UNIVERSIDAD MAYOR DE SAN ANDRÉS

FACULTAD DE DERECHO Y CICENCIAS POLÍTICAS

CARRERA DE DERECHO

BIBLIOTECA

PROCESO DE DIGITALIZACIÓN DEL FONDO BIBLIOGRÁFICO DE LA BIBLIOTECA DE DERECHO

GESTION 2017

Nota importante para el usuario:

"Todo tipo de reproducción del presente documento siempre hacer mención de la fuente del autor y del repositorio digital para evitar cuestiones legales sobre el delito de plagió y/o piratería".

La dirección de la Biblioteca

UNIVERSIDAD MAYOR DE SAN ANDRÉS
FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS
CARRERA DE DERECHO

ACREDITADA POR RESOLUCIÓN
CEUB Nº 1126/02

MONOGRAFIA

"Para optar al titulo académico de Licenciatura en Derecho"

"FUNDAMENTOS PARA LA PROTECCIÓN PENAL SOBRE LA DESTRUCCIÓN, ALTERACIÓN, INUTILIZACIÓN Y DAÑO A PROGRAMAS O DOCUMENTOS ELECTRÓNICOS"

POSTULANTE : EDWIN ADELIO COPA ANARA

INSTITUCION : MINISTERIO DE JUSTICIA

LA PAZ – BOLIVIA
2012

DEDICATORIA

A mis padres, quienes con infinita humildad, cariño dedicación y amor me brindaron su apoyo inculcándome valores, cuidándome con mucha paciencia. Dándome lo más preciado y valioso que una persona puede llegar a tener el "estudio", por lo que les dedico con todo amor y cariño y admiración este trabajo.

Querido Papito y querida Mamita.
Antonio Copa Martínez y Cecilia Anara Mamani.

AGRADECIMIENTO

A Dios, a toda mi familia y seres queridos.

A la Facultada de Derecho y Ciencias Políticas de la Universidad Mayor de San Andrés por ser la fuente que lleno de conocimientos y me formo académicamente.

Al Ministerio de Justicia por brindarme la oportunidad de poner en practica mis conocimientos.

PROLOGO

El presente aporte de investigación, se encuentra circunscrito dentro de la rama del Derecho Penal lográndose evidenciar la falta de actualización tipificación en el código penal sobre los delitos informáticos, tras el trabajo dirigido en el área de coordinación judicial en la comisión codificadora en el proyecto de ley del código de procedimiento laboral y la dirección jurídica en el Ministerio de Justicia donde pude aprender sobre lo que es la técnica legislativa y el análisis de la norma para su proyección y presentación es que a ese aspecto me propuse analizar los vacios jurídicos y la mala aplicación de la norma penal en los delitos, con el conocimiento adquirido y con iniciativa y tras el análisis del código penal y la apelación de la misma tome como punto de referencia para realizar mi trabajo el capitulo XI delitos informáticos.

El proyecto da a conocer lo que son los diferentes tipo de delitos informáticos existentes en el mundo y la falta de tipificación de los mismos en el código penal boliviano y la propuesta de agregar una nueva tipificación penal la cual en el trabajo se expone la diferenciación con las tipificaciones existentes en el código penal boliviano, siendo este trabajo una guía para las futuras comisiones de codificación y modificación del código penal boliviano en el Ministerio de Justicia.

Esperando que este trabajo sea considerado y tomado en cuenta dentro de las comisión de codificación del código penal en el Ministerio de Justicia como iniciativa para la modificación e implementación a este capitulo del código penal lo expuesto en este trabajo, logrando llenar esos vacios jurídicos y la falta y mala aplicación del código penal boliviano.

ÍNDICE GENERAL

PAGINA

DEDICATORIA……

AGRADECIMIENTOS……

PROLOGO……

INTRODUCCION……..

1. ELECCION DEL TEMA DE LA MONOGRAFIA…… 1

2. FUNDAMENTACIÒN E IMPORTANCIA DEL TEMA…… 1

3. DELIMITACION……. 3

3.1. DELIMITACIÓN TEMÁTICA…… 3

3.2. DELIMITACIÓN ESPACIAL…… 3

3.3. DELIMITACIÓN TEMPORAL……. 3

4. MARCO TEORICO O DE REFERENCIA…… 4

4.1. MARCO TEÓRICO……... 4

4.2. MARCO HISTÓRICO……... 6

4.3. MARCO CONCEPTUAL……. 8

4.4. MARCO JURÍDICO…….. 12

5. PLANTEAMIENTO DEL PROBLEMA…… 13

6. OBJETIVOS…….. 13

6.1. OBJETIVO GENERAL…… 13

6.2. OBJETIVO ESPECIFICO…… 14

7. ESTRATEGIA METODOLOGICA Y TECNICAS DE INVESTIGACION…… 14

7.1. METODOLOGÍA…….. 14

7.1.1. MÉTODO DEDUCTIVO……..... 14

7.1.2. MÉTODO DOGMATICO JURÍDICO…… 14

7.1.3. MÉTODO COMPARATIVO…….. 15

7.1.4. MÉTODO TELEOLÓGICO…… 15

7.2. TÉCNICAS DE INVESTIGACIÓN……... 15

7.2.1. TÉCNICA BIBLIOGRÁFICA……..... 15

7.2.2. TÉCNICA DE LA ENTREVISTA ESTRUCTURADA…… 15

CAPITULO I

MARCO HISTORICO.

1. LA EVOLUCION DE LA INFORMATICA Y SU RELACION A LA ACTIVIDAD DELICTIVA……. 16
2. HISTORIA DE LOS ATAQUES A SISTEMAS O PROGRAMAS INFORMATICOS EN EL MUNDO Y SUS AUTORES…… 25
3. LOS DELITOS INFORMATICOS EN BOLIVIA…… 34
4. AVANCES HISTORICOS EN LA LUCHA CONTRA LOS DELITO INFORMATICO EN EL MUNDO…… 41
5. ESTADÍSTICAS SOBRE DELITOS INFORMÁTICOS…… 43

CAPITULO II

MARCO TEORICO Y CONCEPTUAL

1. TEORIAS Y CONCEPTOS DE DELITO INFORMATICO…… 50
2. CLASIFICACIÓN DE LOS DELITOS INFORMÁTICOS…….. 58
3. LA DIFERENCIA ENTRE LOS DELITOS INFORMATICOS CON LOS DEMAS DELITOS……. 76
4. CONCEPTO Y DIFERENCIACIÓN DE DATO, PROGRAMA Y DOCUMENTO ELECTRONICO Y LA APRECIACIÓN DE LOS MISMOS COMO UN VALOR ECONOMICO…… 81

4.1. CONCEPTO DE DATO, PROGRAMA Y DOCUMENTO ELECTRÓNICO……. 81

4.2. DIFERENCIACIÓN ENTRE DATO, PROGRAMA Y DOCUMENTO ELECTRÓNICO……. 85

4.3. APRECIACIÓN ECONÓMICA DEL PROGRAMA Y VALOR PROBATORIO DEL DOCUMENTO ELECTRÓNICO……..... 86

5. CONCEPTO DEL DELITO DE DESTRUCCIÓN, ALTERACIÓN, INUTILIZACIÓN Y DAÑO A PROGRAMAS O DOCUMENTOS ELECTRÓNICOS (Sabotaje informático)…….. 88
5.1. INTRODUCCION…… 88
5.2. CONCEPTO SOBRE DELITO DE DESTRUCCIÓN, ALTERACIÓN, INUTILIZACIÓN Y DAÑO A PROGRAMAS O DOCUMENTOS ELECTRÓNICOS…… 90
6. EL SUJETO ACTIVO Y PASIVO EN EL DELITO DE DESTRUCCIÓN, ALTERACIÓN, INUTILIZACIÓN Y DAÑO A PROGRAMAS O DOCUMENTOS ELECTRÓNICOS…… 94
6.1. PERFIL CRIMINOLÓGICO DEL SUJETO ACTIVO EN EL DELITO DE DESTRUCCIÓN, ALTERACIÓN, INUTILIZACIÓN Y DAÑO A PROGRAMAS O DOCUMENTOS ELECTRÓNICOS……. 95
6.2. EL SUJETO PASIVO EN EL DELITO DE DE DESTRUCCIÓN, ALTERACIÓN, INUTILIZACIÓN Y DAÑO A PROGRAMAS O DOCUMENTOS ELECTRÓNICOS……... 100
7. LEGISLACION COMPARADA SOBRE EL DELITO DE DESTRUCCIÓN, ALTERACIÓN, INUTILIZACIÓN Y DAÑO A PROGRAMAS O DOCUMENTOS ELECTRÓNICOS…….. 101
7.1. INTRODUCCION……... 101
7.2. LEGISLACIÓN EXTRANJERA……. 102

CAPITULO III

PROYECTO DE CREACION DEL TIPO PENAL

1. GENERALIDADES…….. 108
2. TEORIA PENAL PARA LA CREACION DE LA NORMA……... 109
3. PROPUESTA DE LEY SOBRE LA INCORPORACION DEL TIPO PENAL SOBRE DESTRUCCIÓN, ALTERACIÓN, INUTILIZACIÓN Y DAÑO A PROGRAMAS O DOCUMENTOS ELECTRÓNICOS ……. 112
3.1. EXPOSICIÓN DE MOTIVOS…… 112

3.2. MARCO CONSTITUCIONAL…….. 113
3.3. TEXTO DE LA PROPUESTA DEL TIPO PENAL……... 114
4. CONCLUSION……. 117
5. RECOMENDACIÓN Y SUGERENCIAS…….. 118
6. ANEXOS…… 119
7. BIBLIOGRAFIA…… 129

INTRODUCCION

El presente monografía, pretende constituirse en un aporte importante referido a la falta de tipificación en los delitos informáticos en la legislación boliviana y la incorporación de una nueva tipificación penal que es la “DESTRUCCIÓN, ALTERACIÓN, INUTILIZACIÓN Y DAÑO A PROGRAMAS O DOCUMENTOS ELECTRÓNICOS”, esperando que sea de gran aporte para los estudiosos en la materia de penal y que sea un referente mas para la producción de ideas.

Lo que busca el presente trabajo es demostrar mediante la historia del avance informático y la evolución de la computadora el mal uso de los procesadores para fines delictivos y la existencia de varios tipos de delitos informáticos y mediante estadísticas mundiales demostrar que esta clase de delitos se presentan en diferentes partes del mundo a lo cual en el país no se encuentra libre de cometerse estos delitos.

En la legislación boliviana se encuentra un capitulo referente a los delitos informáticos en la cual se encuentra dos articulo referentes a los delitos informáticos, el 363 bis que es la manipulación informática y el 363 ter la alteración, acceso y uso indebido de datos informáticos, a lo cual en el primer articulo mencionado hace referencia a lo que es la manipulación informática del dato, la acción que se encuentra en dicho articulo es la de manipular un procesamiento o transferencia de datos informáticos que conduzca a un resultado incorrecto o evite un procesamiento correcto no entrando este en el tema tocado y demostrando un vacio jurídico, algunos abogados dicen y piensan que no se encuentran vacios jurídicos en lo que es la tipificación penal de los delitos informáticos pero expertos en la materia de informática dicen que no se puede hablar de lo que es el delito informático y tipificarlo penalmente solo colocando como referencia el dato ya que si dato muy bien es la parte básica de la información la informática no es solo eso la rama de la informática es amplia y compuesta de muchas herramientas electrónicas y no solo así del manejo de la información.

Encontramos que el dato en la legislación boliviana esta protegida pero la informática no es solo eso, el instrumento por el cual se procesa los datos y la respuesta o la manipulación de servicios en el tema encontramos la diferencia entre dato como base de la información y la programación como instrumentó por el cual se procesa el dato y el documento electrónico como respuesta al dato colocado.

Como medio de dar a conocer los diferentes tipos de delitos informáticos en la legislación comparada encontramos que en la legislación alemana, española, francesa, italiana se encuentra diferentes tipificaciones de los delitos informáticos para esta clase de delitos.

Con el avance y diferenciación realizada entre dato, programa y documento electrónico y las doctrinas se ha proyectado la tipificación deseada sobre la necesidad de protección penal sobre la “destrucción, alteración, inutilización y daño a programas o documentos electrónicos”.

PERFIL DE MONOGRAFIA

1. ELECCION DEL TEMA DE LA MONOGRAFIA

"FUNDAMENTOS PARA LA PROTECCION PENAL SOBRE LA DESTRUCCIÓN, ALTERACIÓN, INUTILIZACIÓN Y DAÑO A PROGRAMAS O DOCUMENTOS ELECTRÓNICOS"

2. FUNDAMENTOS E IMPORTANCIA DEL TEMA

Con el avance de la tecnología se ha visto la enorme influencia que ha alcanzado la informática en la vida diaria de las personas y organizaciones siendo de suma importancia su progreso para el desarrollo de un país. Con el avance de la tecnología informática han surgido una serie de comportamientos ilícitos llamados genéricamente delitos informáticos que adoptan formas muy distintas, siendo entre estas el acceso ilegal, la difusión de programas perjudiciales y ataques por denegación de servicios.

En base a estas clases de conductas ilícitas cometidas por elementos informáticos y que según doctrinas el concepto de delito informático puede comprender tanto aquellas conductas que valiéndose de medios informáticos lesionan otros intereses jurídicamente protegidos como la intimidad, el patrimonio económico, la fe pública, la seguridad como aquellas que recaen sobre las herramientas informáticas propiamente tales como programas, ordenadores, etc.

En la mayoría de las legislaciones de diferentes países se encuentran tipificaciones sobre lo que son los delitos informáticos dentro de su normativa penal, en lo que es la Legislación Penal boliviana se encuentra un capitulo sobre lo que son los delitos informáticos a la cual se conforma por los siguientes artículos:

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

Siendo esta figura un enlace para la protección del patrimonio económico de las personas que están proclives a conductas que valiéndose de medios informáticos lesionan estos intereses y que si bien según doctrinas delito informático puede comprender tanto aquellas conductas que valiéndose de medios informáticos lesionan otros intereses como el patrimonio económico este debería ser mas exacta ya que la figura debería regular la protección de la información de los datos y programas o documentos electrónicos y otros.

Articulo 363 Ter. (ALTERACION, ACCESO Y USO INDEBIDO DE DATOS INFORMATICOS). El que sin estar autorizado se apodere, acceda, utilice, modifique, suprima o inutilice, datos almacenados en una computadora o en cualquier soporte informático, ocasionando perjuicio al titular de la información, será sancionado con prestación de trabajo hasta un (1) año o multa hasta doscientos días.

En este articulo si bien se habla de lo que es la protección a los datos informáticos sobre lo que es su apoderamiento, acceso, utilización, modificación, supresión o inutilización ocasionando un perjuicio, solo se habla de lo que es el dato, siendo el **dato** unidades básicas de la información, cualquiera que sea su contenido (un número, una palabra, un sonido, una imagen) y que al ser procesados dan lugar a la información que resulta de la conexión de dos o más datos debiendo diferenciarse que estos no son lo mismo que **programa** ya que estos son las secuencias de instrucciones que se utilizan para el procesamiento de los datos, para la realización de tareas específicas y que siendo los **documentos electrónicos** aquellos en que se recogen los

resultados del procesamiento de los datos obtenidos con las distintas aplicaciones.

En la diferenciación se denota que el dato solo es la base de lo que se debería proteger dejando al descuido sobre la protección de lo que es el programa y los documentos electrónicos que son parte del desarrollo de la información ya que la finalidad de la tipificación de delitos informáticos tiene que ser la protección de la información y de sus herramientas y elementos por las cuales se las sostiene debiendo sancionarse a la persona que atente contra tales.

3. DELIMITACION DEL TEMA DE LA MONOGRAFIA

3.1. Delimitación temática

El tema propuesto es sobre la creación de una nueva figura en el código penal boliviano sobre destrucción, alteración, inhabilitación y daño a programas o documentos electrónicos

3.2. Delimitación espacial

La monografía contempla como delimitación espacial al Estado Plurinacional de Bolivia, ya que la norma que se pretende fundamentar para su creación tendría vigencia en todo el territorio del Estado Boliviano.

3.3. Delimitación temporal

Las presentes investigaciones sobre el tema se suscribirán desde la gestión 2008 al 2012 denotándose con mayor énfasis la realización de esta clase de delitos en el mundo y Bolivia.

4. MARCO TEORICO O DE REFERENCIA

4.1. Marco Teórico

A partir de la existencia de nuevas formas de operar con la tecnología, aparecen delitos que no son nuevos, sino que existían desde mucho antes de la aparición de la informática, pero que presentan importantes particularidades que han planteado serios interrogantes que nuestro derecho positivo parece no saber cómo resolver. (1)

En relación a lo que es el delito informático sobre destrucción, alteración, inhabilitación y daño a programas o documentos electrónicos como un delito informático se denota que en los delitos informáticos si bien comprender tanto aquellas conductas que valiéndose de medios informáticos lesionan otros intereses jurídicamente protegidos como la intimidad, el patrimonio económico, la fe pública, la seguridad, la enunciación genérica de una serie de medios dentro de los cuales tenga cabida el uso del ordenador o se permita expresamente el uso de cualquier medio, no otorga al delito el carácter de "informático", sin perjuicio de que se hable de un delito relacionado con la informática(2) y que debería considerarse que al tipificarse un delito informático lo que se busca es tutelar el contenido de información de un sistema informático, y no el hardware en sí mismo, debiendo considerarse delito informático la reproducción ilícita de obras de software, de bases de datos o de topografías de semiconductores, habiendo situaciones en que se dan los dos supuestos, es decir el ordenador se usa como instrumento y es a la vez el objeto sobre el cual recae la acción delictiva, como es la destrucción de datos, programas o documentos electrónicos mediante un programa de virus informático.

---

1. "Delitos Informáticos", R. de Sola Quinteros. Pág. 5
2. "Biblioteca Del Congreso Nacional de Chile Departamento de estudios, extensión y publicaciones. Pág. 2
3. "Delitos Informáticos", Dr. Santiago Acurio Del Pino. Pág. 11

Es así que cuando se trate de delitos que recaen sobre objetos informáticos propiamente dichos, el bien jurídico protegido será la información entendida como proceso que englobe el almacenamiento, tratamiento y transmisión. Así, la información se considera como un valor económico de la actividad de la empresa dedicada al uso y producción de la información.

Al respecto, Romeo Casabona señala que el término Delito Informático debe usarse en su forma plural, en atención a que se utiliza para designar una multiplicidad de conductas ilícitas y no una sola de carácter general. (3)

En síntesis si bien se habla específicamente de lo que es los delitos informáticos en el **Articulo 363 Ter** este solo ataca una clase de delito informático lo que es el apoderamiento, acceso, utilización, modificación, supresión o inutilización del dato ocasionando un perjuicio al titular de dicho dato o datos no resolviendo la necesidad de la protección del medio por el cual también se procesan o se guardan estos datos.

Marco Histórico

Al aparecer la necesidad del hombre en comunicarse y realizar nuevos medios de comunicación también desarrollo el uso de la información entre los diferentes medios siendo uno de ellos el uso de la computación como medio masivo de comunicación y un elemento por el cual se guarda la información desarrollando otros medios aparte del papel para transportar la información y a ese aspecto al desarrollo de los mismo a llevado también a la usurpación y daño a esos medios y elementos informáticos con el fin de afectar a los programas o documentos electrónicos existentes dentro de esos elementos informáticos es así que se desarrollo esta clase de delitos. (4)

Jhon Draper.- Llamado también “Capitan Crunch” [Captain Crunch, en inglés], descubrió que la sorpresa que venía dentro cereal Captain Crunch dublicaba la intensidad de la frecuencia de 2600 hz. de una línea de WATS, permitiéndole hacer llamadas telefónicas gratis.

Bill Gates y Paul Allen.- en el tiempo en el que estos dos hombres de Washington, eran aprendices, se dedicaban a hackear software. Llegaron a ser grandes programadores, y se convirtieron en creadores del imperio de Sistemas Operativos líder. Sus "éxitos" fueron el SO MS-DOS, Windows, Windows 95/NT.

Ian Murphy, también llamado "Captain Zap", a sus 23 años de edad, logró entrar a los sistemas de la Casa Blanca, el Pentágono, BellSouth Corp. TRW, y deliberadamente dejó su currículum. El consideraba que "violar accesos le resultaba divertido". (5)

En ese entendido como estos precursores en la actividad delictiva informática desde la aparición de la maquinaria para remitir información, de personales y programas informáticos denotaron la su actividad siendo ya algunos procesados por actividades ilícitas como hackear o irrumpir ilícitamente programas del Estado donde residen estos sujetos otros dedicándose a la fabricación y mejora de sistemas. Pero no solamente la irrupción de sistemas sino a delinquir en la destrucción de sistemas por medio de los mismos sistemas creando programas maliciosos y apoderándose de datos o sistemas enteros.

En ese fin es que remontando a épocas más antiguas del siglo XX en el año 1939, el famoso científico matemático **John Louis Von Neumann**, de origen húngaro, escribió un artículo, publicado en una revista científica de New York, exponiendo su "Teoría y organización de autómatas complejos", donde demostraba la posibilidad de desarrollar pequeños programas que pudiesen tomar el control de otros, de similar estructura.

4."Manual de Informática Jurídica", Ricardo A. Guibourg, Jorge O. Alende, elena M. Campanella. Pág. 14-16

5. "Delitos Informáticos", Richard Cotrina. Pág. 4

Cabe mencionar que Von Neumann, en 1944 contribuyó en forma directa con John Mauchly y J. Presper Eckert, asesorándolos en la fabricación de la ENIAC, una de las computadoras de Primera Generación, quienes construyeran además la famosa UNIVAC en 1950.

En 1949, en los laboratorios de la Bell Computer, subsidiaria de la AT&T, 3 jóvenes programadores: Robert Thomas Morris, Douglas McIlory y Victor Vysottsky, a manera de entretenimiento crearon un juego al que denominaron CoreWar, inspirados en la teoría de John Von Neumann, escrita y publicada en 1939. (6)

Puesto en la práctica, los contendores del CoreWar ejecutaban programas que iban paulatinamente disminuyendo la memoria del computador y el ganador era el que finalmente conseguía eliminarlos totalmente. Este juego fue motivo de concursos en importantes centros de investigación como el de la Xerox en California y el Massachusetts Technology Institute (MIT), entre otros.
Sin embargo durante muchos años el CoreWar fue mantenido en el anonimato, debido a que por aquellos años la computación era manejada por una pequeña élite de intelectuales.

A pesar de muchos años de clandestinidad, existen reportes acerca del virus CREEPER, creado en 1972 por ROBERTH THOMAS MORRIS que atacaba a las famosas IBM 360, emitiendo periódicamente en la pantalla el mensaje: "I'm a creeper... catch me if you can!" (Soy una enredadera, agárrenme si pueden).
En 1980 la red ARPANET del ministerio de Defensa de los Estados Unidos de América, precursora de Internet, emitió extraños mensajes que aparecían y desaparecían en forma aleatoria, asimismo algunos códigos ejecutables de los programas usados sufrían una mutación. Los altamente calificados técnicos del Pentágono se demoraron 3 largos días en desarrollar el programa antivirus correspondiente.

---

6. “Delitos Informáticos” Microsoft.com

4.2. Marco Conceptual

- **Delito informático.-** son los hechos ilícitos que se cometen o se facilitan mediante el empleo del ordenador con fines de dañar a otra persona en su patrimonio o imagen.
- **Hardware.-** Es la parte sensible y táctil del ordenador compuesto por accesorios como ser las tarjetas placas.
- **Software.-** Es el conjunto de los programas de cómputo, procedimientos, reglas, documentación y datos asociados que forman parte de las operaciones de un sistema de computación.
- **Protección de software:** el modo de garantizar a los autores o productores de programas la rentabilidad de sus productos frente a la notable facilidad de duplicación alteración no autorizada o la destrucción o mal uso de los mismos.
- **Protección del hardware***:* base o elemento de sistema que guarda la información procesada
- **Documentos informáticos:** modo de prueba de los contratos y otros actos jurídicos formalizados por intermedio de la computadora. (7)
- **Ordenador.-** es una máquina electrónica que recibe y procesa datos para convertirlos en información útil. Una computadora es una colección de circuitos integrados y otros componentes relacionados que puede ejecutar con exactitud, rapidez y de acuerdo a lo indicado por un usuario o automáticamente por otro programa, una gran variedad de secuencias o rutinas de instrucciones que son ordenadas, organizadas y sistematizadas en función a una amplia gama de aplicaciones prácticas y precisamente determinadas
- **Sistema informático.-** Es un sistema informático como todo sistema, es el conjunto de partes interrelacionadas, hardware, software y de recurso humano (humanware) que permite almacenar y procesar información.
- **Hacker.-** Un hacker (del inglés hack, recortar), también conocidos como sombreros blancos es el neologismo utilizado para referirse a un experto en varias o algunas ramas relacionadas con la computación y

telecomunicaciones: programación, redes de comunicaciones, sistemas operativos, hardware de red/voz. Usuario de ordenadores especializado en penetrar en las bases de datos de sistemas informáticos estatales con el fin de obtener información secreta.

En la actualidad, el término se identifica con el de delincuente informático, e incluye a los cibernautas que realizan operaciones delictivas a través de las redes de ordenadores existentes.

- **Cracker.-** Básicamente lo opuesto a un hacker, utilizan sus conocimientos para destruir y no obtener nada productivo, usan los conocimientos de otros para fines personales y solo se dedican a destruir y ocasionar perdidas. Entre las variantes de crackers están los que realizan Carding (Tarjeteo: uso ilegal de tarjetas de crédito), Trashing (Basureo, obtención de información en cubos de basura, tal como números de tarjetas de crédito, contraseñas, directorios o recibos); Phreaking y Foning (uso ilegal de las redes telefónicas) y los clásicos y llanamente llamados Piratas (gente del Warez) que se dedican a copiar software legal, música o vídeos, para regalarlo o venderlo por ahí.
- **Lammer.-** Además de estos dos adjetivos que son los más malinterpretados hay otros especificativos dentro del tema de los hackers, estos son eleet (o elite) y lamer (o lammer). El adjetivo de elite se lo aplican determinados hackers para dar a entender que son superiores a la mayoría de los hackers ahora a caído en desuso pero de todas formas los que se llaman a sí mismos elite suelen estar más cerca de lamers. Por último lamer es todo aquel que o desconoce totalmente el mundo underground y se cree hacker por el mero hecho de saber donde bajarse programas utilizados por hackers y saber utilizarlos o bien se trata de gente sin conocimientos que se dedica a hacer mal uso del apelativo de hacker y se dedica a robar claves de correo, passwords de juegos sin otro sentido que el de darse importancia

---

7.”Manual de Informática Jurídica”, Ricardo A. Guibourg, Jorge O. Alende, elena M. Campanella. Pág. 14-16

- **Virus.-** Un virus informático es un malware que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario. Los virus, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este. Los virus pueden destruir, de manera intencionada, los datos almacenados en un ordenador, aunque también existen otros más inofensivos, que solo se caracterizan por ser molestos.
- **Bomba lógica.-** Una bomba lógica es una parte de código insertada intencionalmente en un programa informático que permanece oculto hasta cumplirse una o más condiciones pre programadas, en ese momento se ejecuta una acción maliciosa. Por ejemplo, un programador puede ocultar una pieza de código que comience a borrar archivos cuando sea despedido de la compañía (en un disparador de base de datos (trigger) que se dispare al cambiar la condición de trabajador activo del programador). El software que es inherentemente malicioso, como virus o gusanos informáticos, frecuentemente contiene bombas lógicas que ejecutan algún programa en un tiempo predefinido o cuando cierta condición se cumple. Esta técnica puede ser usada por un virus o un gusano para ganar ímpetu y para esparcirse antes de ser notado. Muchos virus atacan sus sistemas huéspedes en fechas específicas, tales como el viernes 13 o el April fools' day (día de los bufones de abril) o el día de los inocentes. Los troyanos que se activan en ciertas fechas son llamados frecuentemente "bombas de tiempo".
- **Gusano informático.-** Un gusano (también llamados IWorm por su apocope en inglés, I de Internet, Worm de gusano) es un malware que tiene la propiedad de duplicarse a sí mismo. Los gusanos utilizan las partes automáticas de un sistema operativo que generalmente son invisibles al usuario. A diferencia de un virus, un gusano no precisa alterar los archivos de programas, sino que reside en la memoria y se duplica a sí mismo. Los gusanos casi siempre causan problemas en la red (aunque sea simplemente consumiendo ancho de banda), mientras que los virus siempre infectan o corrompen los archivos de la computadora que atacan.

- **Virus troyano.-** En informática, se denomina troyano o caballo de Troya (traducción literal del inglés Trojan horse) a un software malicioso que se presenta al usuario como un programa aparentemente legítimo e inofensivo pero al ejecutarlo ocasiona daños. El término troyano proviene de la historia del caballo de Troya mencionado en la Odisea de Homero. Los troyanos pueden realizar diferentes tareas, pero, en la mayoría de los casos crean una puerta trasera (en inglés backdoor) que permite la administración remota a un usuario no autorizado. Un troyano no es estrictamente un virus informático, y la principal diferencia es que los troyanos no propagan la infección a otros sistemas por sí mismos.

4.3. Marco Jurídico

LEGISLACIÓN BOLIVIANA

CODIGO PENAL BOLIVIANO

Capitulo XI

Delitos informáticos

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

Articulo 363 Ter. (ALTERACION, ACCESO Y USO INDEBIDO DE DATOS INFORMATICOS). El que sin estar autorizado se apodere, acceda, utilice, modifique, suprima o inutilice, datos almacenados en una computadora o en cualquier soporte informático, ocasionando perjuicio al titular de la información, será sancionado con prestación de trabajo hasta un (1) año o multa hasta doscientos días.

En la legislación boliviana en el código penal boliviano se encuentra un capitulo sobre delitos informáticos a la cual se evidencia la falta de normatividad y de ambigüedad de la misma si bien se dice que ya existe la tipificación a los delitos informáticos no podemos hablar de solo dos delitos si en el primero en su nombre jurídico expresa manipulación informática solo se habla del dato y de su manipulación a lo cual otras legislaciones reconocen otros delitos aparte de este es que así vemos la tipificación del delito propuesto en otras legislaciones.

LEGISLACIÓN SOBRE DELITOS INFORMATICOS ESPAÑA

Artículos del Código Penal Español referentes a Delitos Informáticos.

Artículo 264.

2. se impondrá la pena de tres años al que por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.

(ALEMANIA)

Ley referente a delitos informáticos

Párrafo 303b. "Quien destruya una elaboración de datos que sea de esencial importancia para una industria ajena, una empresa ajena o una autoridad,

1. cometiendo el hecho de acuerdo al párrafo 303.a.II, o

2. destruyendo, dañando, inutilizando, eliminando o alterando una instalación de elaboración de datos o un soporte de datos, será castigado con pena de privación de libertad de hasta cinco años o con multa.

II. La tentativa será punible".

(COLOMBIA)

Sobre delitos informáticos

Artículo 269D: DAÑO INFORMÁTICO. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos,

incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

(**CHILE)**

LEY RELATIVA A DELITOS INFORMATICOS

Ley No.:19223

Artículo 1º.- El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo.

Si como consecuencia de estas conductas se afectaren los datos contenidos en el sistema, se aplicará la pena señalada en el inciso anterior, en su grado máximo.

5. PLANTEAMIENTO DEL PROBLEMA

Con la existencia de los delitos informáticos se realizo la tipificación sobre esta clase de delitos en el Código Penal Boliviano, debiendo realizase la mayor exactitud sobre el objeto protegido.

¿Cumplirá el capitulo XI sobre delitos informáticos la finalidad de protección sobre la información siendo este al objeto a proteger o tendrá que crearse una nuevas tipificación en el cual se complemente a los artículos existentes en dicho capitulo?

6. OBJETIVOS

6.1. Objetivo general.

Demostrar si el Capitulo XI delitos informáticos en sus artículos Artículo 363 bis. Articulo 363 Ter del Código Penal si cumplen con la finalidad de proteger al objeto de delito que es la información.

Proponer la creación de una nueva figura penal por el cual se sancione a la persona que cause la destrucción, alteración, utilización y daño a programas o documentos electrónicos.

6.2. Objetivos específicos.

Determinar las desventajas de las tipificaciones realizadas sobre delitos informáticos en el Código Penal estimando su grado de eficacia en las tipificaciones sobre esta clase de delitos.

Explicar diferencia entre dato, programa y documento electrónico y su necesidad de tipificar.

Fundamentar el porque de esta creación de la norma y porque proveer este delito en nuestro medio social.

7. ESTRATEGIA METODOLOGICA Y TECNICAS DE INVESTIGACION

7.1. Metodología

7.1.1. Método deductivo.- Partiremos de la existencia de los diferentes tipos de delitos informáticos asta llegar a identificar el tipo de delito informático para proyectar la tipificación faltante en el código penal boliviano.

7.1.2. Método dogmatico jurídico.- Por que se realizara un análisis de toda la legislación referente al tema en cuestión “interpretar es determinar el sentido y el alcance de la norma”25. Así mismo, al pretender proyectar una norma que tutele la información y otros relacionados con este para su posterior interpretación y sistematización de una norma.

7.1.3. Método comparativo.- Se tomara como parámetro otras legislaciones extranjeras que tengan jurisprudencia sobre lo que es delitos informáticos, viendo como se debe redactar o ver que tipifica exactamente en su legislación, comparando la eficacia de nuestra norma a tales delitos tipificados por otras legislaciones y si estas ocurren en nuestra sociedad, no implicando plagio de la ley extranjera.

7.1.4. Método teleológico.- El método teleológico busca cual es el interés jurídicamente protegido en este caso analizaremos cuales son los intereses protegidos al crear un nuevo tipo penal sobre delitos informáticos en la legislación penal boliviana.

7.2. Técnicas de investigación

7.2.1. Técnica Bibliográfica.- Se apoyan en los documentos contenidos tanto por medios físicos, como los contenidos por medios magnéticos, al ser este un tema que es nuevo en la sociedad en Bolivia ya que no se tiene demasiada documentación física al respecto y por ello los medios magnéticos son trascendental importancia.

7.2.2. Técnica de la entrevista estructurada.- se lo realizara en base de preguntas ya establecidas a ciertas personas:

1. Expertos en la rama de la informática.

CAPITULO I.-
MARCO HISTORICO.

1. LA EVOLUCION DE LA INFORMATICA Y SU RELACION A LA ACTIVIDAD DELICTIVA.

.- El hombre por la suma necesidad de llegar a comunicarse y pasar información a grandes distancias ha llevado a pensar en diferentes medios para lograrlo, en el principio el hombre para comunicarse utilizaba gestos, el hombre en la necesidad de dejar sus conocimientos, para que sus sucesores tengan conocimiento de lo que hacia, como vivía o como pensaba lo llevo a plasmar esa información primeramente en las rocas en el tiempo de las cavernas, con el avance del tiempo s sofistico es así que en Egipto sus conocimientos y lo que querían que supiesen sus sucesores lo plasmaron en simbologías en sus pirámides donde demostraron la necesidad de dejar conocimiento y sabiduría siendo un medio de información los mismo para conocer como vivían, siendo también el origen en la fabricación del papel o común mente llamado papiro en ese tiempo, los egipcios obtenían el papiro de una planta del mismo nombre (llamada thuf en el antiguo Egipto), caracterizada por sus hojas largas, tallos blandos -de parte inferior muy gruesa- y sección triangular. La médula del papiro era consumida como alimento una vez hervida y también se usó en la elaboración de un material similar al papel. (1) En Egipto se fabricó el papiro a partir de capas estiradas de la médula, las que se ordenaban en forma transversal es que así en estas hojas se transcribía información relacionada a varios temas cultura, guerra, arquitectura y otros es así que a lo largo de la historia el hombre ha necesitado transmitir y tratar la información de forma continua. Aun están en el recuerdo las señales de humo y los destellos con espejos, y más recientemente los mensajes transmitidos a través de cables utilizando el código Morse, o la propia voz por medio del teléfono. La humanidad no ha cesado en la creación de métodos para procesar información. (2)

1. "Wikipedia historia de la información" Internet texto digital.
2. **ETORRE** Giannantonio, "Informática y Derecho" Volumen 1. Pág. 5

Al rápido avance sobre los materiales de información como medio de ayuda para superar deficiencias en la memoria facilitando no solo el uso para guardar información si no para reproducirla es que PASCAL en 1642 crea una máquina mecánica de sumar, parecida a los cuenta kilómetros que utilizan en la actualidad los automóviles. Pero ésta tenía algunos problemas con las sumas largas; pero en 1671 LEIBNITZ le agregó la posibilidad de: restar, sumar, multiplicar y dividir. Su máquina estaba formada sobre ruedas dentadas, cada una de estas ruedas tenía diez dientes, éstos correspondían a los números de 0 al 9. Siendo el sistema de tal tipo, que el paso de 9 a 0 daba lugar a un salto de la rueda, siendo esta una de las primeras maquinas para el desarrollo del tratamiento de la información y medio de ayuda para el hombre.

Este descubrimiento que facilitaría la vida del hombre dio paso a una serie de invenciones como ser por el genio BABBAGE que desarrollo la primera computadora de uso general. Fue un genio pero la época no lo ayudó para poder terminar de construirla. Llamó a su descubrimiento "Máquina de las diferencias". En 1833 concibió una segunda máquina que le llevó 20 años. Esta era capaz de realizar una suma en segundos y necesitaba un mínimo tiempo de atención del operador. A esta segunda máquina la llamó "Analítica". Leibniz aplicó la lógica y la materializó en su exitosa maquina de calcular.

Sobre lo que es la primera operación de procesamiento de datos fue lograda en 1890 por HERNAN HOLLERICH. Éste desarrolló un sistema mecánico para calcular y agrupar datos de censos. El nuevo sistema se basaba en tarjetas perforadas. Lo utilizaron en el censo de población en Estados Unidos en donde se logró por primera vez, que los resultados fueran conocidos a los dos años y medio, mientras que el censo anterior se tardó siete años para conocer estos datos. (3)

---

3. **RICARDO** A. Guibourg, Jorge O. Alende, Elena M. Campanella. “Manual de Informática Jurídica” 29-30

Tras el transcurso del tiempo el hombre en razón al avance informático, en 1930el norteamericano Vannevar Bush diseñó en el MIT (Massachusetts Institute of Technology) el analizador diferencial, marcando el inicio de nuestra era de computadoras; el "analizador" era una máquina electrónica que medía grados de cambio en un modelo. La maquina ocupaba la mayor parte de una gran sala; para analizar un nuevo problema, un grupo de ingenieros debía cambiar las proporciones, y sólo aparecían, tras dos o tres días, con las manos cubiertas de aceite. Aun la capacidad de la máquina para resolver complicados cálculos sobrepasaba cualquier invento anterior

El invento de Vannevar Bush dio paso a la primera computadora totalmente electrónica que fue la ENIAC (Electric Numeric Integrator And Calculator), fue construida en 1943 y 1945 por JOHN MANCHI y J. PROPER ECKUT. Podía multiplicar 10.000 veces más rápido que la máquina de AIKEN, pero tenía sus problemas. Como estaba construida con casi 18,000 válvulas de vacío, era enorme la energía que consumía y el calor que producía. Esto hacia que las válvulas se quemaran rápidamente y que las casas de alrededor tuviera cortes de luz. (4)

En la Segunda Guerra Mundial se vio a Alemania y a los otros países occidentales en competencia por desarrollar una mayor velocidad de cálculo, junto a un aumento de la capacidad de trabajo, para así lograr decodificar los mensajes enemigos. En respuesta a su presión EE.UU, desarrolló en Harvard el enorme computador Mark I, con una altura de 2,5 m, inspirado por las ideas de Babbage, el Mark I se dedicó a problemas balísticos de la Marina. En Alemania, se estaba comprobando las aerodinámicas proyectadas en el computador.

Desarrollándose tanto la tecnología es que 1956 se desarrolló el circuito integrado o "IC" que pronto recibiría el sobrenombre de "chip". Se atribuye el mérito de este invento a Robert Noyce. La fabricación del microchip 6,45 mm2 (la décima parte de una pulgada cuadrada), pronto fue seguida por la Capacidad de integrar hasta 10 transistores miniaturizados y eventualmente 1.000 piezas varias en el mismo espacio.

4. **RICARDO** A. Guibourg, Jorge O. Alende, Elena M. Campanella. “Manual de Informática Jurídica” 40.

Tras el avance de siglos el 4 de octubre de 1957, la antigua unión soviética puso en órbita el primer satélite artificial, llamado **SPUTNIK,** adelantándose a los Estados Unidos de América que dos años antes había anunciado el inicio de una carrera inter-espacial.

Siendo el principio para la comunicación global y medio para transmitir información logrando un gran salto a la informática con ese avance se vería nuevos avances en la computación e informática llegando a los avance sobre las programaciones las cuales pueden tener carácter personal o publico para el año 1949, en los laboratorios de la Bell Computer, subsidiaria de la **AT&T**, 3 jóvenes programadores: **Robert Thomas Morris**, **Douglas McIlory** y **Victor Vysottsky**, a manera de entretenimiento crearon un juego al que denominaron **CoreWar**, inspirados en la teoría de **John Von Neumann**, escrita y publicada en 1939.

Puesto en la práctica, los contendores del **CoreWar** ejecutaban programas que iban paulatinamente disminuyendo la memoria del computador y el ganador era el que finalmente conseguía eliminarlos totalmente. Este juego fue motivo de concursos en importantes centros de investigación como el de la **Xerox** en **California** y el **Massachussets Technology Institute** (MIT), entre otros.

Sin embargo durante muchos años el **CoreWar** fue mantenido en el anonimato, debido a que por aquellos años la computación era manejada por una pequeña élite de intelectuales, con el avance de la tecnología y el de que muchas veces la misma puede ser superado por otra tecnología o programa superior al desarrollado demostrándose que en cada año el equipamiento se mejora.

Llegando la era de los procesadores de menor tamaño es que alrededor de 1971, el microprocesador había sido desarrollado por la nueva compañía de Noyce, Intel. Esta novedad colocó en un finito microchip los circuitos para todas las funciones usuales de un computador. Fueron integrados ahora en el chip en una serie de delgadísimas capas. Esto hizo que la computación fuera más rápida y más flexible, al tiempo que los

circuitos mejorados permitieron al computador realizar varias tareas al mismo tiempo y reservar memoria con mayor eficacia.

La nueva era sobre el procesamiento de la información había comenzado en Agosto de 1981 la **International Business Machine** lanza al mercado su primera computadora personal, simplemente llamada **IBM PC**. Un año antes, la IBM habían buscado infructuosamente a **Gary Kildall**, de la **Digital Research**, para adquirirle los derechos de su sistema operativo CP/M, pero éste se hizo de rogar, viajando a Miami donde ignoraba las continuas llamadas de los ejecutivos del "gigante azul". (5)

Es cuando oportunamente aparece **Bill Gates**, de **Microsoft Corporation** y adquiere a la **Seattle Computer Products**, un sistema operativo desarrollado por **Tim Paterson**, que realmente era un "clone" del CP/M. Gates le hizo algunos ligeros cambios y con el nombre de **PC-DOS** se lo vendió a la IBM, sin embargo, Microsoft retuvo el derecho de explotar dicho sistema, bajo el nombre de **MS-DOS**. (6)

El nombre del sistema operativo de Paterson era "**Quick and Dirty DOS**" (Rápido y Rústico Sistema Operativo de Disco) y tenía varios errores de programación (bugs). La enorme prisa con la cual se lanzó la IBM PC impidió que se le dotase de un buen sistema operativo y como resultado de esa imprevisión todas las versiones del llamado PC-DOS y posteriormente del MS-DOS **fueron totalmente vulnerables a los virus**, ya que fundamentalmente heredaron muchos de los conceptos de programación del antiguo sistema operativo CP/M, como por ejemplo el PSP (Program Segment Prefix), una rutina de apenas 256 bytes, que es ejecutada previamente a la ejecución de cualquier programa con extensión EXE o COM.

Para el hombre la evolución del manejo y el procesamiento de los datos e información mediante medios informáticos para llegar a la comunicación y conocimiento sobre otros seres ha sido trascendental donde se denotan las siguientes generaciones en computadoras:

---

5. “DelitosInformáticos.Com” pagina Web
6. “Derechoinformatico.Com” pagina Web

Primera Generación (1945-1955)

Se llama así a la generación de tubos al vacío y válvulas.

Se caracterizó por maquinas muy grandes y pesadas. Muy lentas en sus procesos, tanto que la resolución de programas largos implicaba varios d/as de espera. Pese a todo fue muy útil pues podía resolver 5.000 cálculos por segundo. (7)

Segunda Generación (1955 - 1965)

Se Llamaba de los transistores y sistemas en Lote.

En las computadoras de esta generación se reemplazaron las válvulas por los transistores. Con eso se pudo reducir el tamaño de los ordenadores y aumentar su velocidad de trabajo. Aunque todavía eran un poco lentas (7)

Tercera Generación (1965 - 1980)

Se llama de circuitos integrados y de multiprogramación. El gran descubrimiento de este periodo fueron los circuitos integrados denominados CHIP. El circuito integrado consiste en un gran número de componentes electrónicos (transistores, resistencias, etc.) miniaturizados y encapsulados en un espacio de pocos centímetros. Este descubrimiento produjo grandes cambios en cuanto al tamaño de las computadoras; en velocidad, en compatibilidad, e introduciendo nuevas técnicas de programación. (7)

Cuarta Generación (1980-1990)

Se la denomina de computadora personal o de computadora hogareña. Se llama así ya que los microprocesadores son chips mucho más pequeños que contienen en un centímetro cuadrado, miles de Si hacen memoria quiere decir que la computadora ENIAC con 18.000 válvulas, que ocupaba mas de una habitación, hoy se resume en un centímetro cuadrado. De esta forma muchas familias comenzaron a tener computadoras en sus casas, como por ejemplo las TEXAS INSTRUMENT 99/4A, COMMODORE 64 Y 128, SPECTRUM. (7)

---

7. **RICARDO** A. Guibourg, Jorge O. Alende, Elena M. Campanella. “Manual de Informática Jurídica” pág. 15-18

Quinta Generación (1990) Hasta la Fecha

En la actualidad los piases más adelantados, entre los que figuran Japón y Estados Unidos están investigando y produciendo, los primeros prototipos de nuevos ordenadores que formaran la Quinto Generación. (Estos tendrán la capacidad de realizar deducciones empleando el lenguaje del hombre.) Esta Quinta generación que recién comienza se denominará: Computadora inteligente o inteligencia artificial.

Con el avance de la computadora se crearía un sistema por el cual la información se transmitiría de forma pública o privada mediante servidores este es el internet como su origen entre 1973 y 1974, cuando Robert Kahn y Vinton Cerf estructuraron la complementación de los protocolos TCP e IP, del modo como trabajan aún hoy; o cabe mejor remitir la referencia a 1972, con la primera aplicación de correo electrónico. (8)

Existe una evolución tecnológica que comienza con la primitiva investigación en conmutación de paquetes, ARPANET y tecnologías relacionadas en virtud de la cual la investigación actual continúa tratando de expandir los horizontes de la infraestructura en dimensiones tales como escala, rendimiento y funcionalidades de alto nivel. (8)

Existen aspectos sociales, que tuvieron como consecuencia el nacimiento de una amplia comunidad de internautas trabajando juntos para crear y hacer evolucionar la tecnología.

Y finalmente, el aspecto de comercialización que desemboca en una transición enormemente efectiva desde los resultados de la investigación hacia una infraestructura informática ampliamente desarrollada y disponible en 1990 la ARPANET es disuelta.

En 1991 el Gopher es creado por la Universidad de Minnesota. El Gopher provee al usuario de un método basado en un menú jerarquico, que es capaz de localizar información en la Internet. Esta herramienta facilita enormemente el uso de la Internet y en 1992 se funda la Internet Society.

---

8. **RICARDO** A. Guibourg, Jorge O. Alende, Elena M. Campanella. “Manual de Informática Jurídica” pág. 15-18

El European Laboratory for Particle Physics in Switzerland (CERN) en 1993 - libera el World Wide Web (WWW), desarrollado por Tim Berners-Lee**.** El WWW usa el protocolo de transferencia de hipertexto **(HTTP)** y encadena hipertextos fácilmente, cambiando así la ruta o camino de la información, la cual entonces puede ser organizada, presentada y accesada en la Internet.

Y en 1993 la troncal de la red NSFNET es elevada a "T3" lo que lo habilita para trasmitir datos a una velocidad de 45 millones de bits por segundo, o sea cerca de 1400 paginas de texto por segundo.

Entre 1993-1994 el visualizador (browsers) grafico de web Mosaic y Netscape Navigator aparece y rápidamente son dispersados por la comunidad de la Internet. Debido a su naturaleza intuitiva y a la interface gráfica, estos browsers hacen que los WWW y la Internet sean más atractivos al público en general.

En 1995 la troncal de la red NSFNET es reemplazado por una nueva arquitectura de redes, llamada vBNS (very high speed backbone network system), esto significa sistema de redes con troncal de alta velocidad, que utiliza los Network Service Providers, (Proveedores de Servicios de Redes), redes regionales y Network Access Points (NAPs).

Es así que Internet hoy en día es una infraestructura informática ampliamente extendida. Su primer prototipo es a menudo denominado National Global or Galactic Information Infrastructure (Infraestructura de Información Nacional Global o Galáctica).

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

En 1992 la Asociación Internacional de Derecho Penal, durante el coloquio celebrado en Wurzburgo (Alemania), adoptó diversas recomendaciones respecto a los delitos informáticos, entre ellas que, en la medida que el Derecho Penal no sea suficiente, deberá promoverse la modificación de la definición de los delitos existentes o la creación de otros nuevos, si no basta con la adopción de otras medidas como por ejemplo el "principio de subsidiariedad". Se entiende Delito como: "acción penada por las leyes por realizarse en perjuicio de algo o alguien, o por ser contraria a lo establecido por aquéllas".

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

"Los delitos informáticos se realizan necesariamente con la ayuda de los sistemas informáticos, pero tienen como objeto del injusto la información en sí misma". Adicionalmente, la OCDE elaboró un conjunto de normas para la seguridad de los sistemas de información, con la intención de ofrecer las bases para que los distintos países pudieran erigir un marco de seguridad para los sistemas informáticos.

En esta delincuencia se trata con especialistas capaces de efectuar el crimen y borrar toda huella de los hechos, resultando, muchas veces, imposible de deducir como es como se realizó dicho delito. La Informática reúne características que la convierten en un medio idóneo para la comisión de nuevos tipos de delitos que en gran parte del mundo ni siquiera han podido ser catalogados.

La legislación sobre sistemas informáticos debería perseguir acercarse lo más posible a los distintos medios de protección ya existentes, pero creando una nueva regulación basada en los aspectos del objeto a proteger: la información. En este punto debe hacerse un punto y notar lo siguiente: (9)

9. "www.delitosinfromaticos.com" pagina web

No es la computadora la que atenta contra el hombre, es el hombre el que encontró una nueva herramienta, quizás la más poderosa hasta el momento, para delinquir. No es la computadora la que afecta nuestra vida privada, sino el aprovechamiento que hacen ciertos individuos de los datos que ellas contienen. La humanidad no está frente al peligro de la informática sino frente a individuos sin escrúpulos con aspiraciones de obtener el poder que significa el conocimiento.

Por eso la amenaza futura será directamente proporcional a los adelantos de las tecnologías informáticas. La protección de los sistemas informáticos puede abordarse desde distintos perspectivas: civil, comercial o administrativa.

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

2. HISTORIA DE LOS ATAQUES A SISTEMAS O PROGRAMAS INFORMATICOS EN EL MUNDO Y SUS AUTORES

.- Desde la necesidad de comunicación del hombre a grandes distancias y la necesidad del avance informático en el mundo el ser humano a buscado el desarrollo de la tecnología denotando la necesidad de transmitir información y almacenarla es que en ese transcurso el hombre con su capacidad de creación, después de la antigua Unión Soviética puso en órbita el primer satélite artificial, llamado ***SPUTNIK,*** adelantándose a los Estados Unidos de América que dos años antes había anunciado el inicio de una carrera inter-espacial es que un año después el presidente ***DWIGTH EISENHOWER*** ordenó la creación del ***ADVANCED RESEARCH PROJECTS AGENCY*** (Agencia de avances de proyectos reservados) creado por el departamento de defensa de los estados unidos así como la ***NASA*** resaltando el avance de las comunicaciones globales con tal avance. (10)

10. “historiadelitosinformaticos.com” Pagina web

A los avances informáticos no solo se presentaron ventajas si no que también desventajas que si bien el con el avance de las comunicaciones globales y la informática, el avance del proceso de la información por estos medios manejo informático podían ser susceptibles de delitos ya no como un delito común, sino como un delito que atentaría contra la información transmitida almacenada por estos medios de comunicaciones compuestas por sistemas o elementos informáticos ya que la información es un elemento trascendental para el hombre como base de formación de conocimientos, debiendo el mismo protegerlos para que estos no sean dañados ya que la información tiene un fin de conocimiento económico o de otra índole valorándose el mismo como un valor económico o según el uso a desenvolver o protagonizar por fundamento de la persona.

Entre 1939 y 1949 el precursor John Louis Von Neumann, de origen húngaro, escribió un artículo, publicado en una revista científica de New York, exponiendo su "Teoría y organización de autómatas complejos", donde demostraba la posibilidad de desarrollar pequeños programas que pudiesen tomar el control de otros, de similar estructura. (9)

Cabe mencionar que Von Neumann, en 1944 contribuyó en forma directa con John Mauchly y J. Presper Eckert, asesorándolos en la fabricación de la ENIAC, una de las computadoras de Primera Generación, quienes construyeran además la famosa UNIVAC en 1950, denotando que en este periodo eran pocos los que podían acceder a las computadoras siendo en su mayoría solo intelectuales estando los mismo en la clandestinidad y que a pesar de muchos años de clandestinidad, existen reportes acerca del virus **CREEPER**, creado en 1972 por **ROBERTH THOMAS MORRIS** que atacaba a las famosas IBM 360, emitiendo periódicamente en la pantalla el mensaje: "I'm a creeper... catch me if you can!" (Soy una enredadera, agárrenme si pueden). Para eliminar este problema se creó el primer programa antivirus denominado Reaper (segadora), ya que por aquella época se desconocía el concepto del software antivirus.

Es así que se da el comienzo de los delitos informáticos que como objetivo de tal delito tiene como la finalidad de causar agravios, daños o perjuicios en contra de las personas, grupos de ellas, entidades o instituciones y que por lo general son ejecutados por medio del uso de las computadoras y a través del mundo virtual de la internet dando el ejemplo de lo ocurrido en **1980** la red **ARPANET** del ministerio de **Defensa de los Estados Unidos de América**, precursora de Internet, emitió extraños mensajes que aparecían y desaparecían en forma aleatoria, asimismo algunos códigos ejecutables de los programas usados sufrían una mutación. Los altamente calificados técnicos del Pentágono se demoraron 3 largos días en desarrollar el programa antivirus correspondiente. (11)

Si muy bien se creo los antivirus estos no son un medio de defensa muy seguro para la protección de programas contra otros programas maliciosos como ser los virus y otros, tratar de realizar un medio de seguridad ante estos programas maliciosos es largo y arduo ya que no es fácil detectar el virus o la clase a la que pertenece y realizar el antivirus es trabajo arduo y no siempre puede ser eficaz ante otros virus o programas maliciosos ya que el mismo tiene que ser actualizado.

En 1986 hubo un masivo ataque por programas maliciosos o mayor mente conocida como virus ya en ese año se difundieron los virus **(c) Brain, Bouncing Ball** y Marihuana y que fueron las primeras especies representativas de difusión masiva. Estas 3 especies virales tan sólo infectaban el sector de arranque de los diskettes. Posteriormente aparecieron los virus que infectaban los archivos con extensión **EXE** y **COM**. Los que mayormente que crean esta clase de programas maliciosos son aquellos conocedores y especializados y egresados de escuelas técnicas o informáticas como ser **Robert Tappan Morris** que el 2 de Noviembre de 1988, fue uno de los precursores en la realización de los virus y recién graduado en Computer Science en la Universidad de Cornell, difundió un virus a través de ArpaNet, (precursora de **Internet**) logrando infectar 6,000 servidores conectados a la red. La propagación la realizó desde uno de los terminales del MIT (Instituto Tecnológico de Massashussets).

---

11. **HERMILIO** Tomas Azpilsueta “Derecho Informático” pág. 23

Cabe mencionar que el **ArpaNet** empleaba el **UNIX**, como sistema operativo. Robert Tappan Morris al ser descubierto, fue enjuiciado y condenado en la corte de Syracuse, estado de Nueva York, a 4 años de prisión y el pago de US $ 10,000 de multa, pena que fue conmutada a libertad bajo palabra y condenado a cumplir 400 horas de trabajo comunitario. Actualmente es un experto en Seguridad y ha escrito innumerables obras sobre el tema.

Es así que se desata la fiebre de los virus como sistema de penetración y de daño a los medios y sistemas de información, en Junio de 1991 el **Dr. Vesselin Bontchev**, que por entonces se desempeñaba como director del Laboratorio de Virología de la Academia de Ciencias de Bulgaria, escribió un interesante y polémico artículo en el cual, además de reconocer a su país como el líder mundial en la producción de virus da a saber que la primera especie viral búlgara, creada en 1988, fue el resultado de una mutación del virus **Vienna**, originario de Austria, que fuera desensamblado y modificado por estudiantes de la Universidad de Sofía. Al año siguiente los autores búlgaros de virus, se aburrieron de producir mutaciones y empezaron a desarrollar sus propias creaciones.

En 1989 su connacional, el virus **Dark Avenger** o el "vengador de la oscuridad", se propagó por toda Europa y los Estados Unidos haciéndose terriblemente famoso por su ingeniosa programación, peligrosa y rápida **técnica de infección**, a tal punto que se han escrito muchos artículos y hasta más de un libro acerca de este virus, el mismo que posteriormente inspiró en su propio país la producción masiva de sistema generadores automáticos de virus, que permiten crearlos sin necesidad de programarlos.

Se demuestra que el ingenio del hombre a la necesidad de la información y la adquisición de la información prohibida lleva a delinquir y el uso de los dispositivos computacionales son un medio para la adquisición de información prohibida por medio de la alteración de programaciones o el daño mediante estos se ha vuelto frecuente viéndose y desarrollándose en varios pises el uso de programas dañinos para causar la destrucción de otros programas o del hardware es así que en 1991 apareció en el Perú el primer virus local, autodenominado **Mensaje** y que no era otra cosa que una

simple mutación del virus **Jerusalem-B** y al que su autor le agregó una ventana con su nombre y número telefónico. Los virus con apellidos como **ESPEJO, MARTINEZ Y AGUILAR,** fueron variantes del **Jerusalem-B** y prácticamente se difundieron a nivel nacional. Continuando con la lógica del tedio, en 1993 empezaron a crearse y diseminarse especies nacionales desarrolladas con creatividad propia, siendo alguno de ellos sumamente originales, como los virus Katia, Rogue o F03241 y los polimórficos **Rogge II** y **PLEASE WAIT** (que formateaba el disco duro). La creación de los virus locales ocurre en cualquier país y el Perú no podía ser la excepción.

Tras estos avances sobre la utilización de los virus y otros como medio para dañar, acceder y alterar los datos programaciones y otras informaciones es que a finales del siglo XX en 1995 se reportaron en diversas ciudades del mundo la aparición de una nueva familia de virus que no solamente infectaban documentos, sino que a su vez, sin ser archivos ejecutables podían auto-copiarse infectando a otros documentos.

Los llamados **macro virus** tan sólo infectaban a los archivos de MS-Word, posteriormente apareció una especie que atacaba al Ami Pro, ambos procesadores de textos.

En 1997 se disemina a través de Internet el primer macro virus que infecta hojas de cálculo de MS-Excel, denominado Laroux, y en 1998 surge otra especie de esta misma familia de virus que ataca a los archivos de bases de datos de MS-Access. Para mayor información sírvanse revisar la opción Macro Virus, en este mismo módulo.

Tras ese avance los virus eran un medio especializado para dañar a las programaciones archivos datos y otros como ser en el caso de los **virus anexados** que se propagaron por el internet mediante (adjuntos) a mensajes de correo, como el **Melisa** o el macro virus **Melissa**. Ese mismo año fue difundido a través de Internet el peligroso **CIH** y el **ExploreZip**, entre otros muchos más.

A fines de Noviembre de este mismo año apareció el **BubbleBoy**, primer virus que infecta los sistemas con tan sólo leer el mensaje de correo, el mismo que se muestra

en formato **HTML**. En Junio del 2000 se reportó el **VBS/Stages.SHS**, primer virus oculto dentro del Shell de la extensión **.SHS**.

En la historia de los más destacados personajes delincuenciales de la informática se encuentran personajes destacados por su actividad delincuencial entre ellos uno que paso a ser empresario sobre la protección y elaboración de programas o software como ser.

Jhon Draper.- Llamado también "Capitan Crunch" [Captain Crunch, en inglés], descubrió que la sorpresa que venía dentro cereal Captain Crunch dublicaba la intensidad de la frecuencia de 2600 hz. de una línea de WATS, permitiéndole hacer llamadas telefónicas gratis. (12)

Bill Gates y Paul Allen.- en el tiempo en el que estos dos hombres de Washington, eran aprendices, se dedicaban a hackear software. Llegaron a ser grandes programadores, y se convirtieron en creadores del imperio de Sistemas Operativos líder. Sus "éxitos" fueron el SO MS-DOS, Windows, Windows 95/NT. (12)

Kevin Mitnick, llegó a ser considerado uno de los mayores hackers de la historia; su carrera como hacker tuvo inicios en 1980, cuando rompió la seguridad de su colegio, "solo para mirar", no para alterar sus notas. Es considerado como infractor de la Ley desde que entraron físicamente a la compañía COSMOS (Computer Systems for Mainframe Operations), que era una base de datos utilizada por la mayor parte de las compañías telefónicas norteamericanas utilizada para controlar el registro de las llamadas.

Al ingresar él, y sus dos amigos, obtuvieron claves de seguridad, combinación de las puertas de acceso de varias sucursales y manuales del sistema COSMOS. Él fue considerado como una de las mayores pesadillas del Departamento de Justicia de los Estados Unidos y como hacker más peligroso y escurridizo del mundo por el FBI**.** (13)

12. "Delitosinformaticos.com" paginaweb

Ian Murphy, también llamado “Captain Zap”, a sus 23 años de edad, logró entrar a los sistemas de la Casa Blanca, el Pentágono, BellSouth Corp. TRW, y deliberadamente dejó su currículum. El consideraba que “violar accesos le resultaba divertido”. (13)

En la historia sobre los delincuentes informáticos a esta clase de delincuentes se los conocen como hackers el concepto actual de hacker en los medios se ha extendido del súper espía de alta tecnología, que logra infiltrarse en los sistemas de seguridad capaz de ingresar a sistemas muy controlados como los del Pentágono, al adolescente antisocial que busca entretenimiento.

La realidad, sin embargo, es que los hackers constituyen un grupo muy diverso, un grupo culpado simultáneamente de causar pérdidas por billones de dólares y al mismo tiempo se le atribuye el desarrollo de la World Wide Web (WWW) y de fundar las compañías más importantes de tecnología.

Estos son los hackers más famosos de toda la historia: (14)
Sven Jaschan. Creó dos de los virus informáticos más letales de los últimos: Netsky y Sasser. A estos gusanos se les responsabilizó del 70% de malware que se propagaron por todo Internet en ese momento. Se le condenó a tres años de libertad condicional por este crímen. Posteriormente fue contratado por una empresa de seguridad informática.

David L. Smith. Fue el autor del macro virus Melissa, que atacó a miles de usuarios y empresas el 26 de Marzo de 1999, esparciendolo como un documento de MS-Word infectado en un grupo de noticias de Usenet, que conformaban una lista de interés sobre páginas web porno. David L. Smith, programador de computadoras, alegó su inocencia y manifestó que creó el virus en su departamento de Aberdeen en memoria de una bailarina Topless, del estado de Florida, de la cual se había enamorado, pero sus relaciones sentimentales quedaron frustradas.

13. “Delitosinformaticos.com” paginaweb
14. “Cyberdelito.com” pagina web

Jonathan James. Las más importantes intrusiones de James tuvieron como objetivo organizaciones de alto grado. Él instaló un backdoor en un servidor de la Agencia de Reducción de Amenazas de la Defensa. Esta es una agencia del Departamento de Defensa encargado de reducir las amenazas a los Estados Unidos y sus aliados de armas nucleares, biológicas, químicas, convencionales y especiales. El backdoor que el creó le permitió ver emails de asuntos delicados y capturar los nombres de usuario y clave de los empleados. James también crackeó las computadoras de la NASA robando software por un valor aproximado de 1.7 millones de dólarees. Segun el Departamento de Justicia, "entre el software robado se encontraba un programa utilizado para controlar el medio ambiente -temperatura y humedad- de la Estación Espacial Internacional". La NASA se vio forzada a tener que paralizar 21 días sus computadoras y ocasionó pérdidas calculadas en 41 millones de dólares.

Robert Tappan Morris. Es hijo de un científico de la Agencia Nacional de Seguridad, y conocido como el creador del Gusano Morris, el primer gusano desencadenado en Internet. Morris escribió el código del gusano cuando era estudiante de Cornell University. Su intención era usarlo para ver que tan largo era Internet, pero el gusano se replicaba excesivamente, haciendo las computadoras demasiado lentas. La noticia se fue amplificando gracias a los intereses informativos. Se habló de cientos de millones de dólares de pérdidas y de un 10% de Internet colapsado, Morris fue juzgado en enero de 1990 y el día 22 de ese mes fue declarado culpable según la Ley de Fraude y Delitos Informáticos de 1986, aunque afortunadamente el juez atenuó las penas por no encontrar "fraude y engaño" en la actuación del joven programador. Tras el fracaso de la apelación fue confirmada su condena a 3 años en libertad condicional, una multa de 10.000 dólares y 400 horas de trabajo de servicio a la comunidad. Actualmente trabaja como profesor de ciencias de la computación en el MIT y en el laboratorio de Inteligencia Artificial.

Michael Cale. Bajo el pseudónimo de MafiaBoy, se escondía este niño prodigio, que con 15 años lanzó uno de los mayores ataques a distintas empresas a través de la red. Habiéndose asegurado en primer lugar el control de 75 equipos, lanzó sus ataques del 6 al 14 de febrero de 2000 a compañías como Dell, eBay, o la CNN, colapsando sus sistemas y provocándoles unas pérdidas estimadas en 1.200 millones de dólares. En

este caso, fue el ego del propio Michael el que le delató, ya que se dedicó a proclamar sus logros entre sus compañeros de colegio y en distintas salas de chat. A pesar de todo, y debido a su edad, Michel fue condenado a ocho meses de libertad vigilada, se le restringió el acceso a Internet y se le impuso una multa de escaso importe.

Loyd Blankenship. También conocido como “El Mentor”, era miembro del grupo hacker Legion of Doom, que se enfrentaba a Masters of Deception. Es el autor del manifiesto hacker “La conciencia de un hacker” que escribió en prisión luego de ser detenido en 1986 y del código para el juego de rol “Ciberpunk”, por lo tanto, gran parte de su fama apunta también a su vocación de escritor. Sus ideas inspiraron la película "Hackers", donde actuó Angelina Jolie. Actualmente es programador de Videojuegos.

Stephen Wozniak. Famoso por ser el co-fundador de Apple, Stephen "Woz" su carrera de hacker "sombrero blanco" (dedicados a mejorar la seguridad) con su "phone phreaking" (realizar actividades no permitidas con sistemas telefónicos). Mientras estudiaba en la Universidad de California realizó varios dispositivos para sus amigos llamados *cajas azules*, que permitían realizar llamadas de larga distancia de manera gratuita. Se cuenta que Wozniak incluso, llegó a llamar al Papa. Abandonó la Universidad al comenzar a trabajar en un proyecto sobre un ordenador. Formó Apple con su amigo Steve Jobs, y otros que se conocen en su medio.

Adrian Lamo. Originario de Boston, es conocido en el mundo informático como “El hacker vagabundo” por realizar todos sus ataques desde cibercafés y bibliotecas. Su trabajo más famoso fue la inclusión de su nombre en la lista de expertos de New York Times y penetrar la red de Microsoft. También adquirió fama por tratar de identificar fallas de seguridad en las redes informáticas de Fortune 500 y, a continuación, comunicarles esas fallas encontradas.

Kevin Poulson. Poulson logró fama en 1990 por hackear las líneas telefónicas de la radio KIIS-FM de Los Angeles, para asegurarse la llamada número 102 y ganar así un Porsche 944 S2. Fue apresado tras atacar una base de datos del FBI en 1991. Hoy es periodista y editor de la revista Wired y en 2006 ayudó a identificar a 744 abusadores de niños vía MySpace.

Kevin Mitnick. Es, probablemente el hacker más famoso de las últimas generaciones. Mitnick fue descrito por el Departamento de Justicia de los Estados Unidos como "el criminal informático más buscado de la historia de los EEUU". Autodenominado *hacker poster boy*, ha hackeado los sitemas informáticos de varias de las compañías de telecomunicaciones más importantes del mundo como Nokia o Motorola, entre otras. (15)

Después de una intensa búsqueda por parte del FBI, Mitnick fue arrestado en el año 1995, cumpliendo cinco años de prisión. Al ser puesto en libertad en el año 2000, fundó su propia empresa de seguridad informática. El nunca se ha referido a sus actividades como *hacking*, sino como *ingeniería social*. (15)

3. LOS DELITOS INFORMATICOS EN BOLIVIA

En Bolivia al ser un país que se encuentra en vías de desarrollo y este se encuentra en pleno avance informático, con el desarrollo y acoplamientos de nuevos sistemas informáticos emergentes en el mundo, Bolivia debe adelantarse a los hechos a ser cometidos por los delincuentes mediante herramientas informáticas con la finalidad de afectar a los sistemas y mecanismos informáticos.

Si bien se tipifico el delito informático en Bolivia, en un capitulo especial en el código penal solo se tipifico dos delitos de las varias clases de delitos informáticos existentes.

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

15. “Cyberdelito.com” pagina web

Entre el año 2003 y 2007, la fuerza anticrimen recibió 187 denuncias de manipulación informática y de alteración y acceso y uso indebido de datos en toda Bolivia, pero se desconoce si alguna de ellas fue resuelta.

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

El jefe de la división de lucha contra los delitos informáticos de la FELCC de La Paz Capitán Edson Claure, informo que los primeros nueve meses de la gestión de 2011 se registraron en todo el pis 50 denuncias de manipulación informática, pero ninguno de alteración y uso indebido de datos.

Sin embargo, la Dirección Nacional de Laboratorio de la Policía, que investiga esos casos, sólo da cuenta de 36 procesos que están en etapa de investigación, pero de éstos ninguno fue resuelto. Ni esta última entidad ni la División de Delitos Informáticos saben por qué sólo 36 de las 50 denuncias recibidas están siendo indagadas.

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

Un ejemplo de manipulación informática es el phishing (“pesca de claves”), técnica de estafa electrónica en la que un informático o conocedor de internet ingresa en la página de una entidad financiera, de la que selecciona a su víctima, y mediante correo electrónico le envía un portal falso del banco en el que pide que ingrese sus datos

personales y su PIN (clave secreta) con el pretexto de actualizar la base de datos de los clientes. Una vez que el delincuente cibernético accede a la contraseña, procede a vaciar la cuenta del cliente del banco.

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

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

Según el diario la razón los delitos informáticos se propagaron con mayor denotación a partir del año 2002 al 2011, en esa data los juicios por delitos informáticos crecieron en un 890% de ocho a 79, de los cuales 62 están referidos a manipulación informática y 17, a la alteración, acceso y uso indebido de datos informáticos. Aparte, en esa década, los juzgados paceños recibieron 228 causas referidas al primer delito y 15 del segundo. Asimismo, en los cuatro meses que van de este año, ya se ventilan 29 causas: 27 que incumben al artículo 363 bis y dos al artículo 363 ter del Código Penal.

Según la estadística proporcionada al diario la Razón por parte de la fuerza especial de lucha contra el crimen (FELCC) y el Consejo de la Magistratura de La Paz así lo confirman. La entidad policial informa que el año pasado recibió 574 denuncias referidas a manipulación informática en ocho departamentos, menos en Oruro. Doce más (casi 2%) que las 562 que llegaron a sus oficinas en 2010.

El director nacional de esta repartición, coronel Jorge Toro, opina que el leve incremento demuestra que, cada día, los delincuentes se apoyan más en las herramientas de la tecnología para realizar actos reñidos con la ley. "Primero se comete el delito (informático), que casi siempre es algo novedoso (para nuestros

peritos), mientras la Policía y el Ministerio Público no están debidamente actualizados en el tema y no cuentan con los medios necesarios para combatirlo".

Es que así en el año 2011, el mayor número de casos se registró en Santa Cruz, con un total de 486; seguido por La Paz, donde se presentaron 69. Lo llamativo es que ambas regiones concentran más del 95% de éstos, o sea, 555 de los 574. Posteriormente se ubican Cochabamba, con ocho; Chuquisaca, con cuatro; Tarija, con tres; Beni, con dos, y Pando y Potosí con uno cada uno. Aparte, desde enero hasta marzo de este año ya se suman 47 denuncias en las dependencias policiales.

El fiscal de materia Jorge Álvarez comenta que muchos otros hechos relacionados con estos delitos no llegan a ser investigados por las autoridades porque no son denunciados por las víctimas, por desconfianza en el sistema judicial o porque las sanciones son casi simbólicas. "Tiene que ver más con un cambio en la política criminal por parte del Estado, que debería dar hasta 30 años de cárcel y no cinco como en estos casos". El coronel Toro adiciona que otra razón es el desconocimiento de los damnificados de que hay peritos policiales y del Ministerio Público que averigua estos casos, por lo que recurren a empresas o investigadores privados que cobran por sus servicios.

Por ejemplo, el Instituto de Investigaciones Forenses de la Fiscalía cuenta con equipos para la implementación de la informática forense; su labor empezó hace una década. Pero, desde hace dos años, ante la saturación de trabajo en esta entidad, ocho expertos en el rubro se instalaron en el Instituto de Investigaciones Técnico Científicas de la Universidad Policial, que se organizó sobre la base del exlaboratorio de la Policía Técnica Científica, en el barrio de Següencoma, de la zona Sur de la ciudad de La Paz.

En otros tiempos, este ambiente se dedicaba a indagar exclusivamente hechos delictivos mediante el estudio de las huellas dejadas en la escena del crimen, la balística, la química legal, la toxicología, la accidento logia y otro tipo de pericias. Actualmente, su abanico de acción se ha extendido a los delitos informáticos, aparte de pesquisas forenses y de genética aplicativa, explica el jefe de esta dependencia, el capitán William Llanos, quien es titulado en Ingeniería de Sistemas.

El plantel a su cargo recibe las pruebas remitidas desde la FELCC y la Fiscalía. En cuanto a los delitos informáticos, analiza medios electrónicos y ópticos para el almacenamiento de información, sean discos duros de computadoras, CD, DVD, celulares; busca portales de pornografía infantil y realiza patrullajes cibernéticos. "Rastreamos páginas de Facebook o sospechosas que intentan reclutar potenciales víctimas para la prostitución. Así dimos con una página en la urbe de Cochabamba", indica.

Los especialistas tratan de involucrarse con el mundo de las redes dudosas del ciberespacio, hacer amistad y socializar con quienes las operan, para atraparlos, posteriormente, con ayuda de los agentes de la FELCC. "Primeramente creamos un perfil que sigue la corriente al delincuente, llegamos a ser parte de sus contactos de confianza y, luego, empezamos a hacer un operativo más complejo que pasa de lo cibernético a lo físico", que termina en la detención. Y operan de similar modo cuando van tras las pistas de ciberacosadores o chantajistas informáticos.

Generalmente les llega ordenadores que fueron usados para cometer un delito; su dictamen es considerado como parte del cúmulo de pruebas en los juicios. Para los análisis, añade Llanos, precisan conocer la parte tecnológica y su terminología, y también la parte legal. No obstante, a veces, las normas limitan su accionar. Por ejemplo, la Ley de Telecomunicaciones reconoce desde este año la inviolabilidad de los documentos o archivos particulares que están en un ordenador, lo cual está avalado por la Constitución Política, comenta el investigador.

En el ámbito privado, sobresale la empresa Yanapti, inmersa en la averiguación de delitos informáticos, con un laboratorio forense que se halla provisto con equipos y programas especializados que no contaminan la evidencia digital, y que en la mayoría de los casos accede a la información que los criminales depositaron e intentan borrar de sus computadoras, informa Claudia Araujo, abogada y experta en seguridad informática de esta compañía. Es que así El jefe del Departamento Académico del Instituto Nacional de Investigaciones Técnico-Científicas de la Universidad Policial, capitán William Llanos, recomienda estar alerta ante este tipo de casos.

El Instituto Nacional de Investigaciones Técnico-Científicas de la Universidad Policial ya atendió 40 denuncias de delitos informáticos en todo el país, de los cuales el 90 por ciento ya fue esclarecido.

La información fue proporcionada por el jefe del Departamento Académico y Perito Informático de esta institución, capitán William Llanos Torrico, en una entrevista brindada al programa Alto Impacto de la Red Policial.

A partir de enero a la fecha, se ha realizado 40 pericias sobre informática forense y delitos informáticos, que vienen muy relacionados, de los cuáles el 90 por ciento fue esclarecido, y en este caso la Fiscalía y el Juez ya pueden imputar el delito.

Esta tipificación de delito informático, explicó, se refiere a un acto antijurídico que para su comisión emplea un sistema automático de procesamiento o transmisión de datos, siendo la computadora el equipo más común para esto. Según el especialista hay muchas formas de cometer delitos informáticos, varios de estos son realizados por personas que tienen bastante conocimiento tecnológico sobre la materia; sin embargo, hay otras actividades delincuenciales que caen dentro de este delito, que pueden ser cometidos por personas con escasos conocimientos de computación.

“Hay casos de diferente naturaleza, desde amenazas por Internet, algunos tipos de fraude y ahora estamos trabajando casos mucho más grandes de ataque a los bancos”, afirmó el capitán Llanos.

El capitán Llanos sostiene que gente con más conocimiento en informática crea unas aplicaciones, una base de datos personales, pero por debajo crea “puertas falsas” por donde esta persona —que ha diseñado el sistema— puede ingresar sin ningún tipo de restricciones a otras cuentas.

El delito conocido como el “redondeo”, según Llanos, es cometido por gente que tiene conocimiento, que realiza un programa en una entidad financiera y todos los centavos de las cuentas los va transfiriendo a una particular. Obviamente, cuando los montos

son grandes, las personas no se dan cuenta, pero que en numerosas transacciones se logra reunir bastante dinero.

Otro delito son las bombas lógicas o programadores descontentos, que se relacionan con empleados que fueron echados de sus trabajos y dejan funcionando una aplicación bajo ciertas características para que en un determinado tiempo el software comience a fallar, a colgarse y explote el sistema al crear una rutina que no había sido programada, todo con la finalidad de que la institución vuelva a contratar los servicios de esta persona.

Asimismo, existe el pinchado de líneas de red, que, según Llanos, se asemeja a la conexión de un derivado a una línea telefónica. “Lo propio se puede hacer con una conexión de red donde la información transita por todo lado, nosotros podríamos capturar toda la información, investigar principalmente los nombres y las claves o contraseñas de usuarios para después hacernos pasar por esa persona”, explicó el perito.

El experto señaló que también existen delitos informáticos cometidos por accidente. “El comúnmente error de dedo podría ser uno de ellos, se trata de la introducción de datos falsos. Por ejemplo al realizar una transacción y estar transcribiendo ciertas cantidades nos olvidamos poner un cero voluntariamente y como el instrumento es una computadora entonces se cae en este tipo de delitos”. “También está la navegación sobre el hombro que en nuestro medio no está legislado. Es frecuente y sucede cuando alguien está tratando de mirar qué es lo que está taipeando el de adelante para robarle su nombre de usuario y contraseña, algo muy común que se está dando en la fila de cajeros automáticos. Estos son sólo algunos de los muchos delitos informáticos penados por ley y que además sirven como evidencia legal en juicios”, expresó. (16)

16. “Larazon.com” pagina web

4. AVANCES HISTORICOS EN LA LUCHA CONTRA LOS DELITO INFORMATICO EN EL MUNDO.

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

Se considera que no existe una definición formal y universal de delito informático pero se han formulado conceptos respondiendo a realidades nacionales concretas: "no es labor fácil dar un concepto sobre delitos informáticos, en razón de que su misma denominación alude a una situación muy especial, ya que para hablar de "delitos" en el sentido de acciones típicas, es decir tipificadas o contempladas en textos jurídicos penales, se requiere que la expresión "delitos informáticos" esté consignada en los códigos penales, lo cual en nuestro país, al igual que en otros muchos no han sido objeto de tipificación aún." (17)

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

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

17. **www.unodc.org. Pagina web**

Se entiende Delito como: "acción penada por las leyes por realizarse en perjuicio de algo o alguien, o por ser contraria a lo establecido por aquéllas".
Finalmente la OCDE publicó un estudio sobre delitos informáticos y el análisis de la normativa jurídica en donde se reseñan las normas legislativas vigentes y se define **Delito Informático** como "cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático de datos y/o transmisiones de datos."

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

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

En el año 2000 se realizo el Decimo Congreso de las Naciones Unidas sobre la prevención del delito y tratamiento del delincuente realizado en Viena, del 10 a 17 de abril de 2000 donde se trato sobre Delitos relacionados con las redes informáticas y se quedo de acuerdo sobre cooperación internacional entre las autoridades nacionales encargadas de aplicar la ley donde se debatió que dada la dimensión internacional de las redes electrónicas, es cada vez menos probable que todos los elementos de un delito cibernético se limiten a un solo territorio nacional. En las investigaciones, las autoridades encargadas de aplicar la ley en los diversos Estados necesitarán cooperar a nivel oficial, utilizando mecanismos de asistencia judicial recíproca y estructuras como la Organización Internacional de Policía Criminal (Interpol), y también a nivel extraoficial, proporcionando directamente a las autoridades de otro Estado información de posible utilidad. En general, la cooperación policial internacional presupone el consentimiento de las autoridades de los Estados intervinientes. Según sean las relaciones de los Estados, la naturaleza de la información en cuestión -u otros factores- dicha cooperación también puede requerir un acuerdo internacional en el que se estipulen las autoridades y los procedimientos pertinentes.

Entre los elementos de cooperación práctica examinados cabe señalar:

a) Medidas para garantizar la disponibilidad de personal capacitado en número suficiente provisto de la capacidad técnica adecuada, mediante la cooperación en el equipamiento y la capacitación del personal encargado de aplicar la ley;

b) Cooperación en la elaboración de normas forenses para la recuperación y la autenticación de datos electrónicos.(18)

5. ESTADÍSTICAS SOBRE DELITOS INFORMÁTICOS.

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

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

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

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

18. “www.unodc.org” pagina web

Violaciones a la seguridad informática.

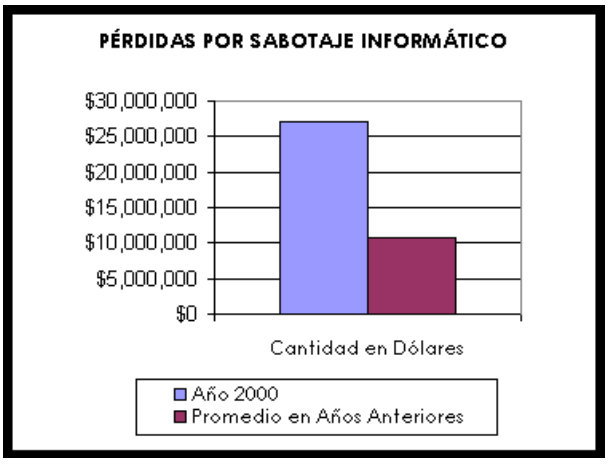
Respuestas	PORCENTAJE (%)
No reportaron Violaciones de Seguridad	10%
 Reportaron Violaciones de Seguridad	90%

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

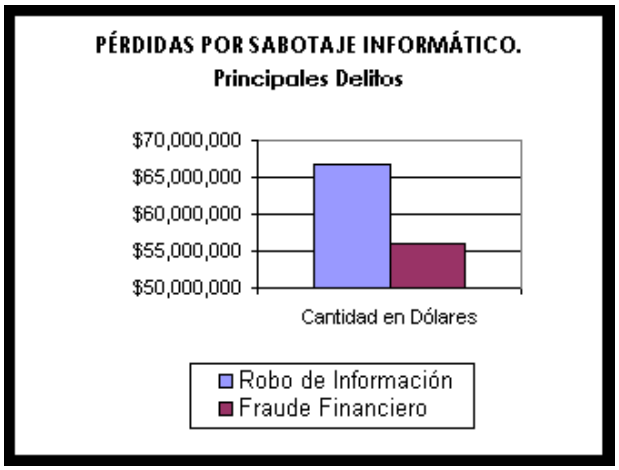
70% reportaron una variedad de serias violaciones de seguridad de las computadoras, y que el más común de estas violaciones son los virus de computadoras, robo de computadoras portátiles o abusos por parte de los empleados -- por ejemplo, robo de información, fraude financiero, penetración del sistema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

Pérdidas Financieras.

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

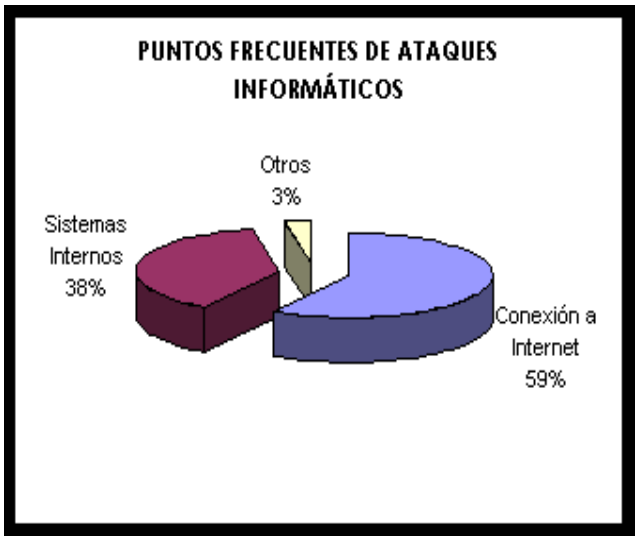


6I encuestados cuantificaron pérdidas debido al sabotaje de datos o redes para un total de $27, 148,000. Las pérdidas financieras totales debido al sabotaje durante los años anteriores combinados ascendido a sólo $10, 848,850.



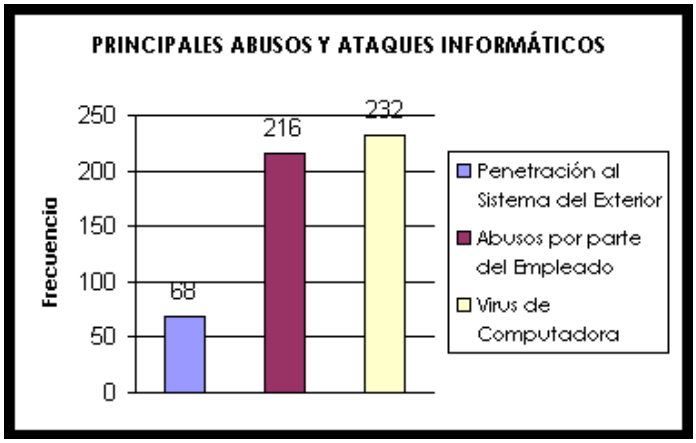
Como en años anteriores, las pérdidas financieras más serias, ocurrieron a través de robo de información (66 encuestados reportaron $66, 708,000) y el fraude financiero (53 encuestados informaron $55, 996,000).

Los resultados del estudio ilustran que esa amenaza del crimen por computadoras a las grandes corporaciones y agencias del gobierno viene de ambos lados dentro y fuera de sus perímetros electrónicos, confirmando la tendencia en años anteriores.
Accesos no autorizados.



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

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



Los encuestados detectaron una amplia gama a de ataques y abusos. Aquí están algunos otros ejemplos:
25% de encuestados descubrieron penetración al sistema del exterior.
79% descubrieron el abuso del empleado por acceso de Internet (por ejemplo, transmitiendo pornografía o pirateó de software, o uso inapropiado de sistemas de correo electrónico).
85% descubrieron virus de computadoras.
Comercio electrónico.

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

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

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

sofisticadas, y lo más importante, por personal adecuado y entrenando, practicantes de seguridad de información en el sector privado y en el gobierno.
Otras estadísticas:

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

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

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

- En Singapur El número de delitos cibernéticos detectados en el primer semestre del 2000, en el que se han recibido 127 denuncias, alcanza ya un 68 por ciento del total del año pasado, la policía de Singapur prevé un aumento este año en los delitos por Internet de un 38% con respecto a 1999.

- En relación con Internet y la informática, la policía de Singapur estableció en diciembre de 1999 una oficina para investigar las violaciones de los derechos

de propiedad y ya ha confiscado copias piratas por valor de 9,4 millones de dólares.

- En El Salvador, existe más de un 75% de computadoras que no cuentan con licencias que amparen los programas (software) que utilizan. Esta proporción tan alta ha ocacionado que organismos Internacionales reacciones ante este tipo de delitos tal es el caso de BSA (Bussines Software Alliance). (19)

19. "www.rincondelvago.com." Estadisticascyeberdelincuenciales. Pagina web

CAPITULO II.-
MARCO TEORICO Y CONCEPTUAL

1. TEORIAS Y CONCEPTOS DE DELITO INFORMATICO.

.- Antes de entrar a hablar de lo que son los delitos informáticos definiremos lo que es la informática como ciencia ya que esta ciencia la utilizan los delincuentes para realizar los delitos, la informática es la ciencia que estudia el tratamiento automático de la información.

Cuando se habla de tratamiento automático de la información decimos que es aquella que se realiza mediante los llamados ordenadores o computadores, no se puede llamar informática el manejar un procesador de textos, este se debe considerar como ofimática, considerándose informática a la creación de programas por las cuales se pueda manejar textos e información textual. (20)

La informática como ciencia estudia lo que los programas son capaces de hacer esta se llama la teoría de la computabilidad, aparte de la eficiencia de sus algoritmos que se emplean así como de la organización y almacenamiento de datos y de la comunicación entre programas, humanos y máquinas (interfaces de usuario, lenguajes de programación, procesadores de lenguajes...), entre otras cosas la importancia de la informática en nuestros días se debe a que está presente en nuestras vidas de forma habitual y de ella depende el avance de las nuevas tecnologías. (20)

En la informática, la computadora como medio por el cual se puede realizar actividades ilícitas fue creada con la finalidad de ayudar es que asir Renato Borruso nos dice que “en verdad, se trata de una maquina que, concebida y utilizada originariamente como simple calculadora, se a descubierto que poco a poco puede ser usada para muchas otras funciones diversas:

---

20. **MAURIE** Claude Mayo “Informática Jurídica” pág. 48

Como ordenador de datos introducidos desordenadamente, como elaborador de ellas mediante distintas operaciones sucesivas, como memorizador, codificador de datos y decodificador, como lector e impresor, como ejecutor de pagos, como ensamblador de partes de maquinas y en general", al hablar de una computadora que puede manejar toda clase de accesorios con capacidad de instrucción mecánica también esta puede ser corrompida para realizar actos ilícitos o utilizar a la maquina con fines ilícitos.

Vario autores definen delito informático como una conducta ilícita a causar un daño a la información, otros autores definen que delito informático tiene como finalidad no solo afecta a la información si no que también el patrimonio real siendo que el medio informático solo es el pasó a cometer estos delitos de orden patrimonial.

Siendo así que el delito informático puede comprender tanto aquellas conductas que valiéndose de medios informáticos lesionan otros intereses jurídicamente protegidos como la intimidad, el patrimonio económico, la fe pública, la seguridad y como aquellas que recaen sobre herramientas informáticas propiamente tales como programas, ordenadores se puede comprender que al hablar que el delito informático puede comprender tanto aquellas conductas que se valen de medios informáticos para lesionar otros intereses jurídicamente protegidos, en este caso es aceptar el uso de la computadora como instrumento delictivo, no importa aplicar analogía de ninguna especie, sino adaptar la figura penal a los avances de la tecnología, es decir que si bien el legislador puso un limite especifico a la interpretación del tipo penal de los delitos calificados viendo muchas veces que en su estructura de la tipificación del delito no permita el empleo de ese medio, sin embargo, la enunciación genérica de una serie de medios dentro de los cuales tenga cabida el uso del ordenador o se permita expresamente el uso de cualquier medio, no otorga al delito el carácter de "informático", sin perjuicio de que se hable de un delito relacionado con la informática.

Al estudiar lo que es el delito informático se tiene que denotar que la informática es objeto del delito, hay que diferenciar el "*hardware"* del *"software",* señalando que al primero son generalmente aplicables las normas tradicionales ya que no constituye una nueva forma de propiedad, siendo diferente en el caso del software y de la información almacenada en una computadora, pues estos constituyen formas intangibles y no

siempre tienen cabida en las instituciones tradicionales del Derecho, hay que señalar que en las situaciones delictuosas en las que los materiales informáticos no tienen otra función que la de simple objeto de uso delictivo, no se figura como un delito informático, ya que al tipificarse un delito informático lo que se busca es tutelar el contenido de lo que es la informática, que estudia lo que los programas los mismos que son capaces de hacer (teoría de la computabilidad), de la eficiencia de los algoritmos que se emplean (complejidad y algorítmica), de la organización y almacenamiento de datos (estructuras de datos, bases de datos) y de la comunicación entre programas, humanos y máquinas (interfaces de usuario, lenguajes de programación, procesadores de lenguajes...), entre otras cosas, a lo cual la legislación penal si bien tipifica lo que es delito informático no lo realiza en si totalidad.

Pude considerarse como delito informático la reproducción ilícita de obras de software, hay casos en los que el ordenador se usa como instrumento y es a la vez el objeto sobre el cual recae la acción delictiva, como es la destrucción de datos mediante un programa de virus informático, según teorías delito informático es aquella conducta ilícita realizada mediante un medio informático por la cual se puede manipular información y alterar destruir los sistemas operativos causando daño a otras personas y maquinas de procesamiento de datos, siendo prudente analizar los diferentes preceptos sobre esta clase de delitos.

Tomando en cuenta los conceptos de autores y expertos sobre Derecho Informático, delito informático lo definen como:

Para **Nidia Callegari** el delito informático es "aquel que se da con la ayuda de la informática o de técnicas anexas".

Al hablar de delito informático de la abogada Nidia Callegari nos habla que es aquel que se realiza con la ayuda de la informática o técnicas anexas, al hablara de informática se habla de una rama muy extensa ya que la informática es aquella que tiene el uso y desarrollo de la tecnología a lo cual también Nidia Callegari nos habla de técnicas anexas pudiendo dar por analogía el uso de diferentes clases de medios técnicos informáticos por los cuales se podría delinquir.

Rafael Fernández Calvo define al delito informático como "la realización de una acción que, reuniendo las características que delimitan el concepto de delito, se ha llevado a cabo utilizando un elemento informático o telemático contra los derechos y libertades de los ciudadanos definidos en el título 1 de la **Constitución Española.** (21)

El concepto del Dr. Rafael Fernández Calvo es relacionado con la normativa de su país siendo el mismo normativista define el uso de la computadora o medios informáticos como medios para dañar los derechos y libertades de los ciudadanos por parte del delincuente a lo cual se atentaría con lo dispuesto por la Constitución Política de su país.

La penalista María de la Luz Lima dice que el "delito electrónico " en un sentido amplio es cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en un sentido estricto, el delito informático, es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin". (21)

María de la Luz Lima al explicar que es una conducta criminal que se basa en el uso de la tecnología electrónica ya sea como métodos o medios informáticos a lo cual la conducta criminal es expresada mediante la tecnología para dañar a otras personas siendo una nueva forma de delito ya que no solo afectara a la persona si no al medio por el cual se realizara.

El delito informático para Davara Rodríguez es “La realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software”.

---

21. **RENE** de Sola Quinteros. “Delitos Informáticos” pág. 15-18

Interpretando Davara Rodríguez delito informático no solo consta de una parte material hardware si no de un elemento lógico que es el software tomando una acción mixta reconociendo como delito informático aquella que solo atenta contra la parte lógica (software) si que afecta la parte material y que también delito informático no solo seria el daño a estos elementos que contienen guardado información si no que también es delito informático la utilización de los elementos informáticos para cometer los delitos comunes y causar daño a otros objetos o bienes personales.

Para expertos de la OCDE, definió, en 1983, el delito informático como "cualquier conducta ilegal, no ética, o no autorizada que involucra el procesamiento automático de datos y/o la transmisión de datos". Esta definición amplia, se ha considerado como ventajosa, ya que abarca no sólo el delito informático sino toda la delincuencia relacionada con la informática y las nuevas tecnologías, siendo futurista ya que si bien los delitos informáticos tiene que tener un orden proteccionista sobre la información y los elementos por las cuales se los contienen este concepto no solo define que la esencia es la protección de los elementos que en los cuales se encuentra la información si no que es la información misma viendo no solamente al presente si no al futuro viendo la necesidad de la protección de nuevas formas por las cuales se manejara..

Para René de Sola se podría definir el delito informático como toda (acción u omisión) culpable realizada por un ser humano, que cause un perjuicio a personas sin que cause un perjuicio a personas sin que necesariamente se beneficie el autor o que, por el contrario, produzca un beneficio ilícito a su autor aunque no perjudique de forma directa o indirecta a la víctima, tipificado por la Ley, que se realiza en el entorno informático y está sancionado con una pena. (22)

22. **RENE** de Sola Quinteros. "Delitos Informáticos" pág. 15-18

René de Sola nos habla de que el elemento esencial para la realización de este delito es el humano el cual busca el perjuicio a una persona o varias personas sin que necesariamente se beneficie el si nos beneficiando a otra no perjudicando directamente a la victima ya que el medio por el cual se lo realiza es mediante un elemento informático y que este se encuentra tipificado en la normativa penal, René de Sola ve el delito informático como un medio por el cual se cometen otros delitos teniendo una visión de delito informático como un medio para llegar a cometer otros delitos por la manipulación informática de datos.

El autor mexicano Julio Téllez Valdez señala que los delitos informáticos son “actitudes ilícitas en que se tienen a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin (concepto típico)”. Al hablar Julio Téllez sobre el delito informático dice que es la conducta ilícita del ser humano el cual utiliza la computadora como instrumento detallando como una conducta típica. Antijurídica y culpable, al cual se ve que la definición va mas a cubrir la acción del hombre por el medio a realizar la conducta antijurídica.

Cabe destacar que **Julio Téllez Valdez** señala que "no es labor fácil dar un concepto sobre delitos informáticos, en razón de que su misma denominación alude a una situación muy especial, ya que para hablar de "delitos" en el sentido de acciones típicas, es decir tipificadas o contempladas en textos jurídicos penales, se requiere que la expresión "delitos informáticos" esté consignada en los códigos penales, lo cual en nuestro país, al igual que en otros muchos no ha sido objeto de tipificación aún

Por su parte, el tratadista penal italiano Carlos Sarzana, sostiene que los delitos informáticos son “cualquier comportamiento criminal en que la computadora está involucrada como material, objeto o mero símbolo.” Al respecto este tratadista dice que el delito informático es cualquier comportamiento criminal relacionado con la utilización de la computadora como objeto material para esto si se debe decir que si muy bien especifico el tratadista al decir el medio por el cual se comete el delito es la computadora pero no hay implícito el hecho de la información como bien protegido,

dejando en analogía que este es el bien jurídico protegido o es un medio la información por el cual se puede cometer el delito.

Santiago de acuario nos dice para definir delito informático, ay que poder delimitar el contenido de este fenómeno, optamos primero por una **DENOMINACIÓN GENÉRICA, FLEXIBLE**, acerca del mismo como sería delincuencia informática o criminalidad informática. Sin circunscribirnos así a términos rígidos, como sería por ejemplo delitos informáticos, en tal razón diremos que "**DELINCUENCIA INFORMÁTICA ES TODO ACTO O CONDUCTA ILÍCITA E ILEGAL QUE PUEDA SER CONSIDERADA COMO CRIMINAL, DIRIGIDA A ALTERAR, SOCAVAR, DESTRUIR, O MANIPULAR, CUALQUIER SISTEMA INFORMÁTICO O ALGUNA DE SUS PARTES COMPONENTES, QUE TENGA COMO FINALIDAD CAUSAR UNA LESIÓN O PONER EN PELIGRO UN BIEN JURÍDICO CUALQUIERA**"

Luego de las definiciones anteriormente señaladas es importante hacer algunas consideraciones sobre las mismas. Cabe destacar sin establecer una regla genérica, se puede inferir que la computadora constituye un medio para cometer un delito o el objeto sobre el cual recae el mismo, se convierte en el primer supuesto de este tipo de conductas antijurídica. Es por eso, que debe entenderse que el aceptar el uso de la computadora como instrumento delictivo no significa aplicar analogía de ninguna especie, sino adaptar la figura penal a los avances de la técnica. Y ello resulta razonable pues el legislador no puede prever la infinidad de medios a través de los cuales es posible afectar un determinado bien jurídico penalmente protegido.

El límite a esta interpretación del tipo penal está dado por los supuestos en que el legislador puede prever un medio determinado, o en los casos en que la estructura del delito no permita el empleo de ese medio. Pero sin perjuicio de que se enuncien genéricamente una serie de medios, dentro de los cuales tenga cabida el uso de ordenadores o se permita expresamente el uso de cualquier medio, el no otorgará al delito el carácter de "informático", lo cual lo que no necesariamente implica de que pueda hablarse de un delito relacionado con la informática. Un ejemplo de ello, es la doble contabilidad llevada por un ordenador con fines de evasión fiscal, la creación de

registros falsos con la finalidad de cobrar créditos inexistentes, jubilaciones, estafas etc.

El segundo supuesto que hay que mencionar es el caso en que la informática es el objeto del delito, aspecto de difícil determinación si tomamos en cuenta que se hace necesario diferenciar el hardware del software, y acotar que al primero son generalmente aplicables las normas delictivas tradicionales pues no constituye una nueva forma de propiedad. Distinta situación es el software y de la información almacenada en una computadora, pues los mismos constituyen formas intangibles y su carácter novedoso hace que no siempre hallen cabida en las instituciones tradicionales del derecho.

De esta manera, constituye delito informático cuando se perjudican a datos o programas informáticos, pero no cuando el objeto del daño es un ordenador cuyo resultado, la información que esta contenía queda malograda.

Por lo que se puede inferir que al tipificar un delito informático, lo que se está buscando es tutelar el contenido de la información de un sistema informático, y no el hardware en sí mismo.

Por último encontramos, la situación en la que influyen ambos supuestos, es decir, el ordenador se usa como instrumento y es a la vez el objeto sobre el cual recae la acción delictiva. El caso más elocuente es la destrucción de datos mediante un programa o un virus informático. (23)

En síntesis, la informática puede constituir un medio o el objeto de una acción típica. En la medida en que se presenten alguno de estos elementos, o ambos, estaremos ante un “delito informático”. (23)

23. **SANTIAGO** Acurio Del Pino. “Delitos Informáticos” pág. 25-30

No todos los delitos donde se utiliza el ordenador o una computadora puede tener el orden de delito informático si no que los delitos informáticos tienen que ir relacionados con los delitos en los cuales se causa daño al procesador de datos o la información que es importante para el titular de dicha información y los medios en los cuales se sustentan siempre que la finalidad de dicha destrucción del soporte de la información es la de dañar o destruir la información. (24)

Después de explicar sobre lo que es el delito informático y cual seria el bien dañado el tema a desarrollar es sobre la protección penal de lo que son los programas y documentos electrónicos a lo cual si bien delito informático es la protección de la información pero a lo que es el programa es el medio por el cual el dato que es la información este pasa por el programa quien lo procesa y como respuesta se crean los documentos electrónicos siendo el tema a desarrollar nuevo ya que en la legislación boliviana si bien se habla de delito informático tiene un orden especifico a la protección de lo que es el dato que es lo básico dejando al aire varios puntos sobre lo que es la informático ya que delito informático tiene que ir en la protección de nuevas figuras, los cuales pueden ser proclives al daño por delincuentes y no a figuras ya existentes..

2. CLASIFICACIÓN DE LOS DELITOS INFORMÁTICOS

.- La clasificación de los delitos informáticos según autores y organizaciones puede ser variada así que se analizara cada uno de ellos para definir que clases de delitos informáticos se pueden presentar y dentro de estos analizaremos que tipos de delitos se enmarcan en el mismo.

a) ***Según la clasificación del "Convenio sobre la Ciberdelincuencia" de 1 de Noviembre de 2001***

24. **SANTIAGO** Acurio Del Pino. "Delitos Informáticos" pág. 25-30

Con el fin de definir un marco de referencia en el campo de las tecnologías y los delitos para la Unión Europea, en Noviembre de 2001 se firmó en Budapest el "Convenio de Ciberdelincuencia del Consejo de Europa". En este convenio de propone una clasificación de los delitos informáticos en cuatro grupos:

- **Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos:**

    - Acceso ilícito a sistemas informáticos.
    - Interceptación ilícita de datos informáticos.
    - Interferencia en el funcionamiento de un sistema informático.
    - Abuso de dispositivos que faciliten la comisión de delitos.

  Algunos ejemplos de este grupo de delitos son: el robo de identidades, la conexión a redes no autorizadas y la utilización de spyware y de keylogger.

- **Delitos informáticos:**
    - Falsificación informática mediante la introducción, borrada o supresión de datos informáticos.
    - Fraude informático mediante la introducción, alteración o borrado de datos informáticos, o la interferencia en sistemas informáticos.

  El borrado fraudulento de datos o la corrupción de ficheros algunos ejemplos de delitos de este tipo.

- **Delitos relacionados con el contenido:**

    - Producción, oferta, difusión, adquisición de contenidos de pornografía infantil, por medio de un sistema informático o posesión de dichos contenidos en un sistema informático o medio de almacenamiento de datos.

- **Delitos relacionados con infracciones de la propiedad intelectual y derechos afines:**

    - Un ejemplo de este grupo de delitos es la copia y distribución de programas informáticos, o piratería informática.

Con el fin de criminalizar los actos de racismo y xenofobia cometidos mediante sistemas informáticos, en Enero de 2008 se promulgó el "Protocolo Adicional al Convenio de Ciberdelincuencia del Consejo de Europa" que incluye, entre otros aspectos, las medidas que se deben tomar en casos de:

- Difusión de material xenófobo o racista.
- Insultos o amenazas con motivación racista o xenófoba.
- Negociación, minimización burda, aprobación o justificación del genocidio o de crímenes contra la humanidad.

La amplia gama de reproducciones ilícitas por medios informáticos de obras protegidas por el derecho de autor, la ***Unión Europea***, en la Propuesta de Decisión-Marco del Consejo Relativa a los ataques de los que son Objeto los Sistemas de Información, de agosto de 2002, identifica las siguientes amenazas:

Acceso no autorizado a sistemas de información, que incluye la "piratería" informática;
Perturbación de los sistemas de información, como la "denegación de servicio";
Ejecución de programas perjudiciales que modifican o destruyen datos, incluye virus, bombas lógicas y gusanos;
Interceptación de las comunicaciones, denominada intromisión (sniffing);
Declaraciones falsas, se trata de la usurpación de la identidad de una persona en internet, se llama "spoofing" (modificación de datos).

b) ***Las Naciones Unidas***, reconoce los siguientes tipos de delitos informáticos

.

Fraudes cometidos mediante manipulación de computadoras: a) Manipulación de datos de entrada; b) manipulación de programas; c) manipulación de datos de salida; d) fraude efectuado por manipulación informática.

Falsificaciones informáticas: a) como objeto, se alteran datos de los documentos almacenados; b) como instrumentos.

Daños o modificaciones de programas o datos computarizados: a) Sabotaje informático; b) virus; c) gusanos: d) bomba lógica o cronológica.

Falsificaciones informáticas: a) Acceso no autorizado a sistemas o servicios; b) piratas informáticos o hackers; c) reproducción no autorizada de programas informáticos.

c) Clasificación según la Brigada de Investigación Tecnológica de la Policía Nacional Española

- **Ataques que se producen contra el derecho a la intimidad:**
  Delito de descubrimiento y revelación de secretos mediante el apoderamiento y difusión de datos reservados registrados en ficheros o soportes informáticos. (Artículos del 197 al 201 del Código Penal)

- **Infracciones a la Propiedad Intelectual a través de la protección de los derechos de autor:**
  Especialmente la copia y distribución no autorizada de programas de ordenador y tenencia de medios para suprimir los dispositivos utilizados para proteger dichos programas. (Artículos 270 y otros del Código Penal)

- **Falsedades:**
  Concepto de documento como todo soporte material que exprese o incorpore datos. Extensión de la falsificación de moneda a las tarjetas de débito y crédito.

Fabricación o tenencia de programas de ordenador para la comisión de delitos de falsedad. (Artículos 386 y ss. del Código Penal)

- **Sabotajes informáticos:**
  Delito de daños mediante la destrucción o alteración de datos, programas o documentos electrónicos contenidos en redes o sistemas informáticos. (Artículo 263 y otros del Código Penal)

- **Fraudes informáticos:**
  Delitos de estafa a través de la manipulación de datos o programas para la obtención de un lucro ilícito. (Artículos 248 y ss. del Código Penal)

- **Amenazas:**
  Realizadas por cualquier medio de comunicación. (Artículos 169 y ss. del Código Penal)

- **Calumnias e injurias:**
  Cuando se propaguen por cualquier medio de eficacia semejante a la imprenta o la radiodifusión. (Artículos 205 y ss. del Código Penal)

- **Pornografía infantil:**
  Entre los delitos relativos a la prostitución al utilizar a menores o incapaces con fines exhibicionistas o pornográficos.

  La inducción, promoción, favorecimiento o facilitamiento de la prostitución de una persona menor de edad o incapaz. (art 187)

  La producción, venta, distribución, exhibición, por cualquier medio, de material pornográfico en cuya elaboración hayan sido utilizados menores de edad o incapaces, aunque el material tuviere su origen en el extranjero o fuere desconocido. (Art 189)

El facilitamiento de las conductas anteriores (El que facilitare la producción, venta, distribución, exhibición...). (Art 189)
La posesión de dicho material para la realización de dichas conductas. (art 189)

d) También encontramos según la **doctrina americana** la clasificación según Actividades Delictivas Graves

Así encontramos la red de que Internet permite dar soporte para la comisión de otro tipo de delitos:

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

Narcotráfico: Transmisión de fórmulas para la fabricación de estupefacientes, para el blanqueo de dinero y para la coordinación de entregas y recogidas.
Tanto el FBI como el Fiscal General de los Estados Unidos han alertado sobre la necesidad de medidas que permitan interceptar y descifrar los mensajes encriptados que utilizan los narcotraficantes para ponerse en contacto con los cárteles.

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

parece que en este caso haya existido en realidad un acto de espionaje, se ha evidenciado una vez más la vulnerabilidad de los sistemas de seguridad gubernamentales.

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

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

Infracciones que no Constituyen Delitos Informáticos

Usos comerciales no éticos: Algunas empresas no han podido escapar a la tentación de aprovechar la red para hacer una oferta a gran escala de sus productos, llevando a cabo "mailings electrónicos" al colectivo de usuarios de un gateway, un nodo o un territorio determinado. Ello, aunque no constituye una infracción, es mal recibido por los usuarios de Internet, poco acostumbrados, hasta fechas recientes, a un uso comercial de la red.

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

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

e) Por su parte la doctrina española analiza los atentados contra la información a partir de sus propiedades esenciales: **confidencialidad**, **integridad** y **disponibilidad**

Desde el punto de vista de las conductas lesivas a la confiabilidad de la información

Se encuentran:
El Espionaje Informático (Industrial o Comercial). Con los términos industrial y comercial se pretende delimitar esta categoría, excluyendo bienes jurídicos distintos como sería el caso de delitos contra el Estado y la defensa nacional o contra la intimidad. Debe entenderse como la obtención con ánimo de lucro y sin autorización, de datos de valor para el tráfico económico de la industria o comercio. Dentro de los comportamientos que pueden ser incluidos en esta descripción se identifican los siguientes: La fuga de datos (Data Leakage), que las empresas o entidades guardan en sus archivos informáticos; las puertas falsas (Trap Doors), consistentes en acceder a un sistema informático a través de entradas diversas a las que se utilizan normalmente dentro de los programas. Las "llaves maestras" (Supperzapping) que implica el uso no autorizado de programas con la finalidad de modificar, destruir, copiar, insertar, utilizar o impedir el uso de datos archivados en los sistemas de información. El pinchado de líneas (Wiretapping), que consiste en la interferencia en líneas telefónicas o telemáticas, mediante las cuales se trasmiten las informaciones procesadas. La apropiación de informaciones residuales (Scavenging) que consiste en la obtención de información a partir de lo que desechan los usuarios legítimos de un sistema informático.

El Intrusismo informático. Se define como la mera introducción a sistemas de información o computadoras, infringiendo medidas de seguridad destinadas a proteger los datos contenidos en ellos. A primera vista pareciera que el Sabotaje Informático y el Intrusismo fueran comportamientos idénticos, sin embargo el elemento subjetivo delimita estos comportamientos. En el primer supuesto, la intencionalidad del agente es obstaculizar el funcionamiento de un

sistema informático, en el segundo caso la acción realizada busca únicamente el ingreso a tales sistemas sin dirigir sus actos a la producción de perjuicio, que se produzca, es ajeno al comportamiento aunque es evidente que lo agrava. (25)

Las Conductas lesivas a la integridad de la Información

Consisten en el acceso directo u oculto no autorizado a un sistema informático mediante la introducción de nuevos programas denominados virus, "gusanos" o "bombas lógicas". El acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema, recibe el nombre de "sabotaje informático".

Conductas lesivas a la disponibilidad

Las bombas lógicas y los virus informáticos pueden afectar transitoriamente la disponibilidad de la información, sin destruirla. Otro de los mecanismos que pueden impedir el acceso a un sistema de información por parte de los usuarios legítimos, son los denominados "spam" o el "electronic-mail bombing", que consisten en el envío de cientos de miles de mensajes de correo electrónico no solicitados o autorizados, para bloquear los sistemas.

f) El mexicano TÉLLEZ VALDEZ clasifica a estos delitos, de acuerdo a dos criterios:

1. Como Instrumento o medio.

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

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

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

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

25. **ETORRE** Giannantonio, "Informática y Derecho" Volumen 1 pág. 50

d) Lectura, sustracción o copiado de información confidencial.

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

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

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

h) Uso no autorizado de programas de cómputo.

i) Introducción de Instrucciones que provocan “interrupciones” en la lógica interna de los programas.

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

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

l) Acceso a áreas informatizadas en forma no autorizada.

m) Intervención en las líneas de comunicación de datos o teleproceso.

2. Como fin u objetivo.

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

a) Programación de instrucciones que producen un bloqueo total al sistema.

b) Destrucción de programas por cualquier método.

c) Daño a la memoria.

d) Atentado físico contra la máquina o sus accesorios.

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

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

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

- Acceso no autorizado: Uso ilegítimo de passwords y la entrada de un sistema informático sin la autorización del propietario. (Violación de la privacidad).
- Destrucción de datos: Los daños causados en la red mediante la introducción de virus, bombas lógicas, etc.
- Infracción al copyright de bases de datos: Uso no autorizado de información almacenada en una base de datos.
- Interceptación de e-mail: Lectura de un mensaje electrónico ajeno.
- Estafas Electrónicas: A través de compras realizadas haciendo uso de la Internet.
- Transferencias de fondos: Engaños en la realización de este tipo de transacciones.

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

- Espionaje: Acceso no autorizado a sistemas de informáticos gubernamentales y de grandes empresas e interceptación de correos electrónicos.
- Terrorismo: Mensajes anónimos aprovechados por grupos terroristas para remitirse consignas y planes de actuación a nivel internacional.
- Narcotráfico: Transmisión de fórmulas para la fabricación de estupefacientes, para el blanqueo de dinero y para la coordinación de entregas y recogidas.
- Otros delitos: Las mismas ventajas que encuentran en la Internet los narcotraficantes puede ser aprovechadas para la planificación de otros delitos como el tráfico de armas, proselitismo de sectas, propaganda de grupos extremistas, y cualquier otro delito que pueda ser trasladado de la vida real al ciberespacio o al revés. (26)

26. **RENE** de Sola Quinteros. “Delitos Informáticos”, pág. 20

g) Según el Profesor de Derecho Informático de la PUCE **Dr. Santiago Acurio Del Pino** los tipos de delitos informáticos son:

- **Los fraudes**

Los datos falsos o engañosos (Data diddling), conocido también como introducción de datos falsos, es una manipulación de datos de entrada al computador con el fin de producir o lograr movimientos falsos en transacciones de una empresa. Este tipo de fraude informático conocido también como ***manipulación de datos de entrada***, 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.

Manipulación de programas o los "caballos de troya" (Troya Horses), 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.

La técnica del salami (salami technique/rounching down),Aprovecha las repeticiones automáticas de los procesos de cómputo.Es una técnica especializada que se denomina "técnica del salchichón" en la que "rodajas muy finas" apenas perceptibles, de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra. Y consiste en introducir al programa unas instrucciones para que remita a una determinada cuenta los céntimos de dinero de muchas cuentas corrientes.

Falsificaciones informáticas: Como objeto: Cuando se alteran datos de los documentos almacenados en forma computarizada.

Como instrumentos: Las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial.

Cuando empezó a disponerse de fotocopiadoras computarizadas en color basándose en rayos láser surgió una nueva generación de falsificaciones o alteraciones fraudulentas. Estas fotocopiadoras pueden hacer reproducciones 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.

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 basándose en tarjetas bancarias robadas, sin embargo, en la actualidad se usan ampliamente equipo y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.

Pishing.- Es una modalidad de fraude informático diseñada con la finalidad de robarle la identidad al sujeto pasivo. El delito consiste en obtener información tal como números de tarjetas de crédito, contraseñas, información de cuentas u otros datos personales por medio de engaños.

Este tipo de fraude se recibe habitualmente a través de mensajes de correo electrónico o de ventanas emergentes. El robo de identidad es uno de los delitos que más ha aumentado. La mayoría de las victimas son golpeadas con secuestros de cuentas de tarjetas de crédito, pero para muchas otras la situación es aun peor. En los últimos cinco años 10 millones de personas han sido víctimas de delincuentes que han abierto cuentas de tarjetas de crédito o

con empresas de servicio público, o que han solicitado hipotecas con el nombre de las víctimas, todo lo cual ha ocasionado una red fraudulenta que tardará años en poderse desenmarañar.

En estos momentos también existe una nueva modalidad de Pishing que es el llamado Spear Pishing o Pishing segmentado, el cual ataca a grupos determinados, es decir se busca grupos de personas vulnerables a diferencia de la modalidad anterior.

- **El 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:

Bombas lógicas (logic bombs), es una especie de bomba de tiempo que debe producir daños posteriormente. 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.

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.

Virus informáticos y malware, son elementos informáticos, que como los microorganismos biológicos, tienden a reproducirse y a extenderse dentro del sistema al que acceden, se contagian de un sistema a otro, exhiben diversos grados de malignidad y son eventualmente, susceptibles de destrucción con el uso de ciertos antivirus, pero algunos son capaces de desarrollar bastante resistencia a estos.

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. Han sido definidos como “pequeños programas que, introducidos subrepticiamente en una computadora, poseen la capacidad de autorreporducirse sobre cualquier soporte apropiado que tengan acceso al computador afectado, multiplicándose en forma descontrolada hasta el momento en que tiene programado actuar”

El malware es otro tipo de ataque informático, que usando las técnicas de los virus informáticos y de los gusanos y las debilidades de los sistemas desactiva los controles informáticos de la máquina atacada y causa que se propaguen los códigos maliciosos.

Ciberterrorismo: Terrorismo informático es el acto de hacer algo para desestabilizar un país o aplicar presión a un gobierno, utilizando métodos clasificados dentro los tipos de delitos informáticos, especialmente los de los de tipo de Sabotaje, sin que esto pueda limitar el uso de otro tipo de delitos informáticos, además lanzar un ataque de terrorismo informático requiere de muchos menos recursos humanos y financiamiento económico que un ataque terrorista común.

Ataques de denegación de servicio: Estos ataques se basan en utilizar la mayor cantidad posible de recursos del sistema objetivo, de manera que nadie más pueda usarlos, perjudicando así seriamente la actuación del sistema, especialmente si debe dar servicio a mucho usuarios Ejemplos típicos de este ataque son: El consumo de memoria de la máquina víctima, hasta que se produce un error general en el sistema por falta de memoria, lo que la deja fuera de servicio, la apertura de cientos o miles de ventanas, con el fin de que se pierda el foco del ratón y del teclado, de manera que la máquina ya no responde a pulsaciones de teclas o de los botones del ratón, siendo así totalmente inutilizada, en máquinas que deban funcionar ininterrumpidamente, cualquier interrupción en su servicio por ataques de este tipo puede acarrear consecuencias desastrosas.

- **El espionaje informático y el robo o hurto de software:**

Fuga de datos (data leakage), también conocida como la divulgación no autorizada de datos reservados, es una variedad del espionaje industrial que sustrae información confidencial de una empresa. A decir de Luis Camacho Loza, “la facilidad de existente para efectuar una copia de un fichero mecanizado es tal magnitud en rapidez y simplicidad que es una forma de delito prácticamente al alcance de cualquiera”.

La forma más sencilla de proteger la información confidencial es la criptografía.
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, considero, que la reproducción no autorizada de programas informáticos no es un delito informático, debido a que, en primer lugar el bien jurídico protegido es en este caso el derecho de autor, la propiedad intelectual y en segundo lugar que la protección al software es uno de los contenidos

específicos del derecho informático al igual que los delitos informáticos, por tal razón considero que la piratería informática debe ser incluida dentro de la protección penal al software y no estar incluida dentro de las conductas que componen la delincuencia informática.

- **El robo de servicios:**

  Hurto del tiempo del computador. Consiste en el hurto de el tiempo de uso de las computadoras, un ejemplo de esto es el uso de internet, en el cual una empresa proveedora de este servicio proporciona una clave de acceso al usuario de internet, para que con esa clave pueda acceder al uso de la súper carretera de la información, pero sucede que el usuario de ese servicio da esa clave a otra persona que no esta autorizada para usarlo, causándole un perjuicio patrimonial a la empresa proveedora de servicios.

  Apropiación de informaciones residuales (scavenging), es el aprovechamiento de la información abandonada sin ninguna protección como residuo de un trabajo previamente autorizado. to scavenge, se traduce en recoger basura. Puede efectuarse físicamente cogiendo papel de desecho de papeleras o electrónicamente, tomando la información residual que ha quedado en memoria o soportes magnéticos.

  Parasitismo informático (piggybacking) y suplantación de personalidad (impersonation), figuras en que concursan a la vez los delitos de suplantación de personas o nombres y el espionaje, entre otros delitos. En estos casos, el delincuente utiliza la suplantación de personas para cometer otro delito informático. Para ello se prevale de artimañas y engaños tendientes a obtener, vía suplantación, el acceso a los sistemas o códigos privados de utilización de ciertos programas generalmente reservados a personas en las que se ha depositado un nivel de confianza importante en razón de su capacidad y posición al interior de una organización o empresa determinada.

- **El acceso no autorizado a servicios informáticos:**

  Las puertas falsas (trap doors), consiste en la práctica de introducir interrupciones en la lógica de los programas con el objeto de chequear en medio de procesos complejos, si los resultados intermedios son correctos, producir salidas de control con el mismo fin o guardar resultados intermedios en ciertas áreas para comprobarlos más adelante.

  La llave maestra (superzapping), es un programa informático que abre cualquier archivo del computador por muy protegido que esté, con el fin de alterar, borrar, copiar, insertar o utilizar, en cualquier forma no permitida, datos almacenados en el computador.

  Su nombre deriva de un programa utilitario llamado *superzap*, que es un programa de acceso universal, que permite ingresar a un computador por muy protegido que se encuentre, es como una especie de llave que abre cualquier rincón del computador.

  Mediante esta modalidad es posible alterar los registros de un fichero sin que quede constancia de tal modificación

  Pinchado de líneas (wiretapping), consiste en interferir las líneas telefónicas de transmisión de datos para recuperar la información que circula por ellas, por medio de un radio, un módem y una impresora.

  Como se señalo anteriormente el método más eficiente para proteger la información que se envía por líneas de comunicaciones es la criptografía que consiste en la aplicación de claves que codifican la información, transformándola en un conjunto de caracteres ininteligibles de letras y números sin sentido aparente, de manera tal que al ser recibida en destino, y por aplicación de las mismas claves, la información se recompone hasta quedar exactamente igual a la que se envió en origen.

  Piratas informáticos o hackers. El acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones, recurriendo a uno de los diversos medios que se mencionan a continuación. el delincuente puede aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o

puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema. a menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sistema; esto suele suceder con frecuencia en los sistemas en los que los usuarios pueden emplear contraseñas comunes o contraseñas de mantenimiento que están en el propio sistema.

Al hablar del delito informático y su clasificación a la cual tras leer las clasificaciones realizadas por las diferentes organizaciones y autores se concluye que los tipos de delitos informáticos mas prudentes a desenvolver serian las del Profesor de Derecho Informático de la PUCE **Dr. Santiago Acurio Del Pino** el cual explica según su clasificación que existen delitos según el fraude realizado con la computadora, el sabotaje informático, el espionaje informático y el robo o hurto de software, el robo de servicio, el acceso no autorizado a servicios informáticos a lo cual en su explicación nos habla la clase de delito se comete en ese tipo de delito informático debiendo tomar en cuenta que esta clase de delitos son cometidos por la computadora y técnicas informáticas. (27)

3. LA DIFERENCIA ENTRE LOS DELITOS INFORMATICOS CON LOS DEMAS DELITOS

Adentrándonos en lo que son los delitos informáticos se realizara la diferenciación con los delitos comunes a lo cual se analizara definición de lo que es delito o crimen para analizara los delitos comunes ya existentes en las legislación y se pasara a la comparación con las definiciones ya propuestas y el análisis llevado a cabo en el anterior numeral sobre lo que es teorías y conceptos sobre delitos informáticos para lograr establecer el fin del tema propuesto definiendo lo que es delito informático y la protección del software o programa y documento electrónico.

27. **SANTIAGO** Acurio Del Pino. “Delitos Informáticos” pág. 29

Para hablar de delito entenderemos primero lo que es delito para Francisco Carrara “el delito no es un ente de hecho sino un ente jurídico” explicando esta formula agrego: “El delito es un ente jurídico, porque su esencia debe consistir necesariamente en la violación de un derecho. Es que así el que comete el delito tiene que tener la voluntad inteligente y libre a un hecho exterior las cuales tendrán que afectar a un derecho ajeno.

Al análisis de la tipología de los delitos encontramos la clasificación de los delitos según la estructura del tipo en la cual nos basaremos para diferenciar los delitos conocidos con los delitos informáticos, encontramos:
Según los elementos del tipo objetivo.- Encontramos las siguientes clases de delitos que son: (28)

1. Por el autor o sujeto activo.- En esta definición se encontrara tres tipos de explicaciones de delitos a los cuales se desarrollara:

   a) Delitos unisubjetivos y plurisubjetivos: los delitos unisubjetivos son aquellos donde el legislador señala que el delincuente es solo una persona. Mientras que los plurisubjetivos son referidos mayor mente a varias personas es decir a dos o mas sujetos que cometan un delito.
   b) Delitos comunes y delitos especiales propios e impropios: hacemos denotar que en los delitos comunes y delitos especiales no se requiere cualidades específicas así pudiendo ser cualquier persona el delincuente. Diferenciándose de estos se encuentra los delitos propios e impropios en esta clase de tipo de delitos se requiere necesariamente cualidades en el sujeto activo es decir en el delincuente.
   c) Delitos por el dominio del hecho y delios de infracción del deber: En los delitos por el dominio del hecho se requiere tener que conocer el dominio de la relación y hecho. Ejemplo el homicidio de tipo doloso.
   En los delitos de infracción del deber se toma en cuenta la falta de cumplimiento de deberes de ejecución. Ejemplo el incumplimiento de función del juez y funcionarios públicos.

28. **RODOLFO** Illanes “Apunte de Derecho Penal I”

2. Por la acción o conducta típica y el resultado.- en esta clasificación de los delitos se vera el aspecto del tipo del delito por el resultado y la conducta típica del delincuente explicando a continuación cuatro puntos sobre esta clasificación:

   a) Delitos de mera conducta y delitos de resultado: Al hablar de los delitos de mera conducta muestran el tipo penal en el que el legislador sanciona la conducta es decir la voluntad del que va a cometer el delito. En los delitos de resultado sanciona la acción y el resultado consumado. Ejemplo homicidio en grado de tentativa.
   b) Delitos de propia mano: en esta clase de delito
   c) el legislador indica que solo es consumado por la persona que lo realiza la acción prohibida. Ejemplo en el articulo 308 el acceso carnal
   d) Delitos de consumación normal y delitos de consumación anticipada: los delitos de consumación normal se agotan con la realización de acción prohibida y otros elementos del tipo penal. Mientras que los delitos de consumación anticipada se consuman antes de realizar la acción prohibida ejemplo. Un incendio para generar peligro.
   e) Delitos simples, compuestos, mixtos y de hábito: en los delitos simples el legislador establece una acción prohibida un solo verbo rector. Ejemplo en el artículo 251 especifica en el verbo por el cual se guiara dicho artículo el que matare. Y al hablar de un delito compuesto se hablara de 2 o mas verbos rectores. Es que así en los delitos mixtos uno o más verbos rectores y a su vez se habrán uno o más resultados. En los de hábito es la repetición de un comportamiento del tipo penal que llega a consumarse.

3. Por el bien jurídicamente protegido.- entre los tipos de delitos encontramos a parte de los ya mencionados a lo que son la siguiente clasificación dentro de este tipo:

a) Delitos de lesión y peligro: Al hablar de este delito de lesión el mismo es vinculado al bien jurídicamente protegido se encuentra en el titulo. Se produce un daño real y efectivo a un bien jurídico. Ejemplo el homicidio don de le bien jurídicamente protegido es la vida y la integridad de la persona. En el delito de peligro no existe daño real al bien jurídico protegido solo existe peligro de mera posibilidad. Ejemplo en el artículo 206 poner en peligro a bienes y personas.

b) Delitos de consumación normal y anticipada: Estas ya son prescritas en la normativa penal es decir estas son acciones o conductas típicas.

c) Delitos instantáneos, permanentes y de estado: Cuando se habla de los delitos instantáneos estos son los que se consuman con la voluntad. Ejemplo la injuria y calumnia. Mientras que los delitos permanentes son aquellos delitos continuados y los elementos del tipo penal siguen consumándose en el futuro. Ejemplo en el artículo 334 secuestro en este artículo se demuestra que persiste la acción antijurídica mientras el delincuente siga cometiendo el hecho antijurídico. En los delitos de estado los efectos no desaparecen además no hay retroceso ejemplo en los delitos de orden político.

d) Delitos uniofensivos y pluriofensivos: al hablar de delito uniofensivo decimos que estas son conductas que atentan a un bien jurídico, tomando en cuenta que serán dentro de Bolivia. Mientras que los delitos pluriofensivos lesionan dos o mas bienes jurídicos protegidos, cuando no es claro el bien jurídico que se protege.

4. Por el sujeto pasivo.- en este tipo encontramos las siguientes clasificaciones.

a) Delitos comunes y propios e impropios: en los delitos impropios en la tipificación no requiere cualidades pudiendo realizar el delito cualquiera. Mientras que en los delitos propios en la realización del hecho y la tipificación el delincuente se identifica por tener una cualidad.

b) Según los elementos del tipo subjetivo: en estos encontramos que hay un tipo penal básico, el cual establece la conducta prohibida por excelencia la acción prohibida básica o la que se desprenderá de otros

tipos penales ejemplo. El matar a un niño o un padre, en el caso de un tipo penal autónomo, en esta tuene una característica propia que lo diferencia del tipo penal básico ejemplo asesinato.

Tras la explicación de los tipos de delitos haremos la diferenciación ver a que clase de delito puede pertenecer es que así el tratadista e ilustre penalista Cuello Calon nos explica los elementos integrantes de los delitos informáticos, los cuales son los siguientes:

- El delito es un acto humano, (acción u omisión).
- Dicho acto humano ha de ser antijurídico, debe lesionar o poner en peligro un interés jurídicamente protegido.
- Debe corresponder a un tipo legal (figura de delito), definido por la ley, ha de ser un acto típico.
- El ha de ser culpable, imputable a dolo (intención) o a culpa (negligencia), y una acción es imputable cuando puede ponerse a cargo de una determinada persona.
- La ejecución u omisión del acto debe estar sancionada por una pena.

Tras la explicación decimos que los delitos informáticos son una nueva forma de daño ya no a algo material si no a algo subjetivo que solo puede ser acogido y visto por un medio electrónico es decir la información digital y manejable por el sistema informático y la ciencia informática a lo cual en la existencia de los demás objetos tangibles de valor que son protegidos por la norma, el delito informático proveniente también del avance de la ciencia es novedoso por que lo protegido solo puede ser realizado y expuesto por medios electrónico o computacionales los que van en relación a la ciencia informática.

Los delitos informáticos por el medio de su modo operandi ya que en estos delitos son de cuello blanco es decir que no son delitos en los cuales el delincuente tenga atacar y actuar directamente hacia la victima ya que en este delito el medio es la tecnología informática en este caso es la computadora, medio por el cual el delincuente de ser un delincuente común pasa a ser un ciber delincuente ya que este puede por el medio de la computadora realizar actos delictivos sin estar en contacto directo con la victima y

ser identificado, diferenciándose este delito de los demás delitos ya que en muchos casos el delincuente siempre entra en contacto con la victima y lo realiza con medios directos y no así por medio en los cuales no se los puede reconocer (29)

4. CONCEPTO Y DIFERENCIACIÓN DE DATO, PROGRAMA Y DOCUMENTO ELECTRONICO Y LA APRECIACIÓN DE LOS MISMOS COMO UN VALOR ECONOMICO

Comenzando con el desarrollo del tema después de explicar y detallar lo que es el delito informático y teniendo en cuenta que en la legislación boliviana existe un capitulo relacionado a los delitos informáticos donde con mayor énfasis nos habla sobre la protección del dato a lo cual en el tema a desarrollar sobre la protección penal de lo que son los programas o la protección del documento electrónico explicando la diferencia de los mismos con el dato ya que muchos creen que con la tipificación y la protección del dato en el código penal boliviano ya se encuentra protegido el amplio mudo de la informática, para eso pasaremos se realizara la conceptualización de lo que es el programa, documento electrónico y dato para después pasar a la diferenciación de los mismos y verificando estos si tienen una apreciación económica en el mundo.

4.1. CONCEPTO DE DATO, PROGRAMA Y DOCUMENTO ELECTRÓNICO:

Comenzaremos esta parte hablando de lo que es el dato, este es la base para la realización de la información como aspecto de órdenes para buscar repuestas es que así encontramos la definición de los técnicos informáticos que dicen que el dato es: son hechos y cifras en bruto, tales como órdenes y pagos, los cuales se procesan para obtener información, por ejemplo el saldo deudor y el monto disponible. Sin embargo, en el uso común, los términos datos e información se toman como sinónimos.

29. **SANTIAGO** Acurio Del Pino. “Delitos Informáticos” 28

La cantidad de datos versus información que se guarda en el computador constituye una compensación. Los datos pueden procesarse en diferentes formas de información, pero toma tiempo clasificar y sumar transacciones. La información actualizada puede proporcionar respuestas inmediatas. Un error frecuente es creer que el software es también datos. El computador ejecuta o corre un software. Los datos se "procesan", mientras que el software se "ejecuta". 2. Cualquier forma de información, ya sea en forma electrónica o sobre papel. En forma electrónica, "datos" se refiere a archivos, bases de datos, documentos de texto, imágenes y, voz y video codificados en forma digital.

El programa como tal es aquella parte esencial por la cual la computadora puede realizar actividades y que sin el no serviría ya que este es la parte vital de la misma ya que la computadora por si misma consta de dos partes como se explico una que es el hardware la misma es el cuerpo de la computadora o parte sensible o aquella que se puede tocar y la segunda es el software esta es la parte lógica aquella que no se puede tocar en si este es la programación de la computadora por el cual podrá analizar otros programas adicionales que serán de apoyo al mismo, dando relación que este puede ser el alma del computador ya que este es la base por el cual analizara y almacenara en la parte sensible del computador es decir en la memoria que el disco duro de la computadora, esta información (datos) tras el proceso por el programa estos son almacenados en carpetas llamados documentos electrónicos en los cuales se almacenan toda la información que manda en respuesta el programa y estos documentos electrónicos se encuentran en dispositivos de almacenamiento que pueden ser discos memorias magnéticas u otras. (30) Al respecto se citara algunos autores que definen lo que es el dato, programa y el documento electrónico: (31)

> Para los ingenieros informáticos de la empresa de tecnología **Microsoft Windows Corporations**, el software (programa o aplicación) es un conjunto de instrucciones detalladas que controlan la operación de un sistema computacional a lo cual se explica los siguientes puntos.

---

30. **RODOLFO** Pagano, “Informática y Derecho” Volumen 2 pag. 95
31. **CHILE** “Biblioteca Del Congreso Nacional de Chile Departamento de Estudios” documento digital Santiago de Chile 18

Las funciones del software son:

- Administrar los recursos computacionales
- Proporcionar las herramientas para optimizar estos recursos.
- Actuar como intermediario entre el usuario y la información almacenada.

Programas de Software

Programa: conjunto de argumentos o instrucciones para la computadora, almacenado en la memoria primaria de la computadora junto con los datos requeridos para ser ejecutado, en otras palabras hacer que las instrucciones sean realizadas por la computadora.

Tipos de Software

- ***Software del sistema:*** Es un conjunto de programas que administran los recursos de la computadora. Ejemplos: Unidad central de proceso, dispositivos de comunicaciones y dispositivos periféricos, el software del sistema administra y controla al acceso del hardware.
- ***Software de aplicaciones:*** Programas que son escritos para o por los usuarios para realizar una tarea especifica en la computadora. Ejemplo: software para procesar un texto, para generar una hoja de cálculo, el software de aplicación debe estar sobre el software del sistema para poder operar.

Software de usuario final: Es el software que permiten el desarrollo de algunas aplicaciones directamente por los usuarios finales, el software del usuario final con frecuencia tiene que trabajar a través del software de aplicación y finalmente a través del software del sistema

Según el diccionario Wikipedia un **programa informático** es un conjunto de instrucciones que una vez ejecutadas realizarán una o varias tareas en una computadora. Sin programas, estas máquinas no pueden funcionar. Al conjunto general de programas, se le denomina software, que más genéricamente se refiere al equipamiento lógico o soporte lógico de una computadora digital.

En informática, se los denomina comúnmente *binarios*, (propio en sistemas Unix, donde debido a la estructura de este último, los ficheros no necesitan hacer uso de extensiones. Posteriormente, los presentaron como ficheros ejecutables, con extensión *.exe*, en los sistemas operativos de la familia Windows) debido a que una vez que han pasado por el proceso de compilación y han sido creados, las instrucciones que se escribieron en un lenguaje de programación que los humanos usan para escribirlos con mayor facilidad, se han traducido al único idioma que la máquina comprende, combinaciones de ceros y unos llamada código máquina. El mismo término, puede referirse tanto a un programa ejecutable, como a su código fuente, el cual es transformado en un binario cuando es compilado.

Generalmente el código fuente lo escriben profesionales conocidos como programadores. Se escribe en un lenguaje que sigue uno de los siguientes dos paradigmas: imperativo o declarativo y que posteriormente puede ser convertido en una imagen ejecutable por un compilador. Cuando se pide que el programa sea ejecutado, el procesador ejecuta instrucción por instrucción.

De acuerdo a sus funciones, se clasifican en software de sistema y software de aplicación. En los computadores actuales, al hecho de ejecutar varios programas de forma simultánea y eficiente, se le conoce como multitarea.

Para los expertos de la Empresa Tecnológica TRIPOD, un programa de computadora es un conjunto de instrucciones que producirán la ejecución de una determinada tarea. En esencia, un programa es un medio para llegar a un fin. El fin será normalmente definido como la información necesaria para solucionar un problema.

Tras la explicación de lo que son los programas los cuales encontramos diferentes clases de programas conocidos como software, el software de sistema y el software de aplicación, a lo cual da como resultado tras el proceso del dato, el documento electrónico que según conceptos es:

Según la enciclopedia Wikipedia Un **documento electrónico** es un documento cuyo soporte material es algún tipo de dispositivo electrónico o magnético, y en el que el

contenido está codificado mediante algún tipo de código digital, que puede ser leído, interpretado, o reproducido, mediante el auxilio de detectores de magnetización.
Según técnicos de la empresa **Microsoft Windows Corporations**, el documento electrónico debe entenderse como toda expresión en lenguaje natural o convencional y cualquier otra expresión gráfica, sonora o en imagen, recogidas en cualquier tipo de soporte material, incluso los soportes informáticos, con eficacia probatoria o cualquier otro tipo de relevancia jurídica.

4.2. DIFERENCIACIÓN ENTRE DATO, PROGRAMA Y DOCUMENTO ELECTRÓNICO.

Al hablar de programa y documento electrónico encontramos que estos son diferentes a lo que es el dato ya que según los autores que estudiaremos decimos que el programa es el software de la computadora la cual a diferencia del dato que es la información colocada en las diferentes clases de software encuentran una respuesta tras el proceso de la información en el software, el mismo conformado por una serie de instrucciones que ayudan a procesar la información recepcionada para dar paso a una respuesta la cual conforma el documento electrónico siendo este la serie de respuestas emitidas por el programa como solución al dato colocado. (32)

Es así que decimos que los Datos, son las unidades básicas de la información, cualquiera que sea su contenido (un número, una palabra, un sonido, una imagen) y que al ser procesados dan lugar a la información que resulta de la conexión de dos o más datos. Programas, son las secuencias de instrucciones que se utilizan para el procesamiento de los datos, para la realización de tareas específicas. Los documentos electrónicos, son aquellos en que se recogen los resultados del procesamiento de los datos obtenidos con las distintas aplicaciones.

32. **CHILE** "Biblioteca Del Congreso Nacional de Chile Departamento de Estudios" documento digital Santiago de Chile pág. 21

Al análisis de lo que es programa y documento electrónico se hace la diferencia que el programa son las secuencias o el medio por el cual se procesan los datos que son puestos a conocimiento del programa mientras que el documento electrónico es el medio por el cual se recogen los resultados del procesamiento de datos obtenidos por los diferentes programas.

4.3. APRECIACIÓN ECONÓMICA DEL PROGRAMA Y VALOR PROBATORIO DEL DOCUMENTO ELECTRÓNICO.

- **Valor probatorio del documento electrónico.**

En nuestro ordenamiento, en el cual rige el principio del libre convencimiento del juez, no hay ningún obstáculo a la posibilidad para las partes de producir y para el juez de admitir como medios de prueba los documentos electrónicos: y esto tanto sea en el proceso penal como en el proceso civil o administrativo. (33)

La posibilidad de producir o admitir los documentos electrónicos como medio de prueba, significa que no hay norma alguna que inhiba al juez para utilizar los documentos electrónicos como medio de prueba, que prevea la admisibilidad solo en el caso de falta de otros medios de prueba o que imponga una determinada eficacia probatoria de ellos. Esto, por lo demás no significa que al documento electrónico el juez deba, en todos los casos, atribuirle plena atendibilidad, sino después de una adecuada valoración de la autenticidad y de la seguridad del documento electrónico.

Se trata de una investigación que, en el estado actual de la legislación italiana, debe ser hecha, caso por caso, según los criterios indicados en los estudios dedicados a la seguridad de los estados.

El documento electrónico se trata de un material imponente y complejo, de origen, en los Estados Unidos el jurista es oportuno que conozca algunos principios fundamentales y en particular, las técnicas necesarias a ser adoptadas para que un documento electrónico pueda ser considerado autentico y seguro.

33. **RENATO** Borruso, “informática y Derecho” Volumen 5 pág. 64

- **La apreciación económica del programa.**

Mayor mente cuando se habla del programa se habla del sistema operativo de la computadora ya que sin este no serviría la maquina ya que es aquel que se encarga de analizar la información y procesarla dando una respuesta a la misma, muchos dicen que la programación tiene una valoración económica según el uso para la empresa a la que a sido destinada también la producción de esta en el momento de ser expuesta según la función del programa que tiene su creador le da un costo teniendo un valor económico.

El almacenamiento, tratamiento y transmisión de datos mediante los sistemas de procesamiento e interconexión conceden el novísimo significado atribuido al término "información", colocando a su poseedor en una privilegiada situación de ventaja respecto al resto de individuos, pues nadie puede dudar que quien ostenta la información y sepa almacenarla, tratarla y transmitirla correctamente mediante los sistemas de procesamiento de datos, será quien obtenga mayores dividendos en sus actividades económicas, fin primordial perseguido en éste tipo de actividades , por lo que debe ser considerado un valor económico de empresa, aunque debe entenderse que al adoptar el vocablo "empresa" nos referimos a ella como actividad (industrial, mercantil, comercial), pues la protección que se pretende fundamentar no esta dirigida a la empresa como sociedad (anónima, encomandita, individual, etc.), sino que se orienta a la información y su nuevo significado en la actividad empresarial.

De allí que el denominado "nuevo paradigma económico", resulte ser un fenómeno comparable tan sólo con el ocurrido con la aparición de la electricidad, aunque en éste caso el fenómeno haya resultado mucho más acelerado, por ello es que Alan Greenspan, Presidente de la Reserva Federal de los Estados Unidos, reconozca que la prosperidad económica de los últimos ocho años en dicho país y sus corporaciones resulta atribuible a la influencia de la informática.

Así podemos decir que el interés social digno de tutela penal sería: "la información (almacenada, tratada y transmitida a través de sistemas informáticos), como valor económico de la actividad de empresa". Ahora bien, habrá que determinar si estamos ante un bien jurídico penal individual o si más bien el interés tutelado es de carácter

colectivo. Si tenemos en consideración que estamos ante un interés social vinculado a la actividad empresarial, toda vez que la información se convierte en un valioso instrumento de la actividad de empresa, el bien jurídico "información" se encontraría encardinado dentro de los llamados delitos socio-económicos y por ello sus repercusiones trascenderían a las propias bases del sistema socio-económico, esto es, estamos a través de bien jurídico colectivo.

5. CONCEPTO DEL DELITO DE DESTRUCCIÓN, ALTERACIÓN, INUTILIZACIÓN Y DAÑO A PROGRAMAS O DOCUMENTOS ELECTRÓNICOS (Sabotaje informático).

5.1. INTRODUCCIÓN.

Tras el estudio de lo que es el programa y el documento electrónico diferenciado de lo que es el dato y que cada uno cumple una función dentro de la rama científica de la informática y antes de entrar a lo que son las teorías y conceptos del delito de destrucción, alteración, inutilización y daño a programas o documentos electrónicos se dará a conocer a las falencias en la tipificación boliviana en sus artículos:

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

Dentro de la tipificación que hace este articulo se encuentra lo que es la protección penal a lo que es la manipulación informática de datos a lo cual nos dice el que manipule un procesamiento o transferencia de datos con la finalidad de ocasionar una transferencia patrimonial en perjuicio de tercero será sancionado con reclusión, este delito cumple la función protectora de lo que son los datos informáticos que son procesados por lo que son los programas pero no habla de si mismo de lo que es la

protección del programa ni del resultado que es producto del análisis del dato la cual se almacena en los documentos electrónicos.

Articulo 363 Ter. (ALTERACION, ACCESO Y USO INDEBIDO DE DATOS INFORMATICOS). El que sin estar autorizado se apodere, acceda, utilice, modifique, suprima o inutilice, datos almacenados en una computadora o en cualquier soporte informático, ocasionando perjuicio al titular de la información, será sancionado con prestación de trabajo hasta (1) año o multa hasta doscientos días. (34)

En el presente artículo la tipificación que realiza es sobre el acceso y uso indebido de datos informatices, al hablar de datos almacenados se refiere a la información de una persona y que estos deben estar almacenados en una computadora o en cualquier soporte magnético a lo cual el fin del delincuente e el apoderamiento el uso o inutilización de la información aquí la información almacenada tiene importancia y dejando de lado lo que es el daño a la programación por la cual se causa daños para que se altere dicha información, pero al respecto, si bien se protege el uso indebido de datos no se califica con una sanción fuerte al que realiza esta clase de delitos y como se hablo en el marco histórico el mismo es un saludo a la bandera, es decir es simbólico ya que los que realizan estas clases de delitos no son denunciados ya que las victimas no ven con mucha importancia a la sanción y que mas tarda el proceso y es costoso para la victima realizarlo dejando así impune esta clase de delitos.

Es que así se da a conocer que si el código penal boliviano tiene un capitulo relacionado con los delitos informáticos y en el mismo se compone por dos artículos que son en defensa de lo que es la manipulación informática y la alteración, acceso y uso indebido de datos informáticos estos son una parte de los delitos sobre los fraudes informáticos, dejando el código penal al descubierto las diferentes clases de delitos informáticos existentes en el mundo y que Bolivia podría ser causa de ataque de las mismas.

34. **BOLIVIA "**Código Penal Boliviano"

Al respecto, al hablar de los delitos informáticos se habla de no solo de dos clases de delitos si no de diferentes tipos de delitos informáticos como ya se expuso en el anterior punto sobre la clasificación de los delitos informáticos, con referencia al tema a desarrollar es sobre un tipo de delito informático que debería considerarse en el código penal boliviano, es sobre el delito de destrucción, alteración, inutilización y daño a programas o documentos contenidos en redes o sistemas informáticos también conocido este delito en la clasificación de su tipología como los delitos de sabotaje informático a lo cual se pasara a exponer y explicar conceptos y teorías referente a esta clase de delito informático.

5.2. CONCEPTO SOBRE DELITO DE DESTRUCCIÓN, ALTERACIÓN, INUTILIZACIÓN Y DAÑO A PROGRAMAS O DOCUMENTOS ELECTRÓNICOS.

Como se expuso anteriormente sobre los tipos de delitos informáticos, se encontraron varios tipos de delitos informáticos y al desarrollo de los mismos se encontraron las clases de delitos informáticos, en el tema a desarrollar veremos que el delito informático de destrucción, alteración, inutilización y daño a programas o documentos electrónicos es un tema que se deja al descubierto en el código penal boliviano y este se enmarca dentro de los tipos de delitos de sabotaje informático a ese aspecto expondremos:

Para el Dr. Santiago de Acurio el acto de destrucción, alteración, inutilización y daño a programas o documentos electrónicos implica un delito de semejanza al sabotaje informático a lo cual nos dice que este es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema. Siendo los mecanismos para cometer este delito los siguientes:

1) **Bombas lógicas (logic bombs)**, es una especie de bomba de tiempo que debe producir daños posteriormente. Exige conocimientos especializados

ya que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro.

2) **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.
3) **Virus informáticos y malware**, son elementos informáticos, que como los microorganismos biológicos, tienden a reproducirse y a extenderse dentro del sistema al que acceden, se contagian de un sistema a otro, exhiben diversos grados de malignidad y son eventualmente, susceptibles de destrucción con el uso de ciertos antivirus, pero algunos son capaces de desarrollar bastante resistencia a estos.
4) **Ciberterrorismo**: Terrorismo informático es el acto de hacer algo para desestabilizar un país o aplicar presión a un gobierno, utilizando métodos clasificados dentro los tipos de delitos informáticos, especialmente los de los de tipo de Sabotaje, sin que esto pueda limitar el uso de otro tipo de delitos informáticos, además lanzar un ataque de terrorismo informático requiere de muchos menos recursos humanos y financiamiento económico que un ataque terrorista común.
5) **Ataques de denegación de servicio**: Estos ataques se basan en utilizar la mayor cantidad posible de recursos del sistema objetivo, de manera que nadie más pueda usarlos, perjudicando así seriamente la actuación del sistema, especialmente si debe dar servicio a mucho usuarios Ejemplos típicos de este ataque son: El consumo de memoria de la máquina víctima, hasta que se produce un error general en el sistema por falta de memoria, lo que la deja fuera de servicio, la apertura de cientos o miles de ventanas, con el fin de que se pierda el foco del ratón y del teclado, de manera que la máquina ya no responde a pulsaciones de teclas o de los botones del ratón, siendo así totalmente inutilizada, en máquinas que deban funcionar ininterrumpidamente, cualquier interrupción en su servicio por ataques de este tipo puede acarrear consecuencias desastrosas.
6) **Virus troyano.-** En informática, se denomina troyano o caballo de Troya (traducción literal del inglés Trojan horse) a un software malicioso que se presenta al usuario como un programa aparentemente legítimo e inofensivo

pero al ejecutarlo ocasiona daños. El término troyano proviene de la historia del caballo de Troya mencionado en la Odisea de Homero. Los troyanos pueden realizar diferentes tareas, pero, en la mayoría de los casos crean una puerta trasera (en inglés backdoor) que permite la administración remota a un usuario no autorizado. Un troyano no es estrictamente un virus informático, y la principal diferencia es que los troyanos no propagan la infección a otros sistemas por sí mismos

Encontramos también que el daño a un programa es conocido también como sabotaje contra un sistema en algunas legislaciones a lo cual se hace mención que el mismo es la destrucción o inutilización de un sistema o de parte de la información contenida en el. Quienes se entregan a estas operaciones reciben a veces el nombre de crackers o phreackers y emplean muy diferentes técnicas. Como ser las siguientes:

1) **La bomba de tiempo.** Es una instrucción que dispone la autodestrucción del programa, luego del transcurso de un lapso de tiempo establecido.

2) **Los virus.** Son elementos informáticos que, como los microorganismos biológicos, tienden a reproducirse y a extenderse dentro del sistema al que acceden, se contagian de un sistema a otro, exhiben diversos grados de malignidad y son, eventualmente, susceptibles de destrucción mediante ciertos antibióticos adecuados frente a los que pueden desarrollar incluso resistencia. Han sido definidos como “pequeños programas que, introducidos subrepticiamente en una computadora, poseen la capacidad de autorreproducirse sobre cualquier soporte apropiado que tenga acceso al ordenador afectando, multiplicándose en forma descontrolada hasta el momento que tienen programado actuar”

3) **Las rutinas cáncer.** Distorsionan el funcionamiento del programa y se autorreproducen al estilo de las células orgánicas alcanzadas por tumor maligno. Se trata, por cierto de una técnica parecida a la del virus.

Al respecto el experto en la materia René De Sola Quintero no dice que dentro de la clasificación de las naciones unidas sobre los delitos informáticos se encuentra lo que es el daño o modificaciones de programas o datos computarizados a lo cual dentro de este se encuentra lo que es el sabotaje informático siendo este delito 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) Virus: Es una serie de claves programáticas que pueden adherirse a los programas legítimos y proporciona 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.

b) Gusanos: Sé fábrica de forma análoga al virus con miras en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus por que puede regenerarse. En términos médicos podría decirse que un gusano es un tumor benigno, mientras que el virus es tumor maligno. Ahora bien, las consecuencias del ataque de un gusano puede ser tan graves como las del ataque de un virus: por ejemplo, un programa gusano subsiguiente se destruirá y puede dar instrucciones a un sistema informático de un banco que transfiera continuamente dinero a una cuenta ilícita.

c) Bomba lógica 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 contrario 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 conocer el lugar en donde se halla la bomba. (35)

Es que así la Brigada de Investigación Tecnológica de la Policía Nacional Española de fine el delito la estudiado como sabotaje informático y dice que este es el daños mediante la destrucción o alteración de datos, programas o documentos electrónicos contenidos en redes o sistemas informáticos.

Decimos que el delito de destrucción**,** alteración, inutilización y daño a programas o documentos electrónicos se encuentra clasificado como un delito de sabotaje a lo cual las diferentes legislaciones dicen que este delito es aquel delito por el cual se daña o se inutiliza al sistema de la computadora o los programas y documentos electrónicos o los datos existentes mediante medios informáticos como ser los virus, bombas lógicas, gusanos, la clase de delincuentes que cometen esta clase de delitos son personas intelectuales no siendo los mismos personas simples, siendo el siguiente punto a desarrollar el sujeto activo en el delito a explicar.

6. EL SUJETO ACTIVO Y PASIVO EN EL DELITO DE DESTRUCCIÓN, ALTERACIÓN, INUTILIZACIÓN Y DAÑO A PROGRAMAS O DOCUMENTOS ELECTRÓNICOS

En el análisis del delito de destrucción**,** alteración, inutilización y daño a programas o documentos electrónicos, es necesario analizar lo que es el delincuente su aspecto su perfil criminológico y el aspecto de sus victimas q que clase de persona mayormente es victima de este delito, pasando en los siguientes puntos a explicarlos:

35. **RICARDO** A. Guibourg, Jorge O. Alende, Elena M. Campanella. “Manual de Informática Jurídica”. Pág. 38-46

6.1. PERFIL CRIMINOLÓGICO DEL SUJETO ACTIVO EN EL DELITO DE DESTRUCCIÓN, ALTERACIÓN, INUTILIZACIÓN Y DAÑO A PROGRAMAS O DOCUMENTOS ELECTRÓNICOS.

En referencia a lo que es el sujeto activo en los delitos encontramos definiciones amplias de lo que clase de delincuentes existen y sus características como ser el trípode lombrosiano el cual nos hace referencia al atavismo que es la tendencia hereditaria a producir los caracteres de antepasados remotos la semejanza del hombre primitivo y el criminal, también se encuentra a Enrique Ferri quien nos habla de las causas del delito las cuales pueden ser el factor físico o telúrico, factores sociales y factores biológicos.

En la tesis de delito natural de Rafael Garófalo no habla lo que es la clasificación de los delincuentes, tomando en cuenta la investigación de Garófalo se clasifican los delincuentes en:

a) **Asesinos.** A este primer grupo pertenece los genuinos delincuentes. Se trata del inpio el que viola completamente la piedad; consiguientemente, carece también de probidad, pues este sentimiento dentro del proceso evolutivo es una adquisición posterior que supone la del primero. Mata con todas las agravantes, viola, asalta, roba; en una palabra, carece de todos los sentimientos altruistas.

b) **Delincuentes violentos.** A esta categoría pertenecen los criminales por defecto del sentimiento de piedad; consiguientemente, carece también de probidad, pues este sentimiento, si bien es debilitado. El mata o hiere, pero no como efecto de una simple anomalía interna si no porque ocurren poderosos factores externos. Puede delinquir por imitación (la obligatoriedad de la venganza que exige la reacción social ante la deshonra social, etc.). por arrebato pasional (ante una bofetada o un insulto grave), además también por carencia de

sensibilidad, que le impide ver el dolor ajeno, dificultando la aparición de sentimiento de simpatía.

c) **Delincuentes ímprobos ladrones.** Se trata de criminales por efecto del sentimiento altruista de probidad. Influyen en el, las causas externas del delito, tales como la tentación, la necesidad de adquirir alimentos, el deseo de brillar en la sociedad, etc.

d) **Los delincuentes cínicos lascivos.** Integran un sub grupo heterogéneo de delincuentes de difícil clasificación incluidos por Garófalo en la última edición de sui obra, llenando el vacio que existía en su clasificación para designar a aquellos que atentan contra el pudor, las buenas costumbres, etc.

Tras el análisis del delincuente habitual podemos comparar con el sujeto activo en el delito de destrucción**,** alteración, inutilización y daño a programas o documentos electrónicos, siendo prudente también estudiar lo que es el perfil que se da a conocer mayormente para el delincuente informático, que las personas que cometen los delitos informáticos son aquellas que poseen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información sensible, o bien son hábiles en el uso de los sistemas informatizados, aún cuando no desarrollen actividades que faciliten la comisión de este tipo de delitos. Se ha dicho que son personas listas, decididas, motivadas y dispuestas a aceptar un reto tecnológico. Los que los diferencia entre sí es la naturaleza del delito cometido. La persona que “entra” en un sistema informático sin intenciones delictivas es muy diferente del empleado de una institución financiera que desvía fondos de las cuentas de sus clientes.

Las principales características que presentan los sujetos activos de esta conducta delictiva son las siguientes:

a) En general, son personas que no poseen antecedentes delictivos.
b) La mayoría de sexo masculino.

c) Actúan en forma individual.

d) Poseen una inteligencia brillante y alta capacidad lógica, ávidas de vencer obstáculos; actitud casi deportiva en vulnerar la seguridad de los sistemas, características que suelen ser comunes en aquellas personas que genéricamente se las difunde con la denominación “hackers”.

e) Son jóvenes con gran solvencia en el manejo de la computadora, con coraje, temeridad y una gran confianza en sí mismo.

f) También hay técnicos no universitarios, autodidactas, competitivos, con gran capacidad de concentración y perseverancia. No se trata de delincuentes profesionales típicos, y por eso, son socialmente aceptados.

g) En el caso de los “hackers”, realizan sus actividades como una especie de deporte de aventura donde el desafío está allí y hay que vencerlo. Aprovechan la falta de rigor de las medidas de seguridad para obtener acceso o poder 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 sitio. Eso suele suceder con frecuencia en los sistemas en que los usuarios emplean contraseñas comunes o de mantenimiento que están en el propio sitio.

h) Dentro de las organizaciones, las personas que cometen fraude han sido destacadas en su ámbito laboral como muy trabajadoras, muy motivadas (Es el que siempre está de guardia, el primero en llegar y el último en irse).

i) Con respecto a los que se dedican a estafar, nos encontramos ante especialistas. Algunos estudiosos de la materia lo han catalogado como “delitos de cuello blanco”, (se debe a que el sujeto activo que los comete es poseedor de cierto status socio-económico.)

Es que así las personas que cometen los “**Delitos Informáticos**” son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son

hábiles en el uso de los sistemas informatizados, aún cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos.

Al respecto, según un estudio publicado en el Manual de las Naciones Unidas para la prevención y control de delitos informáticos (Nros. 43 y 44), el 90% de los delitos realizados mediante la computadora fueron ejecutados por empleados de la propia empresa afectada (**Insiders**). Asimismo, otro reciente estudio realizado en América del Norte y Europa indicó que el 73% de las intrusiones informáticas cometidas eran atribuibles a fuentes interiores y solo el 23% a la actividad delictiva externa (**Outsiders**).

El famoso criminólogo norte americano Edwin Sutherland señala un sinnúmero de conductas que considera como “delitos de cuello blanco”, aún cuando muchas de estas conductas no están tipificadas en los ordenamientos jurídicos como delitos, y dentro de las cuales cabe destacar las “violaciones a las leyes de patentes y fábrica de derechos de autor, el mercado negro, el contrabando en las empresas, la evasión de impuestos, las quiebras fraudulentas, corrupción de altos funcionarios, entre otros”. Asimismo, este criminólogo estadounidense dice que tanto la definición de los “delitos informáticos” como la de los “delitos de cuello blanco” no esta de acuerdo al interés protegido, como sucede en los delitos convencionales sino de acuerdo al sujeto activo que los comete. Entre las características en común que poseen ambos delitos tenemos que: “el sujeto activo del delito es una persona de cierto status socioeconómico, su comisión no puede explicarse por pobreza ni por mala habitación, ni por carencia de recreación, ni por baja educación, ni por poca inteligencia, ni por inestabilidad emocional.”

En el concepto del sujeto activo en el delito informático de destrucción, alteración, inutilización y daño a programas o documentos electrónicos encontramos que el delincuente tiene que ser una persona capaz de manipular la computadora o algún sistema informático o tener conocimiento por lo menos de cómo se maneja la computadora es que así a los expertos en este delito se los conoce con el nombre de:

Hacker.- Un hacker (del inglés hack, recortar), también conocidos como sombreros blancos es el neologismo utilizado para referirse a un experto en varias o algunas ramas relacionadas con la computación y telecomunicaciones: programación, redes de comunicaciones, sistemas operativos, hardware de red/voz. Usuario de ordenadores especializado en penetrar en las bases de datos de sistemas informáticos estatales con el fin de obtener información secreta. En la actualidad, el término se identifica con el de delincuente informático, e incluye a los cibernautas que realizan operaciones delictivas a través de las redes de ordenadores existentes.

Cracker.- Básicamente lo opuesto a un hacker, utilizan sus conocimientos para destruir y no obtener nada productivo, usan los conocimientos de otros para fines personales y solo se dedican a destruir y ocasionar perdidas. Entre las variantes de crackers están los que realizan Carding (Tarjeteo: uso ilegal de tarjetas de crédito), Trashing (Basureo, obtención de información en cubos de basura, tal como números de tarjetas de crédito, contraseñas, directorios o recibos); Phreaking y Foning (uso ilegal de las redes telefónicas) y los clásicos y llanamente llamados Piratas (gente del Warez) que se dedican a copiar software legal, música o vídeos, para regalarlo o venderlo por ahí.

Lammer.- Además de estos dos adjetivos que son los más malinterpretados hay otros especificativos dentro del tema de los hackers, estos son eleet (o elite) y lamer (o lammer). El adjetivo de elite se lo aplican determinados hackers para dar a entender que son superiores a la mayoría de los hackers ahora a caído en desuso pero de todas formas los que se llaman a sí mismos elite suelen estar más cerca de lamers. Por último lamer es todo aquel que o desconoce totalmente el mundo underground y se cree hacker por el mero hecho de saber donde bajarse programas utilizados por hackers y saber utilizarlos o bien se trata de gente sin conocimientos que se dedica a hacer mal uso del apelativo de hacker y se dedica a robar claves de correo, passwords de juegos sin otro sentido que el de darse importancia.

En esta clase de delito informático el delincuente puede ser que este cerca del objetivo a atacar o entre en contacto con algún tipo de acceso al sistema de su objetivo como se explico mayor mente que esta clase de delitos son cometidos por personas expertas en sistemas por medio de los virus, gusanos, bombas lógicas y otros medios informáticos. Decimos con todo lo explicado que el delincuente en el delito informático de destrucción, alteración, inutilización y daño a programas o documentos electrónicos,

es aquel sujeto que causa daño a un sistema o proceso de la información el cual es el documento electrónico por medios informáticos y técnicos relacionados a la informática siendo el sujeto un sujeto de clase culta ecdémica con estudios en el área con acceso al conocimiento sobre la computadora y otros medios informáticos con el pensamiento de reto y superación del sistema a colapsar que actúan de forma individual en su mayoría. (36)

6.2. EL SUJETO PASIVO EN EL DELITO DE DE DESTRUCCIÓN, ALTERACIÓN, INUTILIZACIÓN Y DAÑO A PROGRAMAS O DOCUMENTOS ELECTRÓNICOS.

Es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo. No ha sido posible conocer la verdadera magnitud de estos delitos, ya que la mayor parte de ellos no son descubiertos o no son denunciados a las autoridades responsables, a lo que se añade el temor de las empresas de denunciar este tipo de ilícitos por el desprestigio y su consecuente pérdida económica que pudiera ocasionar.

El sujeto pasivo con mayor precisión es la persona titular del bien jurídico que el legislador protege y sobre la cual recae la actividad típica del sujeto activo. En primer término tenemos que distinguir que sujeto pasivo ó víctima del delito es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo, y en el caso de los “delitos informáticos” las víctimas pueden ser individuos, instituciones crediticias, gobiernos, etcétera que usan sistemas automatizados de información, generalmente conectados a otros.

El sujeto pasivo del delito que nos ocupa, es sumamente importante para el estudio de los “delitos informáticos”, ya que mediante él podemos conocer los diferentes ilícitos que cometen los delincuentes informáticos, con objeto de prever las acciones antes mencionadas debido a que muchos de los delitos son descubiertos casuísticamente por el desconocimiento del modus operandi de los sujetos activos.

---

36. **SANTIAGO** Acurio Del Pino. “Delitos Informáticos 16-17

Se reconoce que para conseguir una prevención efectiva de la criminalidad informática se requiere, en primer lugar, un análisis objetivo de las necesidades de protección y de las fuentes de peligro. Una protección eficaz contra la criminalidad informática presupone ante todo que las víctimas potenciales conozcan las correspondientes técnicas de manipulación, así como sus formas de encubrimiento. Concretizando la victima en el delito de destrucción, alteración, inutilización y daño a programas o documentos electrónicos son individuos, instituciones crediticias, gobiernos, etcétera que manejan la computadora y los diferentes medios donde se puede almacenar la información ya que estos están compuestos por programas ya que el delito es la que va en contra de la programación existente y los documentos dentro de los mismos siendo estos apreciados para sus titulares de una forma económica o importante como prueba de validez para algo. (37)

7. LEGISLACION COMPARADA SOBRE EL DELITO DE DESTRUCCIÓN, ALTERACIÓN, INUTILIZACIÓN Y DAÑO A PROGRAMAS O DOCUMENTOS ELECTRÓNICOS.

7.1. INTRODUCCIÓN.

En varios estados el delito estudiado se encuentra ya tipificado siendo que en Bolivia este delito se cree tipificado o por lo menos que por analogía se sanciona con el **Artículo 363 bis. (MANIPULACION INFORMATICA),** que al respecto dice “el que con la intención de obtener un beneficio indebido para sí o un tercero, manipule un procesamiento o transferencia de datos informáticos que conduzca a un resultado incorrecto o evite un proceso tal cuyo resultado habría sido correcto, ocasionando de esta manera una transferencia patrimonial en perjuicio de tercero, será sancionado con reclusión de uno (1) a cinco (5) años y con multa de sesenta (60) a doscientos (200) días” y que al análisis a desarrollar en el capitulo III, en la parte de las generalidades no puede ser así, a ese aspecto para desarrollar con mayor exactitud lo que es el delito estudiado analizaremos las diferentes legislaciones:

37. **SANTIAGO** Acurio Del Pino. “Delitos Informáticos 16-17

7.2. LEGISLACIÓN EXTRANJERA.

Legislación Española.

En el código penal español de 1995 contiene normas específicas relativas a conductas que tienen a sistemas o a elementos informáticos como objeto de ataque o como instrumento del delito. A los delitos contra los sistemas informáticos que afecten a elementos físicos del mismo, se les aplicará las reglas destinadas a comportamientos semejantes dirigidos contra otros objetos. Así, al hurto, robo, apropiación indebida, estafa, se sancionarán de acuerdo con los criterios interpretativos de cada uno de ellos. Lo mismo sucede con los ficheros de información o con los programas contenidos en soportes de almacenamiento masivo cuando es el objeto físico en el que se encuentran grabados (disquete, cinta, disco duro, CD- ROM, etc.).

Considerando la variedad de posibilidades que pueden darse, el análisis se hará distinguiendo cinco grupos: 1) Borrado, alteración o utilización de datos, programas o documentos electrónicos, denominado comúnmente sabotaje informático, debe ser analizado desde la perspectiva de los daños, incluyéndose los causados en los propios sistemas o elementos físicos de los mismos, 2) acceso ilícito a sistemas informáticos, se incluye el espionaje electrónico, el apoderamiento de datos, ficheros y programas e incluso los daños cuando este sea el fin que se pretenda y se cause. Cuando el acceso ilegítimo es la vía utilizada para obtener un beneficio patrimonial propio o de tercero (transferencias electrónicas de fondos, por ejemplo) se analizará el hecho en los delitos cometidos a través del sistema informático; 3) protección de programas de ordenador, conductas que recaen en la propiedad intelectual; 4) utilización ilegítima de sistemas o elementos informáticos, modalidad de uso prevista expresamente para los terminales de comunicación; 5) vulneración de la intimidad.

La parte que nos interesa analizar en la legislación de España es aquella que protege penalmente la destrucción, alteración, inutilización y daño a programas o documentos electrónicos, siendo este el primer grupo señalado que debe ser denominado comúnmente como sabotaje informático.

En el código español en su **Artículo 264.** Expresa en sus parágrafos 1 y 2 lo siguiente:

1. Será castigado con la pena de prisión de uno a tres años y multa de doce a veinticuatro meses el que causare daños expresados en el Artículo anterior, si concurriere alguno de los supuestos siguientes:

1.º Que se realicen para impedir el libre ejercicio de la autoridad o en venganza de sus determinaciones, bien se cometiere el delito contra funcionarios públicos, bien contra particulares que, como testigos o de cualquier otra manera, hayan contribuido o puedan contribuir a la ejecución o aplicación de las Leyes o disposiciones generales.
2. º Que se cause por cualquier medio infección o contagio de ganado.
3. º Que se empleen sustancias venenosas o corrosivas.
4. º Que afecten a bienes de dominio o uso público o comunal.
5. º Que arruinen al perjudicado o se le coloque en grave situación económica.

2. La misma pena se impondrá al que por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos. Como se explico en la legislación española lo que se hace en los delitos informáticos es aplicar las reglas destinadas a comportamientos semejantes dirigidos contra otros objetos, es así que el delito de destrucción, alteración, inutilización y daño a programas o documentos electrónicos como un delito informático este se encuentra tipificado en el capitulo de los daño se encuentra en su articulo 264. Como se explico la diferenciación de lo que es el dato el programa y documento electrónico explicamos lo que es la acción de dañar, alterar, inutilizar, y destruir en el delito que afecta al programa o documento electrónico. (38)

Respecto a la conducta típica “dañar”, centrada en los elementos lógicos, significa destruir, deteriorar, inutilizar o alterar datos, programas o documentos electrónicos. Así está establecido expresamente en el artículo 264.2, a través de una formulación tan amplia que pareciera aceptar implícitamente que pudiera haber otros elementos lógicos en los que recayeran las modalidades de conducta.

38. **CHILE** “Biblioteca Del Congreso Nacional de Chile Departamento de Estudios” documento digital

Con relación a los daños se discute si es necesario que se altere la sustancia de la cosa y si es necesario que se cause un perjuicio patrimonial efectivo al sujeto pasivo. La opinión mayoritaria mantiene la existencia del delito cuando se priva al propietario del valor de uso a que aparecía destinada la cosa dañada, entre otras razones porque la exigencia que se afecte la estructura material del objeto no está contenida en el Código y porque en las referencias a la inutilización (Art. 264.2 y 265) se acogen los casos en los que simplemente se destruye ese valor. El sector minoritario considera que el delito de daños significa que se afecte la esencia o sustancia de la cosa, de manera que no serían constitutivos del delito los casos en los que permaneciendo inalterada la estructura material del objeto, sólo se lesiona el valor de uso que tiene para su propietario. Un sector intermedio estima que el término "inutilización" es perfectamente congruente con la exigencia de que en los daños se afecte la sustancia, que determine, aún en forma mínima, un menoscabo de la cosa que incide en su propia existencia y suponga una pérdida de valor real independiente de los perjuicios derivados de la imposibilidad de uso, comprendiendo, en todo caso, la pérdida, corrupción o degradación del objeto, así como la alteración o inutilización.

Las referencias del Art. 264.2 a "por cualquier medio" o "de cualquier modo", conducen a entender que dentro del tipo agravado de la norma se incluyen las conductas dirigidas directamente a dañar ciertos elementos físicos que necesariamente comportarán la destrucción de datos. Ahora bien, la destrucción, que determina la existencia del delito del Art. 264.2, debe entenderse como desaparición completa y definitiva de los datos, programas o documentos (Por cualquier forma: destrucción del soporte, interferencias magnéticas, eliminación de enlaces, etc.), en el sentido que no sea posible la recuperación íntegra de los mismos. La alteración, cualquiera que sea su forma (añadiendo nuevos datos, borrando parcialmente los existentes, etc.), debe suponer una perturbación funcional definitiva, esto es, que los datos acaben teniendo un contenido distinto al original. La inutilización, es equivalente a la desaparición de su capacidad funcional, como puede ocurrir cuando se les protege con una clave de acceso desconocida para el titular. La simple ocultación del fichero, no daría lugar al delito, a menos que lo convierta en irrecuperable. Así, la destrucción, la alteración, la inutilización o el daño han de significar el cambio definitivo de la integridad de los

datos, haciendo imposible su utilización o restauración tal y como estaban antes de la realización de la conducta.

Legislación francesa.

En la legislación francesa en lo que es el delito de destrucción, alteración, inutilización y daño a programas o documentos electrónicos encontramos que se diferencia de lo que es el delito de alteración de datos ya que se hace la diferenciación en dicha legislación de lo que es el dato y las demás manifestaciones de la informática. En el Artículo 323-2. “El hecho de obstaculizar o alterar el funcionamiento de un sistema de tratamiento automatizado de datos será castigado con tres años de prisión y multa de 45.000 euros”, encontrando así la acción de alterar o obstaculizar el funcionamiento de un sistema de tratamiento automatizado de datos la cual como se explico en la legislación española la acción de alterar implica el hecho de suponer una perturbación funcional definitiva, esto es, que su funcionamiento acabe teniendo un contenido distinto al original y una aplicabilidad diferente o que no pueda realizar la funciones esperadas. (39)

Legislación alemana.

Como se explico en la legislación francesa la legislación alemana busca diferenciar lo que es el delito de destrucción, alteración, inutilización y daño a programas o documentos electrónicos ya que este delito es conocido como el delito de sabotaje informático, en si la finalidad perseguida por la legislación alemana, al crear el tipo de sabotaje informático diferenciado del tipo de alteración de datos, fue sancionar con mayor severidad las acciones que atentan contra procesos de datos que sean de importancia esencial para una empresa o establecimiento industrial ajenos o para la administración. Estas acciones pueden recaer en los equipos de procesamiento de datos, en los soportes y en los datos mismos. La doctrina entiende que es sancionado penalmente el que arremete a equipos o soportes de datos suyos en los que otras personas tengan un interés jurídicamente protegido o si borra datos que el mismo hubiera almacenado y que fueran procesados para terceros cuyo interés en su existencia se perjudica.

39. **CHILE** “Biblioteca Del Congreso Nacional de Chile Departamento de Estudios” documento digital

Es su articulo 303b dice. “Quien destruya una elaboración de datos que sea de esencial importancia para una industria ajena, una empresa ajena o una autoridad,
1. cometiendo el hecho de acuerdo al párrafo 303.a.II, o
2. destruyendo, dañando, inutilizando, eliminando o alterando una instalación de elaboración de datos o un soporte de datos, será castigado con pena de privación de libertad de hasta cinco años o con multa.
II. La tentativa será punible”.

Al hablar de la acción de destruir una elaboración de datos, se explica que este se refiere también al sistema al programa el cual se encarga también de la elaboración de datos y que estos son de vital importancia para la empresa que las desarrolla, en el numeral 2 del parágrafo I se habla de la destrucción, daño, inutilización, eliminación o alteración de una instalación de elaboración de datos o un soporte de datos, a lo cual se explica ya que los soportes son medios por los cuales se almacenan estos datos y se pueden transportar son de vital importancia y al hablar de una instalación de elaboración de datos puede corresponder al medio o lo material es decir al programa o el conjunto de maquinarias. (40)

Legislación chilena.

La legislación chilena como la alemana realiza la diferencia entre lo que es el dato y la programación o sistema ya que en su Ley Nº 19.223 tiene como finalidad proteger a un nuevo bien jurídico como es: “la calidad, pureza e idoneidad de la información en cuanto a tal, contenida en un sistema automatizado de tratamiento de la misma y de los productos que de su operación se obtengan”. En relación a nuestro tema en la legislación chilena en su Artículo 1. Nos habla de que “El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo.

40. **CHILE** “Biblioteca Del Congreso Nacional de Chile Departamento de Estudios” documento digital

Analizando el articulo en centramos que la destrucción o inutilización de un sistema es parte del delito de sabotaje informático el cual nos interesa y que al hablar de sistema de tratamiento de información se puede entender como el programa por el cual se realiza el tratamiento del dato o la información es que así el articulo también se extiende a sus partes y componentes o partes la diferencia con el dato se encuentra en el articulo Artículo 3. Que dice “El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información, será castigado con presidio menor en su grado medio”. Es que así en la legislación penal chilena se encuentra la diferencia entre dato y el sistema operativo es decirla programación de la computadora. (41)

Legislación colombiana.

En la legislación colombiana sigue la corriente alemana y española es decir mixta si bien se encuentra una diferenciación se lo tipifica en un solo artículo en un solo marco sancionador como se expresa en su artículo 269D: DAÑO INFORMÁTICO. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

En este aspecto en el mismo articulo habla de dos aspectos uno de lo que es la destrucción, daño, borrar, deteriorar, alterar o suprimir datos informáticos, al aspecto seguido de un “o un sistema de tratamiento de información” como medio de unir este al aspecto de la protección no solo de los datos si no del sistema o programa mismo de la computadora y las partes que se pueden tocar que la componen. (41)

41. **SANTIAGO** Acurio Del Pino. “Delitos Informáticos”

CAPITULO III
PROYECTO DE CREACION DEL TIPO PENAL

1. GENERALIDADES

Como se explico en anteriores puntos la diferencia en lo que son los diversos tipos de delitos informáticos y que clases de delitos existen dentro de la mismas, es en ese sentido que al hablar del delito de destrucción, alteración, inutilización y daño a programas o documentos electrónicos hablamos de un delito no existente en la legislación boliviana como se explico reiteradas lo que se dice en el **articulo 363 bis** la manipulación informática nos habla solo de la manipulación de un procesamiento de datos causando un resultado incorrecto o evite un procesamiento ocasionando la perdida patrimonial, pero en este articulo nunca se habla del que ocasionare daño, destrucción, alteración inutilización de un programa o sistema o documento electrónico ya que bien el dato es parte del proceso de la información el medio por el cual es el programa comúnmente conocido como el sistema de la computadora por el cual se pueden realizar varias operaciones siendo el programa una serie de instrucciones por el cual se trabajan los datos y se procesan para dar un resultado que después será almacenado en una carpeta llamada documento electrónico que se puede almacenar en diferentes clases de soportes magnéticos.

Adentrándonos a la norma entendemos que esta debe cumplir el rol de protección en lo que corresponde en el articulo **363 bis** se protege la manipulación del dato y al hablar del delito de destrucción, alteración, inutilización y daño a programas o documentos electrónicos no es lo mismo que la manipulación del dato informático con fines de causar resultados incorrectos ocasionado perdida patrimonial y en el articulo **363 ter** nos habla de la alteración, acceso y uso indebido de datos informáticos no señala el delito tratado en el tema desarrollado como se explico en los delitos informáticos se encuentra varias clases de tipos de delitos en nuestra legislación, en lo que corr4esponde a la tipificación cuando la gente habla de delitos informáticos y algunos conocedores del derecho piensan que la parte de los delitos informáticos ya esta

cubiertos con estos dos artículos no acertando en su pensamiento no se puede hablar del delito de manipulación informática en los delitos de sabotaje mas por el hecho de que el fin buscado no es la manipulación del dato si no la destrucción del mismo o del programa es que así como dice el principio de legalidad al tipificar un delito si este no existe no es delito es decir “nulla crimen, nulla poena sine previa lege” que quiere decir no hay crimen, no hay pena sin ley previa.

2. TEORIA PENAL PARA LA CREACION DE LA NORMA.

En la propuesta de la norma a crearse podemos expresar que esta debe ser según conforme el manual de técnicas normativas DECRETO SUPREMO Nº 25350 y teorías para su aplicación es que para eso el uso de palabras que no expresen un doble sentido, tengan simplicidad y esta se entienda para que el interprete, tomando en cuenta el articulo 20 que es el contenido de cada articulo que en sus puntos dice 20.1. Como unidad básica de cada disposición normativa, el artículo comenzará por una sola idea que debe ser susceptible de desarrollo mediante sucesivas oraciones subordinadas, cada una de las cuales se expresará siguiendo siempre un orden lógico de exposición. 20.2. Cada artículo no debe contener más de un tema, si bien es posible desarrollar dicho tema a través de varios párrafos separados. A lo cual el contenido del articulo seria **“El que por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos de esencial importancia para una empresa o entidad pública la pena de prisión será de uno a cinco años y con multa asta de 60 a 200 días.”** Para explicar el contenido tomaremos en cuenta teorías penales, tomaremos en cuenta la conformación de la tipificación comenzando encontramos:

La objetividad jurídica.- la objetividad jurídica hace referencia a la precisión que el legislador establece en la protección de determinados bienes del ser humano, es la precisión que el legislador hace al crear la ley para la protección penal, al respecto en la norma que se pretende incorporar el bien jurídico protegido son los **programas y documentos** electrónicos aparte en la objetividad también se encuentra que el

legislador establece la conducta delictiva por el cual se piensa afectar el bien protegido en la tipificación realizada es aquella por el cual se **destruya, altere, inutilice o de cualquier otro modo dañe** esta conducta en la que atenta contra el bien jurídico protegido.

Elemento subjetivo.- cuando se habla del elemento subjetivo se dice que se pasa a analizar la conducta que atenta a esa objetividad jurídica, en si al decir el elemento subjetivo hacemos referencia aquel aspecto interno que se encuentra descrito en el tipo penal, es decir para castigar la conducta sea dolosa o culposa en el caso del tipo a desarrollar encontramos que el ismo es dolosa ya que el hecho de dañar por cualquier medio, hay una conducta de conocimiento y en la esencia de conocer lo bueno de lo malo, a lo que uno realiza con conocimiento es el dolo en el articulo 14 del código penal nos explica lo que es el dolo y dice que “actúa dolosamente el que realiza un hecho previsto en un tipo penal con conocimiento y voluntad. Para ello es suficiente que el autor considere seriamente posible su realización y acepte esta posibilidad”.

Elemento sujeto activo.- este elemento hace referencia a la búsqueda de una cualidad común o general o particular o especial de la persona o sujeto que la realiza el tipo penal y el sujeto activo es la persona que realiza el acto criminal.

Elemento material.- hace referencia a la descripción de la conducta de la conducta en el tipo penal, el elemento material en si es aquella palabra que describe genéricamente la acción prohibida es así que hay tipos penales en lo cuales son sencillo de encontrar este elemento material en el caso de la figura del tipo penal desarrollado el elemento material seria destruya, altere, inutilice o de cualquier otro modo dañe, conteniendo así la figura penal elemento material.

Elemento del objeto material.- cuando se habla del objeto material decimos que este corresponde a aquel elemento donde recae la acción prohibida, en el tipo penal el objeto en el cual recae la acción prohibida son las **redes, soportes o sistemas informáticos** los cuales son parte de empresas o entidades publicas.

Elemento del resultado.- cuando se habla de este elemento se habla de cual es el resultado de la acción en este encontramos que es la destrucción y el daño, inutilización de redes, soportes o sistemas informáticos.

Elemento del sujeto pasivo.- es la persona que recibe el daño, la persona la cual sufre el daño en su patrimonio es que así en la figura del tipo penal desarrollado encontramos que el sujeto pasivo son las empresas o entidades públicas que trabajan con sistemas informáticos.

Precepto primario.- es la descripción de la conducta prohibida el cual es **destruya, altere, inutilice o de cualquier otro modo dañe.**

Precepto secundario.- es la sanción este seria en el tipo de **uno a cinco años y con multa asta de 60 a 200 días. (42)**

De acuerdo al DECRETO SUPREMO Nº 25350 Manual de Técnicas Normativas (43) en su artículo 21 el tipo penal tiene que tener una numeración correlativa y un nombre jurídico debiendo estar el mismo en el capito correspondiendo del bien jurídico tutelado siendo así que correspondiendo el mismo llevar el nombre jurídico de **Artículo 363 Cuater. (DAÑO A PROGRAMAS INFORMATICOS O DOCUMENTOS ELECTRÓNICOS).** El que por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos de esencial importancia para una empresa o entidad pública la pena de prisión será de uno a cinco años y con multa asta de 60 a 200 días.

En el tipo penal al colocar como referencia "*por cualquier medio*" o "*de cualquier modo*", conducen a entender que dentro del tipo agravado de la norma se incluyen las conductas dirigidas directamente a dañar ciertos elementos físicos que necesariamente comportarán la destrucción de los programas o documentos electrónicos.

---

42. **RODOLFO** Illanes "Apunte de Derecho Penal I"
43. **BOLIVIA** "DECRETO SUPREMO Nº 25350 Manual de Técnicas Normativas" Texto digital

Taras el análisis del tipo penal desenvuelto en el trabajo pasamos a lo que es la parte de la propuesta del tipo penal como este será que objeto buscara cual es el fin del mismo.

3. PROPUESTA DE LEY SOBRE LA INCOORPORACION DEL TIPO PENAL SOBRE DESTRUCCIÓN, ALTERACIÓN, INUTILIZACIÓN Y DAÑO A PROGRAMAS O DOCUMENTOS.

CONTENIDO.

- Exposición de motivos.
- Marco Constitucional.
- Texto de la propuesta de ley.

3.1. EXPOSICIÓN DE MOTIVOS

Desde la aparición de la informática, el hombre se ha satisfecho de sus ventajas de uso ya que la misma tiene aplicaciones sorprendentes y con la evolución de la informática la computadora ha dado un gran salto a la evolución en la inteligencia artificial con el uso de programas y con el almacenamiento de información en documentos electrónicos,

Al hablar del delito informático en el presente encontramos que este delito cada vez se hace mas frecuente en nuestro medio ya no tan solo como la manipulación de datos o la alteración, acceso y uso de datos si no que estos delitos van mas allá como ser el uso indebido de la computadora la destrucción de sistemas informáticos daño a

soportes informáticos o redes y previendo lo que puede suceder en un futuro no muy lejano, es que me veo en la facultad de exponer que en la legislación penal boliviana encontramos la falta de tipificación como se evidencio en un comentario del periódico la razón se dice que a falta de tipificación sobre el delito informático este se tipifica con los delitos de los artículos 363 bis y ter pero no se puede hablar de delito informático en esos casos de acceso ilícito a sistemas informáticos o muy bien a la destrucción o daño a sistemas, redes o soportes informáticos o muy la alteración de documentos electrónicos y otros delitos que están a posibilidades de cometerse, es que para eso en otras legislaciones se connota el hecho de que su legislación penal sobre los delitos informáticos es amplia y no cerrada como en la legislación boliviana, el tipo penal que se propone favorece a las entidades publicas y privadas siendo aquellas que trabajen con sistemas o programas informáticos los mismos que como grandes entidades se encuentra en la necesidad de proteger el medio con la cual se trabaja.

3.2. MARCO CONSTITUCIONAL.

La Constitución Política del Estado Plurinacional del Bolivia, promulgada el 7 febrero del 2009, sienta las bases para la aprobación y puesta en vigencia de la Ley contra el delito de destrucción, alteración, inutilización y daño a programas o documentos, sustentada en los siguientes artículos:

Artículo 52.

II. El Estado garantizará el reconocimiento de la personalidad jurídica de las asociaciones empresariales, así como las formas democráticas organizativas empresariales, de acuerdo con sus propios estatutos.

Artículo 54.

II. Es deber del Estado y de la sociedad la protección y defensa del aparato industrial y de los servicios estatales.

3.3. TEXTO DE LA PROPUESTA DE LEY.

LEY CONTRA EL DELITO DE DESTRUCCIÓN, ALTERACIÓN, INUTILIZACIÓN Y DAÑO A PROGRAMAS O DOCUMENTOS.

CAPÍTULO I
DISPOSICIONES GENERALES

Articulo 1. (OBJETO).
El objetivo de la presente ley es establecer mecanismos y procedimientos para la prevención y sanción sobre el delito de destrucción, alteración, inutilización y daño a programas o documentos electrónicos.

Articulo 2. (ALCANCE). Las disposiciones de la presente ley, serán aplicables:

I. A los funcionarios o empleados, que manipulen sistemas informáticos de empresas públicas o privadas, entidades públicas donde el trabajo con tal sistema o programación o documentos electrónicos tengan un va.lor importante para el Estado o empresa.

II. A las particulares que irrumpan en sistemas informáticos con fines de destruir, alterar, inutilizar y dañar a programas o documentos electrónicos con el fin de favorecerse o favorecer a terceros.

III. A aquellos que se dedican a la fabricación de software o programas y se vean afectados por terceros que dañen su producción intelectual antes de que este sea concretado.

CAPITULO II

COMPETENCIA Y SANCIONES EN CASOS DESTRUCCIÓN, ALTERACIÓN, INUTILIZACIÓN Y DAÑO A PROGRAMAS O DOCUMENTOS.

Articulo 3. (INSTANCIAS COMPETENTES).

I. Las Entidades públicas, empresas públicas y privadas realizaran la denuncia ante el Ministerio Publico o la Fuerza Especial de Lucha Contra el Crimen mediante su representante legal o bien mediante la directiva de acuerdo a su norma interna.

II. La denuncia ante instancias penales no librara la acción ante instancia civil, en caso de pérdidas económicas pudiendo solicitar el resarcimiento y pago de daños por perdidas.

Articulo 4. (DENUNCIA).

La denuncia podrá ser presentada por la víctima, su representante legal o cualquier persona natural o jurídica, en forma verbal o escrita.

Artículo 5. (OBLIGACIÓN DE DENUNCIAR).

I. Las servidoras y los servidores públicos que conozcan de la comisión de actos de destrucción, alteración, inutilización y daño a programas o documentos en contra de una empresa o entidad pública, tienen la obligación de denunciar ante las instancias competentes.

II. En caso que las servidoras y los servidores públicos incumplan esta obligación serán procesados/as y sancionados de acuerdo a ley.

Articulo 6. (SANCIONES).

I. En caso de los funcionarios aparte de la vía penal se regulara de acuerdo a la norma interna de la entidad o empresa pudiendo acudir a vi acivila aparte de la penal.

II. La empresa privada podrá optar por la vía civil primeramente antes de la vía penal, en caso de incumplimiento se podrá recurrir a la vía penal.

Articulo 7. (AGRAVANTES).

Se agravara el delito de destrucción, alteración, inutilización y daño a programas o documentos en el caso de:

a) Si hubiese participación de dos o más personas en complot para dañar.
b) Si del delito surgiese una gran pérdida material o intelectual para la entidad o empresa publica.
c) Cuando se involucre a menores de edad.

CAPITULO III

PROCEDIMIENTOS EN CASOS DE DENUNCIAS POR DESTRUCCIÓN, ALTERACIÓN, INUTILIZACIÓN Y DAÑO A PROGRAMAS O DOCUMENTOS

Artículo 8. (VÍA ADMINISTRATIVA).

Esta se realizara de acuerdo a la normativa interna de la empresa privada o en su caso de las instituciones públicas de acuerdo su reglamento interno pudiendo llevarlo a vía penal o civil.

Articulo 9. (VIA CIVIL).

Podrá presentarse ante juzgados en lo civil en caso de pérdidas económicas para las empresas privadas de acuerdo a la cuantía de la perdida por el delito pudiendo exigir la reparación del daño.

Articulo 10. (VÍA PENAL).

Debiendo presentar las entidades o empresas publicas denuncia mediante la máxima autoridad o representante legal de la empresa o entidad afectada.

CAPITULO IV

DISPOSICIONES FINALES

DISPOCISION FINAL PRIMERA

Articulo único. (INCORPORACION DEL ARTICULO AL CODIGO PENAL BOLIVIANO).

Se incorpora el presente articulo al capitulo XI de delitos informáticos de acuerdo al manual de técnica legislativa DECRETO SUPREMO Nº 25350.

Artículo 363 Cuater. (DAÑO A PROGRAMAS INFORMATICOS O DOCUMENTOS ELECTRÓNICOS). El que por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos de esencial importancia para una empresa o entidad pública la pena de prisión será de uno a cinco años y con multa asta de 60 a 200 días.

DISPOSICIÓN FINAL SEGUNDA (Vigencia)

La presente ley entrará en vigencia, a partir de la fecha de su promulgación.

4. CONCLUSION Y CRITICA

En el transcurso del trabajo desarrollado el material que se obtuvo fue de la biblioteca en el Ministerio de Justicia y que al hablar con juristas de nuestro medio expusieron que el ámbito de los delitos informáticos estaba ya cubierto no había delito que cubrir siendo así que note la falta de conocimiento del abogado actual al tema ya que muchos abogados no conocieron lo que es la computadora en su plenitud ni la rama de la ciencia de la informática mi persona como ellos no tiene mucho conocimiento en la rama a lo cual se consulto a profesionales en el estudio de la informática a lo cual muchos de estos expusieron que la tipificación realizada en el código penal no cubría lo que son los posibles delitos a cometerse con la computadora y la técnica informática, exponiendo mi tema a los licenciados en informática me dijeron que mi idea no estaba mal pero que se debía abarcar mas.

En conclusión la monografía desarrollada tiene la misión de orientar sobre la falta de tipificación en los delitos informáticos, orientado por licenciados en la carrera de informática se desarrollo la tipificación sobre la protección penal sobre la destrucción, alteración, inutilización y daño a programas o documentos electrónicos".

5. RECOMENDACIÓN Y SUGERENCIAS

El delito informático en nuestro medio es un delito que se desarrolla reciente mente a lo cual el legislador, las autoridades judiciales y las comisiones de codificación del código penal deberían considerar:

- Que mediante instituciones se brinden capacitaciones sobre los delitos informáticos con expertos en la materia como expositores.
- Que se tome en cuenta la sugerencia de expertos en la rama de la informática en las comisiones de codificación del código penal.
- Brindar mayor apoyo a la policía para que se cumpla la especialidad de la división de lucha contra los delitos informáticos con mayor eficacia y celeridad.
- Que las penas en contra de estos delitos no sean muy flexibles para que la gente se anime a denunciarlos.
- Buscar la diferenciación de la acción de los delitos informáticos de unos y otros para que se cumpla con mayor eficacia y cumplimiento de la norma.

ANEXOS

6. BIBLIOGRAFIA

1. **ETORRE** Giannantonio, “Informática y Derecho” Volumen 1. Editorial Buenos Aires – Argentina 2004.

2. **RODOLFO** Pagano, “Informática y Derecho” Volumen 2. Editorial Buenos Aires – Argentina 2005.

3. **RENATO** Borruso, “informática y Derecho” Volumen 5. Editorial Buenos Aires – Argentina 2008.

4. **MAURIE** Claude Mayo “Informática Jurídica”. Editorial jurídica de Chile 2000.

5. **HERMILIO** Tomas Azpilsueta “Derecho Informático” Editorial Ebeledo – Perrot. Buenos Aires – Argentina 1999.

6. **RICARDO** A. Guibourg, Jorge O. Alende, Elena M. Campanella. “Manual de Informática Jurídica”.

7. **RENE** de Sola Quinteros. “Delitos Informáticos”, Editorial Colex - Venezuela 2009.

8. **SANTIAGO** Acurio Del Pino. “Delitos Informáticos”, México 2010.

9. **CHILE** “Biblioteca Del Congreso Nacional de Chile Departamento de Estudios” documento digital Santiago de Chile 2004.

10. **BOLIVIA “**Código Penal Boliviano” Editorial Temis 2010

11. **BOLIVIA** “DECRETO SUPREMO Nº 25350 Manual de Técnicas Normativas” Texto digital.

12. **RODOLFO** Illanes “Apunte de Derecho Penal I” Gestión 2008 La Paz – Bolivia.

13. "WIKIPEDIA historia de la información" Internet texto digital.

14. "DELITOSINFORMÁTICOS.COM" pagina Web

15. "DERECHOINFORMATICO.COM" pagina Web

16. "WWW.UNODC.ORG". www.11uncongress.org pagina web

17. WWW.LARAZON.COM.BO pagina web