO PASIVO.

[8] DAVARA RODRIGUEZ, Miguel Ángel, “Manual de Derecho Informático”, Pamplona Aranzadi, 1997.

[9] GIL ALBARRAN, Guillermo Edward, **Ob. Cit.,** Pág. 489.

En primer término tenemos que distinguir que el sujeto pasivo o víctimas del delito que es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo, y en el caso de los delitos informáticos, mediante el podemos conocer los diferentes ilícitos que cometen los delincuentes informáticos, que generalmente son descubiertos casuísticamente debido al desconocimiento del modus operandi.[10]

Su víctima; quien en su persona, derechos o bienes, o en los de los suyos, aparecido ofensa penada en la ley y punible por el sujeto activo. Aunque se personalice, siempre el sujeto pasivo del delito, en ciertas infracciones penadas no hace sino trasladarse a la colectividad, en alguno de sus grados, como la sociedad o el Estado.[11]

4.4. CLASIFICACIÓN DE DELITOS INFORMATICOS

4.4.1. FRAUDE.

Es en general el engaño, el abuso, la maniobra inescrupulosa. 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.

[10] GIL ALBARRAN, Guillermo Edward, "Derecho Informático", ed., Megabyte, 2007, Pág. 494.

[11] OSSORIO, Manuel. **Ob.cit.,** Editorial Heliasta, Edición 2004.

- Alterar, destruir, suprimir o robar datos, un evento que puede ser difícil de detectar.
- Alterar o borrar archivos.
- Alterar o dar un mal uso a sistemas o software, 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.

4.4.2. PORNOGRAFÍA VIRTUAL INFANTIL.

La pornografía es una de las fuentes económicas más prominentes e importantes que la mafia internacional opera, y que mueve más dinero que muchas multinacionales. Las autoridades policiales y las organizaciones no gubernamentales (ONG´S) están muy preocupadas porque la pornografía infantil vía Internet sigue creciendo pese a todos los esfuerzos realizados para erradicarla.

Al respecto nuestro ordenamiento penal, hace una descripción general enfocando la problemática de los Niños, Niñas o Adolescentes y de Personas Jurídicamente Incapaces. Esta explotación sexual infantil sobre todo en la red informática cobró gran importancia como problemática de la sociedad debido a que gran cantidad de ellos caen en las diferentes redes de la industria pornográfica o explotación sexual, el problema es grave y afectado a casi todos los países, Asia es la región más afectada, pero América Latina no está lejos, en países como el nuestro las dificultades están relacionadas con el desarrollo de nuestras sociedades y el grado de cultura que éstas poseen, la explotación sexual presenta muchísimas dificultades y grandes desafíos para organizaciones no gubernamentales, agencias intergubernamentales y gobiernos, hay muchos factores que imposibilitan la lucha contra este tipo de delitos que se dan en la red informática. Es necesario plantear

desde la sociedad, el Estado nuevas políticas de lucha frente a estos delitos que en la mayoría de los casos no deja huellas ni gastos que puedan conducir a la aprehensión de los autores, al respecto el Código Penal vigente:

ARTÍCULO 323 bis. (Pornografía de Niñas, Niños o Adolescentes y de Personas Jurídicamente Incapaces).

Comete el delito de pornografía de Niñas, Niños o Adolescentes y de personas Incapaces, quien procure, obligue, facilite o induzca, por cualquier medio, a una o varias de estas personas a realizar actos sexuales o de exhibicionismo corporal con fines lascivos o sexuales, reales o simulados, con el objeto de video grabarlos, fotografiarlos, filmarlos, exhibirlos o describirlos a través de anuncios impresos, transmisión de archivos de datos en red pública o privada de telecomunicaciones, sistemas de cómputo, electrónicos o sucedáneos. Al autor de este delito se le impondrá pena de cinco a diez años de presidio.

A quien fije, imprima, video grabe, fotografíe, filme o describa actos de exhibicionismo corporal o lascivos o sexuales, reales o simulados, en que participen una o varias niñas, niños o adolescentes y de personas incapaces, se le impondrá la pena de tres a seis años de reclusión, así como el decomiso de los objetos, instrumentos y productos del delito.[12]

La misma pena del párrafo anterior, se impondrá a quien reproduzca, almacene, distribuya, venda, compre, arriende, exponga, publicite, transmita, importe o exporte el material a que se refieren los párrafos anteriores."

4.4.3. TERRORISMO VIRTUAL.

El terrorismo virtual, llamado también Ciber-terrorismo es cuando concurren en un mismo objetivo, muchos delincuentes criminales informáticos, los cuales deciden atacar masivamente el sistema de ordenadores de una empresa, compañía, centro de estudios, oficinas oficiales, etc. es uno de sus novedosos delitos informáticos

[12] QUIROZ Y LECOÑA, "Código Penal Comentado", Tercera Edición, 2011, Pág. 193.

donde los criminales actúan masivamente para atacar un cierto y determinado objetivo ya sea éste laboral, empresarial u oficial, un ejemplo de ello sucedió cuando un hacker conocido de Nueva Zelanda llamado Thor Walker y apodado AKILL, quien en compañía de otros hackers, dirigió un ataque en contra del sistema de ordenadores de la Universidad de Pennsylvania en el año 2008.

La difusión de noticias falsas en Internet constituye otra modalidad del terrorismo virtual por ejemplo: el publicar que va a explotar una bomba determinada área del metro de una ciudad donde existe gran cantidad de gente que circula por alrededor también es considerado terrorismo informático y debería ser procesado.

Una modalidad de terrorismo virtual se da con mucha frecuencia en el país vecino del Perú, una banda de delincuentes denominados los "ETA-cholos", quienes fueron desarticulados el 28 agosto 2008, éstos enviaban e-mails a centros y clínicas de estética en España, la guardia civil de ese país, recibió las denuncias determinando identificando que provenían de Lima Perú, estos operaban bajo la fachada y argumento de ser miembros de la organización terrorista ETA, amenazando y reclamando un supuesto "*impuesto revolucionario",* atemorizando e intimidando sus víctimas, la banda tenía integrantes en ambos países con diferentes nacionalidades, entre ellos un boliviano.

4.4.4. EL SPAM.

Son aquellos correos electrónicos no deseados, los cuales se infiltran en los correos electrónicos de los usuarios por un supuesto propósito comercial. La regulación jurídica en cuanto al spam es relativamente nueva y aún desconocida en nuestro medio, en muchos países denominados del "*primer mundo"* el spam debe cumplir estrictamente con ciertos requisitos como permitir que el usuario pueda escoger el hecho de recibirlos o desecharlos, dicho mensaje. Pese a que los diferentes proveedores del servicio de Internet, tienen implementadas políticas de restricción frente al spam, además de contar los usuarios con medidas físicas de eliminación de correos electrónicos no deseados, existen spams que vulneran, atraviesan todas estas barreras protectoras y en algunos casos estos sirven para la recolección de

datos del usuario sin su consentimiento, que generalmente éstos son usados para el robo de identidad. Independientemente del tema que trate, muchos de ellos son utilizados para introducir virus en los equipos y destruir la base de datos, para así poder tener acceso posteriormente por los hackers, el correo electrónico no solicitado, conocido habitualmente como Spam o correo basura, está terminantemente prohibido por la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSICE), publicada en el BOE del 12 de julio de 2002. Hay que prestar una atención especial a aquellos correos electrónicos cuyo contenido está relacionado con productos farmacéuticos, ya que, podrían incurrir en infracciones relacionadas con la salud pública.

4.4.5. ROBO DE IDENTIDAD.

También es una modalidad nueva dentro de la categoría de delitos informáticos, esta consiste en la obtención de datos de una persona, obtenida mediante artificios o engaños o falsas paginas, donde la victima inocentemente proporciona detalles, para posteriormente usar esos datos ya sea en fraudes, estafas, en el llenado de formularios con fines de préstamos, o dar los mismos para gravámenes o hipotecas que recaerán sobre el titular de la identidad, en nuestro país la Fuerza Especial de Lucha contra el Crimen recibe este tipo de denuncias, cada vez más en aumento, debido a que este delito deriva en acciones criminales tendientes a sacar ventaja de identidad y económica de quienes son víctimas de ellos. Esta modalidad con la finalidad de robar la identidad de un sujeto se da a través del denominado “phising” que lo veremos más adelante con detalle, en muchos casos el objetivo principal es recabar el “login” o password de la cuenta bancaria de la víctima, que consiste en recomendar a los usuarios visitar un portal web “falso”, haciéndolo creer que es original.

4.4.6. ROBO DE INFORMACION CONFIDENCIAL.

En la mayoría de los casos va relacionada con el comercio, la empresa y servicios esta modalidad de delito ha ido constituyéndose una de las más importantes dentro

su género, debido fundamentalmente a que propiciándose del medio informático muchos criminales o delincuentes informáticos han ido aprovechando las ventajas que esta les brinda para extraer, sustraer, obtener información confidencial o secretos que posibiliten descifrar fórmulas, datos, especificaciones ocultas y utilizarlas en busca de un beneficio personal o patrimonial.

4.4.7. ATENTADO A LA PRIVACIDAD O INTIMIDAD.

Constituyen aquellos delitos de observación, escucha o registro de hechos, palabras, escritos o imágenes, que son respecto a la vida personal o familiar ajena, utilizando para ello instrumentos, procesos técnicos u otros medios, existe una violación a la intimidad de otra persona y es agravado si se utiliza algún medio de comunicación social. La revelación de aspectos de la intimidad conocidas por haber trabajado para el agraviado es un delito, no interesando el medio por donde se realiza la revelación.

4.4.8. CLONACIÓN DE TARJETAS.

Esta también es una modalidad reciente de delito informático, se da principalmente en el entorno bancario quienes proporcionan a sus usuarios claves o PINES para el uso principalmente de cajeros automáticos, la modalidad con la que se conoce la clonación de estas tarjetas se denomina: los datos para clonar tarjetas generalmente son obtenidos en páginas de contenido sexual o pornográfico en donde se solicita como pretexto comprobar la mayoría de edad, a través de una tarjeta de débito o crédito, otras de las veces también estos delincuentes se encargan de averiar, colocar dispositivos o introducir objetos dentro de las ranuras de los cajeros electrónicos, para copiar o cambiar por una duplicada falsa, la tarjeta original de la víctima y así obtener sus datos personales.

4.4.8.1. **PISHING**.

Es el apoderamiento de contraseñas, claves, datos confidenciales para posteriormente vaciar cuentas bancarias o transferir dinero a otras cuentas, el

phishing está enmarcado dentro del ámbito de las estafas cibernéticas, se caracteriza por intentar adquirir la información confidencial de forma fraudulenta, el autor conocido como phiser, se hace pasar por otra persona o suplantando la imagen de una empresa de confianza, el objetivo consiste en obtener datos reales de clientes del sistema financiero. Estos piratas informáticos crean páginas de entidades financieras conocidas, pero con nexos falsos. Cuando el usuario utilice estos enlaces bancarios se conecta con las direcciones de los estafadores que se apropian de sus datos. Otro de los métodos que emplean estos delincuentes radica en enviar mensajes a la gente pidiendo la verificación de las cuentas y del número de PIN bancario. La forma más segura para protegerse de este tipo de estafa es no responder nunca ninguna solicitud de información personal a través de correo electrónico, llamada telefónica o mensajes de texto en los celulares.

4.4.9. SABOTAJE INFORMATICO.

Se da fundamentalmente cuando alguien utiliza, ingresa o irrumpe indebidamente una base de datos, sistema o red de computadoras o cualquier parte de la misma, para alterar un esquema u otro similar, para interferir, interceptar acceder o borrar información en tránsito. El acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones, recurriendo a uno de los diversos medios que se mencionan a continuación.

- El delincuente puede aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema.
- A menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sistema, esto suele suceder con frecuencia en los sistemas en los que los usuarios pueden emplear contraseñas comunes o contraseñas de mantenimiento que están en el propio sistema.
- Es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del

sistema. Las técnicas que permiten cometer sabotajes informáticos son a través de: [13]

- **VIRUS.** Es una serie de claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos. Un virus puede ingresar en un sistema por conducto de una pieza legitima de soporte lógico que ha quedado infectada, así como utilizando el método del Caballo de Troya.
- **GUSANOS.** Se fabrica de forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse. En términos médicos podría decirse que un gusano es un tumor benigno, mientras que el virus es un tumor maligno. Ahora bien, las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus: por ejemplo, un programa gusano que subsiguientemente se destruirá puede dar instrucciones a un sistema informático de un banco pare que transfiera continuamente dinero a una cuenta ilícita.

4.4.10. FALSIFICACIONES INFORMÁTICAS.

Tienen como objetivo alterar los datos y documentos almacenados en forma computarizada, y utilizan como instrumentos a las computadoras para efectuar falsificaciones de documentos de uso comercial, utilizando muchas veces fotocopiadoras computarizadas a color en base a rayos láser, estas fotocopiadoras

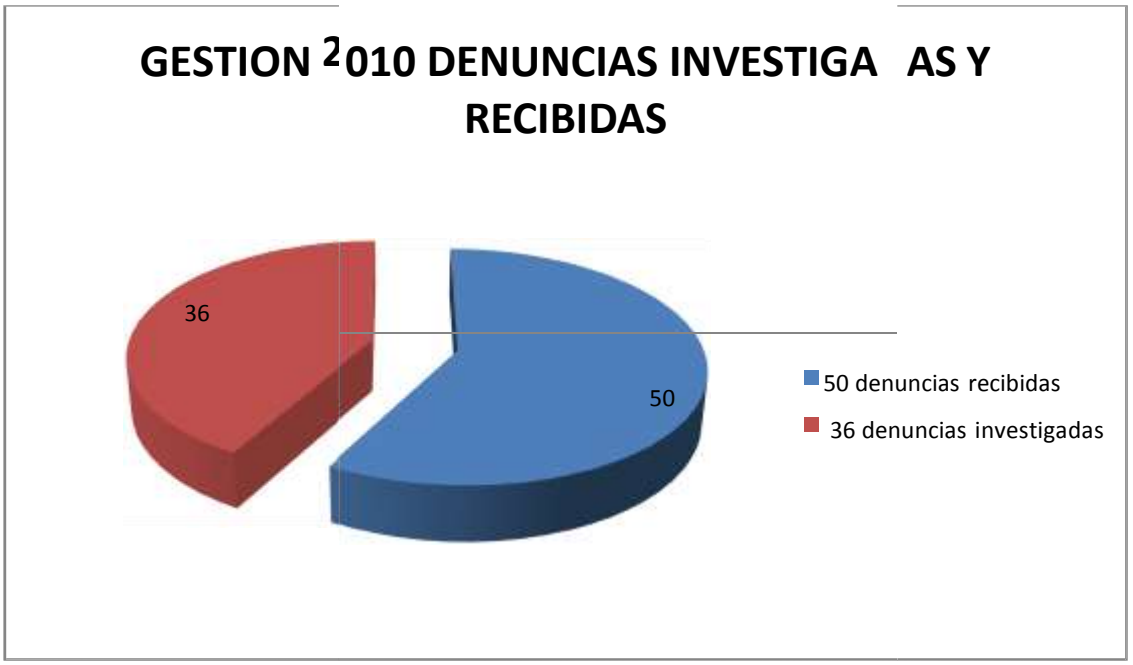
[13] LEVENE Ricardo, CHIARAVALLOTI Alicia, "Introducción a los delitos informáticos, tipos y legislación", http://www.chiaravalloti_asociados.dtj.com.ar/links_1.htm.

pueden hacer copias de alta resolución, pueden modificar documentos e incluso pueden crear documentación nueva y falsa de entidades autorizadas para emitirlas sin tener que recurrir a un original, y los documentos que producen son de tal calidad que solamente un experto puede diferenciarlos de los documentos auténticos. Este delito es muy común en nuestro medio.

4.4.11. ESTADISTICAS RECIENTES SOBRE DELITOS INFORMATICOS.

Las últimas estadísticas con las que se cuenta fueron las de la gestión 2010, la Fuerza Especial de Lucha contra el Crimen, recibió un incremento significativo respecto de otras gestiones se dieron 50 denuncias de delitos informáticos, de las que sólo 36 aún siguen siendo investigadas y ninguna hasta el momento ha sido resuelta por su complejidad, sólo hay dos peritos para atender este tipo de casos a ello se suma la falta de fiscales especializados en la materia para conducir las investigaciones. En el caso del departamento de La Paz, 12 casos están en proceso de investigación y en tres de ellos a importantes avances, el jefe de la división de delitos informáticos de la Fuerza Especial de Lucha contra el Crimen, nos informa que hasta el momento existen dos personas enviadas a la cárcel en espera de una sentencia, uno sobre clonación de tarjeta de crédito y el otro remitido por estafa electrónica.[14]

[14] CLAURE, Edson, Jefe de la "División del Delitos Informáticos de la FELCC", Entrevista.



Fuente: FUERZA ESPECIAL DE LUCHA CONTRA EL CRIMEN (FELCC).

Es difícil elaborar estadísticas sobre este tipo de delitos. La "*cifra negra*" es muy alta; no es fácil descubrirlo y sancionarlo, en razón del poder económico, la habilidad y conocimientos de quienes los cometen, pero los daños económicos son altísimos; existe una gran indiferencia de la opinión pública sobre los daños ocasionados por los delitos informáticos a la sociedad; ésta no considera delincuentes a los sujetos que cometen este tipo de delitos, no los segrega, no los desprecia, ni los desvaloriza, por el contrario, el autor o autores de este tipo de delitos muchas veces en su entorno social se consideran a sí mismos "*respetables*" por sus conocimientos adquiridos. Otra coincidencia que tienen estos tipos de delitos es que, generalmente, son objeto de medidas o sanciones de carácter administrativo y no privativo de la libertad.

4.5. LOS DELITOS INFORMATICOS EN BOLIVIA.

Para José Alfredo Arce Jofre, la tipificación de delitos informáticos está contenida en el capítulo XI del código penal boliviano, toma en cuenta que los sistemas

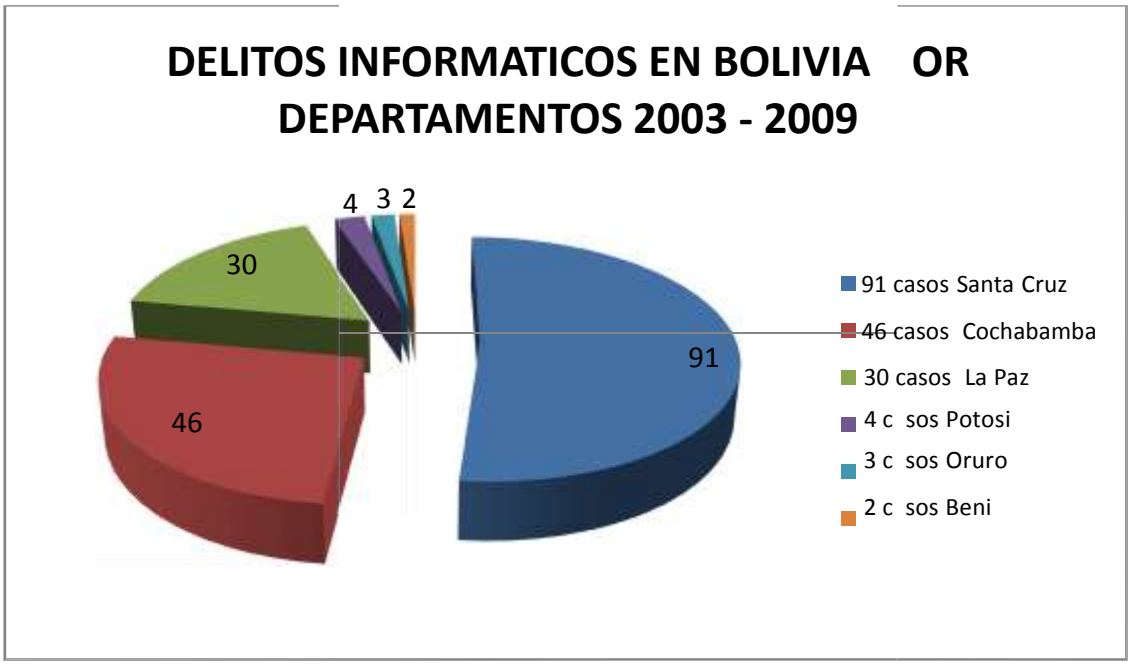
informáticos procesan y transfieren información valiosísima, o que esta información no sólo es valiosa en sí misma sino que puede contener información representativa del patrimonio de las personas, la comisión de estos delitos son mediante el sistema, es decir que requieren el uso de sistemas informáticos, y contra el sistema debido a que la conducta antijurídica es contra la información misma.[15]

Para delimitar en qué sentido se dará la protección penal en el ámbito penal boliviano, es esencial determinar el bien jurídico que se desea proteger. Al respecto, existen dos grandes grupos de valores merecedores de amparo específico por la legislación penal boliviana.

Por una parte, la criminalidad informática puede afectar a:

- Bienes jurídicos tradicionalmente protegidos por el ordenamiento penal, tal el caso de delitos en los que se utiliza el computador para redactar una carta difamando a personas físicas o jurídicas, o atentar contra la integridad personal, la fe pública o la seguridad nacional.
- En otros casos las conductas del agente van dirigidas a lesionar Bienes no protegidos tradicionalmente por la legislación penal, tal el caso de los Bienes Informáticos, consistentes en datos, información computarizada, archivos y programas insertos en el soporte lógico del ordenador. En este tipo de conductas disvaliosas se encontrarían entre otros el fraude electrónico y el sabotaje informático.

[15] ARCE JOFRE, José Alfredo, "INFORMATICA Y DERECHO", ed., Bolivia Dos Mil, Pág. 150.



Fuente: FUERZA ESPECIAL DE LUCHA CONTRA EL CRIMEN (FELCC).

4.5.1. LA POLICIA BOLIVIANA Y EL TRATAMIENTO ACTUAL DE LOS DELITOS INFORMATICOS.

El ministerio público que está compuesto por fiscales no cuenta hasta la fecha con la especialidad requerida en la investigación de delitos informáticos, es esa la razón que motiva que los casos deban ser adecuados a delitos económicos. Al realizar la entrevista a los personeros de la división de casos económicos de la FELCC de La Paz revelaron que hasta el momento no se esclareció ningún caso porque existe la carencia del material de trabajo consistente en tecnología informática de avanzada, presupuesto económico para el personal, ausencia de una capacitación y actualización de conocimientos y sobre todo la falta de expertos en peritaje informático.

El director Nacional de Laboratorio de la FELCC, coronel Jorge Toro, admitió que esta clase de delitos no tienen éxito en su esclarecimiento debido a que para todo el

territorio boliviano sólo hay dos peritos en esa especialidad quienes no abastecen en la investigación de este tipo de casos.[16]

Otra de las causas de las que hemos podido identificar que concurren al no esclarecimiento de los casos informáticos es justamente cuando los interesados o afectados (victimas) abandonan el proceso, tal como suele suceder con los delitos comunes.

4.5.2. PROCEDIMIENTO EN CASO DE DENUNCIAS DE DELITOS INFORMATICOS.

Los datos que proporciona la Fuerza Especial de Lucha contra el Crimen Revelan que en Santa Cruz, departamento de La Paz y Cochabamba son los lugares donde se producen más delitos informáticos desde el año 2003, las divisiones Económicas y de Trata son aquellas encargadas de recibir las primeras denuncias de las víctimas o instituciones afectadas por los "*ciber delincuentes"*, estas oficinas mantienen una coordinación estrecha con los investigadores de la división de delitos informáticos, y esta a su vez con el escaso número de peritos en informática forense dependientes de la dirección Nacional de Laboratorio de la Policía, todos ellos trabajan en conjunto a la cabeza y dirección de un fiscal. Un efectivo de la división de casos económicos de la FELCC, es el encargado de levantar las diligencias de policía para su posterior entrega al fiscal correspondiente, quien a su vez deriva por la gravedad del hecho a la División de Delitos Informáticos.

4.6. LOS DELITOS INFORMATICOS A NIVEL MUNDIAL.

Los diferentes países suelen tener policía especializada en la investigación de estos complejos delitos que al ser cometidos a través de internet, en un gran porcentaje de casos excede las fronteras de un único país complicando su esclarecimiento

[16] TORO, Jorge, "Director Nacional del Laboratorio de la FELCC", Entrevista gestión 2010.

viéndose dificultado por la diferente legislación de cada país o simplemente la inexistencia de ésta. Los últimos reportes de la prensa internacional dan cuenta de ataques a la red y que podemos calificar como de los más graves, en el uso de la red por parte de la mafia internacional que maneja la prostitución y pornografía infantil, por el terrorismo internacional y también por el narcotráfico. Políticos de algunos países han pedido que se reglamente el uso de la red, de modo que quienes prestan el servicio de Internet registren a los clientes, cuándo y dónde llaman y para qué, pero la iniciativa hizo que, en defensa de la libertad y de la privacidad, muchos usuarios honestos y algunas empresas que participan de los beneficios económicos de la red, protestaran enérgicamente.

El desarrollo de las tecnologías informáticas ofrece un aspecto negativo: Ha abierto la puerta a conductas antisociales y delictivas. Los sistemas de computadoras ofrecen oportunidades nuevas, sumamente complicadas para infringir la ley y han creado la posibilidad de cometer delitos de tipo tradicional en formas no tradicionales.

El delito Informático implica actividades criminales que un primer momento los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robo, hurto, fraudes, falsificaciones, perjuicios, estafa, sabotaje, etc., sin embargo, debe destacarse que el uso indebido de las computadoras es lo que ha propiciado la necesidad de regulación por parte del derecho. En los últimos años se ha perfilado en el ámbito internacional un cierto consenso en las valoraciones político- jurídicas de los problemas derivados del mal uso que se hace de las computadoras y la red, lo cual ha dado lugar a que, en algunos casos, se modifiquen los derechos penales nacionales. La ONU ha publicado una descripción de "*Tipos de Delitos Informáticos*", que se transcribió en éste trabajo (ver 1.6.).

CAPITULO V

DE LA ORGANIZACIÓN Y FUNCIONAMIENTO DE LA POLICIA ESPECIALIZADA EN DELITOS INFORMATICOS

5.1. FUNDAMENTACION DE SU CREACION E IMPORTANCIA DE SU FUNCIONAMIENTO.

El desafío que impone la nueva era digital a la sociedad y al conjunto del Estado boliviano, gira en torno a implementar políticas de seguridad ciudadana que garanticen la lucha contra la delincuencia informática en todas las esferas, tecnificando e implementando a organismos de represión, procurando un equilibrio entre la colectividad mediante estos recursos. Al crear la "*unidad Operativa Policial de Reprensión y Prevención de Delitos Informáticos"*, estaríamos dando un paso más en busca de disminuir la delincuencia pero sobre todo de hacer seguro el desenvolvimiento del usuario dentro de una red informática. La importancia radica en incrementar tecnologías de avanzada con peritos expertos en la materia y capacitación permanente, quienes están directamente en relación con el delito, proveerles la tecnología necesaria contribuiría en gran medida a la investigación y aclaración de estos hechos. Un presupuesto otorgado por el Estado boliviano será muy beneficioso en relación a la consecuencia/impacto ocasionado, o al daño económico que producen esta clase de delitos en la sociedad.

5.2. OBJETIVOS Y ALCANCES DE LA UNIDAD ESPECIALIZADA.

Los objetivos específicos de la Policía Informática serían, la recepción directa de todas aquellas denuncias, la investigación, el patrullaje, el peritaje informático y una adecuada capacitación de sus miembros. El alcance de esta unidad especializada estaría delimitado en tanto y cuanto surjan la aparición de nuevas figuras delictivas dentro del campo de los delitos informáticos, el alcance físico de esta unidad sería de manera experimental en el plano departamental, la ciudad de La Paz, constituyéndose posteriormente en un modelo para otros departamentos. Por tanto

combatir investigar y sancionar el crimen organizado conllevaría traspasar fronteras, adoptar legislaciones recomendadas por organismos que reúnen a comunidades de naciones, quienes están en la posibilidad de brindar cooperación, asesoramiento, debido a que es una problemática de carácter global con el peligro que ello implica el mal uso de la tecnología. Entre sus objetivos:

- La, "*unidad Operativa Policial de Reprensión y Prevención de Delitos Informáticos"* es el órgano que tiene como misión, investigar, denunciar y combatir el crimen organizado, nacional y transnacional (Globalizado) y otros 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.
- 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.
- Solicitar las incautaciones y confiscaciones de equipos tecnológicos de las Personas plenamente identificadas, a quienes se les ha probado responsabilidad en la comisión de los delitos investigados.

5.3. CAPACITACION Y ACTUALIZACION PERMANENTE.

Es una importante finalidad contar con capacitación y actualización permanente de todos los miembros que compondrán este ente policial de lucha contra el delito informático, esta capacitación podría abarcar la asistencia a cursos, seminarios y talleres que tecnifiquen y profesionalicen a sus miembros que la componen, ya sean

estos dentro del ámbito nacional o internacional. Las relaciones con otras similares será a la vez una finalidad importante por cuanto, el intercambio de información y conocimientos será fundamental a la hora de esclarecer el investigar estos delitos que generalmente traspasan fronteras y nacionalidades. Esta capacitación enmarcada en la ley Orgánica de la Policía Boliviana, Título IV, Capítulos I y II.

5.4. ASESORAMIENTO Y PERITAJE BRINDADO EN MATERIA DE DELITOS INFORMATICOS.

Al mismo tiempo esta unidad operativa brindaría asesoramiento y labor en peritaje informático, constituyéndose en un instrumento de colaboración, apoyo y certificación para fiscales y jueces en procesos de delitos informáticos. Este apoyo consistirá en:

5.5. PERITAJE INFORMÁTICO.

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

5.5.1. FASES DEL PERITAJE.

La elaboración del informe pericial constara a su vez de tres fases:

- **Fase de adquisición de las pruebas:**

  Recogerá todos aquellos elementos que van a intervenir en la investigación, que son importantes en el proceso de intervención e investigación de los equipos informáticos y que 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.

- **Fase de la investigación:**

El perito informático realizara 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 todas 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.

- **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 analizara 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 el fiscal y este ante los Tribunales.

En el caso del "*manejo de las evidencias",* las recomendaciones generales son: que los Investigadores que llegan primero a una escena del crimen tienen ciertas Responsabilidades, las cuales resumimos:

- **OBSERVE Y ESTABLEZCA LOS PARÁMETROS DE LA ESCENA DEL DELITO**: El primero en llegar a la escena, debe establecer si el delito está todavía en progreso, luego tiene que tomar nota de las características físicas del área circundante. Para los investigadores forenses esta etapa debe ser extendida a todo sistema de información y de red que se encuentre dentro de la escena.
- **INICIE LAS MEDIDAS DE SEGURIDAD**: El objetivo principal en toda investigación es la seguridad de los investigadores y de la escena. Si uno observa y establece en una condición insegura dentro de una escena del

delito, debe tomar las medidas necesarias para mitigar dicha situación. Se deben tomar las acciones necesarias a fin de evitar riesgos eléctricos, químicos o biológicos, de igual forma cualquier actividad criminal.

- **ASEGURE FÍSICAMENTE LA ESCENA**: Esta etapa es crucial durante una investigación, se debe retirar de la escena del delito a todas las personas extrañas a la misma, el objetivo principal es el prevenir el acceso no autorizado de personal a la escena, evitando así la contaminación de la evidencia o su posible alteración.
- **ASEGURE FÍSICAMENTE LAS EVIDENCIAS**: Este paso es muy importante a fin de mantener la cadena de custodia de las evidencias, se debe guardar y etiquetar cada una de ellas. En este caso se aplican los principios y la metodología correspondiente a la recolección de evidencias de una forma práctica. Esta recolección debe ser realizada por personal entrenado en manejar, guardar y etiquetar evidencias.
- **ENTREGAR LA ESCENA DEL DELITO**: Después de que se han cumplido todas las etapas anteriores, la escena puede ser entregada a las autoridades que se harán cargo de la misma. Lo esencial de esta etapa es verificar que todas las evidencias del caso se hayan recogido y almacenado de forma correcta, y que los sistemas y redes comprometidos pueden volver a su normal operación.
- **ELABORAR LA DOCUMENTACIÓN DE LA EXPLOTACIÓN DE LA ESCENA**: Es Indispensable para los investigadores documentar cada una de las etapas de este proceso, a fin de tener una completa bitácora de los hechos sucedidos durante la explotación de la escena del delito, las evidencias encontradas y su posible relación con los sospechosos. Un investigador puede encontrar buenas referencias sobre los hechos ocurridos en las notas recopiladas en la explotación de la escena del Delito.[1]

[1] ACURIO DEL PINO, Santiago, "Manual de Manejo de Evidencias Digitales y Entornos Informáticos", Págs. 8-9.

5.5.2. PRINCIPIOS DEL PERITAJE.

- OBJETIVIDAD: el perito debe ser objetivo, debe observar los códigos de ética profesional.
- AUTENTICIDAD Y CONSERVACIÓN: durante la investigación, se debe conservar la autenticidad e integridad de los medios probatorios.
- LEGALIDAD: el perito debe ser preciso en sus observaciones, opiniones y resultados, conocer la legislación respecto de su actividad pericial y cumplir con los requisitos establecidos por ella.
- IDONEIDAD: los medios probatorios deben ser auténticos, ser relevantes y suficientes para el caso.
- INALTERABILIDAD: en todos los casos, existirá una cadena de custodiar debidamente asegurada que demuestre que los medios no han sido modificados durante la pericia.
- DOCUMENTACIÓN: deberá establecerse por escrito los pasos dados en el procedimiento pericial.

Estos principios deben cumplirse en todas las pericias por todos los peritos involucrados.[2]

5.6. UBICACIÓN DE LA POLICIA INFORMATICA DENTRO LA ESTRUCTURA ORGANICA DE LA POLICIA.

La unidad operativa de la Policía Informática, estará al interior de lo que hoy en día se constituye la FELCC (FUERZA ESPECIAL DE LUCHA CONTRA EL CRIMEN), unidad que depende en línea directa del Comando Departamental de Policía, quienes tienen bajo su responsabilidad la actividad policial departamental dentro del límite de cada departamento. Esta ubicación dentro de la estructura policial contribuirá a una mejor coordinación y relación con los departamentos de combate

[2] ACURIO DEL PINO, Santiago. **Ob. Cit.,** Pág. 4.

del crimen organizado, pero sobre todo el de mantener una colaboración estrecha con todas las direcciones y departamentos que están encargados en la prevención y lucha frente a la delincuencia.

5.7. MODO OPERACIONAL Y PATRULLAJE EN EL MUNDO VIRTUAL DE LA INFORMATICA.

El modo operativo de recepción de denuncias se la podrá hacer ya sea por vía de la red, telefónica o personal, este sección de recepción de denuncias al interior de la unidad Operativa, estará sujeto a una reglamentación especial adecuando su normativa a las leyes vigentes, permitirá una vez constatada la gravedad del hecho, y vulnerado el bien jurídico tutelado, el accionar de expertos/peritos en informática, refiriéndose a la, investigación, análisis, peritaje, informe y conclusiones de todos aquellos delitos contemplados en nuestro ordenamiento jurídico penal, que requieran de expertos en tecnología.

El "*patrullaje"* estará dedicado a la ciber-navegación (estar inmerso y conectado en la red del internet) detectando posibles amenazas, brindando una actuación oportuna para frenar las actividades delictivas, pero además tiene una labor preventiva, informativa explicando a los usuarios, las formas de evitar la realización de estos tipos de delitos, respetando esencialmente el derecho a la intimidad, la inviolabilidad de las comunicaciones y sobre todo la libertad de expresión cuál es la característica especial de la red informática. Todas sus actuaciones estarán basadas de oficio o a denuncia de las víctimas, de oficio cuando atenten la integridad moral o el patrimonio de las personas y a denuncia cuando existan elementos suficientes para presumir que cierto tipo de acción concurren los elementos para considerarlos delitos. Enmarcando sus actividades e investigaciones dentro de lo que establecen las convenciones declaraciones de los Derechos Humanos teniendo como premisa la intromisión mínima y sólo necesaria.

5.8. MISIONES DE ESTUDIO AL EXTERIOR PARA LOGRAR OBJETIVOS ACADEMICOS DE ACTUALIZACION.

Con el propósito de lograr una permanente actual relación de sus miembros al interior de la policía y en particular de la Policía Informática, es necesario trazar políticas académicas con el objetivo de buscar la capacitación y perfeccionamiento en el manejo de tecnologías, el conocimiento de las mismas y sobre todo el intercambio de información y conocimientos con instituciones similares o gobiernos amigos. Estos objetivos serán alcanzados a través de misiones de estudio que realizarán los miembros asignados a la policía informática, contemplados en la Ley Orgánica de la Policía Boliviana. Asimismo el artículo 110 de la mencionada ley faculta al Comando General de la Policía Nacional, a enviar misiones de estudio el exterior con el objeto de conseguir una mayor tecnificación de los diferentes servicios, propiciando de la misma manera la visita de policías extranjeros con la finalidad de mejorar constantemente la actividad institucional, objetivo para el cual el gobierno a través de las instancias correspondientes deberá prestar las facilidades correspondientes.

CAPITULO VI

DIAGNOSTICO PROPOSITIVO: DEL PROYECTO DE CREACION Y REGLAMENTACION DE LA UNIDAD DE POLICIA ESPECIALIZADA EN DELITOS INFORMATICOS

LEY Nº

LEY DEL 5 SEPTIEMBRE 2011

EVO MORALES AYMA

PRESIDENTE CONSTITUCIONAL DEL ESTADO PLURINACIONAL DE BOLIVIA

CONSIDERANDO:

Que el Parágrafo I del artículo 251 de la Constitución Política del Estado, establece que la Policía Boliviana, como fuerza pública, tiene 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 boliviano. Ejercer la función policial de manera integral, indivisible y bajo mando único, en conformidad con la Ley Orgánica de la Policía Boliviana y las demás leyes del Estado.

Que el Articulo 2 de la Ley Orgánica de la Policía Boliviana sobre los principios generales de la Policía Nacional, señala que la Policía Nacional tiene a su cargo la totalidad de la actividad policial; centraliza bajo un solo mando y escalafón único los organismos policiales mencionados en el artículo 215 de la Constitución Política Del Estado, con la finalidad de cumplir las funciones específicas que le asignan las leyes y reglamentos.

Que el Artículo 6 de la Ley Orgánica de la Policía Boliviana sobre la misión y atribuciones señala, la Policía Nacional tiene por misión fundamental, conservar el orden público, la defensa de la sociedad y la garantía del cumplimiento de las leyes,

con la finalidad de hacer posible que los habitantes y la sociedad se desarrollan a plenitud, en un clima de paz y tranquilidad.

Que el Artículo 10 de la Ley Orgánica de la Policía Boliviana sobre Organización y Funciones señala, el Comando General creará o suprimir a las unidades de los organismos operativos de la administración desconcentrada, de acuerdo a las necesidades del servicio.

EN CONSEJO DE MINISTROS,

DECRETA:

CREASE: POR REGLAMENTO, LA FUERZA ESPECIAL DE LUCHA CONTRA EL CRIMEN INFORMÁTICO (FELCCI) EN DIRECTA RELACIÓN DE DEPENDENCIA A LA FUERZA ESPECIAL DE LUCHA CONTRA EL CRIMEN (FELCC) DENTRO DE LA ESTRUCTURA ORGÁNICA DE LA POLICÍA NACIONAL.

TITULO I

CAPITULO UNICO

OBJETIVOS, FINALIDAD, FUNCIONES Y AMBITO DE APLICACION

ARTICULO 1.- (OBJETIVOS). El Organismo Operativo Policial denominado Fuerza Especial de Lucha contra el Crimen Informático, unidad operativa que será la encargada de la recepción de denuncias, detección, investigación y patrullaje de Delitos Informáticos, además del seguimiento y captura de aquellas personas naturales o jurídicas quienes hacen uso fraudulento de las tecnologías de información y comunicación en coordinación con los fiscales asignados.

ARTÍCULO 2.- (FINALIDAD). Su finalidad es cautelar, proteger y resguardar a la sociedad e instituciones de ser víctimas de delitos Informáticos, en el marco del respeto a la Constitución, Tratados y Convenios y demás leyes.

ARTÍCULO 3.- (FUNCIONES). Entre sus funciones principales están:

DE DEFENSA. Colaborar con la defensa, interior y externa del Estado, a través de la investigación, cooperación brindando seguridad a los sistemas informáticos contra posibles delitos informáticos.

DE PREVENCION. Prevenir la realización de posibles delitos que pongan en riesgo el patrimonio y el honor de los habitantes a través del denominado patrullaje virtual, permitiendo la acción oportuna para combatir actividades delictivas.

DE INVESTIGACION. Encargada de la recepción de denuncias y la posterior investigación hasta su culminación y posterior remisión al fiscal dependiente del Ministerio Publico.

DE COOPERACION. Mantendrá estrecha relación de cooperación con todas aquellas instituciones al interior del Estado, de la Policía, quienes hacen uso de la base de datos en la búsqueda y análisis de información a través de la red informática, además de mantener estrecha relación con organismos similares del extranjero.

ARTÍCULO 4.- (AMBITO DE APLICACIÓN). El ámbito de aplicación del presente Reglamento a cargo de la Policía Nacional, tendrá vigencia en todo el territorio Nacional, en donde exista el uso y manejo de base de datos fraudulento sea así en la modalidad de interferencia, acceso o transferencia no autorizado, copia ilícita, alteración de datos, daño o destrucción parcial o total en bases de datos, clonación de tarjetas, exhibición o publicación de contenido pornográfico infantil, terrorismo virtual y todo otro delito tipificado en el ordenamiento penal que atente mediante la red informática el patrimonio privado público y el honor de las personas.

TITULO II

CAPITULO I

ESTRUCTURA Y ORGANIZACIÓN

ARTÍCULO 5.- (ORGANIZACIÓN) La Fuerza Especial de Lucha contra el Crimen Informático es una institución técnico -científica organizada según los principios generales que establece la Ley Orgánica de la Policía Nacional, integrando funciones para la investigación, prevención y coordinación en la lucha contra el crimen, organismo que para el cumplimiento de sus funciones está organizado de la siguiente manera:

ARTICULO 6.- (DEPENDENCIA) Al constituirse en un organismo policial tiene estricta relación de dependencia de lo que establece la Ley Orgánica de la Policía Boliviana en lo que se refiere a organismos operativos, arts. 41 y siguientes.

ARTICULO 7.- (DIRECCION Y CONTROL) La Fuerza Especial de Lucha contra el Crimen, (FELCC), tendrá a cargo la conformación, supervisión, dirección y control en estrecha relación de cooperación con todos los organismos operativos de la policía.

ARTICULO 8.- (DEPARTAMENTO DE ASESORIA, APOYO Y PERITAJE INFORMATICO) Brindará asesoramiento en materia de prevención, apoyando en el peritaje forense, recobrando registros y mensajes de datos existentes dentro de un equipo informático digital para que ésta pueda ser usada como prueba ante un tribunal, demostrando la autoría y complicidad de quienes cometen estos actos delictivos.

ARTICULO 9.- (DEPARTAMENTO DE CAPACITACION Y TECNOLOGIA) El Departamento de Capacitación y Tecnología estará conformado por oficiales egresados de la Academia Nacional de Policías y peritos informáticos quienes tengan especialización en manejo de base de datos y serán designados por el Comandante General de la Policía por sus méritos, quienes brindarán capacitación

permanente a todo el personal en el manejo de la tecnología a cargo de este organismo.

ARTÍCULO 10.- (DIVISION DE INVESTIGACION) Estará encargada de la evaluación y recepción de denuncias siendo realizadas éstas a través de un medio virtual, telefónico o personal, haciendo el seguimiento correspondiente en coordinación con un fiscal en materia penal hasta la conclusión del caso para posteriormente remitirlo a un juez competente

ARTICULO 11.- (DIVISION DE PATRULLAJE Y PREVENCION) Tendrá a su cargo patrullaje continuo y permanente de forma preventiva dentro la red informática del Internet, ubicando el identificando posibles comisiones de delitos que atenten la seguridad, la propiedad, la moral sexual, ultrajes al pudor público y la confidencialidad en el manejo de datos, respetando el derecho a la libertad de información que consagra la constitución y los convenios internacionales, bajo el principio de intervención mínima.

ARTICULO 12.- (DIVISION DE COORDINACION Y ANALISIS INSTITUCIONAL) Tendrá como función primordial la coordinación y cooperación con todas aquellas instituciones al interior del Estado boliviano y la Policía Nacional u otras similares de países amigos y vecinos quienes contribuyan a la capacitación, asesoramiento, obtención de información en materia de delitos informáticos.

CAPITULO II

DE LA CAPACITACION

ARTICULO 13.- (ACTUALIZACION PERMANENTE) Es función primordial de este organismo policial operativo el velar por una actualización permanente de sus efectivos en cuanto al manejo de tecnología innovadora en software y hardware que coadyuven al esclarecimiento de las investigaciones.

ARTICULO 14.- (INCLUSION DEL PENSUM EN INSTITUTOS, ACADEMIAS Y ESCUELAS POLICIALES) El Comando General dispondrá por el departamento correspondiente la inclusión en el pensum de materias "el manejo de tecnologías informáticas" en todas aquellas universidades, institutos, academias y escuelas policiales quienes tendrán como función brindar el aprendizaje y capacitación de sus alumnos.

DISPOSICIONES ADICIONALES.

PRIMERA. Es el Comando General de la Policía Boliviana, el encargado de la creación e implementación previo desembolso de recursos por la vía administrativa, del organismo denominado Fuerza Especial de Lucha contra el Crimen (FELCCI) para su funcionamiento en el plazo de 180 días calendario a partir de la fecha.

DISPOSICIONES TRANSITORIAS

PRIMERA. El Comandante General de la Policía instruirá a los Comandantes Departamentales, la misión de socializar, comunicar y capacitar a todo el efectivo policial, en el conocimiento de la presente ley, en un plazo que no excederá los 90 días a partir de su publicación, bajo responsabilidad.

SEGUNDA. La asignación presupuestaria será derivada de un presupuesto especial asignado anualmente por el Ministerio del Ramo al Comando General de la Policía Boliviana.

Remítase al Órgano Legislativo, para fines constitucionales.

Es dada en Consejo de ministros, a los cinco días del mes de septiembre del año dos mil once. Por tanto, la promulgó para que se tenga y cumpla.

Es dado en Palacio de Gobierno de la Ciudad de La Paz, a los cinco días del mes de septiembre de dos mil once años. Firmado. EVO MORALES AYMA.

CONCLUSIONES.

- Toda esta nueva modalidad de delitos en Internet surge por la novedad en este tipo de servicios y la falta de regulación que existe. Conforme se siga desarrollando el comercio electrónico se perfeccionara tanto la seguridad como las políticas de operación y reglamentos correspondientes. Es evidente que los hackers representan una seria amenaza para las empresas y las personas, por ser causantes de pérdidas millonarias y de imagen. Sin embargo, de la misma manera, los hackers representan una especie de consultores que advierten a las empresas de fallas en sus sistemas de información y sirven de indicador de la necesidad de mejora en dichos sistemas.
- En esta medida, los hackers están impulsando al comercio electrónico y perfeccionándolo cada vez más en sus medidas de seguridad. Cada vez en mayor medida las empresas desarrollan conciencia de la importancia de invertir en sistemas de seguridad efectivos, lo cual es correcto, pero también deben enfocarse en su gente, en capacitarlos y crear un ambiente de trabajo propicio para su desarrollo y con justicia ya que se crean así barreras de seguridad por convertirse los empleados en defensores de la información y además por disminuir las probabilidades de tener hackers internos a la empresa.
- Debemos señalar que el anonimato, sumado a la inexistencia de una norma que tipifique los delitos señalados, es un factor criminógeno que favorece la multiplicación de autores que utilicen los medios electrónicos para cometer delitos a sabiendas que no serán alcanzados por la ley. No solo debe pensarse en la forma de castigo, sino algo mucho más importante como lograr probar el delito y a esto justamente obedece la propuesta de crear nuevos organismos de control y vigilancia
- Desde el punto de vista social, es conveniente, educar y enseñar la correcta utilización de todas las herramientas informáticas, impartiendo conocimientos

específicos acerca de las conductas prohibidas, algunas reseñadas en éste trabajo, que no deben ejecutarse. No solo con el afán de protegerse, sino para evitar convertirse en un agente de dispersión que contribuya a que un virus informático siga extendiéndose y alcance una computadora en la que, debido a su entorno crítico, produzca un daño realmente grave e irreparable. Desde la óptica legal, y ante la inexistencia de normas que tipifiquen los delitos cometidos a través de la computadora, es necesario: proteger toda creación industrial y comercial que se halle en soportes electrónicos, CD, o de producir disquetes u otros de creación futura incluyéndolo en el Código Penal, también los delitos cometidos a través de la computadora o a través del software.

- Legislar un tipo culposo para aquellos que, por imprudencia, negligencia, impericia causaren daños, introduzcan virus u otros, con capacidad de dañar a través de la computadora. Considerando culposa la conducta de quien a través de la computadora dañen parte o en todo sistemas informáticos.
- Legislar la instigación al delito cometido a través de la computadora. Adherimos por nuestra parte, a los postulados de la ONU sobre los delitos informáticos, con el fin de unificar la legislación internacional que regule la problemática de la cibernética y su utilización tan generalizada en el mundo.
- Por otro lado legislar la serie de entretenimientos que tienen a un menor frente a una PC como víctima pasiva, incitado a la violencia, alejado de los procesos de socialización y con posibles intromisiones de redes de pornografía infantil.
- Frente a la generalización en el uso de las tecnologías informáticas, son los legisladores de cada país quienes están frente a un desafío, demarcar límites y conductas de quienes tienen relación directa con el mundo virtual o red informática, pero estas reglas deben estar acordes al principio de intervención mínima sin desmerecer el principio de intervención suficiente.

RECOMENDACIONES

- Una de las principales recomendaciones es la adecuada instauración de medidas de prevención y seguridad para la población en general.
- El Estado debe implementar políticas de información sobre el uso y manejo de estas tecnologías, advirtiendo de los posibles peligros que pudieran ocurrir por el desconocimiento de la sociedad.
- La policía boliviana, a través de los departamentos correspondientes debe ser la encargada de la investigación en casos confirmados de atentados a la información y a la vez debe dar capacitación permanente de su personal en cuestiones tecnológicas, debiendo el ministerio del ramo proveer los recursos necesarios para hacer efectivo este plan.
- El derecho a la intimidad, la privacidad no debe ser vulnerado con el pretexto de la investigación de este tipo de delitos.
- Debe dictarse normas claras y específicas, para regular el desenvolvimiento de los operadores del dominio Internet en Bolivia, el proyecto de ley de Telecomunicaciones actualmente en tratamiento debe ser consensuado con todos los actores e interesados en que exista libertad en las comunicaciones y acceso libre a la información pero con seguridad.
- El consejo para los Padres es de ser amigo de tus hijos y enséñales a cuidarse en Internet, creando reglas para su uso.
- Insiste en que tus hijos nunca faciliten su dirección, número de teléfono u otra información personal, como la escuela a la que van o dónde les gusta jugar.
- Alerte a su hijo del riesgo de intimar por Internet con personas desconocidas, púes ocultar identidades por Internet es muy fácil.
- Eduque a su hijo sobre las consecuencias negativas de vulnerar las leyes. El que "mucha gente lo haga" no implica que es legal. La piratería digital tiene como única solución la educación del ciudadano.
- Desconfíe de los mensajes de correo procedentes de supuestas entidades bancarias. confirme vía telefónica con su banco cualquier petición que reciba

de datos de banca electrónica. Utilizar un buen producto antivirus y actualizarlo, frecuentemente. Utilice un Software Antivirus, mensualmente se generan entre 600 y 800 virus, es preciso que los antivirus sean actualizados periódicamente, evite copias piratas.

BIBLIOGRAFIA.

- ACURIO DEL PINO, Santiago, “Manual de Manejo de Evidencias Digitales y Entornos Informáticos”.
- ARCE JOFRE, José Alfredo, “Informática y Derecho”, Edit. Bolivia Dos Mil
- BARAN, Paul, “The Origins of the Internet”, http// www.rand. org/ about/ history/baran. Html, 2006.
- CARRASCOSA LOPEZ, V, “Informática y Derecho”, UNED, 1992.
- CLAURE, Edson, Jefe de la “División del Delitos Informáticos de la FELCC”, Entrevista.
- CONSTITUCIÓN POLÍTICA DEL ESTADO, Gaceta Oficial de Bolivia, 7 Feb. 2009, La Paz Bolivia.
- CONVENCIÓN AMERICANA SOBRE DERECHOS HUMANOS, Pacto de San José de Costa Rica, 22 noviembre 1969, Ratificada mediante LEY Nº 1430, de 11 febrero 1993.
- COSTA FERRECCIO, Julio, "Poder y derecho de Policía".
- DAVARA RODRIGUEZ, Miguel Ángel, “Manual de Derecho Informático”, Pamplona Aranzadi, 1997.
- FRIEDMAN L., Thomas, “The Lexus And The Alive Tree”, Farrar Straus & Giroux, 1999.
- FUERZA ESPECIAL DE LUCHA CONTRA EL CRIMEN,” Manual de Organización y Funciones”.
- GIL ALBARRAN, Guillermo Edward, “Derecho Informático”, ed., Megabyte Primera Edición, 2007.
- HINOSTROZA RODRIGUEZ, Guillermo, “Fundamentos de Doctrina y Ciencia Policial”, www.monografias/ciencia policial.com.
- http://www. delitos informaticos.com/HTML.
- INTERNET HISTORY IN ASIA, “Advanced Network Conference in Busan”, 16th APAN Meetings, 2005.
- J.C.R.LICKLIDER, "Man Computer Symbiosis", http.//groups.csail.mit. edu/medg/people/psz/Licklider, html.

- JURISPRUDENCIA ARGENTINA, “Documento Electrónico”, Tomo II. Año 1999.
- JIMENEZ DE ASUA, Luis, “Principios del Derecho penal”, ed., Sudamericana, Buenos Aires- Argentina, 1997.
- KELSEN, Hans, “Teoría Pura del Derecho”, ed., Unión Ltda., Santa Fe Bogotá,
- KRAMER, Pedro, “Historia de Bolivia”, Taller Tipo litográfico, La Paz, 1889.
- LA RUE, Frank, Relator Especial de la ONU, Comunicado de prensa.
- LEVENE Ricardo, CHIARAVALLOTI Alicia, “Introducción a los delitos informáticos, tipos y legislación”, http://www. chiaravalloti_asociados. dtj.com.ar/links_1.htm.
- LEY ORGÁNICA DE LA POLICÍA BOLIVIANA, Ley nº 734, “Gaceta Oficial de Bolivia”, 8 abril 1985.
- LORENZETTI L., Ricardo, “Comercio Electrónico”, Edit. Abeledo-Perrot. Bs. As. Argentina.
- LUÑO, Antonio Enrique, “Ensayo de Informática Jurídica”, Edit. Fontamar, México, 2005.
- MOLINA Roberto, MOLINA Juvenal, CESPEDES Jaime, CASTAÑON Carlos, “Historia de la Policía Nacional”, Tomos I y II, ed., Cima, La Paz Bolivia.
- MOLINA VIAÑA, Oscar, “Seguridad Ciudadana”, La Paz –Bolivia, 2001.
- MOSCOSO DELGADO, Jaime, “Introducción al Derecho”, Librería Editorial Juventud.
- ORGANIZACIÓN de las NACIONES UNIDAS, “Delitos Reconocidos”, http://www.forodeseguridad.com.
- OSSORIO, Manuel, “Manual y Diccionario de Ciencias Jurídicas, Políticas y Sociales”, ed., Heliasta. Buenos Aires, 2004.
- OSSORIO, Manuel, “Policía de Seguridad”, Diccionario Jurídico Omeba, Ed. Driskill, Buenos Aires-Argentina, 2003.
- PROGRAMA DE INVESTIGACIÓN ESTRATÉGICA EN BOLIVIA, “Policía y Democracia En Bolivia”, 2003.

- PROYECTO LEY GENERAL DE TELECOMUNICACIONES, Tecnologías de Información y Comunicación, Titulo I, Disposiciones Generales, ARTÍCULO 6.- (PRINCIPIOS).
- QUIROZ & LECOÑA, "Código Penal", Tercera Edición, 2011.
- ROMEO CASABONA, Carlos María, "Poder y Informático y Seguridad Jurídica", Madrid, 1988.
- SEGAL, Ben, "A Short History of Internet Protocolo at CERN", (1995).
- SUÑE LLINAS, Emilio, "Tratado de Derecho Informático", Introducción y Protección de datos personales, Publicaciones de la Facultad de Derecho de la Universidad Complutense de Madrid, 2000.
- TELLEZ VALDEZ, Julio, "Derecho Informático", ed., Mc Graw Hill. México, 2003.
- THE FIRST NETWORK EMAIL, http://openmap.bbn.com.html, 23 de diciembre de 2005.
- THE RISKS DIGEST, "Great moments in e-mail history", html//catless. ncl.ac.uk, 27 de abril de 2006.
- TORO, Jorge, "Director Nacional del Laboratorio de la FELCC", Entrevista gestión 2010.
- VILLANUEVA GARAY, José. Catedrático de la ESUPOL, "Ciencia Policial, parte de las ciencias sociales".

ANEXO Nº 1 INDICE DE EVENTOS HISTORICOS. POLICIA BOLIVIANA

Fuente: Policia y Democracia: Una politica institucional Independiente: Programa de Investigacion Estrategica en Bolivia.

Índice de eventos históricos relacionados con la policía		
Año	**Constituciones, decretos, reglamentos y tendencias de reforma**	**Eventos**
1825	• La raciente república unitaria asume un régimen de gobierno popular y representativo con cuatro poderes (electoral, legislativo, ejecutivo y judicial), tres cámaras (tribunos, senadores y censores), tres ministerios y dos fuerzas militares.	• Creación de la República de Boliva
1826	**Ley Reglamentaria del 24 de junio.** • Creación de intendencias y comisarías de policía dependientes del prefecto del departamento. Su misión es precautelar el orden interno, conservar obras públicas, controlar vagancia y juegos de azar, limpieza de calles, vigilancia hospitalaria, alojamiento de tropa y otros servicios urbanos. Disponían de un piquete de tropa armada pagada por el Estado. • El presupuesto para 1827 fija la dotación de 120 sargentos, cabos y soldados para la policía y 29 gobernadores. Para una población de más de un millón de habitantes, la relación población-policía es de 1 policía por cada 7 mil habitantes.	• Las mayores amenazas al orden público residen en la vagancia, las riñas y peleas, juegos de azar y pequeños hurtos.
1830	• Creación de la Guardia Nacional, cuerpo militar de alcance departamental, organizado para la conservación del orden público y reservas en caso de amenaza externa. La movilización e instrucción de las guardias nacionales se llevan a cabo mediante los prefectos, subprefectos y corregidores.	• La existencia de la Guardia Nacional se formaliza en la CPE de 1831
1831	• Segunda Constitución Política del Estado	
1831	• Promulgación del Código Penal y Civil y Procedimental (1832) • Promulgación del Reglamento de Policía. Se le asigna funciones de orden interior, censo y control de los gremios, requisitoria de jueces, censura, salubridad, ornato, comodidad, matriculación de la población urbana, control de domicilios y pasaportes, fondas, posadas y mesones, juegos de azar y armas, control de vagos y mendigos, bebidas alcohólicas, hurtos y desórdenes públicos.	• Presidente de la República, Mcal Andrés de Santa Cruz, 1829-1839
1834	• Tercera Constitución Política del Estado	
1839	• Supresión de las Intendencias de Policía • Cuarta Constitución Política del Estado	
1840	• Los efectivos policiales siguen siendo reducidos. Para una población de 1.245.650 personas la dotación presupuestaria de personal policial es de 181 hombres entre comisarios, segundos comisarios, sargentos, cabos y gendarmes. Un policía para cada 6.882 personas. La cobertura territorial de la policía sólo abarca seis departamentos, incluido Litoral	

1843	• Quinta Constitución Política del Estado	
1845	• Promulgación del Reglamento de Policía. Además de la existencia de intendentes y comisarios designados políticamente se crean puestos para gendarmes y rondines. Sólo se podía acceder a estos cargos en condición de ciudadanos y a la gendarmería de preferencia soldados del Ejército. Las atribuciones policiales residían en: seguridad de las personas y bienes de los habitantes, salubridad, buenas costumbres, comodidad y ornato de los pueblos y auxilio a autoridades. Se amplían las funciones: cuidado de cárceles, control de ferias, ritas, pesos y medidas, diversiones públicas, control de vacunas y abastecimiento urbano, cementerios y entierros, limpieza y aseo de calles, caminos públicos y puentes, moral pública y buenas costumbres. Se crea una caja y fondos policiales en cada departamento sustentados con el pago de multas e infracciones.	• Luego de un breve interinato del Gral. Velasco asume como Presidente de la República, Gral. José Ballivián (1841-1847). • Ballivián lleva a cabo importantes reformas militares como la reducción de planillas de personal, sueldos y beneficios inocuos.
1851	• Sexta Constitución Política del Estado • El personal aumenta a 335 hombres. Su composición es la siguiente: comisario, comisario auxiliar, sargentos, cabos, gendarmes y serenos. Un policía para cada 4.328 personas.	• Gobierno del Gral. Manuel I. Belzu, 1848-1855
	• Séptima Constitución Política del Estado	
1862	• Las intendencias de policía pasan a depender del Ministerio de Guerra. Ministro de Gobierno solicita a Asamblea elaborar un Código de Policía.	
1868	• Octava Constitución Política del Estado.	
1871	• Se promulga el Reglamento de Celadores por el Jefe Superior Político y Militar de los Departamentos del Norte. Los celadores, custodios del orden público y de la propiedad, eran voluntarios contratados por dos años. Debían cumplir requisitos de edad, ciudadanía, educación y estar exentos de pasado de servidumbre. Gozaban de fuero militar	• Presidente de la República, Agustín Morales, 1871-1872
	• Novena Constitución Política del Estado.	
1873	• Orden General del 28 de Julio. • Los cuerpos de celadores se reorganizan bajo la denominación de "Columnas del Orden" sujetos a un pago semejante al de los soldados de infantería del Ejército. Asumen orden público mientras los cuerpos de gendarmes se encargan de los servicios de salubridad, comodidad y ornato bajo autoridad del municipio.	• Presidente de la República, Gral. Adolfo Ballivián, 1873-1874
1874	• Mediante Decreto Supremo del 27 de noviembre la fuerza policial compuesta de celadores y columnas del orden pasan a depender del Ministerio de Guerra y se la considera parte del Ejército. Gozan de fuero militar y se someten a códigos militares.	• Presidente de la República, Dr. Tomás Frías (1874-1876)

	• Entre 1874 y 1880 se crean guardias privadas en los asientos mineros de la costa bajo la denominación de "Guardia Conservadora del Orden" compuesta de súbditos extranjeros, principalmente chilenos. Su misión era controlar el robo de minerales.	
1878	• Décima Constitución Política del Estado. • Reglamento Orgánico de las Municipalidades que establece la existencia de policía municipal.	
1879-1884	• Bolivia pierde acceso soberano a costas del Pacífico, luego de más de cinco años de traumático conflicto militar.	• Guerra del Pacífico
1880	• Undécima Constitución Política del Estado	
1882	• Creación de Guardias Urbanos. • El efectivo policial es de 680 hombres para una población de 1.097.600. Un policía para cada 1.614 personas.	
1884	• Promulgación de la Ley Orgánica del Poder Ejecutivo. • Gobierno asigna al Ejército la responsabilidad de la disciplina policial. • Ejército sufre recortes presupuestarios, pero aumentan dotaciones policiales.	• Ciclo de estabilidad. Presidente, Dr. Gregorio Pacheco, 1884-1888
1886	- Ley Reglamentaria de Policía de Seguridad que la declara institución civil despojada de fuero militar. Instrumento jurídico más moderno del siglo XIX. Asigna a la policía la función de conservar el orden público, resguardar garantías personales y reales, prevenir delitos y faltas, y perseguir delincuentes para ponerlos a disposición de las autoridades. Se le asignan también roles novedosos como el control de comicios electorales junto al Ejército. No obstante, se agudizan conflictos entre policías de seguridad y municipales debido a cobros de multas. Las áreas conflictivas son el control de casas de juego, castigo a ebrios, represión a juegos de azar.	• Entre 1884 y 1900, crece el número de efectivos policiales y se reduce personal del Ejército. Crece población urbana lo que exige más columnas policiales y en áreas rurales, piquetes de policía.
1887	• Decreto del 10 de enero de 1887 restablece régimen militar en la Policía de Seguridad. Militarización coincide con levantamientos indígenas.	
1890	- En Trinidad y Sucre la Policía de Seguridad es manipulada por liberales que provocan motines. En Punata se toma el cuartel de celadores.	
1894	• Aprobación de Ordenanzas Militares. Policía de Seguridad se sujeta a este marco jurídico que reconoce existencia de celadores y gendarmes a pie y a caballo en cada departamento. Cuerpos de gendarmería y celadores de a pie estaban sujetos a organización de la infantería del Ejército. Gendarmerías a caballo debían adoptar organización	- Presidente de la República, Dr. Mariano Baptista, 1892-1896 • Tenso período de estabilidad política. La conspiración orienta sus armas a los

	de caballería militar. Celadores y gendarmes estaban sujetos a reclutamiento y servicio militar.	cuerpos armados de celadores.
	- Repetidos hechos de sedición en la columna de Policía de Seguridad en Uyuni alentados por liberales de la línea del Gral. Camacho	
1896	• Se crea Papel Especial para Control de Multas para disminuir denuncias de corrupción y malos manejos en recaudaciones departamentales.	• Guerra Federal que evidencia el racismo oligárquico. Se fusila a Zárate Willka.
1898-1899	• Conflicto militar en el que se enfrentan, bajo el argumento de la federalización del norte contra el centralismo del sur, ejércitos del gobierno y de liberales.	• Gobierno del Gral. José M. Pando, 1099-1904
	• 814 policías para población de 1.555.800 personas. 1 policía para 2.007 personas.	
1901	• Creación de la Policía Rural. • Policía montada cumple funciones de vigilancia, control y represión indígena en zonas amenazadas por restitución de tierras comunitarias.	• Temor de élite minero-feudal motiva elevados gastos en seguridad.
1903	- Diversos actos de sedición policial protagonizados por las Policías de Seguridad de Potosí y Cinti alentadas por la fracción conservadora	
1904	• Proyecto de Policía Modelo de Oruro que perseguía replicar modelo de policía argentina. Fracasó por falta de voluntad política. Oruro y Potosí reciben flujo de migración extranjera que provoca disturbios y desórdenes. • Policía y Ejército arremeten contra las comunidades indígenas con el argumento de la "pacificación".	• Se introduce importante división de funciones policiales para prevenir vagancia, juegos de azar y control migratorio.
1910	• Nacionalización de la Policía de Seguridad mediante la creación de Brigadas de Policías de Seguridad. Se crea Dirección General de Policía bajo autoridad del Ministerio de Gobierno. Posteriormente se reemplaza la Dirección General por un Inspector General. • Efectivos policiales ascienden a 1.704 para una población de 2.159.715 personas. Esto es, un policía para cada 1.267 personas.	• Presidente de la República, Dr. Eliodoro Villazón, 1909-1913.
1923	- Se crea "Guardia Republicana", cuerpo uniformado y militarizado al servicio del gobierno republicano. Se convirtió en cuerpo militar de represión. • Creación de "Escuela de Policías" para formar gendarmes, agentes, investigadores y comisarios. No funciona hasta 1937.	- Presidente Dr. Bautista Saavedra, 1921-1925. Inestabilidad provoca control político policial.
1930	• Creación de la Dirección General de Policía. Se configuran Regimientos de Policía en cada departamento.	

	• 3.169 efectivos para una población de 2.619.274 personas. 1 policía para cada 826 personas.	
1932-1935	• Dos regimientos policiales asisten a la Guerra del Chaco. • Se crea la "Legión Cívica", organización paramilitar que además de reclutar indígenas y enviarlos a la guerra, asume el papel que dejó vacante la policía en el área rural.	• Guerra del Chaco. Mueren más de 50 mil soldados y cuesta más de 114 millones de dólares.
1937	• Reorganización de la Policía bajo denominación de "Carabineros de Bolivia". Se fusionan policías de seguridad, comerciales y regimientos. Se organizan en escuadrones, regimientos y brigadas similares a las unidades militares. Se introdujo mayor división profesional en el trabajo a través de funciones de vigilancia política, control social y propaganda a cargo del Min. de Gobierno.	• Misión de carabineros de Italia. Importantes reformas. Primeras expresiones de identidad, cohesión y espíritu de cuerpo en la institución.
	• Creación de la Escuela Nacional de Policía, instituto técnico militar • Se introduce el patrullaje motorizado con camionetas	
1938	• Duodécima Constitución Política del Estado	
1945	• Decimotercera Constitución Política del Estado	
1943-1946	• Importantes reformas normativas y organizacionales militarizan la policía. Brigadas departamentales copadas por oficiales del Ejército. Un sector policial se politiza a favor del gobierno. • El gobierno autorizó incorporación de servicio militar obligatorio en Cuerpo de Carabineros. Crea conflictos y susceptibilidad en el Ejército. Se crea Escuadrón de Seguridad, policía al mando de un oficial alemán. • Se aprobó Reglamento de la Escuela de Carabineros y se estableció Escalafón Policial que regulaba la calificación profesional, ascensos, años de servicio, hojas de concepto, condecoraciones, etc.	• 1943: Luego de golpe de Estado, MNR y RADEPA asumen el gobierno a la cabeza del Cnl. Gualberto Villarroel (1943-1946). Este gobierno nacionalista contó con apoyo policial.
1946-1952	• Corta duración de la "Policía Universitaria", formada durante derrocamiento de Villarroel. Se reorganiza la policía. En 1947 se crea Policía Rural Móvil para contener sublevaciones indígenas. • Se crea la Biblioteca del Oficial de Policía. • Organización de la Comisión Codificadora Nacional de Legislación Policiaria. A partir de leyes de países americanos se elaboran 3 instrumentos jurídicos: Ley de Organización Policiaria y del Cuerpo de Carabineros, Código de Policía de Seguridad y Procedimiento de Policía de Seguridad.	• Villarroel es derrocado en diciembre de 1946. Se instala el llamado "sexenio" (1946 y 1952). En esta fase de recomposición oligárquica se hacen mayores reformas policiales de los primeros 50 años del siglo XX en el intento más serio, pero conservador, de modernización policial.
1949	• Gobierno aprueba Ley de Organización Policiaria y de Carabineros asignando a la Policía una naturaleza civil y militar dividida en brigadas departamentales. • El Cuerpo de Carabineros se sujeta a códigos penal y procesal militar.	

1950	• Militarización del Cuerpo de Carabineros y Policías: adoptan organización, entrenamiento y valores militares. • Primeros esfuerzos de profesionalización de la clase de tropa. Creciente clima de indisciplina e insubordinación.	
1951	• Se aprueba la primera Ley Orgánica de Policías y Carabineros de Bolivia. • Se reglamenta el uso de uniformes. Se abolió el reglamento de 1945. • Se crea el servicio de radiocomunicaciones a nivel nacional. • Se crea Papel Membretado para control de ingresos policiales por multas. • Normalización del servicio de patrullaje diurno y nocturno • Funcionamiento policial sustentado en reglamentos militares. • Sorprendente crecimiento de efectivos (1946 - 1951). En 1951 había un policía para cada 427 personas.	• Gobierno del Gral. Hugo Ballivián, 1951-1952.
1952-1964	• En reconocimiento al apoyo brindado al MNR, presidente designa Ministro de Gobierno a connotado miembro policial con activa militancia partidaria. • Creación de organismos de vigilancia y represión como Control Político. • Reestructuración de Escuela de Policía. Cambio de nombre por el actual. • Se implanta Célula Armada del Cuerpo de Carabineros y Policías de Bolivia, organismo facilitador de la clientela partidaria dentro del cuerpo policial. • Amplia estrategia prebendal del gobierno a favor de la policía. Se nacionaliza servicio de identificación nacional administrado por la Policía • Restablecimiento de la Policía Rural • 1960: Policía Aduanera. Se incorpora el 16% de efectivos policiales. • Revalorización del costo de multas policiales.	• El ciclo de la Revolución se inicia con la derrota política y militar del Ejército (abril de 1952) propiciada por alianza entre policías, mineros y población civil en La Paz. Gobiernos promueven desarrollo policial. Politizan la institución a través de redes clientelares.
1959	• Intervención militar y depuración policial. Gobierno recompone Ejército con ayuda de EE.UU. Se empieza a romper el equilibrio político entre militares, policías y milicias armadas.	• Divisiones en partido gobernante. Oficiales de Policía de la FSB intentan golpe de Estado.
1961	• Decimocuarta Constitución Política del Estado. Se reconoce coexistencia de 3 cuerpos armados: FFAA, Policía y Milicias del Pueblo. • Luego de 136 años de vida republicana la Constitución reconoce por primera vez existencia de la Policía. Se le asigna la totalidad de la función policial. Depende del Presidente de la República quien además nombra y decide la duración de funciones del Comandante General.	• Desde finales de los 50, USAID provee asistencia técnica, recursos, entrenamiento, becas y apoyo financiero a infraestructura policial.
1962	• Aprobación de la segunda Ley Orgánica de la Policía Nacional. • Reconocimiento de estructura jerárquica semejante al Ejército.	• Junto al Ejército, la Policía Nacional desarrolla y aplica la doctrina de la seguridad

	• Creación del cargo de Comandante General de la Policía Boliviana. • Se modifica la denominación de Brigadas por Distritos Policiales • Se aprueba el Reglamento orgánico del departamento nacional de personal. • Se aprueba primer manual de investigación criminal con apoyo de USAID. • Durante 12 años de la Revolución Nacional el promedio de efectivos policiales no superó los 7.200. 1 policía para cada 435 personas.	nacional cuyo objetivo es la lucha contra el comunismo.
1964	• Golpe militar de 1964 restablece dominio militar sobre policía. Se divide en tres cuerpos: guardia nacional de seguridad pública, dirección nacional de investigación criminal y tránsito. En acto público el Ejército desarma a la Policía y reintroduce, como en la década del 40, la "doctrina del pito y laque". • Nuevo gobierno militar desplaza lealtad política hacia la dirección nacional de investigación criminal, organismo policial civil que adquiere poder represivo. Actúa como agente de infidencia dentro del propio cuerpo policial.	• Prolongado periodo de intervención militar desde noviembre de 1964 hasta octubre de 1982. Policía es dividida, desarmada públicamente y depurada sin clemencia.
1967	• Se funda Asoc. de sub-oficiales, clases y guardias de seguridad pública.	
1968	• Creación de la Escuela de Aplicación Policial.	
1967	• Decimoquinta Constitución Política del Estado.	
1970	• Gobierno encarga Plan de Reestructuración Policial a civiles y policías. Sus resultados son: proyecto de ley orgánica, reglamento orgánico, reglamento de juzgados policiales, reglamento de régimen económico y social. Corto periodo gubernamental impide su aplicación.	• 1971: gobierno el Gral. J. J. Torres, de tendencia nacionalista. Reformas a sistema penitenciario.
1971-1978	• 1971: inicio de uno de los procesos de reforma y modernización policial más importantes de la segunda mitad del siglo XX. Se encarga a policía lucha contra las drogas y se reestructura aparato represivo y de inteligencia a través de creación de Departamento de Orden Político (DOP) y Departamento de Orden Social (DOS). Además de dar impulso a ideología anticomunista, se promueve reforma del sistema educativo, la inclusión de mujeres en la organización así como el fortalecimiento de su capacidad represiva mediante la militarización de regimientos y grupos especiales. La dictadura construye amplia base de prebendas y corrupción. Se otorgan amplias facilidades económicas mediante recaudación paralela. • Aprobación del Código de Tránsito. • Creación de Comisión de Reestructuración policial que propone reformas a Ley Orgánica, sistema educativo, comunicación social, situación económica.	• En agosto de 1971 se produce el derrocamiento del Gral. Torrez y asume el gobierno el Cnl. Hugo Banzer S. (1971-1978) con apoyo de miembros de la Policía. El gobierno introduce importantes reformas en el sistema penal mediante la aprobación de nuevos códigos. Entre 1978 y 1982 se produce la inflexión de la dictadura militar, período en el que la Policía empieza a recuperar su autonomía.

	• Durante casi toda la década del 70, Policía Nacional mantiene promedio de 8.500 hombres para población de aprox. 4.500.000 personas. un policía por cada 529 personas.	
1981	• Proyecto de Ley Orgánica de la Policía. Amplias facultades a la Policía. • Ascenso a General de la Policía Boliviana como expresión prebendal del régimen militar en descomposición. • Reestructuración del sistema educativo de la Policía Nacional. • Propuesta de incorporación de la Policía Nacional a las Fuerzas Armadas. - Amplia participación policial en lucha contra narcotráfico y contrabando. • Creación y funcionamiento del Estado Mayor Policial. Incorporación de policías a la Escuela de Altos Estudios Nacionales dirigido por las FF. AA.	• Gobierno del Gral. García Mesa (1980-1981). Régimen signado por corrupción narcotráfico, promueve lealtades policiales a través de redes de inteligencia, corrupción y chantaje.
1982	• Restablecimiento de la democracia luego de un complejo proceso de crisis militar, presión de movimientos sociales y cívicos y presión internacional.	• Primer gobierno democrático. Presidente: Dr. Hernán Siles.
1982	• Centralización de organismos policiales bajo mando único previo conflicto entre instituciones uniformadas y policías civiles. • 1er Comandante General de Policía nombrado por un gobierno democrático.	• Restablecimiento de la democracia luego de casi 20 años de dictadura.
	• En 1984 se crea la Unidad Móvil de Patrullaje Rural (UMOPAR). • Se aprueba 3ra. Ley Orgánica de la Policía en 1985. Asume amplia gama de funciones con diversas atribuciones, muchas veces sin recursos. - Fortalecimiento del funcionamiento del Estado Mayor Policial, creación de diversas unidades operativas, administrativas y de gestión económica. • Expansión de la presencia policial en el territorio nacional junto al crecimiento de unidades mixtas de seguridad física privada y seguridad física estatal. • Organización y fortalecimiento de entrenamiento policial-militar en torno a lucha contra las drogas, inteligencia y grupos operativos especializados. • Desarrollo de enfoque de género en la prestación de servicios públicos a través de brigadas de protección a la familia e incorporación de mujeres a cuerpos especializados.	• Controvertida modernización bajo liderazgo corporativo de tipo patrimonial y liderazgo político de signo prebendal, marcada por la inestabilidad, informalidad y politización. Expansión de burocracia administrativa y débil esfuerzo por mejorar capacidad operativa para luchar contra el delito.
1985	• Segundo gobierno democrático - 1987: se crea la Fuerza Especial de Lucha Contra el Narcotráfico (FELCN). • Creación de organismos de inteligencia • Prioridad al fortalecimiento y expansión policial en la ciudad de El Alto y Santa Cruz a través de creación de numerosas unidades policiales como el comando regional, batallón de seguridad física, distrito y policía montada.	• Dr. Víctor Paz, 1985-1989. • Énfasis en lucha contra drogas, inteligencia, control social. En menor medida potenciamiento preventivo, desarrollo tecnológico o inteligencia criminal.

	• En 1986, la Policía sostuvo un efectivo de aproximadamente 14.000 hombres para una población cercana a las 5.500.000 personas. Un policía para cada 392 personas.	
1989	• **Tercer gobierno democrático**	• Lic. Jaime Paz Zamora, 1989-1993
1990-2000	• A principios de los 90 se reglamentan funciones, ámbitos de competencia, dependencia, composición, control interno y mando de la FELCN. • Mandos policiales hacen diversas reformas en gestiones breves e interrumpidas por escándalos públicos, abuso de poder, corrupción, etc. • Reformas gestionadas por mando policial para mejorar capacidad de reacción y respuesta a demandas de seguridad ciudadana. Impulso a temática educativa en diversos niveles de formación. Homologación, titulación y acreditación con estatus universitario al cuerpo de oficiales así como impulso a la formación de personal subalterno, clases y policías, mediante CEFOCAP • Esfuerzos para mejorar relación con la sociedad: creación de brigadas escolares, escuelas de seguridad ciudadana y grupos de apoyo a la policía. • Creación de mecanismos de lucha contra la corrupción, abuso de poder y tráfico de influencias. • Esfuerzos dirigidos a mejorar el enfoque de género en el cuerpo policial y desarrollo de políticas educativas de derechos humanos en institutos y unidades operativas. • Énfasis en la institucionalización de mecanismos, unidades de coordinación y planificación para enfrentar problemas de seguridad ciudadana. • Aprobación de nuevo Reglamento de Faltas y Sanciones • Aprobación del Decreto Supremo de Reestructuración de la Policía Nacional. • Ejecución de planes de seguridad ciudadana insuficientes. Aumenta inseguridad pública. • Visita de equipo asesor de la Policía de Colombia a la Policía de Bolivia. Informe identifica y destaca graves problemas de diversa naturaleza. • En 1998 se conforma la Fuerza de Tarea Conjunta (FTC) para llevar a cabo tareas de erradicación. • Tensiones institucionales entre fiscales, jueces y policías generadas por la aplicación del NCPP	• Década de importantes cambios en la organización, mando y trabajo • Controvertido proceso de reformas y modernización Proceso de militarización, corrupción, relación informal con el sistema político, desprestigio, participación en lucha antidrogas. Integración de militares y policías en una sola organización para la erradicación de cocales en el Chapare. • Actividad política intensa dentro de la Policía Nacional impulsada por VIMA. Organización que promueve nueva forma de clientelismo corporativo que compite con el clientelismo de partidos tradicionales. • Reforma y aplicación del Nuevo Código de Procedimiento Penal (NCP).
1993-1997	• **Cuarto gobierno democrático** • Llevó a cabo la política de capitalización, participación popular, reforma educativa, asignación de subsidio a personas mayores de 65 años. Policías y militares intervienen en la denominada "Masacre de Amayapampa y Capasirca". Se produjeron 5 huelgas policiales.	• Lic. Gonzalo Sanchez de Lozada.

2000 2001	• Motín policial en las instalaciones del GES cuyas consecuencias para la estabilidad y gobernabilidad democrática son traumáticas. Firma de acuerdo entre gobierno y Policía Nacional aprobando aumento de sueldos al personal subalterno en 50%. Significativo poder político alcanzado por el asociacionismo policial que linda en actos penados por ley. • Caso de coronel Blas Valencia y la implicación de miembros de la Policía Nacional con organizaciones criminales internacionales pone en jaque el prestigio y la credibilidad policial. • Explosión de coche-bomba en instalaciones policiales en Santa Cruz. Luego del caso PROSEGUR aumenta la crisis interna. • Creciente aumento de denuncias contra conductas policiales ilícitas. • Aprobación del D.S. Nº 26364 del 24 de octubre del 2001. • Nueva estructura jerárquica para los generales de la Policía Nacional.	• Rápido deterioro de la unidad policial, liderazgo corporativo débil, empañado por politización y gestión política de la seguridad pública en crisis. Severo impacto del caso Blas Valencia en la opinión pública coloca a la Policía en el centro del cuestionamiento.
2002	• **Quinto gobierno democrático.** • Entre 1985 y el 2002 el crecimiento de efectivos fue modesto. Para la seguridad de una población de 8.274.300 personas (2001) se cuenta con casi 22 mil hombres. Una relación de un policía por cada 376 personas. Casi el 80% del personal policial se concentra en departamentos del eje.	• Lic. Gonzalo Sanchez de Lozada, 2002-2007.
2002	• Aprobación de Reglamento de Empresas de Seguridad Privada. Hasta agosto del 2002 existían más de 200 empresas de seguridad sin control efectivo sobre su proceso de selección de personal, salarios, costos de funcionamiento, utilidades, seguros y delimitación de funciones y manejo de armas y equipo electrónico. • Creación del Consejo de Seguridad Ciudadana a cargo de Min. de Gobierno.	• Aumento alarmante del clima de inseguridad ciudadana.
2003	• Segundo hecho de sedición policial de magnitud iniciada en el GES con amplio apoyo en el país propiciado por la asociación de clases y suboficiales. Intervención militar para garantizar la seguridad del Poder Ejecutivo y preservar el imperio del orden constitucional. Detona enfrentamiento armado entre policías y militares con saldos de numerosas víctimas. Pérdida de autoridad del Poder Ejecutivo ante la Policía, crisis de liderazgo corporativo, deliberación latente. • Aprobación de Reglamento de beneficios colaterales de la Policía Nacional, D.S. 26970 que forma parte del juego prebendal entre mandos policiales y gobierno. • Creación del Tesoro Policial, institución que pretende concentrar y fiscalizar los recursos recaudados por la Policía • Presentación del Plan Nacional de Seguridad Ciudadana y Orden Público.	• Dramáticos sucesos del 12 y 13 de febrero en la ciudad de La Paz. Crisis policial tiene como corolario un acuerdo entre partes que otorga beneficios institucionales, ratifica la impunidad y deja abierto el camino para otras crisis en la medida en que no se cumpla el convenio. • Gestión directa del Presidente de la República ante el gobierno de España para la Reforma Policial. • Dificultad para restablecer la

	• Policía de Santa Cruz se declara impotente ante la magnitud de la delincuencia. • Gobierno gestiona recursos de cooperación internacional. Pide apoyo al gobierno de España para programa de reforma policial en 6 áreas: reforma educativa, equipamiento e innovación tecnológica, seguridad ciudadana, violencia política, lucha contra terrorismo y narcotráfico, migración. • Intervención de unidades policiales que recaudan recursos por la prestación de servicios públicos. Múltiples denuncias de corrupción preceden intervención de estos organismos.	autoridad del gobierno sobre la Policía Nacional.
	• Más de 20 años de democracia ininterrumpida (1982-2003). Se produjeron 10 intentos frustrados de reforma institucional, más de 30 actos de protesta deliberativa y dos hechos de sedición que llevaron al país al filo del colapso democrático. • Ningún acto deliberativo fue procesado hasta hoy. De acuerdo a versiones de prensa son excepcionales los casos de sanción a oficiales pese a centenares de denuncias de corrupción, tráfico de influencias o abuso de poder. La impunidad corporativa daña la gobernabilidad democrática y debilita el Estado de Derecho. - Presupuesto de seguridad pública, distribuido entre el Ministerio de Gobierno y policía aumentó en 340 % en la última década. Durante los últimos cinco años, los delitos comunes crecieron en 360%. La tasa de homicidio subió de 7 a 22 homicidios por cada 100 mil habitantes entre 1997 y el año 2001. Encuestas de opinión pública destacan que los robos totales de vehículos aumentaron en 422% entre el 90 y 2001. • En la última década el gasto per cápita en seguridad aumentó en 103%. Cada ciudadano paga por su seguridad la suma de 77.3 Bs. a precio nominal y 41.9 Bs. a precio real. - El 46% de los efectivos policiales ocupan cargos burocráticos o funciones desvinculadas de tareas operativas. Nadie conoce con exactitud el volumen periódico de ingresos económicos por concepto de recaudaciones y multas. - Durante los últimos cinco años, la Policía Nacional ocupa el penúltimo lugar en la percepción de confianza pública. - Se estima que la policía privada cuenta con más de 8 mil agentes de seguridad –es decir la mitad de efectivos policiales- distribuidos en más de 150 empresas. • No obstante la crisis, existe una importante reserva moral en el personal subalterno que continúa esperando cambios profundos en su institución. - 6 de cada 10 oficiales posee título académico universitario. Este es un avance notable en la formación profesional. • La transformación de la Policía Nacional depende fundamentalmente de una reforma moral e intelectual del sistema político, de la calidad de liderazgo, de un vigoroso compromiso de los mandos policiales, de la excelencia, rigurosidad y seguimiento constante del trabajo de los medios de comunicación, de un mayor control social y un desempeño eficaz de los órganos de fiscalización parlamentaria	• BALANCE FINAL: Policía y democracia en Bolivia: Una política pendiente.

ANEXO Nº 2 ORGANIGRAMAS Y ESTADISTICAS. POLICIA BOLIVIANA

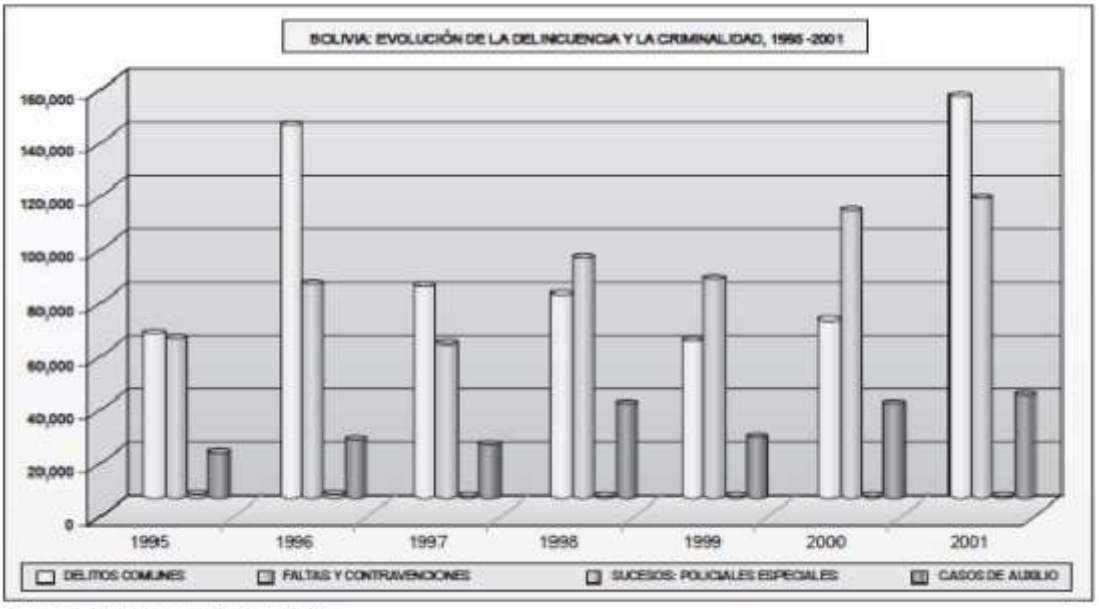
BOLIVIA: POBLACIÓN Y NÚMERO DE EFECTIVOS POLICIALES E INDICADOR SELECCIONADO, 1831 - 2001

(A partir de censos de 1831, 1835, 1845, 1854, 1882, 1900, 1950, 1976, 1992 y 2001)

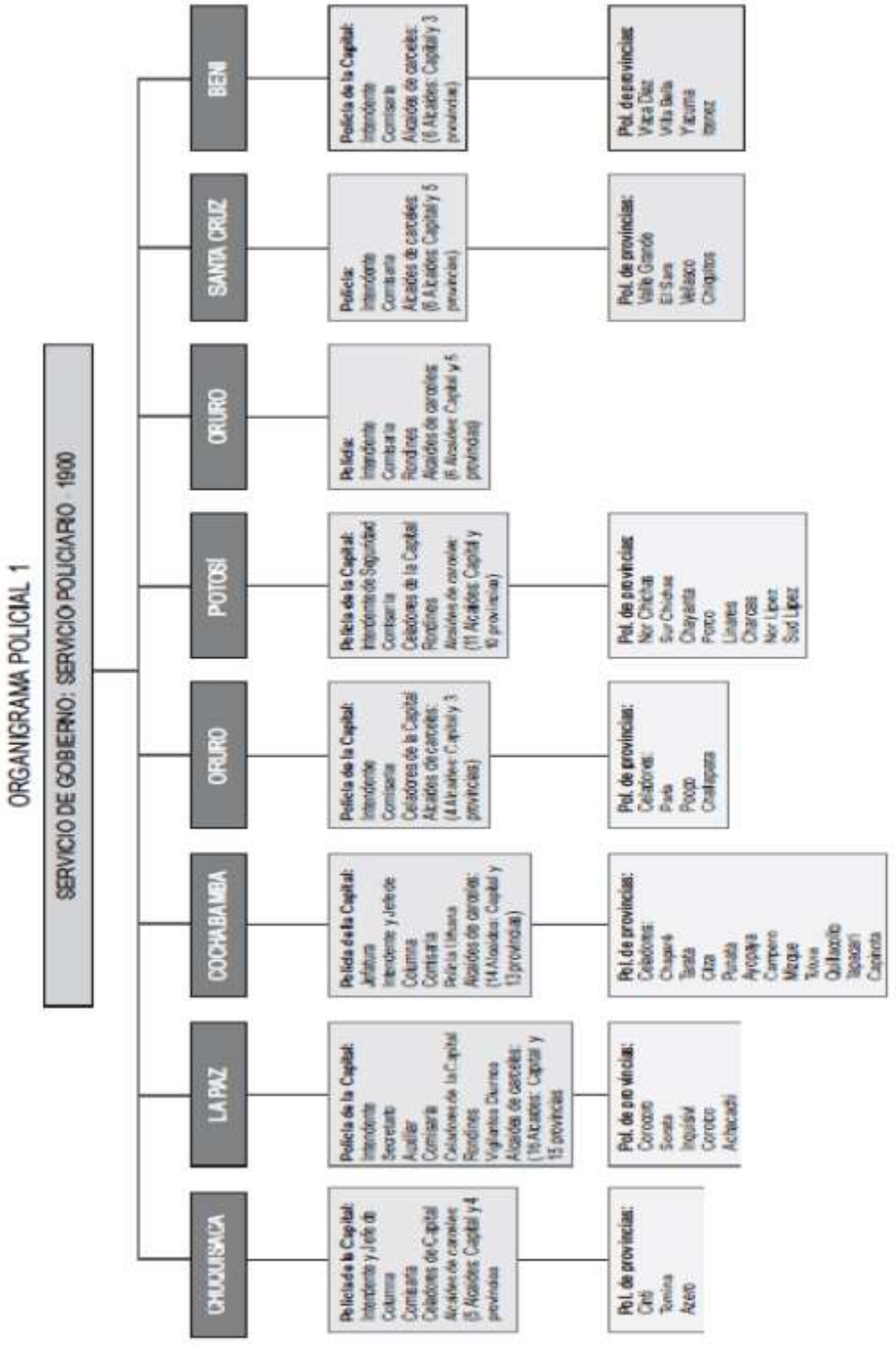
AÑOS DE CENSOS Y GOBIERNOS	POBLACIÓN	EFECTIVOS POLICIALES	EFECTIVOS POLICIALES POR CADA CIEN MIL HABITANTES	EFECTIVOS POLICIALES POR CADA DIEZ MIL HABITANTES	NÚMERO DE HABITANTES POR POLICIA
1831 Andrés de Santa Cruz	1,089,000	120	11	1	9,075
1835 Andrés de Santa Cruz	1,061,000	120	11	1	8,842
1845 José Ballivián	1,379,000	278	20	2	4,960
1854 Manuel Isidoro Belzu	1,854,000	335	18	2	5,534
1882 Narciso Campero	1,098,000	680	62	6	1,615
1900 José Manuel Pando	1,633,610	814	50	5	2,007
1950 Mamerto Urriolagoitia	3,019,031	6,503	215	22	464
1976 Hugo Banzer Suárez	4,583,101	8,239	180	18	556
1992 Jaime Paz Zamora	6,420,742	11,306	176	18	568
2001 Jorge Quiroga R.	8,274,325	19,386	234	23	427

Fuente: Presupuesto General, Siglo XIX y XX. Instituto Nacional de Estadística

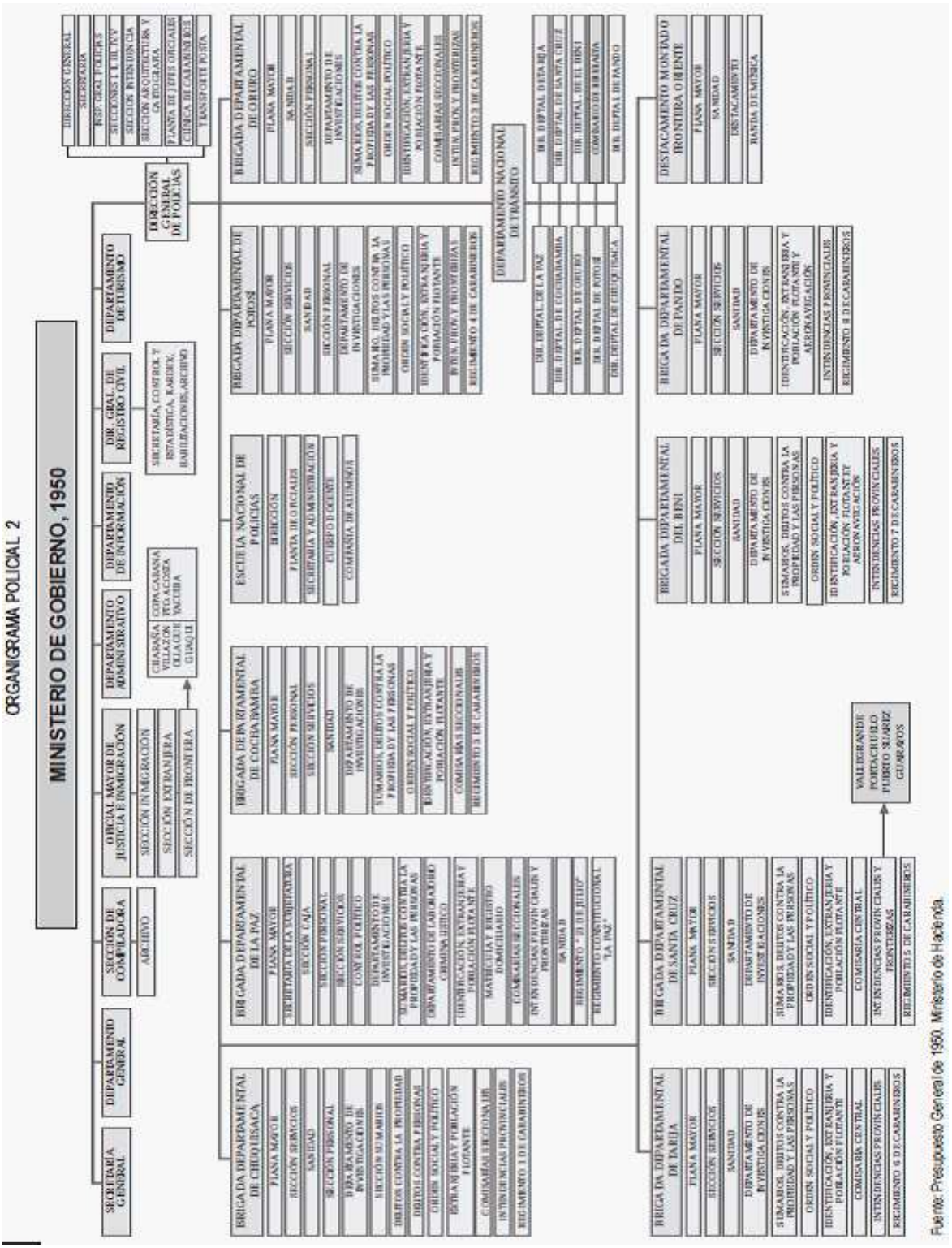
GRÁFICO 5

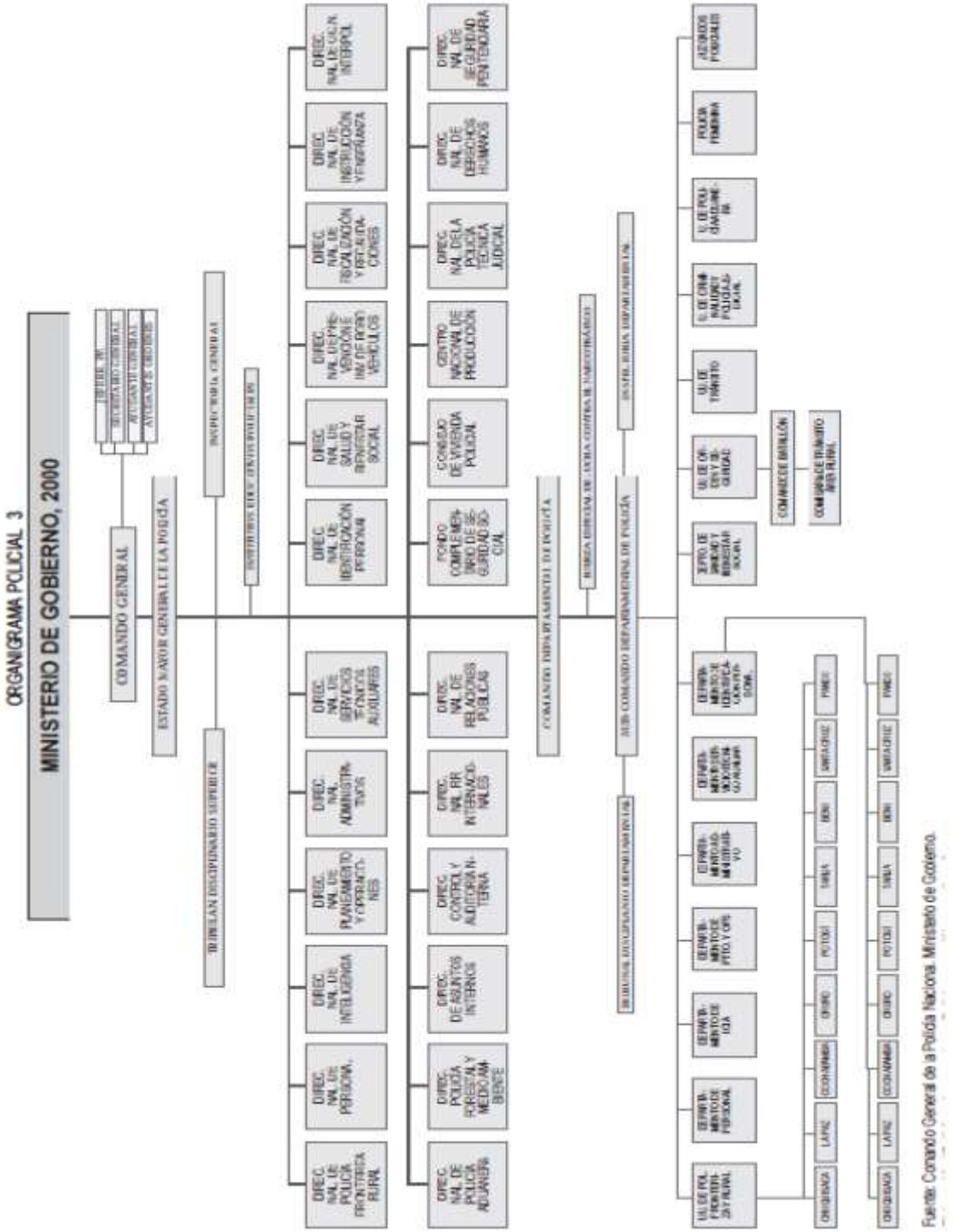


Fuente:INE-Policía Nacional-Defensor del Pueblo



Fuente: Presupuesto General de 1950. Ministerio de Hacienda


ORGANIGRAMA POLICIAL 2
MINISTERIO DE GOBIERNO, 1950
Fuente: Presupuesto General de 1950. Ministerio de Hacienda.



Fuente: Comando General de la Policía Nacional. Ministerio de Gobierno.

BOLIVIA: EVOLUCIÓN DE LA DELINCUENCIA Y LA CRIMINALIDAD, 1995-2001

DESCRIPCIÓN	GESTION						
	1995	1996	1997	1998	1999	2000	2001
Total general	**139.690**	**241.474**	**164.093**	**201.523**	**162.276**	**209.218**	**298.602**
Delitos comunes	63.529	138.246	84.331	79.944	56.161	67.052	149.663
Faltas y contravenciones	58.776	78.779	57.183	90.044	82.118	104.903	110.908
Sucesos policiales especiales	1.293	1.930	1.144	1.561	1.496	1.626	1.660
Casos de auxilio	16.092	22.519	21.435	33.974	22.481	35.637	36.371

Fuente: INE-Policía Nacional-Defensor del Pueblo

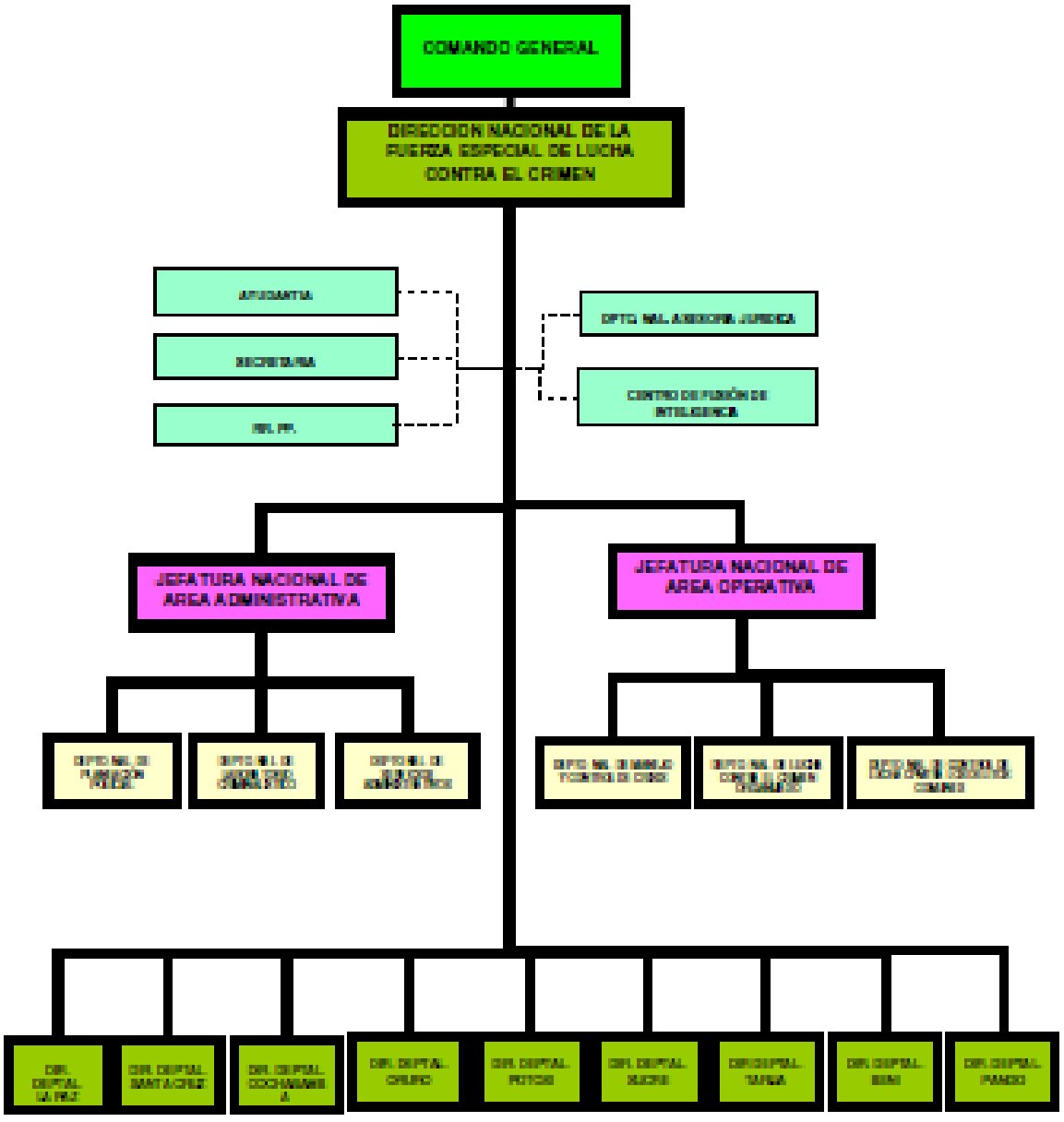
BOLIVIA: POBLACIÓN Y NÚMERO DE EFECTIVOS POLICIALES E INDICADOR SELECCIONADO, 1831 - 2001

(A patir de censos de 1831, 1835, 1845, 1854, 1882, 1900, 1950, 1976, 1992 y 2001)

AÑOS DE CENSOS Y GOBIERNOS	POBLACIÓN	EFECTIVOS POLICIALES	EFECTIVOS POLICIALES POR CADA CIEN MIL HABITANTES	EFECTIVOS POLICIALES POR CADA DIEZ MIL HABITANTES	NÚMERO DE HABITANTES POR POLICIA
1831 Andrés de Santa Cruz	1,089,000	120	11	1	9,075
1835 Andrés de Santa Cruz	1,061,000	120	11	1	8,842
1845 José Ballivián	1,379,000	278	20	2	4,960
1854 Manuel Isidoro Belzu	1,854,000	335	18	2	5,534
1882 Narciso Campero	1,098,000	680	62	6	1,615
1900 José Manuel Pando	1,633,610	814	50	5	2,007
1950 Mamerto Urriolagoitia	3,019,031	6,503	215	22	464
1976 Hugo Banzer Suárez	4,583,101	8,239	180	18	556
1992 Jaime Paz Zamora	6,420,742	11,306	176	18	568
2001 Jorge Quiroga R.	8,274,325	19,386	234	23	427

Fuente: Presupuesto General, Siglo XIX y XX. Instituto Nacional de Estadística

ORGANIGRAMA DE LA DIRECCION NACIONAL DE LA FUERZA ESPECIAL DE LUCHA CONTRA EL CRIMEN



GESTION 2010

C. III. V. SECCION MANIPULACION INFORMATICA

DEPARTAMENTO NACIONAL DE LA POLICIA TECNICA CIENTIFICA
DIVISION LABORATORIO CRIMINALISTICO
SECCION MANIPULACION INFORMATICA

RESPONDE ANTE:

- Jefatura de División

RESPONDEN A ESTE CARGO:

A NIVEL INTERNO:

- Auxiliares

A NIVEL EXTERNO:

- Ninguno

RELACIONES INTERNAS:

- Jefaturas de Departamentos de la Dirección Administrativa
- Jefaturas de Departamentos de la Dirección Operativa

RELACIONES EXTERNAS:

- Ninguno

FUNCION GENERAL

Controlar, analizar y evaluar todas las evidencias de carácter informático que le sean asignadas.

FUNCIONES ESPECIFICAS

1. Solicitar en forma oportuna los requerimientos de material y equipos necesarios para un mejor desempeño de sus tareas.
2. Informar y verificar en forma oportuna si las muestras remitidas son insuficientes.
3. Identificar a los autores de fraude en los procesos: de falsificación, manipulación, sabotajes informáticos, invasión, piratería, reproducciones no autorizadas.
4. Realizar análisis de inspecciones oculares de carácter informático.

GESTION 2010

ANEXO Nº 3 UN SIGLO DE IMÁGENES. POLICIA BOLIVIANA

Miembro de la Policía de Seguridad de La Paz principio del siglo 1900-1910
Fuente: Foto Cordero
Museo Policial

Gendarme y Carabinero de la policía de seguridad La Paz, 1911.
Fuente: Foto Cordero

Tcnl. Manuel Isaac Tellería Jefe de Policía de La Paz. 1914.
Fuente: Foto Cordero

Policía Rural creada en 1902 y re-fundada en la década del 40. La Paz.
Fuente: Foto Cordero
Museo Policial

Inspectores militares de la Policía de Seguridad 1920-1925.
Fuente: Foto Cordero
Museo Policial

Gabinete de investigación criminológico (1937)
Sra. Benigna Manzano
Fuente: Foto Cordero
Museo Policial

Intendencia seccional de
Policía (1945)
Fuente: Foto Cordero
Museo Policial

Milicianos y cadetes de la Policía
durante la Revolución Nacional,
11 de abril de 1952
Fuente: Lucio Flores

Cuerpo de oficiales de la Policia jurando a MNR. 1960
Fuente: Museo Policial

Desfile de la Brigada departamental de policias de Cochabamba 1958.
Fuente. Museo Policial

Oficiales, suboficiales, sargentos y cadetes jurando al MNR. 1954
Fuente: Lucio Flores
Fuente. Museo Policial

Brigada policial femenina
Sesquisentenario de la República
6 de agosto de 1975
Fuente: Presencia

Damas cadetes de la Academia
Nacional de Policía. 1996
Fuente: Museo Policial

Policías del Grupo Especial de
Seguridad (GES) en estado de
sedición. La Paz, febrero de 2003
Fuente: El Nuevo Día - Santa Cruz

ANEXO Nº 4 MANEJO DE EVIDENCIAS DIGITALES

5.– Reconocimiento de la Evidencia Digital

Es importante clarificar los conceptos y describir la terminología adecuada que nos señale el rol que tiene un sistema informático dentro del *iter criminis* o camino del delito. Esto a fin de encaminar correctamente el tipo de investigación, la obtención de indicios y posteriormente los elementos probatorios necesarios para sostener nuestro caso. Es así que por ejemplo, el procedimiento de una investigación por homicidio que tenga relación con evidencia digital será totalmente distinto al que, se utilice en un fraude informático, por tanto el rol que cumpla el sistema informático determinara DONDE DEBE SER UBICADA Y COMO DEBE SER USADA LA EVIDENCIA.

Ahora bien para este propósito se han creado categorías a fin de hacer una necesaria distinción entre el elemento material de un sistema informático o hardware (*evidencia electrónica*) y la información contenida en este (*evidencia digital*). Esta distinción es útil al momento de diseñar los procedimientos adecuados para tratar cada tipo de evidencia y crear un paralelo entre una escena física del crimen y una digital. En este contexto el hardware se refiere a todos los componentes físicos de un sistema informático, mientras que la información, se refiere a todos los datos, programas almacenados y mensajes de datos trasmitidos usando el sistema informático.

5.3.- Clases de Equipos Informáticos y Electrónicos

Algunas personas tienden a confundir los términos evidencia digital y evidencia electrónica, dichos términos pueden ser usados indistintamente como sinónimos, sin embargo es necesario distingair entre aparatos electrónicos como los celulares y PDAs y la información digital que estos contengan. Esto es indispensable ya que el foco de nuestra investigación siempre será la evidencia digital aunque en algunos casos también serán los aparatos electrónicos.

A fin de que los investigadores forenses tengan una idea de dónde buscar evidencia digital, éstos deben identificar las fuentes más comunes de evidencia. Situación que brindará al investigador el método más adecuando para su posterior recolección y preservación

Las fuentes de evidencia digital pueden ser clasificadas en tres grande grupos:

1. **SISTEMAS DE COMPUTACIÓN ABIERTOS**, son aquellos que están compuestos de las llamadas computadores personales y todos sus periféricos como teclados, ratones y monitores, las computadoras portátiles, y los servidores. Actualmente estos computadores tiene la capacidad de guardar gran cantidad de información dentro de sus discos duros, lo que los convierte en una gran fuente de evidencia digital.
2. **SISTEMAS DE COMUNICACIÓN**, estos están compuestos por las redes de telecomunicaciones, la comunicación inalámbrica y el Internet. Son también una gran fuente de información y de evidencia digital.
3. **SISTEMAS CONVERGENTES DE COMPUTACIÓN**, son los que están formados por los teléfonos celulares llamados inteligentes o SMARTPHONES, los asistentes personales digitales PDAs, las tarjetas inteligentes y cualquier otro aparato electrónico que posea convergencia digital y que puede contener evidencia digital.

6.2.- Qué hacer al encontrar un dispositivo informático o electrónico

- No tome los objetos sin guantes de hule, podría alterar, encubrir o hacer desaparecer las huellas dactilares o adeníticas existentes en el equipo o en el área donde se encuentra residiendo el sistema informático.
- Asegure el lugar.
- Asegure los equipos. De cualquier tipo de intervención física o electrónica hecha por extraños.
- Si no está encendido, no lo encienda *(para evitar el inicio de cualquier tipo de programa de autoprotección*
- Verifique si es posible el Sistema Operativo a fin de iniciar la secuencia de apagado a fin de evitar pérdida de información.
- Si usted cree razonablemente que el equipo informático o electrónico está destruyendo la evidencia, debe desconectarlo inmediatamente.
- Si está encendido, no lo apague inmediatamente *(para evitar la pérdida de información "volátil")*
- - SI ES POSIBLE, LLAME UN TÉCNICO.

Cuando no hay técnico:

- No use el equipo informático que está siendo investigado, ni intente buscar evidencias sin el entrenamiento adecuado.
- Si está encendido, no lo apague inmediatamente.
- Si tiene un "Mouse", muévalo cada minuto para no permitir que la pantalla se cierre o se bloquee.
- Si una Computadora Portátil (Laptop) no se apaga cuando es removido el cable de alimentación, localice y remueva la batería, esta generalmente se encuentra debajo del equipo, y tiene un botón para liberar la batería del equipo. Una vez que está es removida debe guardarse en un lugar seguro y no dentro de la misma máquina, a fin de prevenir un encendido accidental.
- Si el aparato está conectado a una red, anote los números de conexión, (números IP).
- Fotografíe la pantalla, las conexiones y cables
- Usar bolsas especiales antiestática para almacenar disketes, discos rígidos, y otros dispositivos de almacenamiento informáticos que sean electromagnéticos (si no se cuenta, pueden utilizarse bolsas de papel madera). Evitar el uso de bolsas plásticas, ya que pueden causar una descarga de electricidad estática que puede destruir los datos
- Coloque etiquetas en los cables para facilitar reconexión posteriormente
- Anote la información de los menús y los archivos activos (sin utilizar el teclado) *Cualquier movimiento del teclado puede borrar información importante.*
- Si hay un disco, una disquete, una cinta, un CD u otro medio de grabación en alguna unidad de disco o grabación, retírelo, protéjalo y guárdelo en un contenedor de papel

- Bloqueé toda unidad de grabación con una cinta, un disco o un disquere vacío aportado por el investigador (NO DEL LUGAR DE LOS HECHOS). *Al utilizar algún elemento del lugar del allanamiento o de los hechos, se contamina un elemento materia de prueba con otro.*
- Selle cada entrada o puerto de información con cinta de evidencia
- De igual manera deben selle los tornillos del sistema a fin de que no se puedan remover o reemplazar las piezas internas del mismo.
- Desconecte la fuente de poder
- Quite las baterías y almacénela de forma separada el equipo (si funciona a base de baterías o es una computadora portátil)
- Mantenga el sistema y medios de grabación separados de cualquier tipo de imán, o campo magnético
- Al llevar aparatos, anote todo número de identificación, mantenga siempre la CADENA DE CUSTODIA
- Lleve todo cable, accesorio, conexión
- Lleve, si es posible, manuales, documentación, anotaciones
- Tenga en cuenta que es posible que existen otros datos importantes en sistemas periféricos, si el aparato fue conectado a una red, por tanto desconecte el cable de poder de todo hardware de Red (Router, modem, Swich, Hub).

Si el equipo es una estación de trabajo o un Servidor (conectado en red) o está en un negocio, el desconectarla puede acarrear (SIEMPRE CONSULTE A UN TÉCNICO EXPERTO EN REDES):

- Daño permanente al equipo
- Responsabilidad Civil para la Policía Judicial y la Fiscalía General del Estado
- Interrupción ilegal del giro del negocio.

7.1.- Teléfonos Inalámbricos, Celulares, Smartfones, Cámaras Digitales

Se puede encontrar evidencia potencial contenida en los teléfonos inalámbricos tal como:

- Números llamados
- Números guardados en la memoria y en el marcado rápido
- Identificador de llamadas, llamadas entrantes
- Otra información guardada en la memoria del teléfono
- Números marcados
- Nombres y direcciones
- Números personales de Identificación (PIN)
- Número de acceso al correo de voz
- Contraseña del correo de voz
- Números de tarjetas de crédito
- Números de llamadas hechas con tarjeta
- Información de acceso al Internet y al correo electrónico
- Se puede encontrar valiosa información en la pantalla del aparato
- Imágenes. Fotos, grabaciones de voz
- Información guardada en las tarjetas de expansión de memoria

REGLA DEL ENCENDIDO "ON" Y APAGADO "OFF"

1. Si el aparato está encendido "ON", no lo apague "OFF".
   - Si lo apaga "OFF" puede iniciarse el bloqueo del aparato.
   - Transcriba toda la información de la pantalla del aparato y de ser posible tómele una fotografía.
   - Vigile la batería del aparato, el transporte del mismo puede hacer que se descargue. Tenga a mano un cargador
   - Selle todas las entradas y salidas.
   - Selle todos los puntos de conexión o de admisión de tarjetas o dispositivos de memoria
   - Selle los tornillos para evitar que se puedan retirar o reemplazar piezas internas.
   - Buscar y asegurar el conector eléctrico.
   - Colocar en una bolsa de FARADAY, (especial para aislar de emisiones electromagnéticas), si no hubiere disponible, en un recipiente vacío de pintura con su respectiva tapa.
   - Revise los dispositivos de almacenamiento removibles. (Algunos aparatos contienen en su interior dispositivos de almacenamiento removibles tales como tarjetas SD, Compact flash, Tarjetas XD, Memory Stick, etc.)

2. Si el aparato está apagado "OFF", déjelo apagado "OFF".
   - Prenderlo puede alterar evidencia al igual que en las computadoras.
   - Antes del análisis del aparato consiga un técnico capacitado en el mismo.
   - Si no existe un técnico use otro teléfono.
   - Es necesario que el investigador busque el manual del usuario relacionado con el aparato encontrado.

7.2.- Aparatos de mensajería instantánea, beepers.

1. Beepers Numéricos (reciben solo números y sirven para transmitir números y códigos)
2. Beepers Alfanuméricos (reciben números y letras, pueden cargar mensajes completos en texto)
3. Beepers de Voz (pueden transmitir la voz y también caracteres alfanuméricos)
4. Beepers de dos vías (contienen mensajes de entrada y salida)
5. Buenas Prácticas
   - Una vez que el beeper está alejado del sospechoso, este debe ser apagado. Si se mantiene encendido los mensajes recibidos, sin tener una orden judicial para ello puede implicar una interceptación no autorizada de comunicaciones.
6. Cuando se debe buscar en el contenido del aparato.
   - Cuando es la causa de la aprehensión del sospechoso
   - Cuando haya presunción del cometimiento de un delito Flagrante
   - Con el consentimiento del dueño o receptor de los mensajes

7.3.- Máquinas de Fax

1. En las máquinas de fax podemos encontrar:
   - Listas de marcado rápido
   - Fax guardados (transmitidos o recibidos)
   - Bitácoras de transmisión del Fax (transmitidos o recibidos)
   - Línea del Encabezado
   - Fijación de la Hora y Fecha de la transmisión del Fax
2. Buenas Prácticas
   - Si la máquina de fax es encontrada prendida "ON", el apagarla causaría la perdida de la memoria de último número marcados así como de los facsímiles guardados.
3. Otras consideraciones
   - Busque la concordancia entre el número de teléfono asignado a la máquina de fax y la línea de teléfono a la que está conectada.
   - De igual forma busque que el encabezado del mensaje y el número impreso coincidan con el del usuario y la línea telefónica.
   - Es necesario que el investigador busque el manual del usuario relacionado con el aparato encontrado.

7.4.- Dispositivos de Almacenamiento

Los dispositivos de almacenamiento son usados para guardar mensajes de datos e información de los aparatos electrónicos. Existen dispositivos de almacenamiento de tres clases, a saber: dispositivo magnético (como discos duros o los disquetes), dispositivos de estado sólido[3] o memoria solida (como las memorias flash y dispositivos USB) y los dispositivos ópticos (como los discos compactos y DVD).

Existen gran cantidad de Memorias USB en el mercado y otros dispositivos de almacenamiento como tarjetas SD, Compact flash, Tarjetas XD, Memory Stick, etc.

1. BUENAS PRÁCTICAS

- Recolecte las instrucciones de uso, los manuales y las notas de cada uno de los dispositivos encontrados.
- Documente todos los pasos al revisar y recolectar los dispositivos de almacenamiento
- Aleje a los dispositivos de almacenamiento de cualquier magneto, radio trasmisores y otros dispositivos potencialmente dañinos.

8.– Rastreo del Correo Electrónico

El Correo Electrónico nos permite enviar cartas escritas con el computador a otras personas que tengan acceso a la Red. El correo electrónico es casi instantáneo, a diferencia del correo normal. Podemos enviar correo a cualquier persona en el Mundo que disponga de conexión a Internet y tenga una cuenta de Correo Electrónico.

Al enviar un correo electrónico, la computadora se identifica con una serie de números al sistema del proveedor de servicios de Internet (*ISP*). Enseguida se le asigna una dirección IP y es dividido en paquetes pequeños de información a través del protocolo *TCP/IP*. Los paquetes pasan por una computadora especial llamada servidor *(server)* que los fija con una identificación única (*Message-ID*) posteriormente los sellan con la fecha y hora de recepción (*Sello de tiempo*). Más tarde al momento del envió se examina su dirección de correo para ver si corresponde la dirección IP de alguna de las computadoras conectadas en una red local (*dominio*). Si no corresponde, envía los paquetes a otros servidores, hasta que encuentra al que reconoce la dirección como una computadora dentro de su dominio, y los dirigen a ella, es aquí donde los paquetes su unen otra vez en su forma original a través del protocolo *TCP/IP*. (Protocolo de Control de Transferencia y Protocolo de Internet). Siendo visible su contenido a través de la interface gráfica del programa de correo electrónico instalado en la máquina destinataria.

Hay que tomar en cuenta que los correos electrónicos se mantienen sobre un servidor de correo, y no en la computadora del emisor o del destinatario, a menos que el operador los guarde allí. Al redactarlos se transmiten al servidor de correo para ser enviados. Al recibirlas, nuestra computadora hace una petición al Servidor de correo, para los mensajes sean transmitidos luego a la computadora del destinatario, donde el operador la puede guardar o leer y cerrar. Al cerrar sin guardar, la copia de la carta visualizada en la pantalla del destinatario desaparece, pero se mantiene en el servidor, hasta que el operador solicita que sea borrada.

En algunas ocasiones es necesario seguir el rastro de los Correos Electrónicos enviados por el Internet. Los rastros se graban en el encabezamiento del e-mail recibido. Normalmente, el encabezamiento que aparece es breve. La apariencia del encabezamiento está determinada por el proveedor de servicios de Internet utilizado por nuestra computadora, o la de quien recibe el correo electrónico. Para encontrar los rastros, se requiere un encabezamiento completo o avanzado, posibilidad que existe como una opción en nuestro proveedor de servicios de Internet.