# UNIVERSIDAD DEL PACIFICO
# ESCUELA DE NEGOCIOS

## FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS
## RAMIRO BORJA Y BORJA

**PLAN DE TESIS PREVIA A LA OBTENCIÓN DEL TÍTULO DE ABOGADO DE LOS TRIBUNALES Y JUZGADOS DE LA REPUBLICA DEL ECUADOR CON MENCIÓN EN**

COMERCIO INTERNACIONAL

# DELITOS INFORMÁTICOS: PREVENCIÓN, MODIFICACIÓN Y CREACIÓN DE NUEVOS TIPOS

**Francisco X. Jaramillo Barea** **Ab. Hugo F. Landívar Orellana**

**Guayaquil - Ecuador**

**Enero – 2012**

JARAMILLO, Francisco X., Delitos Informáticos: Prevención, Modificación y Creación de los Nuevos Tipos Penales. Guayaquil: UPACIFICO, 2011, 61p.

DIRECTOR: PROF. ABG. HUGO LANDIVAR (Trabajo de Conclusión de Carrera-TCC presentado a La Facultad de Derecho de La Universidad Del Pacífico).

RESUMEN

Hablar de informática o computación, es hablar de un tema apasionante en todos los sentidos, nos hace soñar sobre el futuro, nos hace discutir sobre las tecnologías nuevas, apropiadas personalmente y sus costos, las políticas para desarrollar una industria, institución y un país.

Pero fundamentalmente hablar de computación o informática es hablar de la necesidad de recursos humanos capacitados, de los cambios en la forma de trabajar y los nuevos empleos, de las nuevas posibilidades de desarrollo individual y hasta de aprendizaje, con la inserción de la computadora; hablar de computación es hablar de educación, de progreso y bienestar. Y al mismo tiempo hemos descubierto que algunos entes lo utilizan de manera dolosa, para vulnerar. Que en un concepto más general, hablar de informática, es hablar de oportunidades, que sin los debidos controles y prevenciones, será usada para mal.

Actualmente vivimos en lo que podemos denominar la "era digital", etapa que cómo se puede apreciar o se podrá más adelante, no es constante y regular, sino más bien todo lo contrario. Es una etapa irregular y en inconstante ritmo evolutivo, expandiéndose no solo en un sentido, sino en una amplia gama de ramas.

Permitiendo así, un gran avance a la sociedad, tanto científico, como al ser humano en general, permitiendo una serie de acciones que aunque tienen cabida en el pensamiento humano, no se encontraban concretas, ni concebidas en el mundo, brindando no solo conocimiento, sino también velocidad, y comodidades a gran cantidad de usuarios que disfrutan del uso y goce de la tecnología en nuestros días.

Aquí es donde podemos ver que no existe mal, que por bien no venga, porque así como en la actualidad nos vemos enriquecidos de una amplia gama de herramientas que nos brindan, agilidad facilidad, comodidad y soluciones, es así también como todas estas tecnologías vulneran nuestro patrimonio y nuestra privacidad, ya que en muchos aspectos de este avance, se utiliza para llevar a cabo una serie de violaciones y vejaciones en contra de los ciudadanos y las entidades jurídicas, no sólo dentro del país, sino también es acertado indicar que esto ocurre a nivel mundial, por la facilidad de comunicación y transmisión, causando pérdidas, daños pequeños y grandes, con montos de cientos de miles de dólares.

En materia de delitos informáticos, no se puede seguir rastros a medias o continuar en la penumbra, de allí la necesidad imperiosa y crucial de esta investigación, para dar un aporte a la reorganización del derecho penal y los organismos gubernamentales sobre una nueva modalidad comisiva de amplias repercusiones sociales y económicas.

Existe una necesidad urgente de incluir en el derecho penal vigente de Ecuador una tipificación más amplia y puntual de los delitos informáticos que afectan el interés social y el patrimonio público.

En primer término en lo que concierne a las conductas punibles, sería imprescindible crear nuevos tipos penales y en otros casos modificar los ya existentes, acorde al avance del uso de la tecnología en el Ecuador.

Palabras claves: Delitos Informáticos, Seguridad Tecnológica, Derecho Procesal Penal, Constitución de la Republica del Ecuador, Ley de Comercio Informático, Código de Propiedad Intelectual, Amenaza Informática, nuevos tipos penales.

# INFORME

Yo, Hugo F. Landívar Orellana, profesor de la Facultad de Derecho de la Universidad Del Pacífico, como Director de la presente Tesis de Grado, informo que el trabajo de tesis del señor Francisco Xavier Jaramillo Barea, egresado de esta Institución, se encuentra finalizado, completo y listo para someterse a la respectiva sustentación de su autor.

Guayaquil – Ecuador, Enero 2012

.....

Ab. Hugo F. Landívar Orellana

# DECLARACIÓN DE AUTORÍA

Yo, Francisco Xavier Jaramillo Barea declaro ser el autor exclusivo de la presente tesis.

Todos los efectos académicos y legales que se desprendieren de la misma son de mi responsabilidad.

Por medio del presente documento autorizo a la Universidad del Pacífico – Escuela de Negocios – para que pueda hacer uso del texto completo de la Tesis de Grado "Delitos Informáticos: Prevención, Modificación y creación de nuevos tipos" con fines académicos y/o de investigación.

Guayaquil – Ecuador, Enero 2012

Francisco Xavier Jaramillo Barea

# CERTIFICACIÓN

Yo, Hugo Landivar, profesor de la Facultad de Derecho de la Universidad Del Pacífico, como Director de la presente Tesis de Grado, certifico que el señor Francisco Xavier Jaramillo Barea, egresado de esta Institución, es autor exclusivo del presente trabajo, el mismo que es autentico, original e inédito.

Guayaquil – Ecuador, Enero 2012

.....

Ab. Hugo F. Landivar Orellana

# DOCUMENTO DE CONFIDENCIALIDAD

La Universidad Del Pacífico, se compromete a no difundir públicamente la información establecida en la presente Tesis de Grado "Delitos Informáticos: Prevención, Modificación y creación de nuevos tipos", de autoría de Francisco Xavier Jaramillo Barea, en razón que ésta ha sido elaborada con información confidencial.

Tres copias, escritas y digitales, de esta Tesis de Grado quedan en custodia de la Universidad Del Pacífico, las mismas que podrán ser utilizadas para fines académicos y de investigación.

Para constancia de este compromiso, suscribe

Guayaquil – Ecuador, Enero 2012

Abg. Martha Vallejo
DECANO FACULTAD

# AGRADECIMIENTOS

Es de una forma encarecida, en el que me dirijo a mis padres Mónica y Francisco, por todo aquello que me han brindado durante todo este tiempo, y por haber creído, algunas veces empujado y sobre todo por cómo me han dado su apoyo y guía de forma incondicional, como hijo y profesional.

A mi hermano Jaime, por su paciencia, guía, apoyo y colaboración, el ha sido mi mas fuerte inspiración y modelo de vida.

A mi familia que en lo numerosa que es, me brindado un mundo de aliento, oraciones y deseos de éxito durante preparación profesional.

A mis amigos, que me han ayudado a crecer por experiencias y han crearon en mi, innumerables momentos de felicidad.

A mis compañeros de la facultad, que no solo recibieron clases, sino también en más de un momento me enseñaron y compartieron junto a mi esta carrera que por momentos parecía infinita.

A los profesionales del derecho con los que tuve el privilegio de tratar y aprender de sus amplios conocimientos, fruto del ejercicio de la carrera.

A Hugo Landivar, mi director de Tesis, por haber hecho tangible este trabajo, haber dirigido de forma eficaz, brindado sus conocimientos personales y profesionales, pero sobre todo por haber confiado en mis conocimientos, aptitudes y capacidades en todo momento.

**TABLA DE CONTENIDOS:**

RESUMEN

DECLARACIÓN DE AUTORÍA

CERTIFICACIÓN

DOCUMENTO CONFIDENCIALIDAD

AGRADECIMIENTOS

TABLA DE CONTENIDOS

INTRODUCCIÓN

OBJETIVOS GENERALES

OBJETIVOS ESPECÍFICOS

PROBLEMA

JUSTIFICACIÓN

ORGANIZACIÓN DE LA TESIS

**CAPITULO I: EL MEDIO INFORMÁTICO**

I.A ANTECEDENTES

I.B SISTEMA INFORMÁTICO
I.B.1 El hardware
I.B.2 El software
I.B.3 Componente humano o humanware

I.C DESARROLLO DE LOS SISTEMAS INFORMÁTICOS

I.D ESTRUCTURA

I.E CLASIFICACIÓN

I.F HERRAMIENTAS Y APLICACIÓN DEL MEDIO INFORMÁTICO

I.G LOS DATOS EN UN SISTEMA INFORMÁTICO

**CAPITULO II: SEGURIDAD INFORMÁTICA**

II.A ANÁLISIS OBJETIVO DE LA SEGURIDAD INFORMÁTICA
II.A.1 INFORMACIÓN
II.A.2 CARACTERÍSTICAS DE LA INFORMACIÓN
II.A.3 AMENAZAS DE SEGURIDAD
II.A.4 DAÑO
II.A.5 CUAL ES EL PERFIL DEL ATACANTE INFORMÁTICO
II.A.6 CLASIFICACIÓN DE ATAQUES INFORMÁTICOS
II.A.6.a. ATAQUES PASIVOS
II.A.6.b. ATAQUES ACTIVOS

II.B SEGURIDAD FÍSICA DEL SISTEMA INFORMÁTICO
II.B.1. CABLEADO

II.C ACCIONES HOSTILES
II.C.1 ROBO INFORMÁTICO
II.C.2 FRAUDE INFORMÁTICO

II.D CONTROL DE ACCESOS
II.D.1 UTILIZACIÓN DE SISTEMAS BIOMÉTRICOS

II.E SEGURIDAD LÓGICA
II.E.1 OBJETIVOS PROTECCIÓN EFECTIVA

II.F SISTEMAS Y EMPRESAS CON MAYOR RIESGO

**CAPITULO III: DELITOS INFORMÁTICOS**

III.A CARACTERÍSTICAS DE LOS DELITOS

III.B SUJETOS DE DELITO INFORMÁTICOS
III.B.1 SUJETO ACTIVO
III.B.2 SUJETO PASIVO:

III.C EL BIEN JURÍDICO PROTEGIDO

III.D AUDITORIA O PERITAJE INFORMÁTICO
III.D.1 TIPOS DE AUDITORIA INFORMÁTICA
III.D.2 RESULTADOS DE LA AUDITORIA
III.D.3 AUDITORIA LEGAL

III.E LA PRUEBA INFORMÁTICA
III.E.1 REQUISITOS DE LA PRUEBA
III.E.2 PROCEDENCIA DE LA PRUEBA

III.F IMPACTO A NIVEL SOCIAL

III.G DELINCUENTES INFORMÁTICOS
III.G.1 PIRATAS INFORMÁTICOS
III.G.2 HACKERS
III.G.2.a SCRIPT KIDDIES
III.G.2.b HACKTIVISTAS
III.G.2.c HACKERS PATROCINADOS POR EL ESTADO
III.G.2.d HACKERS ESPIA
III.G.2.e SOMBRERO BLANCO
III.G.3 CRACKER
III.G.3.a CRACKERS DE SISTEMAS
III.G.3.b CRACKERS DE CRIPTOGRAFIA
III.G.3.c PHREAKER
III.G.3.d CIBERPUNK
III.G.4 CIBERTERRORISTA

III.H TIPOS DE SOFTWARE DELICTIVO
III.H.1 ADWARE
III.H.2 CRIMEWARE
III.H.3 MALWARE
III.H.4 SPYWARE
III.H.5 RANSOMWARE
III.H.6 ROGUE SOFTWARE

III.I TIPOS DE ATAQUES INFORMÁTICOS
III.I.1 BULLYING INFORMÁTICO
III.I.2 LOS DATOS FALSOS O ENGAÑOSOS
III.I.3 EAVESDROPPING Y PACKET SNIFFING
III.I.4 SNOOPING Y DOWNLOADING
III.I.5 SPOOFING
III.I.6 JAMMING O FLOODING
III.I.7 HUEVO DE PASCUA (VIRTUAL)
III.I.8 MANIPULACIÓN DE PROGRAMAS O LOS “CABALLOS DE TROYA”

III.I.9 LA TÉCNICA DEL SALAMI
III.I.10 FALSIFICACIONES INFORMÁTICAS
III.I.11 ENTRADAS FALSAS
III.I.12 MANIPULACIÓN DE LOS DATOS DE SALIDA
III.I.13 PHISHING
III.I.14 EL SABOTAJE INFORMÁTICO
III.I.14.a BOMBAS LÓGICAS O LOGIC BOMBS
III.I.14.b GUSANOS
III.I.14.c VIRUS INFORMÁTICOS
III.I.15 PORNOGRAFÍA
III.I.16 CIBERTERRORISMO
III.I.16.a OBJETIVOS COMUNES DE CIBER ATAQUES
III.I.16.b TIPOS DE ATAQUES
III.I.17 ATAQUES DE DENEGACIÓN DE SERVICIO
III.I.18 BACK DOORS Y TRAP DOORS
III.I.19 LA LLAVE MAESTRA O SUPERZAPPING
III.I.20 PINCHADO DE LÍNEAS O WIRETAPPING
III.I.21 HIJACKING
III.I.22 KEYLOGGER
III.I.23 PHARMING
III.I.24 SPAMMING
III.I.25 CARDING
III.I.26 SICARIATO INFORMATICO

III.J SITUACIÓN ECUADOR

III.K FIGURAS DELICTIVAS EN NUESTRA LEGISLACIÓN
III.K.1 ESPIONAJE O INTRUISMO INFORMÁTICO
III.K.2 DELITO CONTRA LA INTIMIDAD O PRIVACIDAD INFORMÁTICA
III.K.3 SABOTAJE INFORMÁTICO
III.K.4 FALSIFICACIÓN ELECTRÓNICA
III.K.5 DAÑO INFORMÁTICO
III.K.6 APROPIACIÓN ILÍCITA
III.K.7 ESTAFA INFORMÁTICA

III.L. ANÁLISIS CÓDIGO ORGÁNICO INTEGRAL PENAL

III.M. LEGISLACIÓN INTERNACIONAL
III.M.1 CHILE
III.M.2 ESPAÑA
III.M.3 FRANCIA

III.M.4 HOLANDA
III.M.5 GRAN BRETAÑA
III.M.6 AUSTRIA
III.M.7 ALEMANIA
III.M.8 ESTADOS UNIDOS
III.M.8.a Business to business
III.M.8.b Business to consumers

III.N VISIÓN DE LA INFORMÁTICA NACIONAL E INTERNACIONAL

III.O ENCUESTA DELITOS INFORMÁTICOS

**CAPITULO IV: PROYECTO**

CONCLUSIONES

GLOSARIO

BIBLIOGRAFÍA

# INTRODUCCIÓN:

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. Con ése fin nace la informática, como ciencia encargada del estudio y desarrollo de máquinas y métodos, con la idea de ayudar al hombre en aquellos trabajos rutinarios y repetitivos, generalmente de cálculo, de gestión, control y manejos remotos.

Los sistemas Informáticos, ofrecen oportunidades nuevas y sumamente complicadas para infringir la ley y han creado la posibilidad de cometer delitos de tipo tradicional en formas no tradicionales.

En el Ecuador, podemos comprender como jurisprudencia informática lo que nos describen en la Ley de Comercio Electrónico, Firma Electrónica y Mensaje de Datos, siete artículos agregados al Código Penal y en algunos incisos de la Ley de Propiedad Intelectual, que en su tiempo generaron un cierto status legal al accionar electrónico o digital, luego de esto se inicia una serie de reformas, en las cuales se empieza a tipificar algunos delitos informáticos, entre los cuales podemos mencionar el espionaje o intrusismo informático, intimidad o privacidad informática, sabotaje informático, falsificación electrónica, daño informático, apropiación ilícita, estafa informática.

En un plano general es acertado señalar que, el delito informático, es toda conducta típica que vulnera los derechos de una persona, sea ésta natural o jurídica, en el que se utiliza un computador, un celular, un ipad o cualquier dispositivo electrónico, como instrumento, medio o fin.

Es fundamental y lógico comprender, que lo que se haga hoy tendrá repercusiones y debería a su vez, más en el caso informático, actualizarse y adaptarse continuamente a la gama de posibilidades que la misma tecnología genera y aporta a la sociedad, es sumamente importante entender que este tipo de iniciativa, como sus predecesores buscan la protección actual y de cierta forma anticipar, los posibles a futuro.

En nuestros días no es difícil, sino más bien común, el escuchar sobre delitos informáticos, especialmente de sus trasgresores, entre los cuales, el mas activo y radical, es la sociedad Anonymous, un grupo, conformado por hackers, piratas, por navegadores del mundo online, que han saboteado páginas en todo el mundo, no tienen un líder, ni reglas para sus actuaciones, sus miembros se encuentran en cada país y buscan manifestarse en acciones de protesta a favor de la libertad de expresión, de la independencia de internet y en contra de diversas organizaciones, afectando, de una o varias maneras a la sociedad nacional e internacional.

Esta red Anonymous, amenazó al gobierno del Ecuador con ataques a sus entidades por el supuesto acoso de éste a los medios de comunicación y las limitaciones a la libertad de

expresión, están en contra de la incautación de medios de comunicación y suben videos a la Web, que proponen luchas en contra del gobierno.

De hecho en el mes de Agosto de este año en Ecuador, lo hicieron, haciendo caer los portales Web, de la Presidencia de la República, Vice- Presidencia, algunos Ministerios y Municipalidades, adicionalmente hicieron publicaciones online, de un listado de funcionarios del aeropuerto de Quito, con todos sus datos personales, también la CNT, fue parte de estos ataques, publicaron un link con el diagrama de la ubicación de sus servidores.

Todos estos actos, con el fin de demostrar al gobierno la vulnerabilidad de nuestros sistemas informáticos y a su vez su gran poderío y penetración a nivel nacional en este tema.

## OBJETIVOS GENERALES:

- El objetivo de este trabajo es analizar, las conductas delictivas que en la actualidad, ha generado el gran avance tecnológico, sobre todo en el campo de la informática, desde tres puntos de vista: normativo, delincuencia y prevención.

- Analizar el impacto de las infracciones informáticas, a fin de esclarecer los hechos ilícitos relacionados a la informática y obtener resultados para la adopción de medidas de precaución en la administración de justicia.

## OBJETIVOS ESPECÍFICOS:

El motivo de esta investigación, es desarrollar un estudio completo, del estado actual y futuro posible en nuestro país, sobre los delitos informáticos, que continuamente se colocan sobre el tapete y en realidad, aun conocemos muy poco; se suele manejar con el amarillismo de los medios no especializados, dificultando esto, el accionar de los profesionales, además colocando en tela de juicio el arduo trabajo de los especialistas.

- Introducir de forma clara y precisa, qué es el Medio Electrónico o Informático?, para con esto tener una idea específica, de cuáles son los riesgos que corremos, bajo los tipos de delitos no sólo nacionales, sino también internacionales y no sólo a nivel de personas naturales, sino también de personas jurídicas y aun más preocupantes a nivel de Estado.

- Reconocer mediante Derecho Comparado cuales son las tendencias y problemáticas en este ámbito a nivel mundial (mediante soluciones basadas en la cooperación internacional), buscando así emprender las medidas preventivas que fuesen necesarias para combatir estos delitos a nivel nacional.

- Presentar un proyecto para la creación de un Título sobre estos delitos informáticos, para que se deroguen los artículos antes existentes, que por sus generalidades permiten vacíos, que se implementen nuevos artículos específicos, permitiendo así una real y mejor aplicación de la justicia.

- Analizar el articulado, conceptualizando la naturaleza de las infracciones por sus características principales.

- Definir delincuencia tradicional, a fin de identificar a quienes de manera ilícita y dolosamente cometen dichos delitos informáticos.

## PROBLEMAS

Para la determinación de los diferentes problemas existentes en este ámbito delictivo, no necesitaré de largas, ni complejas explicaciones, debido a que, los conflictos en este ámbito son claros y sencillos, entre los que se pueden puntualizar los siguientes:

**Primero:** Falta de concientización, en lo concerniente al tema del Medio Informático, los delitos que este medio permite, el problema es concreto y real, al momento nos encontramos totalmente enlazados en una cadena sistemática, de información, producción, entre otros. Ante esta falta de conocimiento exponemos, no a un individuo o institución que fue atacado, sino también, en el peor de los casos, se puede, incluso generar un efecto dómino. Dos ejemplos puntuales, uno cotidiano y uno de alto riesgo para el Estado.

Ejemplo 1: Al momento la empresa eléctrica está implementando, los medidores digitales, que busca impedir, hasta cierto punto que la sociedad los pueda alterar o manipular, estos serán manejados directamente desde la central de la empresa eléctrica, qué sucede si alguien por buscar la frecuencia, el número de conexión, para reconectar su servicio haciéndose pasar por la matriz de la empresa, se equivoca en el proceso y deja sin luz a todo el sector, el ilícito afectará a una gran cantidad de hogares.

Ejemplo 2: ¿Qué pasa si por probarse así mismo, o a modo de protesta alguien decide derrumbar los sistemas informáticos de una petrolera, los mismos que no sólo manejan la parte burocrática y económica, sino también las operaciones de la maquinaria que extrae el petróleo? Entonces, lo que va a pasar es que, la petrolera obviamente deja de generar barriles, los mismos que significan una pérdida económica para la empresa pero también significará una pérdida económica para el Estado; Así como también una tardanza a todas aquellas empresas que realizan alguna labor y reciben un monto económico por eso, y así le sucederá también a las empresas que hacen trabajos para las anteriores, teniendo como punto final, también una escases de combustibles a nivel nacional, delito que fragmentará varias áreas de la economía social.

Con estos ejemplos, podemos ver la transcendencia de una pequeña y simple acción, teniendo en cuenta estos escenarios, vemos la necesidad de regular apropiadamente la norma jurídica en cuanto a los delitos informáticos.

**Segundo:** La Informática, los medios de red, internet, redes sociales, afines; en fin, es lo que hoy, puede denominarse como una forma de Poder Social. Las facultades que el fenómeno pone a disposición de Gobiernos y de privados, en cualquier ámbito, configuran un cuadro de realidades de aplicación y de posibilidades de juegos lícitos e ilícitos, en donde es necesario el

derecho para regular los múltiples efectos de una situación, nueva y de tantas potencialidades en el medio social.

**Tercero:** La principal limitante es la débil infraestructura legal que posee nuestro país, como muchos otros a nivel mundial, con respecto a la identificación de los ataques de este tipo de delitos; El delito informático ha sido abarcado dentro de nuestra jurisprudencia de forma somera y general, es visto como factor criminógeno, más no, con la gravedad que los efectos de estos indican, muchos estudiados del tema opinan, que es redundante y contraproducente la creación de nuevos tipos penales, más, se pierde la visión delincuencial, permitiendo la existencias de los conocidos "vacíos jurídicos" y, a su vez, se subestima el hecho, de que el delito informático, si bien es cierto, encierra tipos tradicionales, abarca también mucho más, y he ahí la necesidad de crear un tipificación más específica en cuanto a los delitos actuales de este nivel y hasta cierto punto, tratar de abarcar las posibilidades que pueden contravenir en el futuro.

**Cuarto:** No existe al momento un verdadero documento, formato o directivo de cómo llevar o manejar la seguridad apropiada de los sistemas informáticos, que ayude a la prevención de los Delitos Informáticos, dado que aprovechándose de la incertidumbre y de la demanda de los mismos directivos, supuestos "profesionales informáticos", se proporcionan guías erróneas y equivocadas, causando un daño aún mayor hacia lo que se busca proteger.

**Quinto:** Aunque ya existe un Departamento de Criminalística, éste tiene una serie de falencias, en lo que respecta a los delitos informáticos, que le impiden llevar a cabo las acciones de acuerdo a esta competencia, entre estas tenemos, la falta de herramientas para la recolección de pruebas, (por ejemplo: un sistema de reconocimiento facial para los casos de cajeros, o captura de cámaras públicas o privadas), se puede mencionar también, la falta de programas para detectar hacking o fraudes en la web, la falta de peritos autorizados, sólo en la provincia del Guayas, hay más o menos unos diez, para un promedio de 3 millones de habitantes y por último, se aprecia la falta de infraestructura, es decir una oficina para los peritos informáticos, que les permitiría poder evaluar y comparar resultados de investigaciones, en la actualidad desempeñan sus labores de forma independiente, manejan su información muy celosamente, lo que ayuda a que no haya mayor difusión de lo que encuentran en sus peritajes y no puedan ver hasta dónde, es el alcance cada día de este tipo de delitos.

# JUSTIFICACIÓN

El medio informático o electrónico avanza a pasos agigantados y a la misma velocidad, la utilización fraudulenta, de estos mismos métodos tecnológicos , en el que, el criminal está generando e ideando délitos, es por esto, que en esta investigación se busca realizar una serie de análisis bajo la herramienta de Derecho Comparado y bajo el resultado del mismo, poder llenar un vació jurídico, establecido a su vez por la generalidad del articulado respectivo, este vacío legal, latente y existente en nuestra legislación, acerca de este tipo de criminalidad informática va aumentando por la imaginación y destrezas de los autores.

¿Por qué?, el computador y los diferentes dispositivos electrónicos se están usando de una manera inapropiada a sus principios, esto es, como instrumento sujeto de actividades ilícitas y socialmente reprochables.

Sencillamente porque son aparatos, cuya utilización se ha masificado tanto, que su manejo es muy fácil para cualquiera, además el nacimiento del Internet, como una forma de comunicación, achica todas las distancias y fronteras, permitiendo visualizar a diario el gran horizonte que abarca la tecnología.

Además al momento se aplica una incorrecta restricción de los delitos informáticos, causa de la incorrecta aplicación de la ley penal. Existe en la Fiscalía General del Estado, una Unidad de Delitos Informáticos, desde el 2009, hasta finales del 2010, sólo se habían registrado unas 400 indagaciones, de las cuales sólo unas 10 recibieron sentencia.

Existe un nivel bajísimo de inversión en cuanto a seguridades informáticas a nivel general, en lo que comprende, el sistema público y privado, es decir, que las instituciones debido a la subestima otorgada y a la falta de conocimiento sobre estos delitos y sus repercusiones, prefieren invertir en hacer más atractivo su producto que en tomar precauciones apropiadas y necesarias, lo mismo sucede en la empresa privada.

# ORGANIZACIÓN DE LA TESIS:

El texto está organizado en cuatro capítulos. En el primer capítulo, se dará una breve introducción al medio informático como tal, su terminología, su historia, sus partes, todo con el fin de llegar a comprender mejor, como inicio este tipo de herramienta y como se involucra, en todos los sectores y al estilo de vida en nuestros días.

En el segundo capítulo se estudiará en qué consisten los delitos informáticos, sus clasificaciones, gravedades, modo de prueba dentro de Ecuador.

En el tercer capítulo se hará un sondeo de la situación jurídica de nuestro país acorde a este tipo penal, aplicando la legislación comparativa.

Finalmente, en el cuarto capítulo me aventuraré a la realización de propuestas sobre tipificaciones nuevas que deberían ser puestas en consideración para su inclusión dentro del Código Orgánico Penal, que ayuden a prevenir, que se adecúen a los nuevos tipos de criminología digital en nuestra realidad social actual.

# CAPITULO I: EL MEDIO INFORMÁTICO

## I.A ANTECEDENTES

La palabra Informática, nace del Francés “informatique”, creado por el ingeniero Philippe Dreyfus, pionero de la informática en Francia, a principios de los años 60´. La palabra a su vez es un acrónimo de “information y automatique”.

Es considerada una invención, equivalente a los grandes descubrimientos, como el fuego, la pólvora, la rueda y la industria.

La Informática, es una ciencia, cuyo alcance es muy amplio, y que al pasar el tiempo, se ha vuelto sumamente compleja.

Nació, bajo la idea, de crear un procesamiento automático de la información, mediante dispositivos electrónicos. Son varias disciplinas que se unen y que trabajando conjuntamente lograrán la automatización de procesos, entre estas disciplinas tenemos, fundamentos de la computación, programación, metodologías para desarrollos de programas, arquitectura de computadores, redes de computadores, la inteligencia artificial, podemos tener una lista muy larga, ya que son muchísimas las que han ido naciendo, para poder lograr, la magia de la tecnología que se vive en nuestros días.

La idea siempre fue crear una forma de mecanización, que simplificara, acortara y agilitara procesos, nunca se pensó, en que ésta en algún momento, aparte de llegar a ser un instrumento importantísimo en el transcurrir diario de todas nuestras actividades de toda índole, también se llegara ha convertir, en uno de los grandes enemigos de la vida actual...

## I.B SISTEMA INFORMÁTICO

Sistema Informático, es el conjunto de partes interrelacionadas, como hardware, software y el recurso humano (humanware) que permiten, almacenar y procesar información.

La ISO (ORGANIZACION INTERNACIONAL DE NORMALIZACIÓN) en su NORMA ISO 010110, define, "Sistema Informático, como el Sistema compuesto de equipos y de personal pertinente, que realiza funciones de entrada, proceso, almacenamiento, salida y control con el fin de llevar a cabo una secuencia de operaciones con datos"

Los sistemas informáticos deben tener la capacidad de cumplir tres tareas básicas, Entrada, Procesamiento y Salida, el conjunto de estos tres procesos, se conoce como Algoritmo.

Para tener una clara visión de los elementos, que en su momento deberán analizarse y estudiarse, para establecer un Delito Informático, es necesario dar una pequeña descripción de los componentes más importantes que conforman un Sistema Informático.

**I.B.1 El Hardware:** Es el conjunto de dispositivos físicos que componen una computadora, como, disco duro, CD Rom, tarjeta madre, memoria, DVD, teclado, ratón, en general, es todo lo que se puede ver y tocar, es decir es la parte tangible de un Sistema Informático.

Dentro del Hardware, tenemos partes muy importantes , como el Disco Duro, que adquiere un papel importantísimo, en la evaluación de un Delito Informático, ya que al momento de detectar y buscar pruebas de ataque o alteraciones que haya sufrido un sistema, es, en este dispositivo, en donde quedaran gravadas todas las acciones que se hayan hecho en el computador, el análisis del disco duro, nos dará como resultado, programas que se hayan instalado, información que haya sido impresa, el detalle de dispositivos de almacenamientos

que hayan sido conectados al sistema con el fin de dañar un programa, alterar datos o robar información.

Como ejemplo de esto, podemos mencionar, un caso muy actual en nuestro país, como es "CHUCKY SEVEN", que aparecería como autor del fallo, en la querella del Presidente contra el diario El Universo.

Por la rapidez, con que fue entregada la resolución en este juicio, la defensa consideró que era imposible que en 25 horas, un juez pudiese conocer la querella y redactar sentencia, por este motivo la fiscalía, pidió un peritaje informático del Disco duro de la maquina del Juzgado XV Penal del Guayas, donde había sido trabajada y emitida la resolución.

Este peritaje fue realizado por un perito informático, Frank López y 7 expertos más, durante tres meses en la ciudad de la Florida, Estados Unidos, López cuenta con una experiencia de 7 años trabajando para el gobierno de Estados Unidos, realizando este tipo de análisis.

El resultado de este peritaje dió como resultado lo siguiente: Identificación de CHUCKY SEVEN, que es un usuario predeterminado al instalar una versión pirata de Windows.

Se constató también la instalación de un programa pirata que convierte archivos escaneados en formato PDF a texto, de acuerdo a lo que va quedando gravado en el disco, se pudo ver que esta acción le tomo a la persona aproximadamente 3 minutos.

Esta investigación, permitió determinar que en este computador habría sido insertado un dispositivo móvil, con su marca y características propias, la hora exacta en que se insertó y los archivos que se abrieron y copiaron en la maquina, provenientes de este dispositivo.

"La conclusión de su informe forense, de 33 páginas, es que "la sentencia no fue escrita en el juzgado" donde estuvo el juez temporal Juan Paredes. Sino que se elaboró en otra computadora con un usuario 'Chucky Seven', que se guardó en la máquina del juzgado a través de un 'pen drive', a las 23:08 del 19 de julio. Ese día fue la audiencia de juzgamiento en la demanda del presidente Rafael Correa contra el diario". (1)

Para llegar a la conclusión, de que este archivo habría sido entregado al juez, se analizó, el disco duro de un computador, que utilizaba el abogado querellante cuando fue conjuez de la segunda Sala Penal, que también tiene registrado en el historial del disco, la versión Chucky Seven, esta versión queda registrada en cualquier maquina, al momento que el usuario que trabaja con esta versión, ingrese su dispositivo extraíble, Es muy importante enfatizar que el registro de usuario (CHUCKY SEVEN) que queda gravado en los discos del computador, no es un virus, simplemente es la denominación de un usuario, que es propia del dueño o utilitario del computador.

"El forense contó que al estudiar las propiedades del fallo contra El Universo y la ponencia de Vera encontró 11 características similares. Según el analista, esas semejanzas son suficientes para determinar que "los documentos comparten el mismo origen". Explicó que esas características toman en cuenta datos como: el nombre de usuario ('Chucky Seven'), la

(1) Periódico El Comercio 21 de diciembre 2011, Página 17.

versión de la aplicación utilizada para crearlo, nombre de la compañía, tipo de archivo y las cabeceras de los documentos".

Toda esta cantidad de datos ha sido posible obtenerlos, gracias a la capacidad de registro de información que tienen los discos duros de un computador, ya que no hay forma de alterar el metadata original de estos.

**I.B.2 El Software:** Son los programas que pueden ejecutarse en los computadores, son las instrucciones y las órdenes que el computador necesita para funcionar.

El Software, deberá ser siempre un elemento de análisis, al momento de hablar de un Delito Informático. Tenemos como principales formas de Software.

Software de Base: Es el que normalmente es desarrollado por el fabricante del equipo o por empresas especializadas en el desarrollo de programas. Comprende: El Sistema Operativo, los Sistemas de Gestión de datos, el sistema de comunicaciones y las utilidades.

Software de Aplicación: Es el software diseñado y desarrollado, acorde a una necesidad para resolver problemas específicos. La variedad, es enormemente grande y variada,

Sistema Operativo: Es un conjunto de programas que controlan los programas de los usuarios y los dispositivos de entrada y salida.

El análisis del Sistema operativo, de un equipo, es el que nos permitirá, saber qué tipo de programas tiene un sistema, cuáles son nuevos o cuales han sido alterados. Todo esto se volverá en su momento dado, en pruebas de trascendental importancia al momento de evaluar y catalogar un Delito Informático.

**I.B.3 Componente humano o humanware**: Se refiere al personal técnico, que crea, maneja y mantiene un Sistema Informático, está constituido por las personas que participan en la dirección, diseño, desarrollo, implementación y explotación de todos los componentes del Sistema.

El componente humano es de gran importancia, en el manejo de la Informática y sus partes, y son también al momento de la investigación de un Delito Informático, los principales sospechosos. Ya que serán ellos, en muchas de las veces, los que realizan el daño, por un mal manejo de programas o equipos, como una forma de venganza, o porque dieron datos, como claves, a terceros, que las mal utilizarán perjudicándolos.

Un ejemplo en nuestro país, de un delito informático perpetrado por personas que han manejado un sistema, se dio en el mes de Agosto cuando el Ministerio de Finanzas, reconoció haber sido objeto de una estafa informática, $3,4 millones en el presupuesto del estado, con un sistema llamado E-Sigef, esto ocurrió en un Centro de salud, en el sector de Cotocollao en la ciudad de Quito.

El contador Herrera Márquez, de dicha entidad, logró penetrar al sistema encargado del manejo de todo el presupuesto del estado ($23,950 millones), por medio de una clave que consiguió al encontrar una falla en el sistema que manejaba, el defalco lo realizaba por medio de transferencias a cuentas particulares, esto lo venía haciendo desde el 2008.

Con esta noticia se supo también que habría otros ministerios en donde estaría pasando algo parecido, sin embargo no ha habido denuncias concretas al respecto.

## I.C DESARROLLO DE LOS SISTEMAS INFORMÁTICOS

Desde la creación de la informática, los Sistemas, han evolucionado grandemente, en un primer momento, los componentes, del Sistema físico, lógico y personal de la informatización se encontraban centralizados en un solo lugar, lo cual hacia todo más personal y seguro.

En la actualidad, llegamos a versiones más avanzadas de informática, en donde vemos, que tanto la capacidad de proceso, como la capacidad de almacenamiento, se encuentran distribuidas en diferentes lugares. Este avance aunque exitoso, en el momento de la operatividad de la información, lo vuelve riesgoso al momento de ser atacado.

Dentro del desarrollo de Sistemas Informáticos, tenemos los "Mainframes", que soportan el sistema general de información de una corporación o entidad, es lo que se llama "informática corporativa". Los mainframes admiten entrada remota de trabajos, trabajan en tiempo compartido, satisfaciendo las necesidades de los equipos situados en niveles inferiores.

Al permitir ingresos remotos, se tiene la vulnerabilidad de ser víctima de un Delito o de un intento.

Tenemos la "Informática Departamental", que por lo general está constituida por computadores, que interaccionan con los mainframes y con elementos del nivel inferior. En la actualidad, en algunos casos, las redes locales, pueden constituir los Sistemas informáticos Departamentales en lugar de los computadores.

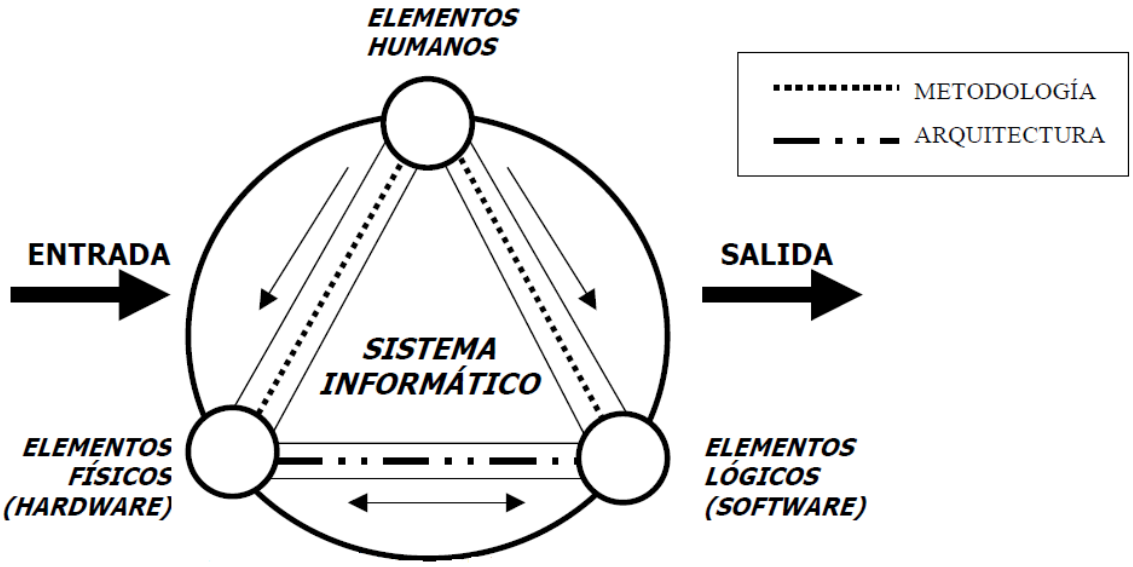
La "Informática Personal" constituida, por un computador o una estación de trabajo. Éste dispone de herramientas especializadas para el trabajo e interacciona a través de las redes con los Sistemas Departamentales y Corporativos.

Al momento se emplean numerosos sistemas informáticos en la administración pública y privada optimizando los procesos, reduciendo costos, aumentando la inversión y la producción nacional.

## I.D ESTRUCTURA:

Nos permite entender claramente, cómo funciona un Sistema Informático.

TABLA 1: Estructura del sistema informático.
(http://guindo.pntic.mec.es/pold0000/apuntes/ut01/tema01/tema01.htm)




## I.E. CLASIFICACIÓN

.

En relación con las prestaciones que ofrecen los Sistemas informáticos se pueden clasificar:

- **Supercomputadores**
- **Sistemas grandes o mainframes**
- **Sistemas Medios**
- **Estaciones de Trabajo**
- **Microcomputadores:** Como
  Computadores profesionales.
  Computadores personales.
  Computadores domésticos

## I.F HERRAMIENTAS Y APLICACIÓN DEL MEDIO INFORMÁTICO

La herramienta más importante de un Medio Informático, es el Computador, un aparato que fue creado como el instrumento primordial, para el desarrollo del medio informático y que se ha perfeccionado con el propósito de potenciar las capacidades de pensamiento, memoria, y comunicación.

Sin embargo el "Computador", hoy en día, es también, la principal herramienta, que permite y ayuda a llevar a cabo una gran diversidad de Delitos Informáticos.

Su área de aplicación, no tiene límites, esta disciplina se aplica a numerosas y variadas áreas del conocimiento o la actividad humana, procesos penales, gestión de negocios, almacenamiento y consulta de información, monitorización y control de procesos, industria, robótica, derecho, comunicaciones, control de transportes, investigación, desarrollo de juegos,

diseño computarizado, aplicaciones o herramientas multimedia, medicina, biología, física, química, meteorología, ingeniería, arte, etc.

En este tiempo que vivimos es difícil e imposible concebir, empresas, instituciones, personas naturales, actividades de toda índole que no usen, de alguna forma, el apoyo de la informática.

## I.G LOS DATOS EN UN SISTEMA INFORMÁTICO

La base de datos o "data base": Es el conjunto de datos que pertenecen a un mismo contexto, que son almacenados de manera sistemática, y que pueden ser, estáticos (que no varían, pese al paso del tiempo) o dinámicos (estos se modifican con el tiempo; estas bases, por lo tanto, requieren de actualizaciones periódicas).

Esta Base, dependiendo de su información, se puede volver una información muy codiciada, por ajenos, lo que la hará altamente susceptible a diversas formas de ataques, con el propósito de ser Copiada, Adulterada o Extraída totalmente de su sistema.

La información es una adición de datos que tiene un significado específico más allá de cada uno de estos, y tendrá un sentido particular según como y quien la procese.

La información debido a su intangibilidad, no se valora adecuadamente, al momento de cuantificar el resultado monetario de un ataque al Sistema, cosa que no ocurre con los equipos, las aplicaciones y la documentación.

El robo de base de datos a nivel empresarial, gubernamental o privada, en nuestra época, es uno de los Delitos Informáticos más comunes y cuya penalización, no se encuentra del todo completa, ya que debería hacerse una separación puntual, de los diferentes tipos de robo de bases, para establecer castigos, es decir no podría tener, la misma pena, un robo de bases o información de una entidad gubernamental, que la del equipo de una persona particular.

# CAPITULO II: SEGURIDAD INFORMÁTICA

"Ser lo que soy, no es nada sin la seguridad". Sin duda W. Shakespeare (1564 – 1616) tenía un concepto más evolucionado que sus contemporáneos del siglo XV y quizás también que algunos de los nuestros.

"La seguridad nacional depende, de su seguridad económica y la seguridad de su información, en la vanguardia de ambas, hay un sistema de seguridad débil, sin proteger y manejado por corporaciones" y "Muchos analistas y observadores de seguridad en internet, han rechazado reconocer los aspectos físicos del Ciber-terrorismo, la mayoría debido a una carencia de educación oficial y experiencia en aproximaciones holísticas de la seguridad". Dan Verton en su publicación Black Ice. "La amenaza invisible del Ciberterrorismo".

Por ejemplo: Los terroristas cibernéticos han tratado por mucho tiempo, a veces con éxito, de penetrar redes de instalaciones importantes, como las plantas generadoras de energía y otras

infraestructuras básicas de todo el mundo. El 25 de Septiembre del 2010, Irán confirmó por primera vez haber sufrido un ataque ciberterrorista, cuando un funcionario del Ministerio iraní de Minas y Metales dijo que un total de 30.000 computadoras de sectores industriales estaban infectadas, por el virus Stuxnet que está diseñado expresamente para atacar esos sistemas y transferir al extranjero datos clasificados. Varios ministerios tuvieron que unir esfuerzos para combatir el "virus espía" y evitar mayores daños a datos industriales y de infraestructura clasificados en el país.

La seguridad informática como una materia académica no existe, pero en nuestra forma de vida, es considerada como una herramienta importante, dentro del ámbito de la prevención de crímenes y pérdidas informáticas. Un sistema informático se puede proteger desde un punto de vista lógico (con el desarrollo de software) o físico (hardware).

Las amenazas al Sistema, pueden proceder desde programas dañinos que se instalan en la computadora (como un virus) o llegar por la vía remota (delincuentes que se conectan a Internet e ingresan a distintos sistemas).

Entre las herramientas más comunes de la seguridad informática, están los programas de antivirus, los cortafuegos o firewalls, la encriptación de la información y el uso de contraseñas o passwords.

Un sistema seguro debe ser integro (con información modificable sólo por las personas autorizadas), confidencial (los datos tienen que ser legibles únicamente para los usuarios autorizados), irrefutable (el usuario no debe poder negar las acciones que realizó) y tener buena disponibilidad (debe ser estable).

El desarrollo acelerado de la tecnología, la facilidad de acceso a información de todo tipo, la posibilidad de planificar un delito, sólo con bajar un video de la red, ha dado paso a la acción de antisociales, en formas imposibles de imaginar, los delitos tradicionales, como un robo, se cometen en formas no tradicionales (sólo con un mensaje), sin moverse de su sitio y sin arriesgarse, se puede obtener gran cantidad de dinero.

Es muy común en nuestros días escuchar sobre la clonación de las tarjetas de crédito o debito, delito que ha presentado cerca de 96 casos denunciados desde el inicio del presente año y consiste en la captura de los datos de la banda de la tarjeta, mediante un aparato electrónico, para después colocar esta información en una nueva banda magnética. Generalmente esto también sucede a nivel internacional, cuando las tarjetas robadas o la información es llevada a países como Perú o Colombia. Este delito informático fue uno de los primeros que apareció en Ecuador.

# II.A ANÁLISIS DEL OBJETIVO DE LA SEGURIDAD INFORMÁTICA

## II.A.1 INFORMACIÓN

Al realizar un análisis de la Seguridad Informática se deberá conocer las características de lo que se pretende proteger, como es la Información, los datos, los sistemas, la economía, entre otros.

El Dato es la unidad mínima con la que se compone la información. Datum es una palabra en latín, que significa "lo que se da".

Dentro de una institución gubernamental, existe información que debe o puede ser pública y puede ser vista por cualquier persona, (por ejemplo, el listado de las principales empresas del país, de acuerdo a su tributación); y, aquella que debe ser privada: sólo puede ser visualizada por un grupo autorizado de personas, como los movimientos financieros de empresas.

## II.A.2 CARACTERÍSTICAS DE LA INFORMACIÓN

**Crítica:** Es indispensable para garantizar la continuidad operativa.

**Valiosa:** Es un activo con valor en sí misma.

**Sensitiva:** Debe ser conocida por las personas que la procesan y solo por ellas.

La Integridad de la Información es la característica que hace que su contenido permanezca inalterado, a menos que sea modificado por personal autorizado, y esta modificación sea Registrada para posteriores controles o auditorias. Una falla de integridad puede estar dada por anomalías en el hardware, software, virus informáticos o modificaciones realizadas por personas que se infiltran en el sistema.

La Disponibilidad u Operatividad de la información: requerirá que ésta se mantenga correctamente almacenada, con el hardware y el software funcionando perfectamente.

La Privacidad de la información, dependerá de que ésta, sólo sea conocida y manejada por personas autorizadas, que deciden cuándo y cómo permitir el acceso a la misma.

Con respecto a la Seguridad de la Información, es importante considerar algunos aspectos adicionales, relacionados con los anteriores, pero que incorporan aspectos particulares:

- **Protección a la Replica:** Proceso que asegura que una transacción sólo puede realizarse una vez, a menos que se especifique lo contrario. No se podrá grabar una transacción para luego reproducirla, con el propósito de copiarla, para que parezca que se recibieron múltiples peticiones del mismo remitente original. Al existir esta protección, la réplica que realizase un atacante, podría ser fácilmente descubierta.

- **No Repudio:** Evita que cualquier entidad, que envió o recibió información alegue, ante terceros, que no la envió o recibió.

- **Consistencia:** Se debe poder asegurar que el sistema, se comporte como se supone que debe hacerlo ante los usuarios que corresponda.

- **Aislamiento:** Este aspecto, íntimamente relacionado con la Confidencialidad, permite regular el acceso al sistema, impidiendo que personas no autorizadas hagan uso del mismo.

- **Auditoria:** Determina, que acciones o procesos se están llevando a cabo en el sistema, así como quien y cuando las realiza.

## II.A.3 AMENAZAS DE SEGURIDAD

Amenaza, en el entorno informático, como cualquier elemento que vulnere y ponga en total o relativo peligro, al sistema y todo aquello que lo compone, lógico o físico.

Las amenazas pueden ser analizadas en tres momentos: Antes, Durante y Después del ataque.

- **La Prevención (antes):** Mecanismos que aumentan la seguridad (o fiabilidad) de un sistema durante su funcionamiento normal. Por ejemplo: el cifrado de información para su posterior transmisión.

- **La Detección (durante):** Mecanismos orientados a revelar violaciones a la seguridad. Generalmente son programas de auditoría.

- **La Recuperación (después):** Programas que se aplican, cuando la violación del sistema ya se ha detectado, para reactivar los equipos, tratando de recuperar la mayor cantidad información posible. Por ejemplo: recuperación desde las copias de seguridad (backup).

TABLA 2: Amenazas para la seguridad.
(http://dspace.espoch.edu.ec/bitstream/123456789/93/1/18T00369.pdf, pagina 27)


Las principales amenazas para la Seguridad Tecnológica, que me interesa evaluar, son las que provienen de los humanos, pues son estos, los que idearan, diferentes y variadas formas de ataques.

## II.A.4 DAÑO

El Daño es el resultado de una amenaza; este se produce, porque el afectado, empresa o particular no supo identificar adecuadamente la amenaza y, sí lo hizo, se impusieron criterios comerciales por encima de los de seguridad.

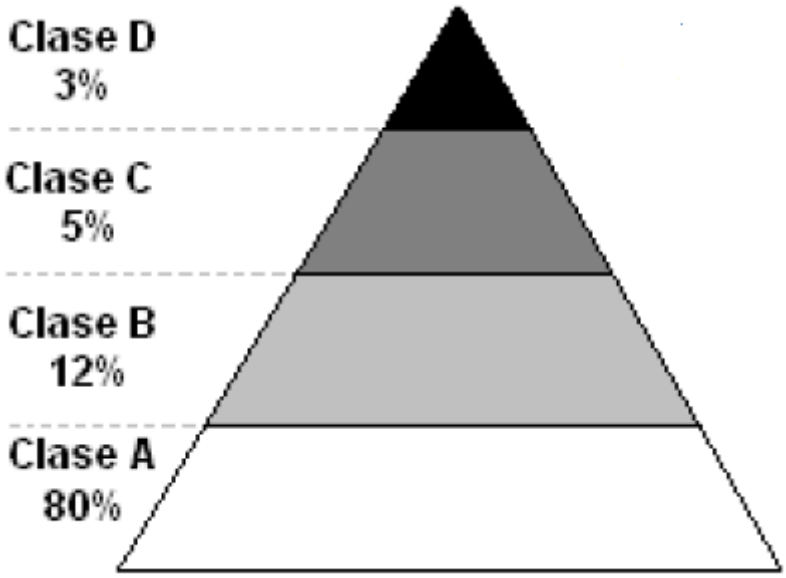
La seguridad, indicará, el índice en que un Sistema Informático está libre de todo peligro, daño o riesgo. Esta característica es muy difícil de conseguir en un 100% por lo que solo se habla de la probabilidad de que un sistema se acorde a su naturaleza y como se espera que funcione, y se habla de sistema fiable en vez de sistema seguro.

## II.A.5 CUAL ES EL PERFIL DEL ATACANTE INFORMÁTICO

Es muy importante en materia de Delito Informático, saber quién y cómo podría ser el atacante, este puede ser, una persona, un medio informático, medio electrónico, medio telemático o sistemático, que busca o intenta acceder sin autorización a un sistema, computador o servidor ajeno, en forma intencional o no.

Acerca de los tipos de intrusos, Julio C. Ardita, el Hacker más famoso contemporáneo de Latino América, nos dice: "Los tipos de intrusos existentes actualmente los podríamos caracterizar desde el punto de vista del nivel de conocimiento, formando una pirámide."(2) Que los identifica por Clases y tenemos lo siguiente.

TABLA 3: Pirámide Clasificatoria de Intrusos Informáticos. (http://www.cybsec.com)




1. **"Clase A:** El 80% en la base, son los nuevos intrusos que descargan programas de Internet, están jugando, tanteando, se conforman en pequeños grupitos y prueban que hacer con la información que bajan.

2. **Clase B:** Es el 12%, el más peligroso, saben compilar programas, aunque no saben programar. Realizan pruebas, conocen como detectar el sistema operativo que está usando la víctima, testean las vulnerabilidades del mismo e ingresan por ellas.

3. **Clase C:** Es el 5%, es gente que sabe, que conoce y define sus objetivos. Por lo que, buscan todos los accesos remotos e intentan ingresar.

(1) Julio C. Ardita, Entrevista sobre el mundo hacker, CTO de CYBSEC.- www.cybsec

4. **Clase D:** Es el 3% restante. Cuando entran a determinados sistemas por casualidad, buscan la información o fin que les pueda interesar."(3)

En nuestro país ya existe interés, de parte de los artífices de los delitos, por reclutar expertos informáticos, los interesados, se han acercado a universidades ecuatorianas, buscando un acercamiento con estudiantes de Ingeniería de sistemas, les ofrecen trabajo, indicándoles que ganaran bastante dinero, de una forma fácil y rápida.

## II.A.6 CLASIFICACIÓN DE ATAQUES INFORMÁTICOS

### ➢ II.A.6.a. Ataques Pasivos:

El atacante, no realizará ningún cambio, ni daño en la información, sólo le interesa escuchar, ver, leer, la información a la cual tiene acceso. Su único propósito, será lograr obtener la mayor cantidad de información, generalmente sobre horarios de transmisiones, transferencias, horas activas o inactivas de un proceso.

### ➢ II.A.6.b. Ataques Activos:

Estos ataques conllevan siempre alguna modificación del flujo de datos transmitido o la creación de un falso flujo de datos. Generalmente son realizados por hackers, piratas informáticos o intrusos remunerados y se los puede subdividir en cinco categorías, cuya explicación ayudara al estudio, al momento de visualizar que clase de ataque se ha sufrido.

- **Interrupción:** Es cuando la información del sistema se pierde, quede inutilizable o no disponible.

  Por ejemplo: Esto sucede cuando el intruso, por diferentes medios, como bombas electrónicas o keyloggers, busca ingresar a un sistema, en algunos casos, la seguridad del mismo es extremadamente fuerte, lo que busca es el colapso, una vez colapsado el sistema (en el caso de los que cumplen acciones comerciales), reactivan el sistema sin sus defensas, permitiendo el acceso al atacante, esto ocurrió con la plataforma de Play Station a principios del 2011.

- **Intercepción:** Un elemento no autorizado, consigue el acceso a una determinada información del sistema.
  Con el propósito de obtener acceso al sistema; robar información, como secretos industriales o propiedad intelectual, recopilar información personal acerca de un usuario; obtener información de cuentas bancarias; obtener información acerca de una organización (la compañía del usuario, etc.); afectar el funcionamiento normal de un servicio; utilizar el sistema de un usuario como un "rebote" para un ataque; usar los recursos del sistema del usuario, en particular cuando la red en la que está ubicado tiene un ancho de banda considerable.

- **Modificación:** Aparte de lograr el acceso, consigue modificar la información.

(2) Julio C. Ardita, Entrevista sobre el mundo hacker, CTO de CYBSEC.- www.cybsec

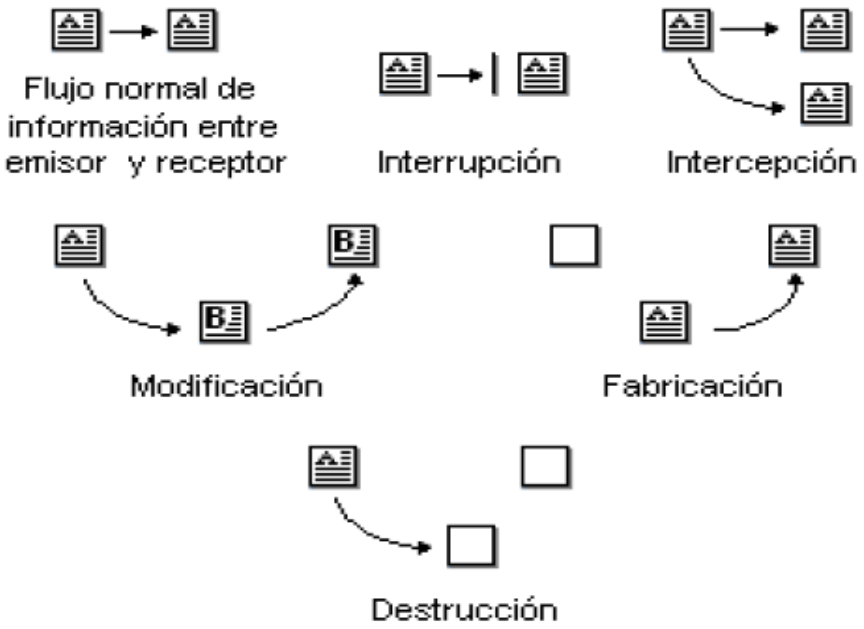
- **Fabricación.** Crean un objeto similar al original atacado, de manera que es difícil distinguir uno de otro, en este caso el sistema vulnerado, está alimentando al atacante con información sin quererlo.

  Un ejemplo de esto, sucede cuando se generan páginas web ficticias, sobre todo de las páginas de las grandes corporaciones o entidades financieras, en el Ecuador, le ocurrió al Banco Pichincha, le duplicaron la página principal de la Web del banco, el usuario le extendía su nombre y clave al delincuente en forma directa, datos con los que se perpetraban hurtos de información o de dinero, por la vía informática.

- **Destrucción:** Es una modificación que inutiliza la información o el equipo

  Por ejemplo: Diariamente se fabrican y se realizan pruebas de virus informáticos, algunos controlables, otros realmente variables y destructivos, durante los últimos 5 años, la sociedad lo ha podido palpar, al recibir correos o spams cargados con estos virus, uno de los más famosos, hace unos 3 años en Ecuador y que creo todos pueden recordar, se denominaba la "vida es bella", este se presentaba como un archivo de diapositivas en PowerPoint, que por el nombre inocente lo abríamos, permitiendo así la propagación del virus que en menos de 5 minutos, formateaba y destruía el sistema con un ultimo label "la vida es bella", antes de que termine de colapsar.

  TABLA 4: Procesos de los Ataque Activos.-
  (http://dspace.espoch.edu.ec/bitstream/123456789/93/1/18T00369.pdf, pagina 30)




  Siempre se cree que los piratas informáticos son los únicos que amenazan el sistema, siendo pocos los administradores que consideran todos los demás riesgos a los que está expuesto un Sistema Informático.

# II.B SEGURIDAD FÍSICA DEL SISTEMA INFORMÁTICO

La seguridad física consiste básicamente en la "aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas, a los recursos e información confidencial" (4). Son controles y mecanismos de seguridad, dentro y alrededor del centro de computo así como los cuidados a medios de acceso remoto al sistema y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos.

Una de las causas de mayor daño dentro de los centros de cómputo, puede provenir de una simple gotera, hasta una acumulación del agua que invade el área de Sistemas debido a una falla, que puede ser natural o premeditada.

Esta premeditación hacia el área de Sistema Informático, deberá ser penalizada, pues logra su cometido, de provocar una gran pérdida de información, de tiempo y lógicamente de dinero.

También se puede considerar un ataque Informático, al acto de mojar premeditadamente un teléfono celular, considerando que al momento, estos son aparatos, no sólo para hablar por teléfono, sino que por su gran tecnología, almacenan muchísima información, que los convierte en un dispositivo tecnológico, susceptible a ataques.

El trabajar con equipos tecnológicos, implica trabajar con la electricidad. Por lo que ésta podría considerarse también, en una herramienta que ayude a provocar un delito, al hecho de provocar una falla eléctrica intencional, con el fin de hacer un daño momentáneo o total de equipos, haciendo esto, que se pierda valiosa información.

## II.B.1. CABLEADO

Dentro de los Sistemas Informáticos, tenemos el cableado, que proporciona la conexión de todos equipos, y es uno de los transportes de Información y Datos más importantes en la actualidad a nivel mundial.

Los Delitos más comunes que podemos destacar en el área del Cableado serían:

Es importante mencionar, algunos de ellos, ya que se deben catalogar como un Delito Informático, pues son actos vandálicos, realizados con el propósito de extraer, seguir o desviar información privada.

**Interferencia:** Una forma de interferir, es desviando o estableciendo una conexión no autorizada en la red, lo que hará que los datos que fluyen a través del cable pueden estar en peligro.

Se pueda implementar una escucha sin establecer conexión, para de esta forma lograr un seguimiento de datos.

---

(3) HUERTA, Antonio Villalon, Seguridad en Unix y Redes, Version 1.2 Digital – Open Publication License v.10 o Later 2 de Octubre del 2000

**Corte del cable:** La conexión establecida se rompe, lo que impide que el flujo de datos circule por el cable.

**Daños del cable:** Por malas conexiones, empates, que dañen el apantallamiento que preserva la integridad de los datos transmitidos.

# II.C. ACCIONES HOSTILES

## II.C.1 ROBO INFORMÁTICO

Un robo común, es sacar los computadores o equipos tecnológicos de un sitio, estos son activos de las empresas y están expuestos, como cualquier activo de una institución.

Pero, un Delito de Robo Informático frecuente que cometen los empleados de entidades o empresas privadas, es el hecho de utilizar la computadora de la empresa, para realizar trabajos privados o para otras organizaciones, de esta manera, están robando tiempo a la máquina y a la empresa, en su tiempo de trabajo.

Otro Robo frecuente en las empresas, es que los empleados extraigan pequeños fragmentos de documentos con informaciones puntuales, que pueden comercializar con otras empresas, usualmente las competencias, en la actualidad se hace normalmente por medio de memorias extraíbles, considerando que es una forma, que Aparentemente no deja rastros.

Entregar datos a un compañero (como listas de clientes), con el objeto de privilegiarlo frente a otros compañeros de su área, es un Delito, ya que Roba información, para ir tras un propósito que le dará un beneficio.

## II.C.2 FRAUDE INFORMÁTICO

Cada año, que avanza son más los millones de dólares que son sustraídos de empresas, en donde, las computadoras son el principal instrumento utilizado para dichos fines.

Lamentablemente por un tema de imagen, es decir la seguridad que proyecta hacia fuera una institución o empresa, y el estar claros, además, de que llegar a probar y castigar, el fraude al que fueron sometidos, llevará mucho tiempo, y adicionalmente, aparte del dinero perdido, esta investigación, los lleva a perder credibilidad o fidelidad, pues los vuelve a los ojos externos, como una entidad vulnerable a ataques, esto hace que la gran mayoría, ni lo informe, ni lo denuncie y lo asuman.

Es lo que ocurre en la actualidad con todos los bancos del país, que están siendo diariamente vulnerados y sufriendo una gran cantidad de ataques Informáticos de diferente índole y formas, pocos se dan a conocer públicamente, la posición del banco en la actualidad, de acuerdo a ultimas regulaciones, es asumir la perdida con el cliente, con un seguro de respaldo. Pero este mutismo ante el dolo sufrido, lleva a que los ataques no paren, al contrario cada día se vuelven más ingeniosos y costosos para el seguro.

## II.D CONTROL DE ACCESOS

En los controles de accesos, se pueden identificar como Delitos Informáticos, los que vulneren la seguridad de un lugar. Como la falsificación de una tarjeta electrónica de acceso, la suplantación de una huella digital.

El cambio de códigos de Identificación dentro del sistema, para que éste permita el acceso a determinada persona, a un área donde no debiera estar. Este cambio de código, normalmente lo realiza un sujeto que está dentro de la entidad.

Existen modos de ingreso controlados, que le permiten al usuario aplicar sobre los recursos y la información que está manejando modificaciones. Debo mencionar los más importantes, con el propósito de dar una base a la investigación de procesos en el tema de accesos.

**Lectura:** El usuario podrá únicamente leer o ver la información, pero no puede alterarla.

**Escritura:** Le permite al usuario agregar datos, modificar o borrar información.

**Ejecución:** Da al usuario el privilegio de ejecutar programas.

**Borrado:** El usuario podrá eliminar recursos del sistema, como programas, campos de datos o archivos. El borrado es considerado una forma de modificación.

Existen otras modificaciones de accesos especiales, que generalmente se incluyen en los sistemas de aplicación:

**Creación:** Permite al usuario crear nuevos archivos, registros o campos.

**Búsqueda:** Permite listar los archivos de un directorio determinado

### II.D.1 UTILIZACIÓN DE SISTEMAS BIOMÉTRICOS

La Biometría es una tecnología que realiza mediciones en forma electrónica, guarda y compara características únicas para la identificación de personas.

La forma de identificación, consiste en la comparación de características físicas de cada persona con un patrón conocido y almacenado en una base de datos. Los lectores biométricos identifican a la persona por (manos, ojos, huellas digitales y voz).

Los sistemas biométricos son altamente seguros, sin embargo, ante el rápido avance de la tecnología y sobre todo el gran alcance, que al momento han logrado todos aquellos personajes, que están detrás de los Delitos Informáticos, este sistema, deja de ser totalmente seguro y se vuelve vulnerable.

# II.E SEGURIDAD LÓGICA

La seguridad lógica se basa, en gran medida, en la efectiva administración de los permisos de acceso a los recursos informáticos, basados en la identificación, autentificación y autorización de accesos, es la que implementa barreras y procedimientos, que solo permitirán el ingreso a las personas autorizadas para hacerlo.

"Todo lo que no está permitido debe estar prohibido" A.S.S. Borghello, (renombrado Manager Técnico y Educacional de la empresa ESET, para Latinoamérica), y esto es lo que debe de asegurar la Seguridad Lógica.

Un resguardo importantísimo, que se debe tener en cuenta siempre, son las desvinculaciones de personal con la organización, llevadas a cabo en forma amistosa o no.

Los despidos del personal de sistemas, serán siempre un alto riesgo, ya que en general son los empleados, los que cuentan con todo tipo de información y por lo tanto con una gran capacidad para modificar las aplicaciones o la configuración del Sistema, pudiendo dejar "bombas lógicas", destruyendo sistemas o recursos informáticos.

Por ejemplo: Existen algunos casos en el que los programadores o personal de sistemas, aseguran su puesto, alterando comandos de tal manera, que al sacar su nombre del rol de pagos de la empresa, automáticamente se activa algún proceso de destrucción del sistema.

Para evitar estas situaciones, que pueden ocasionar oportunidades muy grandes de efectuar un Delito Informático, se debería anular los permisos de acceso a las personas que se desvincularan de la organización, lo antes posible. En caso de despido, el permiso de acceso debería anularse previamente a la notificación de la persona sobre la situación.

Últimamente se ha visto en nuestro país, que al despedir empleados públicos, por medio de Compra de renuncias, al momento de entregarle la notificación al empleado, que le indica su salida, esta persona va acompañada de un contingente de seguridad, que le pide que abandone su puesto, esto a visión popular, ha dado una mala imagen de trato, pero realmente se hace con el propósito de evitar, que este empleado, no tome represalias, sacando o modificando información privada de la institución, que la perjudique

## II.E.1 Los objetivos para lograr una protección efectiva son:

1. Restringir el acceso a los programas y archivos;

2. Los operadores deben trabajar con una supervisión minuciosa y no pueden realizar modificaciones a los programas o los archivos que no les correspondan;

3. Verificación de que los datos, archivos y programas que se están usando son correctos en y con el procedimiento adecuado;

4. La información transmitida debe ser recibida, solo por el destinatario al cual ha sido enviada y no por otro al mismo tiempo o por equivocación;

5. Que la información recibida, sea la misma que ha sido transmitida; y

6. Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.

## II.F SISTEMAS Y EMPRESAS CON MAYOR RIESGO

El bien que resulta más atractivo robar, siempre es el dinero o algo de valor. Por lo tanto, los sistemas que pueden estar más expuestos a fraude, estafa, hurto, entre otros; son los que manejan grandes transacciones, como pagos, nominas, ventas o compras. Serán ellos, donde les será más fácil convertir transacciones ilícitas de dinero y sacarlo de la empresa.

Hace unos años se consideraba que dentro de este rubro se podían encasillar grandes empresas, como bancos, compañías de seguros, constructoras, etc.

Sin embargo al momento, no se necesita tener una gran empresa, de grandes transacciones, para ser objeto de este tipo de Delitos Informáticos, ocurren a diario, y a personas jurídicas y naturales, pues el uso de la tecnología nos ha llevado a una comodidad atractiva, ya que en vez de hacer grandes filas para un pago, ahora preferimos hacerlo todo por medio de transferencias bancarias, las cuales resultan bien hasta que un intruso entra en nuestra línea y duplica datos, lo que le permitirá sacar nuestro dinero y enviarlo a otro lado con una gran facilidad.

El mundo de las transferencias de dinero para pagos o depósitos en líneas, es un servicio espectacular, muy llamativo para todos, por su facilidad de manejo, por comodidad y sobre todo por rapidez en la transacción, pero lamentablemente es el mundo que ofrece la mayor cabida a los Delincuentes Informáticos.

Otras instituciones que son muy susceptibles, a ataques y Delitos Informáticos, son aquellas que manejan el envió "online", de grandes volúmenes de datos e interviene poco personal, lo que impide verificar todos.

# CAPITULO III: DELITOS INFORMÁTICOS

En este capítulo analizaré y determinaré, en base a la pronunciación de ciertos autores (de varios escritos sobre el tema), el concepto de lo que se debe considerar como delitos informáticos, sus características, sobre los sujetos de derecho, (víctima y victimario). Así también sobre cuál es el bien jurídico que se busca proteger en este tipo delitos, quién es la figura encargada de salvaguardar, mantener o encontrar fallos en la seguridad, a nivel privado, como judicial. Lo que comprende la prueba, su manejo, cuidado y presentación, sobre las clases de delincuentes y los tipos de programas que usan para corromper y delinquir. Por último también mencionare lo que comprende la legislación nacional e internacional en la que se contempla el delito informático, así como una visión legal del futuro informático.

**Viega Rodríguez.** "Los llamados delitos informáticos no constituyen una nueva categoría delictiva, sino que son los mismos delitos que ya se vienen castigando: delitos contra las personas, contra el honor, la libertad, la seguridad pública o la nación" (5).

**Davara Rodríguez.** Lo define como "La realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático, ya sea hardware o software" (6).

**Jijena Leiva.** Aporta, que "Toda acción típica, antijurídica y culpable, para cuya consumación se usa la tecnología computacional o se afecta la información contenida en los sistemas de tratamiento automatizado de la misma". (7)

**Nidia Callegari.** Define al delito informático como "aquel que se da con la ayuda de la informática o de técnicas anexas"(8).

**Carlos Sarzana.** "Los crímenes por computadora comprenden cualquier comportamiento criminógeno en el cual la computadora ha estado involucrada como material o como objeto de la acción criminógena, como mero símbolo" (9).

**María de 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" (10).

**Parker** Define a los delitos informáticos como "todo acto intencional asociado de una manera u otra a los computadores; en los cuales la víctima ha o habría podido sufrir una pérdida; y cuyo autor ha o habría podido obtener un beneficio" (11).

El delito informático, es de una forma simple, la conducta típica que vulnera los derechos físicos o virtuales de una o varias personas naturales o jurídicas, en la que se utilizan los medios tecnológicos, informáticos, telemáticos y afines (como lo es el computador, la red o inclusive, lo que se podría creer inofensivo, como lo es el celular), como instrumento, medio o fin.

Como he mencionado, la tecnología y los medios informáticos, han dejado una puerta abierta a la imaginación del educado en este ámbito, ya que transgrede los crímenes tradicionales e innova, haciendo experimentar a la sociedad, la incertidumbre de la falta de seguridad y la impunidad que esto conlleva.

---

(5) VIEGA RODRIGUEZ, María José. "Contratos sobre Bienes y Servicios Informáticos", Editorial y Librería Jurídica Amalio M. Fernández, Montevideo, 2008.
(6) DAVARA RODRÍGUEZ, Miguel Ángel. "Manual de Derecho Informático", Editorial Aranzadi, Pamplona, 1997.
(7) JIJENA LEIVA, Renato, Chile: Protección Penal a la Intimidad y los Delitos Informáticos, Editorial Jurídica de Chile, 1993.
(8) CALLEGARI NIDIA, citada por TELLEZ VALDES, Julio, Los Delitos Informáticos, Editorial Temis, 1999.
(9) SARZANA, Carlos, Criminalista e tecnoligia, Gennaio, Roma, 2000
(10) LIMA LUZ, María, Delitos Electrónicos, en Criminalia, México, 1984
(11) PARKER D.B., Citado por ROMEO CASABONA, Carlos, Poder Informático y Seguridad Jurídica, Colección Impactos, Madrid 1987.

Dentro del ámbito legal existen dos posturas al respecto de la tradición de los delitos, por un lado existe, el que los delitos realmente ya existen y que el legislador tiene que simplemente introducir las modificaciones legales pertinentes a fin de permitir la adecuación de los tipos tradicionales a las nuevas circunstancias; y por otro lado existe el hecho, que por el tipo de delincuente y sus delitos, se genera un cierto tipo de evolución, que rompe con los paradigmas y el núcleo de los delitos tradicionales. Y esta última postura es en sí, la más acertada en mi opinión.

Durante ya algunos años, juristas e inclusive una serie de países, han querido o intencionado crear un encasillamiento de los diferentes delitos informáticos, a las figuras típicas de carácter tradicional ya existentes en la ley y no ha sido encontrada todavía una fórmula adecuada que se complemente con los códigos vigentes.

Se subestima en demasía las posibilidades licitas e ilícitas que brinda este medio, por desconocimiento de sus capacidades y oportunidades completas o parciales, arriesgándonos así a continuar con el relleno de "vacíos y baches". Un ejemplo claro de esto es la numerosa cantidad de reformas que se le ha hecho y sigue haciendo al Código Penal vigente, en vez de, así como se ha generado un Departamento de Delitos Informáticos, se genere también, un Titulo de Delitos Informáticos, que en primera instancia otorgarían un mayor control y normamiento de la justicia en este ámbito legal.

La individualización de las penalizaciones, de una manera más explícita y específica, es no sólo necesaria, sino también menester, al momento de brindar justicia, respecto a los delitos informáticos que aquejan actualmente a nuestra sociedad.

## III.A CARACTERÍSTICAS DE LOS DELITOS

Las características de este tipo de delitos no son tan amplias, como podríamos suponer de acuerdo a la amplia gama de delitos posibles, que más adelante detallaré.

Estos tipos de delitos son conductas, realizadas en su mayor porcentaje por lo que se podría denominar como un "criminal de cuello blanco", más no, por el típico formato de criminal tradicional, por lo que, para el cometimiento de este tipo de atipicidades, se requiere de un conocimiento técnico básico o muy especifico y avanzado, para ser llevados a cabo.

Es muy común que el actor o victimario de estos delitos, no sea ajeno a la escena del crimen, sino más bien que mantengan cierta familiaridad, nexo laboral o personal, siendo esto a su vez un agravante en su contra al momento de realizarse el delito, ya que lo realiza con dolo.

Son delitos que se accionan o realizan en torno a la oportunidad, ya sea está fabricada por el atacante o fomentada por la fuerte tentación, de encontrarse en su responsabilidad o en sus funciones, estas dos son de las principales razones que empujan o animan a delinquir en este ámbito.

Absolutamente todos los delitos informáticos, causan o provocan pérdidas económicas de gran cuantía, ya sea por desvió de fondos, como por sabotaje lógico e incluso alteraciones de

procesos en sistemas básicos, como luz y agua. El simple hecho de traspasar la seguridad de un sistema le cuesta miles de dólares en credibilidad a una empresa, en lo que respecta a su imagen de seguridad informática, sin contar con la información que se puede sustraer o los efectos que tengan lugar una vez traspasada la seguridad del sistema al que se atacó.

"Los delitos informáticos representan grandes dificultades, esto por su mismo carácter técnico. Tienden a proliferar cada vez más, por lo que requieren una urgente regulación. Son muchos los casos y pocas las denuncias, y todo ello debido a la misma falta de regulación por parte del Derecho" (12).

## III.B. SUJETOS DE DELITO INFORMÁTICO

En derecho penal, la ejecución de la conducta punible supone la existencia de dos sujetos, un sujeto activo y otro pasivo, los cuales, a su vez, pueden ser una o varias personas naturales o jurídicas.

De tal manera al ser vulnerado el bien jurídico protegido, se determina quién o quienes corresponden al sujeto activo y al sujeto pasivo, se entiende que el dueño o propietario del bien jurídico protegido afectado es el sujeto pasivo y el que vulnere o lesione, naturalmente es el sujeto activo del delito.

### III.B.1. SUJETO ACTIVO

De acuerdo al profesor y presidente de la Corte Suprema (2002 – 2003) chilena Mario Garrido Montt, se entiende por tal "a quien realiza toda o una parte de la acción descrita por el tipo penal" (13).

Como mencione anteriormente el sujeto activo de este delito, posee cultura, entendimiento y por ende conocimientos de electrónica e informática, es decir con una instrucción básica o elevada, puede también ignorar totalmente el tema, y actuar bajo guía de un cómplice que sea el experto, en orden de poder interactuar y realizar el delito.

Existe una diversidad en cuanto a los autores de los delitos informáticos y lo que los diferencia en esencia es la naturaleza de los mismos delitos efectuados, esto teniendo en cuenta, que no es lo mismo, el que encuentra una falla en un sistema y se aprovecha, que el que busca o crea una situación delictiva.

### III.B.2. SUJETO PASIVO

Ahora, el sujeto pasivo, no es nada más y nada menos, que la víctima del accionar delictivo o agravio por parte del sujeto activo, por supuesto es la seguridad de este, que en este trabajo y en el día a día laboral del legislador se busca proteger y salvaguardar.

(12) TELLEZ VALDES, Julio, Los Delitos Informáticos, Editorial Temis, 1999.
(13) GARRIDO MONTT, Mario, Nociones Fundamentales de la Teoría del Delito, Editorial Jurídica de Chile, 1992.

El sujeto pasivo es el individuo, instituciones privadas, crediticias o gubernamentales, que hacen uso de sistemas informáticos, y que de una manera u otra se encuentran interconectados entre sí.

El sujeto pasivo del delito, es de suma importancia para el estudio de los delitos informáticos, dado que según esto, mediante su aportación podemos, conocer y encuadrar, los diversos tipos de ilícitos que se generan, cada vez más diferentes, cometidos por los delincuentes informáticos.

Debido al desconocimiento de los reales delitos y sus características, no se ha podido administrar en algunos casos la justicia de forma adecuada o peor, no han sido llevados ante la justicia, porque no se ha podido encontrar la forma de penalizarlo, hay una falta clave y neurálgica de leyes que protejan de forma más efectiva a los sujetos pasivos de este tipo de criminalidad.

## III.C. EL BIEN JURÍDICO PROTEGIDO

El bien jurídico es el bien material o inmaterial, que se encuentra guardado y protegido por el derecho, estos bienes son valores legalizados, como la salud, la vida, la propiedad, entre otros. El bien jurídico dentro de los delitos informáticos, asumen una protección proveniente de los delitos tradicionales, reinterpretados por supuesto, para así adaptarse a lo que involucra el ámbito tecnológico e informático, subsanando así las lagunas que se originan debido a los diferentes tipos de comportamientos delictivos.

El bien jurídico en este aspecto, involucra y se desenvuelve básicamente, en un marco del principio de "lesividad". El bien protegido por el derecho, sea este por su valor económico, intrínseco de la persona, como también por los sistemas que la procesan o automatizan, no podrá ser vulnerado, por ningún tipo de acción, que atente contra el bien jurídico asegurado, ya que de darse esto, se podrá conminar con una pena y así brindar justicia legal a la transgresión realizada.

De acuerdo a la Constitución de la Republica del Ecuador, en su artículo 66, numeral 26 y en el artículo 321, dicta:

Art. 66.- Se reconoce y garantizará a las personas:

26. El derecho a la propiedad en todas sus formas, con función y responsabilidad social y ambiental. El derecho al acceso a la propiedad se hará efectivo con la adopción de políticas públicas, entre otras medidas.

Art. 321.- El Estado reconoce y garantiza el derecho a la propiedad en sus formas pública, privada, comunitaria, estatal, asociativa, cooperativa, mixta, y que deberá cumplir su función social y ambiental.

- La propiedad es el bien tangible o intangible que se ve comprometido en cualquier delito informático.

## III.D. AUDITORIA INFORMÁTICA O PERITAJE INFORMÁTICO

Tiene el propósito de evaluar los sistemas informáticos, realizar una verificación que indique si los componentes que manejan estos sistemas de información fueron de algún modo vulnerados, si se encuentran trabajando de acuerdo a los objetivos establecidos, si los programas, van de acuerdo a su orden, auditar si se han realizado cambios que se deberían realizar o no , y muy importante, analizar si no existen, adecuaciones extrañas.

Todo esto con el propósito de mantener intacta toda la base de información de una institución, esto debe realizarse periódicamente, lo que dará como resultado la identificación rápida de algún intruso en la red. Con el trabajo del auditor informático, se obtendrá el resultado de cualquier ilícito realizado en el sistema.

Es muy importante el papel que juega el auditor o perito informático, en el momento de detectar un delito informático, ya que será él, quien indique los pasos a seguir, tanto en la parte de reinstalación, prevención, pero también en la parte legal, con el aporte que dará su información, que determinará el tipo de delito ocurrido y ayudará a encontrar la penalización para el culpable.

En lo que concierne a los peritos informáticos, en nuestro país contamos con profesionales con preparación y conocimientos superiores a la de los transgresores, que con su potencial pueden encontrar posibles fallas o "leaks", detectar y prevenir el delito, encontrar y recuperar procedimientos, pruebas e ilegalidades acontecidas, el problema no es en si la preparación de los peritos informáticos sino más bien la falta de infraestructura y equipamientos que en la actualidad son deficientes. El ejemplo más claro que tenemos de este tipo de actuación es el caso "Rafael Correa vs Diario El Universo", con la investigación al disco, que se tuvo que llevar a Estados Unidos el disco, que debía ser investigado, pues en el Ecuador, no contamos con laboratorios tecnológicos adecuados para este tipo de análisis.

### III.D.1 TIPOS DE AUDITORIA INFORMÁTICA

Existen muchas tipos de auditoría que se clasifican específicamente de acuerdo a la función en la que se desempeña, sin embargo es importante mencionar las principales de estas, que son las que darán al auditor o perito informático el resultado real de su investigación del delito.

**Auditoría Legal**: Es la que se encarga del cumplimiento legal de todas las medidas de seguridad exigidas por la ley, y la evaluación de acusaciones sobre delitos identificados en red.

**Auditoría de los datos**: Realiza la clasificación de los datos, estudio de las aplicaciones y análisis de los flujo gramas, es decir la velocidad y caminos por los que recorren los datos.

**Auditoría de las bases de datos**: Está a cargo de la verificación de los controles de acceso, de actualización, de integridad y calidad de los datos, dentro del sistema.

**Auditoría de la seguridad**: Es la que se encarga de la verificación de la disponibilidad, integridad, confidencialidad, autenticación y no repudio de los datos e información competente.

**Auditoría de la seguridad física**: Es la que se encarga de evaluar la ubicación de la organización y sistemas, evitando ubicaciones de riesgo, y en algunos casos no revelando la situación física de esta para su debida protección, comprendiendo las protecciones externas como arcos de seguridad, vigilancia, entre otros protocolos y protecciones del entorno.

**Auditoría de la seguridad lógica**: Es la que se encarga del desarrollo de los métodos de autenticación de los sistemas de información, es decir que estos sean veraces, confiables e invulnerables, para esto así como encriptaciones logísticas también se comprende el uso de medios de identificación lógica, como lo son lectores de retina, huellas digitales, entre otros afines.

**Auditoría de la seguridad en producción**: Es la que se encarga de realizar las revisiones a todos los posibles escenarios o márgenes de errores, accidentes y fraudes, que se hayan o se puedan suscitar.

## III.D.2 RESULTADOS DE LA AUDITORIA

El resultado de las auditorias, no siempre será perfecto, hoy en día, esto se vuelve cada vez más difícil, ya que los sistemas informáticos, están siendo constantemente tratados de vulnerar, total o parcialmente.

Sin embargo, si esto fuera así, el informe indicará nuevas formas de prevención, de lo contrario, mostrara las pequeñas o grandes fallas encontradas y las soluciones inmediatas que deben tomarse para la solución de los problemas.

## III.D.3 AUDITORIA LEGAL

Ahora este es un punto muy importante y porque no, neurálgico de este trabajo, es el deber del perito informático, con su investigación, el determinar, establecer e informar si se está cometiendo o si se va a cometer un delito dentro del sistema, buscar pruebas claras y precisas, que apunten a la afirmación o negación de este hecho, encontrar los vacíos de seguridad que permitieron o que podrían permitir en un futuro, la inclusión de un delito por parte un agente interno o externo a la compañía.

El perito legal debe ser una persona muy preparada en el tema tecnológico y conocedor de todos los sistemas y sus propiedades, esto le permitirá, una evaluación sin errores u omisiones.

Ante estos puntos también se debe de tener en cuenta que el auditor o perito, durante su investigación, debe sobre todos las cosas mantener y guardar un sigilo o silencio profesional, manejando las situaciones con la mayor de las discreciones, para evitar desconfianza y fundamentos de fallo a los empleados o personas que interactúan en un mismo entorno o

sistema, para no generar más posibilidades o oportunidades delictivas, y sobre todo para evitar menoscabar la imagen del auditado a la sociedad en general.

Para realizar una auditoria apropiadamente, el auditor se valdrá de pruebas y herramientas, que permitirán una buena indagación. En cuanto a las pruebas estas pueden ser sustantivas o de cumplimiento. La primera, sustantiva, sirve para verificar el grado de fiabilidad del sistema, así como también la exactitud, integridad y validez de la información. La segunda, de cumplimiento, sirve para verificar el grado de cumplimiento de lo revelado, proporciona evidencias de que los controles claves existen y que son aplicables.

Realmente la única clasificación que se le puede otorgar a los auditores es el de interno y externo, el interno siendo el encargado específicamente de la seguridad y los preceptos impuestos por la empresa a la que presta sus servicios, mientras que el auditor externo realiza una labor más general en cuanto a la auditoria en sí, no sigue un aspecto definitivo, sino que, busca todos los escenarios posibles.

## III.E LA PRUEBA

La prueba será la herramienta indispensable y fundamental, al momento de establecer un delito informático, es la prueba, la que dará el soporte al procedimiento que se pueda establecer para penalizar un delito.

Esta puede ser tangible como documentos escritos o herramientas, pero también puede ser intangible, como un email, mensaje, inclusión en la red de un sistema. Ambas opciones tendrán igual valor jurídico, al momento de presentarse como pruebas esenciales en un procedimiento.

En el caso de que durante la audiencia o juicio, algunas de las autoridades lo creyesen y determinaran necesario, la prueba digital será expuesta de forma impresa, esto se procederá mediante la impresión normal o de capturas de pantalla, ya sea en una computadora, como de un celular o incluso en la lectura de algún aparato electrónico, entre otros. Manteniendo a su vez la prueba original para posterior consulta, este procedimiento debe de ser realizado por un perito a elección de la autoridad pertinente.

Se considera que un medio digital, electrónico o telemático permanece integro e impoluto, si mantiene completo e inalterable su contenido, para el cumplimiento de esto, se designara por la autoridad correspondiente, a los peritos y a los responsables.

### III.E.1 REQUISITOS DE LA PRUEBA

Para que la prueba informática sea validada debe de cumplir una serie de requisitos, como el que he mencionado antes, que es, el que la prueba debe de ser accesible para su posterior consulta, que se conserve y mantenga en su estado original, que se reproduzca con exactitud y claridad, que incluya, fecha, hora, mes, día, en el que fue generada y su autor correspondiente.

La mantención y protección de la pruebas Digitales, deberá ser regida y establecida por la autoridad designada o por un particular que cumpla las condiciones necesarias, para que la prueba permanezca inalterada.

Cabe indicar que para la utilización como prueba de datos personales, ubicaciones debe contarse directamente con la autorización de quien se mencionara.

"No será preciso el consentimiento para recopilar datos personales de fuentes accesibles al público, cuando se recojan para el ejercicio de las funciones propias de la administración pública o judicial, en el ámbito de su competencia, y cuando se refieran a personas vinculadas por una relación de negocios, laboral, administrativa o contractual y sean necesarios para la obtención de la verdad, como conductor de la acción de justicia". (2)

### III.E.2 PROCEDENCIA DE LA PRUEBA

En cuanto a esto, se entiende claramente que la prueba, es decir los datos, archivo o afines tecnológicos o telemáticos, son generados por quien los envía o registra al cometimiento del acto delictual y son usables como prueba en contra del emisor, una vez comprobada la conexión vinculante.

"En caso de que alguna de las partes niegue la validez de un mensaje de datos, deberá probar, conforme a la ley, que éste adolece de uno o varios vicios que lo invalidan, o que el procedimiento de seguridad, incluyendo los datos de creación y los medios utilizados para verificar la firma, no puedan ser reconocidos técnicamente como seguros. Cualquier duda sobre la validez podrá ser objeto de comprobación técnica". (Artículo 54, Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, código vigente).

"Para la valoración de las pruebas, el juez o árbitro competente que conozca el caso deberá designar los peritos que considere necesarios para el análisis y estudio técnico y tecnológico de las pruebas presentadas". (3)

## III.F IMPACTO A NIVEL SOCIAL

La tecnología avanza rápidamente, esto es un hecho que no se puede dejar de mencionar, a su vez los delincuentes informáticos también avanzan, con nuevas técnicas y desarrollos en este ámbito. Lo que sí, es acertado asegurar es que la sociedad, no para de querer mayores adelantos tecnológicos, aun viviendo, la incertidumbre de lo que pueda ocurrir, de lo que aparecerá al siguiente día o inclusive en las próximas horas, es acertado decir que, al igual que yo con este trabajo, existen muchas personas tratando de brindar una mayor seguridad tecnológica y justicia para aquellos que han sido victimados, por estas acciones delictuales.

El grado de especialización, conocimientos y las técnicas delictivas se incrementan a pasos agigantados, debido a que las personas con este conocimiento ya no solo actúan culposamente al azar, sino que maliciosamente, maquinan planes y proyectos para delinquir, ya sea a nivel nacional o global, este último, predilecto de estos delincuentes, ya que brinda mayores opciones de escapes con impunidad.

---

(2) Artículo 9, Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, código vigente.

(3) Artículo 55, Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, código vigente).

Se ha fomentado la idiomática de que, el delincuente informático, muchas veces es parte de la familia, ya sea laboral, como personal, se está creando un celo y una exigencia rigurosa, en lo que comprende a la contratación o designación, del componente humano o humanare, afectando así positiva o negativamente acorde a la situación, al trabajador activo de la sociedad en esta área.

Los más afectados por estos delitos, por supuesto son los menos cautelosos o poco culturizados en este aspecto. Los cuales suelen recibir, el por decir, desquite delictual y son engañados o manipulados para convertirse en víctimas o son usados sin saberlo como herramienta del victimario para vulnerar a los demás.

Por esto, es que una vez más la educación es revelada, como un factor clave en la minimización de este problema, como la cura, para la seguridad y desarrollo de los pueblos, ante una mayor cultura y enseñanza, guiadas en el camino apropiado acorde a la ley, brindaran el armamento intelectual que necesita la sociedad, para protegerse, saber cómo proceder y en el mejor caso saber cómo actuar ante un delito, es decir denunciar el delito y buscar castigo para sus autores que carcomen el cálido vientre de nuestro Ecuador.

Muchos de estos delitos son cometidos por menores de edad, aprovechando la habilidad y conocimiento de estos jóvenes son algunos los casos en los que se los contrata para la acción delictiva, para esto la Constitución de la Republica del Ecuador dicta:

Art. 46.- El Estado adoptará, entre otras, las siguientes medidas que aseguren a las niñas, niños y adolescentes:

2. Protección especial contra cualquier tipo de explotación laboral o económica. Se prohíbe el trabajo de menores de quince años, y se implementarán políticas de erradicación progresiva del trabajo infantil.

El trabajo de las adolescentes y los adolescentes será excepcional, y no podrá conculcar su derecho a la educación ni realizarse en situaciones nocivas o peligrosas para su salud o su desarrollo personal. Se respetará, reconocerá y respaldará su trabajo y las demás actividades siempre que no atenten a su formación y a su desarrollo integral.

- En el caso en que se contrate o se haga delinquir a un menor de edad a cambio de algún tipo de beneficio

## III.G DELINCUENTES INFORMÁTICOS

Los que podemos considerar como delincuentes son los que vulneran los derechos de la sociedad, como los que estipula protegidos, la Constitución de la Republica del Ecuador, en su artículo 83, numerales 7, 8,9,15 y 17.

Art. 83.- Son deberes y responsabilidades de las ecuatorianas y los ecuatorianos, sin perjuicio de otros previstos en la Constitución y la ley:

7. Promover el bien común y anteponer el interés general al interés particular, conforme al buen vivir.

8. Administrar honradamente y con apego irrestricto a la ley el patrimonio público, y denunciar y combatir los actos de corrupción.

9. Practicar la justicia y la solidaridad en el ejercicio de sus derechos y en el disfrute de bienes y servicios.

15. Cooperar con el Estado y la comunidad en la seguridad social, y pagar los tributos establecidos por la ley.

17. Participar en la vida política, cívica y comunitaria del país, de manera honesta y transparente.

Existen diversos tipos de delincuentes informáticos, entre los cuales puntualizo a continuación los más importantes.

## III.G.1 PIRATAS INFORMÁTICOS

Hace ya mucho tiempo que los piratas han dejado de rondar los siete mares y han entrado al océano digital, actualmente el pirata informático es un ser, estilizado, de conocimientos agudos y precisos, con un cerebro desarrollado y la única arma, con que cuentan, en un dispositivo tecnológico con conexión a la web o Internet.

Este tipo de delincuente, en cada acción que comete señala y demuestra dolo y alevosía, debido a que su única razón de ataque es apropiarse y beneficiarse económicamente, de lo que encuentra o busca colocar en su camino, a través de la web.

Estos generalmente no actúan en grupos, sino más bien en forma solitaria, con el fin de brindarse seguridad a sí mismos, aplicando uno de sus credos "no hay confianza entre bribones". Su acceso raramente se suscita dentro de su entorno y son muy difíciles de rastrear, debido a que su modus operandi de predilección, es desde el exterior, sobretodo en países en los cuales no existe la extradición y pueden desarrollar sus actividades delictivas, sin frenos o barreras que les impidan su accionar.

## III.G.2 HACKERS

Un Hacker es de una naturaleza completamente diferente al pirata informático, para el hacker el único objetivo de su travesía por la web, es el de investigar y saciar su hambre de conocimiento, mismo que a medida que va avanzando, se le abren más puertas en el mundo digital. Este tipo de delincuente, aunque es menos perjudicial que el pirata informático, no deja de delinquir con sus acciones, este rompe o esquiva las seguridades para obtener sus preciados conocimientos, si bien es cierto los usa para sí mismo, el delito radica en el traspaso ilegal de seguridades, creación de herramientas delictuales y en la violación de un sigilo informático.

El hacker, es un usuario sumamente preparado en todo lo relacionado con la informática, ellos crean y desarrollan, su delito no radica en realizar ilegalidades o daños, ellos solo están interesados en la información.

Dentro de lo que comprende el mundo del Hacker, existen una serie de sub-categorías, entre las cuales las más importantes son las siguientes:

**III.G.2.a Script Kiddies.-**

Son los hackers que buscan fama traspasando seguridades de sistemas y deforman o cambian las características de las páginas web.

**III.G.2.b Hacktivistas.-**

Este es el nombre que se le otorga a todos aquellos hackers, que están motivados por la política o la religión, los ecosistemas, es esta la base que tienen para irrumpir e investigar en grandes sistemas.

**III.G.2.c Hackers patrocinados por el estado.-**

Aunque parezca increíble y extraño, en la actualidad muchos países en el mundo han recurrido a la contratación de grandes y famosos Hackers para la protección de las redes de estado, son los encargados directos de monitorear los grandes sistemas informáticos que controlan un país son los que deben estar al tanto, de los ataques que reciben a cada momento los sistemas y son lógicamente los que se deben asegurar que sus barreras de seguridad no podrán ser traspasadas, ni atacadas por ciberterroristas, cuentan con autorización de atacar en forma tecnológica, personas ,instituciones y gobiernos si amerita.

Un ejemplo de esto, es Kevin Mitnick, un hacker que violó las seguridades de grandes empresas en Estados Unidos, por lo cual fue juzgado y encarcelado durante 6 años, luego de esto, ha sido contratado por el gobierno americano, como uno de sus salvaguardas de las redes informáticas del país.

.

**III.G.2.d Hackers espía.-**

Existen empresas de alquiler de Hackers, los cuales tienen como servicio, el infiltrarse en la competencia y robar secretos comerciales. Este procedimiento se realiza tanto fuera como dentro de la empresa o gobierno que se piensa espiar, muchas veces desde dentro, con el fin de actuar como un topo, es un trabajo remunerado.

**III.G.2.e Sombrero Blanco.-**

Son los “buenos” de la informática, estos son expertos en seguridad informática se especializan en las pruebas de penetración y otras metodologías para garantizar que los

sistemas de información de una compañía, son seguros. Estos poseen un arsenal en constante evolución de la tecnología y libran una constante batalla en contra de los piratas informáticos.

## III.G.3 CRACKERS

Cracker, denominación creada en 1985 por hackers en defensa del uso periodístico del término y distinción al público general.

Son los que se infiltran en los sistemas o crean virus informáticos. Lamentablemente es un hecho que estos superan a los hackers de sombrero blanco. Muy frecuentemente buscan encontrar los caminos con menor seguridad, así sea por error de humanware, o por simple pereza y su principal objetivo es obtener réditos económicos.

El Cracker es un ente dañino que ronda por la web expectante de encontrar oportunidades de beneficiarse así mismo, sin importar el daño que pudiese invocar en los demás. Sus destrezas radican en la invasión de sistemas, descubrir claves y contraseñas con programas, algoritmos o encriptaciones de su autoridad, pero sobre todo para el robo de datos, delito que le sustenta económicamente. Algunos intentan ganar dinero vendiendo la información robada, otros sólo lo hacen por fama o diversión.

Un ejemplo en Ecuador, le ocurrió a la asambleísta María Cristina Kronfle, a quien le capturaron sus cuentas de correo y redes sociales, robando su identidad, para desde éstas, "emitir comentarios que van en contra de todos mis principios morales, legales y constitucionales como mujer y con la dignidad que ostento", habría tenido también amenazas de que sus cuentas bancarias y las de su familia también serian intervenidas.

Al realizar la denuncia y la respectiva investigación se llegó al culpable, en la ciudad de Quito, realizando un allanamiento en su vivienda, solo se encontraron 2 computadores, que fueron incautados, en donde un perito informático, que acompañaba a la fiscal, pudo determinar que a estas correspondían las IP, que habrían sido usadas por las computadoras que cometieron el delito, faltando una portátil, que aparentemente tenía el acusado, que no se encontraba, en su poder.

El perfil del acusado, un egresado de ingeniería de sistemas informáticos y computación, de la Escuela Politécnica Nacional, además tiene conocimientos de auditoría y evaluación de sistemas, dominio de lenguajes de programación y algunos conocimientos más, en resultado un semi experto de la tecnología, dedicado al delito informático.

Entre la comunidad de los Crackers podemos encontrar algunos sub-tipos:

**III.G.3.a Crackers de sistemas**: Se les llama a los generadores de programas y a aquellos que alteran el contenido de un determinado programa, por ejemplo, configurando las fechas de expiración de un programa, para que este nunca expire y se mantenga bajo el status de legítimo.

**III.G.3.b Crackers de Criptografía**: Se le llama a aquellos que se dedican a la ruptura de criptografía.

**III.G.3.c Phreaker:** Especializado en las funciones telemáticas, posee un amplio conocimiento para hacer conexiones gratuitas, reprogramar centrales telefónicas, grabar conversaciones de otros teléfonos para luego poder escuchar la conversación en su propio teléfono.

**III.G.3.d Ciberpunk:** Son aquellos, que realizan actos de vandalismo electrónico o digital, destruyen y atentan, en contra de las páginas web o sistemas informatizados.

Tales como nombres de dominios erróneos, crean dominios similares al que quieren atacar, esta fue una de las primeras formas de ataque informático, el algo que en la actualidad, se puede rastrear e inhabilitar, aun hay muchos que lo siguen haciendo por ejemplo, www.bancoenlinea.com a www.bancoenlineas.com.

## III.G.4 CIBER TERRORISTA

Este es el nombre que se le otorga a todos aquellos que se encuentran motivados por creencias religiosas o políticas, buscan causar el miedo, caos e incertidumbre, por medio de la interrupción de las infraestructuras criticas, incluso en algunos casos pueden causar asesinatos. Estos son categorizados como el tipo más peligroso, con una amplia gama de habilidades y objetivos.

Es considerado, el más peligroso atacante digital, existente hasta el momento, en vista de que las regulaciones, restricciones y transportación, se ha vuelto tan estricta en el mundo físico, los terroristas han buscado evolucionar con el mundo de hoy, interactuando de una forma mucho más activa en las redes y sistemas, que representan un sin número de beneficios para sus propósitos delictivos.

Algunos de estos grupos son: KKK en Estados Unidos, ETA en España, grupos neonazis de Bélgica y Holanda y Verdad Suprema en Japón.

**Ejemplos de ciber terrorismo:**

1- Un ciberterrorista podría cambiar remotamente la presión de los gasoductos causando fallas en las válvulas, y desencadenando una serie de explosiones e incendios.

2- Podrían atacar a la próxima generación de sistemas de tráfico aéreo, y hacer que dos aviones choquen entre sí. Este es un escenario realista, desde el momento en que el ciberterrorista también puede interferir los sensores del interior de la cabina.

3- Puede interferir los sistemas de la banca, sus transacciones financieras de dinero y los centros bursátiles.

4- Podrían alterar, en el sistema de un laboratorio farmacéutico, las fórmulas de remedios, causando una gran cantidad de pérdidas humanas.

Las naciones deben de preocuparse y reflexionar mucho sobre el tipo de restricciones y acciones de respuesta en cuanto a este tipo de delincuentes cibernéticos.

## III.H TIPOS DE SOFTWARE DELICTIVOS

Una vez que he descrito los tipos más importantes de agresores en el medio informático, es importante, también describir cuales son las herramientas o software, de los que se valen para cometer los actos delictivos.

### III.H.1 ADWARE

Este es un software de anuncios o advertising, mediante este programa automáticamente recibimos muestras de publicidad durante la instalación de un programa o durante la navegación en la web, usualmente es el que permite la creación de la bombas informáticas o ebombs, que causan que el sistema se vuelva más lento permitiendo así el ataque directo y evitando la defensa apropiada. A su vez, es usual, que algunos de estos adware traigan incorporados protocolos de seguimiento de información personal del usuario. Generalmente este tipo de software no es tan lesivo, ante la protección adecuada de un firewall.

### III.H.2 CRIMEWARE

Este es un software diseñado de manera especial para el cometimiento de delitos financieros o diferentes tipos de fraude en línea, con la finalidad de robar identidades, para acceder a los datos financieros del usuario y así poder obtener los fondos de sus cuentas o realizar otro tipo de transacciones no autorizadas por el dueño de la información, creando réditos económicos para el controlador del crimeware.

Este software instala sin aviso un keylogger que actualiza los cambios en los datos obtenidos, creando una base de datos actualizada, para el que se enriquece, ilícitamente a expensas de otros usuarios.

Este software generalmente puede ser identificado como un troyano y redirigir al navegador de la web de la página original a un duplicado exacto permitiendo al dueño de este recibir, directamente la información que necesita para apropiarse de los bienes económicos del afectado.

Un ejemplo de ataque con este tipo de software, en nuestro país, se pudo ver en el mes de Agosto de este año, cuando una denuncia de delito informático, le permitió ver a las autoridades, la facilidad con que se realizó el desvió ilícito de dinero ($20.000 dólares) desde las cuentas de más o menos 30 funcionarios del Consejo de Participación Ciudadana, lamentablemente de acuerdo a la fiscalía, estos no son hechos aislados.

Y nuevamente hablamos de lo repetitivos que se están volviendo estos delitos, solo por el hecho del ingenio que tienen los delincuentes para cometer esta actividad ilícita y de la dificultad que significa probar el hecho (falta de peritos tecnológicos), para poder encontrar a un culpable, que debería ser sancionado con leyes puntuales al delito cometido.

## III.H.3 MALWARE

Software llamado también, badware, es caracterizado como un código maligno, malicioso o malintencionado, cuyo objetivo principal es el infiltrarse y dañar los equipos tecnológicos e informáticos, en esencia el computador.

Dentro de los Malware, podemos encontrar, virus, gusanos, troyanos, rootkits, entre otros, realmente se considera en función de los efectos que, pensados por el creador, provoque en un computador.

Es importante destacar los estudios realizados por las empresas más importantes en el medio de antivirus, que han realizado con respecto a estos atacantes.

- Resultados provisionales de Symantec publicados en el 2008 sugieren que "Al ritmo al que se ponen en circulación códigos maliciosos y otros programas no deseados podría haber superado, al de las aplicaciones legítimas".

- Según un reporte de F-Secure, "Se produjo tanto malware en el 2007 como en los 20 años anteriores juntos".

- Según Panda Security, "En los primeros meses del 2011 se han creado 73.000 nuevos ejemplares de amenazas informáticas por día, 10.000 más de la media registrada en todo el año 2010. De éstas, el 70 por ciento son troyanos, y crecen de forma exponencial los del subtipo downloaders".

En nuestro país ejemplos de Malware, hay muchos, sin embargo este año el SRI, fue objeto de uno de estos ataques, mediante la proliferación de envíos de emails falsos, que era una carta que pedía a los destinatarios, seguir un manual de instrucciones para evitar futuras sanciones a su empresa, el propósito de estos correos era el de accesar y robar información privada. Se comprobó que algo similar estaba ocurriendo en las oficinas de rentas de Chile.

## III.H.4 SPYWARE

Este software se encuentra diseñado para recopilar información, para después transmitirla a una entidad externa sin consentimiento o aviso alguno, a su debido propietario. Su funcionamiento es muy simple. Se auto instala en el sistema y se ejecuta cada vez que el sistema arranca, utiliza el CPU y se alimenta de la memoria RAM, aminorando la estabilidad del sistema y controlando la navegación del usuario en el internet.

Las consecuencias de la infección de este software, son la perdida de privacidad, una pérdida considerable del rendimiento del sistema de hasta un 50%, con riesgo de que el sistema quede "congelado" y causan problemas al momento de la conexión a la red.

### III.H.5 RANSOMWARE

Es un tipo de Malware, que llega al sistema por medio de spams y que por varios métodos impide al dueño del documento acceder al mismo, colocando una clave y pidiendo un pago en condición de la devolución del archivo impedido, este es un delito no muy conocido públicamente, sin embargo sus ataques son más frecuentes de lo que se sabe. En este tipo de casos se realiza un depósito en una cuenta determinada por el delincuente informático, una vez realizado el depósito por el valor pactado, se devuelve el archivo al usuario.

Por ser recientes este tipo de ataques, las claves han sido fáciles por lo que no ha existido mayor dificultad de los expertos de salvar los archivos, sin necesidad de pagar, pero es seguro que las encriptación irán madurando hasta el punto que el pago, por la no perdida será inminente. Por otro lado el usar una cuenta de banco para cobrar el dolo, hace que el rastrear al delincuente causante del delito, se lo ubique con facilidad.

### III.H.6 ROGUE SOFTWARE

Es un software que se descarga e instala sin conocimiento del usuario o el mismo lo instala creyendo que es una versión de prueba de algún producto, una vez instalado, este software engaña al usuario haciéndole creer que su sistema está infectado con algún tipo de virus y que para arreglarlo debe de pagar una suma monetaria, para eliminarlo.

A menos que el software Rogue sea demasiado fuerte y eficaz, los antivirus y antispyware de mayor renombre actualizados pueden evitar la instalación y la activación del mismo.

## III.I TIPOS DE ATAQUE INFORMÁTICOS

Entre la amplia gama de ataques y formas delictivas que atentan constante y diariamente a la sociedad mencionare los más importantes, pues es muy importante tener muy claras las características de cómo se aplicaran o como se presentaran en un Sistema Informático.:

### III.I.1 BULLYING INFORMÁTICO

Una persona puede ser víctima directa, o sea en forma personal, de un delito informático, cuando ésta recibe ataques tecnológicos directos, que atentan contra su persona, su integridad, su imagen, su desempeño, su vida diaria, a este tipo de ataque se lo denomina Bullying Informático.

Este tipo de Delito se lleva acabo gracias al manejo inadecuado de herramientas informáticas y de comunicación, como son correos electrónicos, mensajes de texto desde celulares, chat,

blogs, o paginas donde se pueden publicar fotos, videos, que generalmente son montajes, todo esto con la intención de ridiculizar a la persona, sin medir las consecuencias del daño que se puede llegar a crear. Es uno de los delitos que debiera tener sanciones importantes, pues la furia y reacción que provoca en el afectado, puede desatar una cadena de acciones maliciosas por lado y lado.

Esto afecta directamente a los derechos constitucionales, de los cuales gozamos todos los ecuatorianos, en este caso se estaría vulnerando el artículo 11, numeral segundo; el artículo 38 numeral cuarto y el artículo 46 numeral 4 y 7 de la Constitución de la Republica del Ecuador:

Art. 11.- EI ejercicio de los derechos se regirá por los siguientes principios:

2. “Todas las personas son iguales y gozaran de los mismos derechos, deberes y oportunidades.

Nadie podrá ser discriminado por razones de etnia, lugar de nacimiento, edad, sexo, identidad de género, identidad cultural, estado civil, idioma, religión, ideología, filiación política, pasado judicial, condición socio-económica, condición migratoria, orientación sexual, estado de salud, portar VIH, discapacidad, diferencia física; ni por cualquier otra distinción, personal o colectiva, temporal o permanente, que tenga por objeto o resultado menoscabar o anular el reconocimiento, goce o ejercicio de los derechos. La ley sancionará toda forma de discriminación”.

El Estado adoptará medidas de acción afirmativa que promuevan la igualdad real en favor de los titulares de derechos que se encuentren en situación de desigualdad.

Art. 38.- El Estado establecerá políticas públicas y programas de atención a las personas adultas mayores, que tendrán en cuenta las diferencias específicas entre áreas urbanas y rurales, las inequidades de género, la etnia, la cultura y las diferencias propias de las personas, comunidades, pueblos y nacionalidades; asimismo, fomentará el mayor grado posible de autonomía personal y participación en la definición y ejecución de estas
Políticas.

En particular, el Estado tomará medidas de:

4. Protección y atención contra todo tipo de violencia, maltrato, explotación sexual o de cualquier otra índole, o negligencia que provoque tales situaciones.

Art. 46.- El Estado adoptará, entre otras, las siguientes medidas que aseguren a las niñas, niños y adolescentes:

4. Protección y atención contra todo tipo de violencia, maltrato, explotación sexual o de cualquier otra índole, o contra la negligencia que provoque tales situaciones.

7. Protección frente a la influencia de programas o mensajes, difundidos a través de cualquier medio, que promuevan la violencia, o la discriminación racial o de género. Las políticas públicas de comunicación priorizarán su educación y el respeto a sus derechos de imagen, integridad y los demás específicos de su edad. Se establecerán limitaciones y sanciones para hacer efectivos estos derechos.

Estos artículos antes mencionados contienen una serie de derechos, que son afectados al momento de sufrir por bullying informático, debido a que el Bullying es considerado un maltrato del bully al afectado.

## III.I.2 DATOS FALSOS O ENGAÑOSOS, (DATA DIDDLING)

Este tipo de delito se realiza desde dentro o fuera del Sistema, el propósito de este ataque generalmente, es dejar fuera de línea a un competidor directo, esta manipulación de datos se torna muy grave, cuando quien la está realizando, tiene claves que le permiten accesar ilimitadamente, con seguridad logrará hacer caer el sistema totalmente, aunque su intensión, sólo haya sido, la de cambiar o manosear los datos del sistema.

Un ejemplo de este delito se presenta comúnmente también, en los bancos, cuando empleados crean cuentas ficticias con el fin de desviar fondos, logran un gran juego, ya que transfieren entre varias cuentas, el dinero. También, se lo ve en estudiantes que entran al sistema de la institución para modificar, calificaciones de exámenes propias y ajenas.

Es parte de este tipo de delitos también, el cambio de los home page, por imágenes turísticas o escandalosas, que reciben los Web sites, generalmente, este, delito queda en total impunidad, pues la falta de conocimiento al respecto y la de personal especializado, no permite desarrollar una investigación que nos lleve al culpable y una penalización.

Todos estos delitos, si se castigan, lo hace directamente el afectado con el culpable, y en la mayoría de las veces quedan sin castigar.

## III.I.3 EAVESDROPPING Y PACKET SNIFFING

Es una de las formas más conocida y utilizada para capturar, loginIDs y Passwords de usuarios, que generalmente viajan sin encrestar, al ingresar a sistemas de acceso remoto. También son comúnmente utilizados para capturar los números de tarjetas de crédito y direcciones de correo electrónico entrante y saliente. Este análisis de tráfico puede ser utilizado también para determinar relaciones entre organizaciones e individuos. Se lo hace por medio del Sniffer, que puede ser colocado tanto, en una estación de trabajo conectada en red, como en un equipo router de Internet, esto lo puede hacer, un usuario con legítimo acceso, o un intruso que ha ingresado por otras vías.

La ubicación y captura del Sniffer, dentro del equipo o la red, constituirá la prueba principal al momento de procesar penalmente al culpable de esta acción.

## III.I.4 SNOOPING Y DOWNLOADING

Estos ataques trabajan en forma muy similar al sniffing, solo que este se realiza con fines de espionaje y robo de información. La idea es no sólo entrar al sistema, sino que descargar a un equipo externo la información capturada.

Un caso de este tipo de delito, se dio en abril de este año, y fue el ataque que sufrió la base de datos de Play-Station de SONY, en donde después de atacar en forma reiterada el sistema, por el daño causado play-station, se ve obligado a liberar sus seguridades, lo que permitió a los atacantes penetrar y extraer miles de números de tarjetas de crédito.

## III.I.5 SPOOFING

La finalidad de este ataque es tomar el nombre o contraseña de otra persona y actuar como ellos. Para llegar a esto, el delincuente ha usado varios tipos de ataques que le ha permitido compilar toda la información que necesita para poder cometer el delito.

También se lo conoce como Looping y tiene la finalidad de hacer desaparecer la identificación y la ubicación del delincuente, que fácilmente se puede encontrar fuera del país. Otra característica del Looping, es que una compañía puede pensar que están siendo atacados por un competidor, cuando en realidad están siendo atacados por un insider, o por un estudiante a miles de kilómetros de distancia, pero que ha tomado la identidad de otros.

Un ejemplo de esto, en la actualidad es muy común en el país que personas o empresas reciban llamadas telefónicas, indicando, que son el banco o cualquier institución que requiera de claves para su utilización, informan que están realizando una verificación de datos rutinaria, por la falta de cultura de seguridad de los usuarios, obtienen con toda facilidad los datos principales de identificación del futuro afectado.

## III.I.6 JAMMING O FLOODING

Este tipo de ataques desactivan o saturan los recursos del sistema. Por ejemplo, un atacante puede consumir toda la memoria o espacio en el disco disponible, así como enviar tanto tráfico a la red que nadie más puede utilizarla.

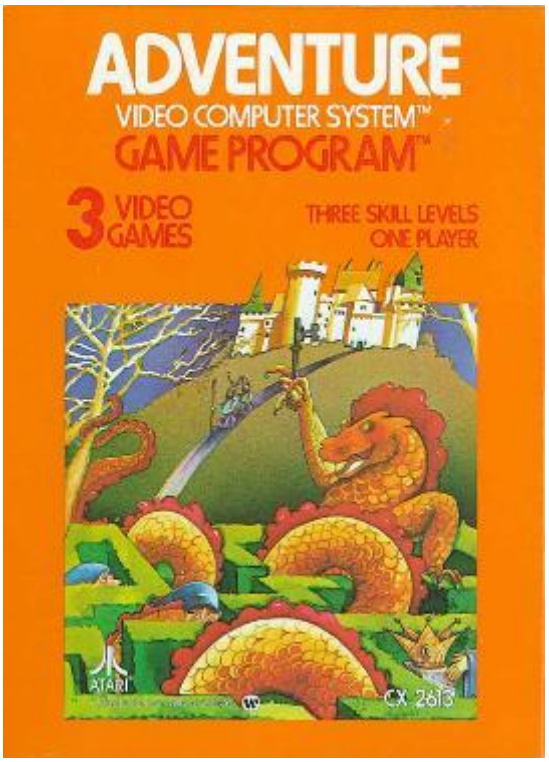
Muchos ISPs (proveedores de Internet) han sufrido bajas temporales del servicio por ataques que explotan el protocolo TCP. Aquí el atacante satura el sistema con mensajes que requieren establecer conexión.

Un ejemplo, es lo que se conoce normalmente como Correos Masivos, envían tal cantidad, que colapsan e interrumpen toda la red, causando bajas totales momentáneas de un sistema, logrando que la red de una empresa este fuera de línea por un periodo determinado de tiempo, lo que le causara una gran pérdida económica.

## III.I.7 HUEVO DE PASCUA (VIRTUAL)

Un "Easter Egg" o huevo de pascua virtual es un mensaje contenido en películas, discos compactos, DVD, programas informáticos o videojuegos. El origen del término se encuentra en el videojuego de Atari Adventure de 1978, que contenía el primer huevo de pascua virtual que se conoce, introducido por el programador Warren Robinett.

Cuadro 1: Primer Easter Egg conocido.
http://en.wikipedia.org/wiki/File:Adventure_Box_Front.jpg




Este tipo de ataque deja al descubierto el tema de que los programadores tendrán el dominio de sus programas siempre y de alguna manera tendrán forma de poder controlarlo.

Este ilícito se realizaría, cuando en el programa adquirido, los programadores han colocado mensajes maliciosos, con el propósito de poder cometer el delito, en el momento que éste se activa como instalado.

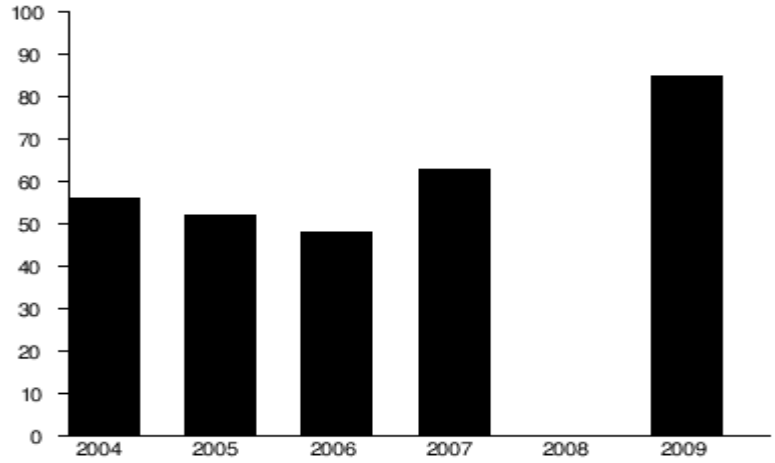
## III.I.8 MANIPULACIÓN DE PROGRAMAS O LOS "CABALLOS DE TROYA"

"El Troyano", es uno de los virus más conocidos en la informática, se presenta como un programa legal. Pero al correrlo ocasiona grandes daños al sistema, el programa crea un acceso que le da el control total, en forma remota a un usuario no autorizado.

Desde que apareció en los sistemas, éste fue conceptuado como un ataque muy maligno, que está dotado de órdenes para realizar el mayor daño posible, en la actualidad también realiza robos de datos e información. Es muy difícil de detectar, es un programa que pesa muy poco, por lo que pasa fácilmente inadvertido.

De acuerdo a un estudio de una empresa responsable del software de seguridad, desde enero hasta junio de 2009, "El número de troyanos está creciendo, y representan el 83% del malware detectado".

TABLA 5: Crecimiento de los Troyanos entre el 2004 y el 2009.-




"Desde el último trimestre del 2010 y durante todo lo que llevamos de 2011, se han detectado 73.000 nuevos ejemplares de malware diarios a nivel mundial, lo que supone un aumento del 26% en el número de amenazas, en comparación con los datos del año pasado. "La mayoría de los nuevos ejemplares de malware son troyanos (70%)", según Luis Corrons, director técnico de PandaLasb.

Este crecimiento desenfrenado de formas de delinquir en la informática, que se muestra en estos estudios, se debe lamentablemente a que, a nivel mundial, no existen castigos drásticos sobre estos delitos, ya que éstos sobrepasan muchas veces los códigos penales, por lo que no hay freno, a este desarrollo sin control de herramientas tecnológicas, que permiten violar todo tipo de información y a todo nivel.

## III.I.9 LA TÉCNICA DEL SALAMI

Es una forma de robo informático, casi totalmente imperceptible a la víctima, que consiste en el robo de pequeñas cantidades de activos de un gran número de fuentes, de allí su nombre, ya que el método equivale al hecho de tomar rebanadas muy delgadas de un trozo de SALAMI sin reducir mucho el trozo total, por lo que las víctimas de este tipo de delito no se dan cuenta que están siendo objeto de un robo, o las diferencias que perciben en sus cuentas, son tan pequeñas que no les interesa reclamarlas.

Este tipo de robo resulta muy valioso, ya que este proceso lo realizan al unísono en muchas cuentas, lo que sumado da una sustracción de un valor interesante.

## III.I.10 FALSIFICACIONES INFORMÁTICAS

Las falsificaciones informáticas se dan, ccuando se alteran datos en los documentos almacenados en forma computarizada, o en documentos escaneados con el propósito de modificarlo a conveniencia. Las herramientas para realizar este delito son los computadores, scanner, ahora también lo son las copiadoras computarizadas, ya que éstas son las que dan el resultado final del delito, es decir la impresión perfecta con todos los detalles del documento falsificado, incluso sin haber tenido un documento original.

Este es uno de los delitos informáticos que lleva varios años, en nuestro mercado, cada vez más perfeccionado, la falsificación de títulos universitarios, para mejorar una hoja de vida, el falsificar un certificado de votación, con el fin de no pagar una multa. Todo esto ha ido en aumento, ya que en los lugares donde se solicitan estos documentos, no son expertos que puedan determinar una falsedad.

## III.I.11 ENTRADAS FALSAS

Son palabras, direcciones, entre otros datos, que se agregan a una información segura y puntual, como sería una base de datos. Tiene dos funciones.

La función original es poder coger una infracción de propiedad intelectual. Mediante la inclusión de una pieza de información falsa en una obra mayor, es mucho más fácil demostrar que alguien ha plagiado ese trabajo.

La segunda función, es en sí maliciosa, dado que se efectúa para crear confusión social, paralizar procesos, mal direccionar al lector.

## III.I.12 MANIPULACIÓN DE LOS DATOS DE SALIDA

Es aquel donde con datos robados mediante una tarjeta de crédito o códigos obtenidos en forma ilícita, se obtiene un beneficio para el delincuente, ya sea haciendo cargos de compras a terceros o burlando los cajeros automáticos.

Un ejemplo directo de este delito seria el robo por cajero automático, antes se lograba solo con el robo de tarjetas y claves, ahora existe toda una tecnología especializada para esto, que al estar en contacto con la tarjeta, extrae y codifica toda la información necesaria, para que el delincuente pueda realizar su ilícito en forma tranquila y segura. Esto no sólo se aplica a las tarjetas de retiro, sino también a las compras realizadas con tarjeta de crédito, cuyo consumo se carga a otra cualquiera.

## III.I.13 PHISHING

Phishing es un término informático que denomina un tipo de delito encuadrado dentro del ámbito de las estafas cibernéticas, y que se comete mediante el uso de una ingeniería social caracterizada por sacar información confidencial de forma fraudulenta, como una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria. El delincuente, conocido como phisher, se presenta como el representante de una empresa, pidiendo la información para él necesaria, luego de esto se crean los escenarios necesarios para hacer creíble toda la información que está dando el delincuente a su víctima.

Luego de verificarse por la victima, y encontrar una aparente veracidad en todo, cae sin problema y acepta el trabajo ofrecido, que tendrá grandes réditos, esto es siempre muy atractivo, Al aceptar la oferta de trabajo, se convierten en víctimas que incurren en un grave delito sin saberlo, el blanqueo de dinero obtenido a través del acto fraudulento de phishing. Una vez contratada, la víctima se convierte automáticamente en lo que se conoce vulgarmente como mulero.

Con cada acto fraudulento de phishing la víctima recibe un interesante ingreso económico en su cuenta bancaria, Una vez recibido este ingreso, la víctima se quedará con un porcentaje del dinero total, pudiendo rondar entre el 10 a 20%, como comisión de trabajo y el resto lo reenviará a través de sistemas de envío de dinero a cuentas indicadas por la pseudo-empresa.

Esto se da generalmente por las necesidades económicas de las personas, este tipo de delito se califica como estafa, que sí, lo es, pero debiera ser tipificada como un delito informático, pues se realiza sólo en forma online, por lo difícil de probar, tipificar, sancionar, ya que hay incluso fronteras de por medio, normalmente, se resuelven privadamente con la reposición del dinero.

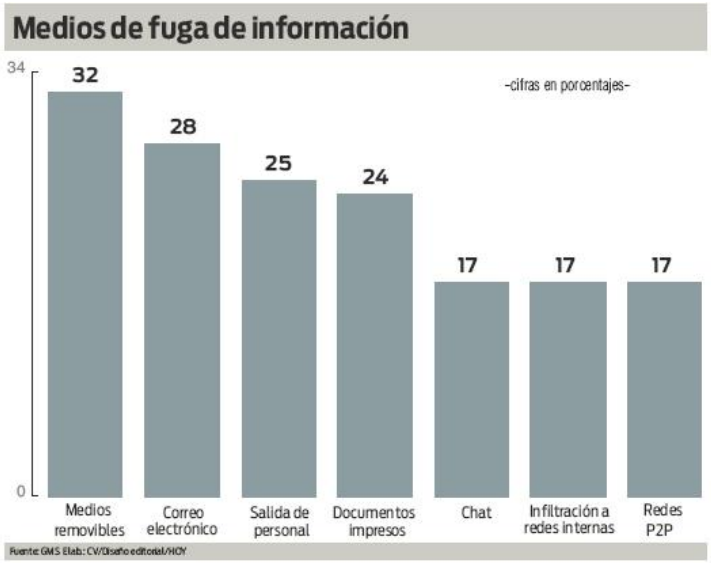
Uno de los tantos ejemplos de esto en nuestro país, se tiene en Octubre del 2011, el caso de Raúl Vásquez, que mediante este sistema, le sacaron de su cuenta $13.000 dólares, luego de realizadas las diferentes investigaciones, se descubrió, que el dinero fue enviado a 3 cuentas, cuyos IP, se encontraban en Perú.

El experto en delitos informáticos de la Fiscalía, indica que es complicado llegar a los autores del delito, primero, porque es por medio online y segundo, casi siempre las maquinas desde donde se realiza el robo, se encuentra en otro país, como Perú y Colombia.

Se logro capturar una banda, que estaba compuesta por ecuatorianos, colombianos y venezolanos, estas bandas arman redes, que se complementan para obtener las informaciones, hay una parte que obtiene datos enviando correos falsos, pero hay otro grupo, los clonadores, que son los que compran a los que roban en las calles, carteras, billeteras, etc., éstos le venden las tarjetas de crédito, el valor que reciben, esta entre $5 y $10 dólares.

En Ecuador los delitos más frecuentes son los virus diseñados para extraer contraseñas y los ataques de phishing, según un estudio realizado por GMC, empresa especializada en soluciones integradas de telecomunicaciones y seguridades.

TABLA 5: Medios de fuga de información. (GMS Elab: CV/diseño editorial/Diario Hoy)




## III.I.14 EL SABOTAJE INFORMÁTICO

El sabotaje consiste en la destrucción con alevosía de información, que contienen los equipos de Informática, con el fin de perjudicar a la entidad dueña de los datos. Esto es una acción considerada como un Delito Informático, que debe penalizarse, por el daño que causa al perjudicado y sobre todo, porque quien realiza este acto, lo hace con toda la intención y con la certeza del daño que está ocasionando.

Dentro de la gran cantidad de delitos de sabotaje Informático, puedo mencionar, actos como el mandar a formatear, el Disco Duro de una maquina, sin haber hecho ningún respaldo de información, y en una fracción cortísima de tiempo borra todo el sistema.

Apagar un Servidor, que nunca se debe apagar, pues su trabajo es soporte de información, por lo que están, 24 horas prendidos y el apagarlo significaría una pérdida enorme de información y un atasco en la transmisión de datos.

## III.I.14.a BOMBAS LÓGICAS O LOGIC BOMBS

Las bombas lógicas, dentro de todos los delitos informáticos y tecnológicos, son los que tienen una mayor capacidad de daño a un sistema, ya que no se detectan con facilidad y solo se sabe de ellas cuando explotan y terminan con la información total del sistema.

El delincuente que instale este dispositivo, debe de tener conocimientos especializados, ya que este necesita una programación, que puede ser para tiempo mediato o para mucho tiempo después. Este delito también se usa como una extorsión, ya que se pide algún rédito a cambio de indicar donde se encuentra ubicada la bomba

## III.I.14.b GUSANOS

El delito realizado por medio de gusanos, tiene la finalidad, de infiltrarlos en los programas de procesamiento de datos, su tarea es modificar o eliminar los datos.

Dentro de los delitos se puede decir que los gusanos serán los ataques, que menos repercusiones le hagan al sistema informático, aunque no por esto su intervención deja de ser muy grave, pueden dejar implementado en los sistemas, ordenes que seguirán ejecutándose aun después de haber sido destruidos.

## III.I.14.c VIRUS INFORMÁTICOS

Son elementos informáticos, que se reproducen y se extienden dentro del sistema al que acceden, se contagian con facilidad de un sistema a otro, tienen diversos grados de malignidad y son eventualmente, susceptibles de destrucción con el uso de ciertos antivirus, pero algunos son bastante resistentes.

## III.I.15 PORNOGRAFÍA INFANTIL EN LA WEB

Las redes virtuales de pornografía infantil, son quizás el delito informático mas proliferado y menos castigado, a nivel mundial, el internet como medio de comunicación se ha vuelto el principal instrumento para quienes cometen este delito. Lo que ha hecho, que este ilícito se escape de las manos de la ley.

Se ha aumentado a esto, la gran cantidad de redes sociales como medio de comunicación que existen en la actualidad, que ayudan a difundir y buscar fotografías de menores de edad. Existen grupos de blogueros (personas que tienen una página Web, para emitir diferentes contenidos y opiniones), que se dedican a vender o intercambiar fotos de menores entre los interesados.

Dentro de este delito, también entra el chat infantil, una forma de comunicación que ha adquirido una importancia enorme dentro de la vida diaria de cada persona, esta se realiza, ya

no sólo mediante el uso de un computador, sino también a través de teléfonos celulares que tienen navegación por internet, o a través de un cyber café, que no tienen control de ninguna autoridad con respecto al contenido que están revisando los usuarios y a la edad de estos.

Con este tipo de comunicación, es posible que menores sin el control debido, puedan tomar contacto con desconocidos, que haciéndose pasar por menores, les pidan fotos o acciones que laceren su integridad.

Este tipo de delito, requiere de investigaciones profundas y técnicas para llegar a los culpables, sin embargo, el perseguido al verse cercado, puede fácilmente formatear su computador, borrando de raíz, toda prueba que lo implicase, Es ahí, donde deben actuar los peritos calificados, donde deben, aplicarse fuertes sanciones especificas a estas acciones, que no permitan que estos ilícitos, sigan creciendo y quedando impunes.

## III.I.16 CIBERTERRORISMO

El Ciberterrorismo nacen de la combinación del terrorismo con el Internet, los atacantes que componen los grupos de ciberterrorismo, no juegan, no buscan información, ellos, están en contra de normas y sistemas, son directos y con sus acciones buscan hacer un daño total a la entidad que atacan.

Con sus actos buscan crear una desestabilización de país, hacer presión a gobiernos, utilizando métodos clasificados dentro los tipos de delitos informáticos, especialmente los de los de tipo de Sabotaje.

Realizar un ataque de terrorismo informático, tiene un costo de realización bajo y la mano de obra a utilizar es poca.

El ciberterrorismo puede llevar a una cyberguerra entre países, que a ojos del mundo están bien, sin embargo ambos, se lanzan ataques constantes a sus redes de sistemas, es una guerra en la cual no se ven, no existe daño físico en personas, pero los daños en los sistemas tecnológicos pueden ser de grandes magnitudes.

La ciberguerra y el ciberterrorismo son una parte de las negativas en cuanto a la globalización.

Estos tipo de delitos ya están sucediendo a nivel mundial, un claro ejemplo de esto es lo que aconteció el pasado 30 de Septiembre del 2011, fecha en la que mas de 1400 ordenadores se vieron comprometidos en Asia y Europa del este, mediante un email masivo que afecto a las agencias especiales e instituciones de investigación. Los atacantes se concentraron en 47 víctimas, incluyendo organismos gubernamentales relacionados con el espacio, las misiones diplomáticas, instituciones de investigación y empresas ubicadas en 61 países, incluidos

Rusia, India, Mongolia, Vietnam y la Comunidad de Estados Independientes (antigua Unión Soviética).

En total, los atacantes utilizaron una red de comando y control de los 15 nombres de dominio relacionados con los atacantes y 10 direcciones IP activas para mantener el control sobre la persistencia de 1.465 víctimas.

## III.I.16.a OBJETIVOS COMUNES DE CYBER ATAQUES

Redes de Gobierno y FFAA
Servidores de nodos de comunicación
Servidores DNS locales
Centrales telefónicas digitales
Estaciones de radio y televisión
Centros satelitales
Represas, centrales eléctricas, centrales nucleares.

## III.I.16.b TIPOS DE ATAQUES

Siembra de virus y gusanos
DNS (Cambio en las direcciones de dominio)
Intrusiones no autorizadas.
DDoS (Distributed Denial of Service)
Saturación de correos
Bloquear servicios públicos
Blind radars (bloquear tráfico aéreo)
Interferencia electrónica de comunicaciones

## III.I.17 ATAQUES DE DENEGACIÓN DE SERVICIO

Este ataque se produce por una saturación que sobrecarga el servidor, haciendo que este no pueda trabajar más, no se da abasto para responder la cantidad de solicitudes que recibe. Este tipo de ataque es usado por los Crackers.

Al atacar el sistema o red, lo hace inaccesible para los usuarios verdaderos, provoca perdida de conectividad, porque consume un gran ancho de banda.

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.

## III.I.18 BACK DOORS Y TRAP DOORS

Back Doors o puertas traseras, son programas o partes de estos que permiten acceso no autorizado a un sistema, se insertan, más en la mayoría de los casos, el o los programadores del sistema, los instalan con el fin de realizar procesos de evaluación, depuración, mantenimiento y monitoreo en el proceso de desarrollo del sistema.

El encontrar y utilizar una puerta trasera, es en sí, lo mejor que le puede suceder a un delincuente, debido a que las acciones y procedimientos se reducen a ir libremente por el sistema sin restricciones. Es muy usual que las puertas traseras queden habilitadas y olvidadas, existiendo por años sin ser encontradas o utilizadas.

Los Trap doors son una trampa, que consiste en insertar intervenciones en los procesos, con el fin de recibir movimientos, resultados y acciones realizadas por el usuario, así también guarda la información que recibe y en caso de tener condiciones de habilitación, es decir que algún proceso en el sistema lo activa, causa que estas realicen sus acciones destructivas en el sistema.

## III.I.19 LA LLAVE MAESTRA O SUPERZAPPING

La llave maestra, haciendo merito a su nombre es el medio que se utiliza para abrir cualquier seguridad o archivo en un sistema, este ingreso usualmente se realiza para alterar, eliminar, copiar, agregar o dar uso desautorizado de la información o datos en el sistema.

Un ejemplo de esto, es el, que un delincuente de este tipo sea denunciado y procesado, teniendo a alguien con sus mismas capacidades, podría ingresar al sistema judicial, alterar la sentencia, emitir orden de liberación e incluso realizar suplantación y falsificaciones que anularían el proceso.

## III.I.20 PINCHADO DE LÍNEAS O WIRETAPPING

Uno de los delitos informáticos, más comunes, cometidos en el Ecuador, y aunque existe una sanción con multas, a muy pocos se les multa, por lo que continúan en el ejercicio de este acto delictivo, el cual consiste en la interferencia simultanea de las vías de trasmisión de datos, actúa en forma de filtro, copiando la información a medida que esta fluye, adueñándose de la misma, sin ser notado por los afectados involucrados. Se utiliza un modem, una radio e impresora.

Existen muchas formas para el pinchado, la más simple es el directo, lo que involucra un acercamiento al objetivo, también existen los a distancia, son un poco más complejos, pero a su vez brindan mayor seguridad al delincuente.

El método más efectivo al de transmitir información sea verbal, digital o escrita (en el caso del celular, computador o facsímile), es encriptar o criptografía, de esta manera la persona que está escuchando, no podrá descifrar la información obtenida.

## III.I.21 HIJACKING

El Hijacking no es más que una técnica ilegal, que tiene como objetivo, el secuestro de información, no solamente se puede dirigir a datos, se puede secuestrar, una conexión TCP/IP, una página Web, un dominio, del navegador y sus configuraciones.

Reverse domain hijacking o Domain hijacking: Secuestro de dominio
Home Page Browser hijacking: Secuestro de la página de inicio del navegador

## III.I.22 KEYLOGGER

El keylogger, es un rastro sumamente importante al momento de la recolección de pruebas, en el caso de software, al igual que sus análogos, es enviado por el Internet o por la red, inclusive ingresar al sistema desde una memoria extraíble y en el caso de hardware, interesantemente, es a mi parecer, el más peligroso de todos, físicamente es un símil de plantilla en los de mayor tamaño y un sensor diminuto. Es colocado o instalado en el teclado del sistema que se busca atacar o inclusive en un cajero automático, grabando así todo lo que se digite.

Como hardware estos dispositivos se encuentran disponibles en el mercado y vienen en varios tipos, se los puede encontrar, como adaptadores en línea que se intercalan en la conexión del teclado, como teclados reales del reemplazo que contienen el Keylogger ya integrado y como chips.

## III.I.23 PHARMING

Este tipo de delitos se realizan, creando la explotación de un falla encontrada en los servidores DNS o en los equipos, de manera que, con cualquier acción que realice el usuario en el navegador será redireccionado, a la página de interés o a un duplicado generado por pharmer, esto se realiza con el objetivo de obtener los datos privados del usuario, generalmente datos bancarios.

Este tipo de delitos ocurre en su mayoría, por no decir completamente a nivel internacional y fue de los primeros delitos identificados, debido a las grandes pérdidas económicas que generaban. En el 2005, en Estados Unidos, se inserto un artículo de ley, para combatir el Phishing y el Pharming, imponiendo una pena de cinco años de prisión y una sanción económica a los que realicen y se beneficien de este tipo de actos delictuales.

## III.I.24 SPAMMING

El Spam, es en sí, el correo más común de todos los revisados anteriormente, este nace con el concepto de la cadena, en vez de enviar información uno a uno, se les colocaba en grupos y se les enviaba a todos, esto se genero, de forma que se brindaría una comodidad y facilidad, a los usuarios al momento de quererse comunicar con varias personas.

Este concepto se desvirtúo y corrompió al momento en el que se empezó a utilizar esta facilidad para el marketing, ante el rotundo o parcial éxito de esta acción, inicia el auge del spam o correo basura, denominado de esta manera, debido a que no brindaba más que advertising, causando el colapso de los servicios de correo electrónico y trayendo consigo una serie de virus, gusanos y troyanos, que se enviaban adjuntos, para mayor facilidad de ingreso en los sistemas.

El Spam que al inicio solo afectaba al computador, ahora se extiende de modo que ataca a todos los dispositivos electrónicos o telemáticos, que posea habilitado una conexión a la Web o recepción de mensajes. Esta extensión no se queda ahí, sino también se ha encontrado la forma de infectar a los dispositivos, de forma que sin que el propietario de este sepa, envía spams a los demás por comando del victimario.

## III.I.25 CARDING

Es la denominación que se le imputa, a todos aquellos que realizan un uso ilegal de la información de tarjetas de magnéticas, ópticas, crédito, debito, descuento, duplicándolas para beneficio propio o de terceros.

Así también se puede crear de la nada, es decir, que mediante procedimientos digitales similares a los que utilizan las entidades emisoras de tarjetas de crédito, se crea un fantasma, el cual es reconocido por el sistema como si fuese real y se utiliza generalmente para realizar compras a distancia por Internet y efectuar pagos.

Un ejemplo de esto ocurrió el pasado 1 de Octubre del 2011, cuando la víctima Marieta Campaña, recibió 3 mensajes del Banco de Guayaquil que avisaban de la sustracción de 100 dólares en cada uno, su mayor sorpresa fue encontrar que su tarjeta seguía en su poder, El robo que sufrió la señora Campaña de su cuenta bancaria le hace parte de las más de 1.600 denuncias por delitos informáticos receptadas por el Ministerio Público a nivel nacional hasta octubre del 2011.

Un reporte emitido por la Fiscalía, en agosto pasado, señalaba un aumento en este tipo de fraudes. El análisis afirma que se pasó de 168 casos denunciados en el 2009 a 2.099 en el 2010, y se registraron 1.360 solo entre enero y junio del 2011.

La tarjeta de crédito Visa, ha aumentado sus movimientos para combatir el fraude en la Red así como para aumentar la confianza de los consumidores en el comercio electrónico.

En un comunicado la empresa de tarjetas de crédito, expresó que “es más fácil tomar medidas por nosotros mismos, antes que, esperar medidas regulatorias por parte del gobierno”.

## III.I.26 SICARIATO INFORMÁTICO

Cuando escuchamos la palabra "sicariato", en lo primero que pensamos es a quien se mato o a quien se mando a matar y el tipo informático en realidad no es muy diferente con el concepto de que, se busca castigar a aquellos a los cuales se les ordena dar por terminado una vida o un sistema.

Aquí se puede apreciar algunos aspectos, primero esta la contratación, planificación, organización, guía o directiva de acción contra algún ser vivo, es decir todo lo que indique vestigios del proceso del delito.

Segundo esta el castigar este tipo de acción directamente en los sistemas informáticos, electrónicos, magnéticos, telemáticos o análogos, con el objeto de prevenir algo que ya ocurre y sólo puede ponerse más en uso, que es el pago a personas para destruir sistemas físicos o digitales, por beneficio de un tercero, el cual puede ser económico o estratégico.

Como mencioné esto es algo muy importante, debido a que, ya es una realidad en nuestro país, en la web sé puede encontrar sin mucha investigación, paginas que ofertan servicios de sicariato, tanto hacia personas, como hacia sistemas informáticos importantes, y esto, se esta difundiendo más y más, de forma alarmante al punto, que en poco tiempo llegará a ser una preocupación significativa para el órgano rector.

Esto porque, ya en Ecuador, se entra a un buscador de internet y es común encontrar paginas,

"Anuncio n.º A21155 ¿Tienes problemas graves con otras personas?, ¿te molestan los cobradores de tus deudas?, ¿no te pagan y se ríen de ti?, ¿quieres librarte de quien te molesta?, ¿tu pareja te es infiel y lo quieres fuera de tu vida para siempre?, ¿quieres cobrarle con la vida a quien te falló?, ¿quieres heredar rápido y no puedes hacerlo porque aún vive?, ¿tu jefe te botó de tu trabajo y quieres vengarte?, ¿hay otra persona atrás de tu pareja y quieres librate de ella?, ¿quieres cobrar un seguro de vida pero aún no muere?, ¿quieres quedarte con la pareja de otra persona pero esa persona te está haciendo tato?, ¿quieres quedarte con la fortuna de tu pareja?, Nosotros te libramos y te ayudamos en todos estos problemas. Contáctanos a nuestro correo: santo-tomas-2008@hotmail.com, y danos detalles de tu problema y te ayudaremos con toda la discreción del caso, 100% de eficiencia". Tan "profesional" es el trabajo que ofrecen entregar fotos del "cliente" (víctima) una vez realizada la tarea". (1)

Los servicios de asesinos a sueldos que ofrecen, es hasta por $400 dólares.

## III.J SITUACIÓN ECUADOR

Los delitos informáticos, en realidad no son noticia nueva en nuestro país, es más, es algo que ha convivido con nuestra sociedad desde los inicios de la informática y en alguna forma se ha cubierto hasta cierto punto, lo que se creía, era necesario para evitarlos legalmente hablando, en los últimos cinco años, estos actos delictuales han despuntado de forma alarmante y

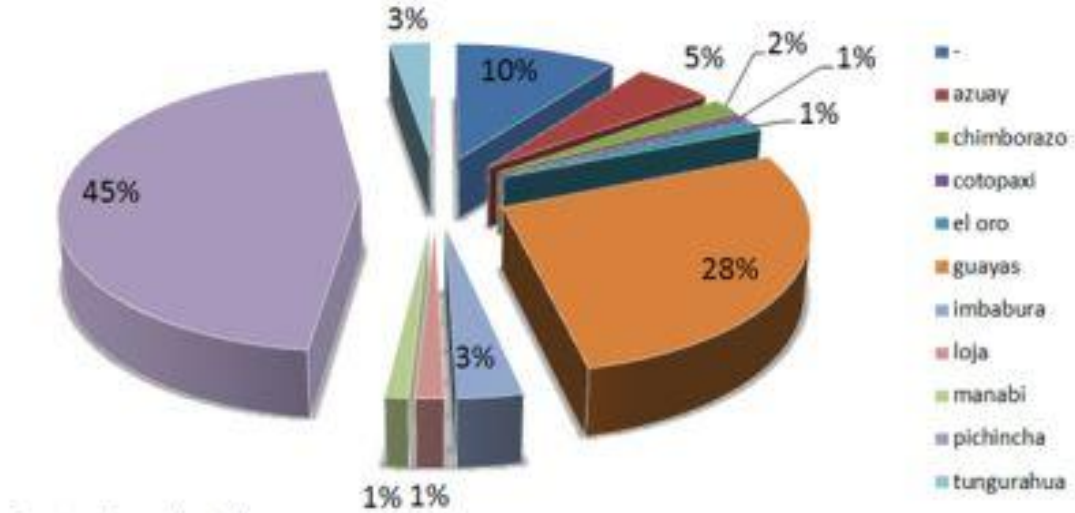
(1) Diario Hoy, Sección Actualidad, 21 de abril del 2008.

desproporcionada, cosa que no debería sorprendernos, pues la tecnología avanza extremadamente rápido.

El Ecuador, es un país que a nivel de Sudamérica, está considerado entre los cinco más prominentes y desarrollados en el mercado tecnológico, ojo, no como productor, sino como consumidor tecnológico, es decir, la plaza ecuatoriana es una de las más rentables y atractiva para las diferentes marcas de productos tecnológicos, que ven a Ecuador, como un cliente potencial, pero este gran desarrollo, nos ha vuelto muy vulnerables, junto a otros países como Colombia, Chile y Argentina.

Según los estadistas, el Ecuador, solamente en este año, ha tenido un promedio aproximado de 6000 denuncias, en lo que respecta al sector bancario, 1364, en el sector privado, el sector público, también ha recibido su parte, en lo que concierne a este ámbito delictual.

Ha sido tal el auge y magnitud en cantidad, que las empresas de Seguridad y Antivirus, que tienen representaciones en el país, se han encargado de realizar, censos, cuadros porcentuales y estudios, sobre los ataques que han sido objeto las provincias del Ecuador, a continuación se presenta un esquema estadístico, realizado por la empresa Karpersky, de los intentos de infección en diferentes dispositivos y empresas. Este cuadro se realizó con los resultados obtenidos de los registros en las maquinas, de los usuarios por sus direcciones IP y su ubicación geográfica dentro del país.




Fuente: Kaspersky Lab

Como se puede ver en la grafica las provincias más afectadas por esta ola de delitos son Pichincha con un 45%, seguido por el Guayas con un 28% y el Azuay con un 10%, esto se da pues son las provincias con mayor cantidad de población y por ende se encuentran las ciudades con un avance tecnológico considerado.

Al momento, se están realizando una serie de revisiones a las leyes actuales, por diferentes figuras públicas, sobre todo en el sector financiero del Ecuador, que a fin de cuentas es el más afectado, en torno a estos delitos, y es el que más alarma a la sociedad, más no es el único campo, en el que se están realizando los delitos informáticos en nuestro país.

De acuerdo a la Constitución de la Republica del Ecuador y a varios artículos dicta que:

Art. 3.- Son deberes primordiales del Estado:

1. "Garantizar sin discriminación alguna el efectivo goce de los derechos establecidos en la Constitución y en los instrumentos internacionales, en particular la educación, la salud, la alimentación, la seguridad social y el agua para sus habitantes".

Esto no se puede llevar a cabo si gracias a estos delincuentes se afecta a la economía del Estado y sus contribuyentes, luego según el artículo 277 del mismo marco legal, encontramos que:

Art. 277.-Para la consecución del buen vivir, serán deberes generales del Estado:

3. "Generar y ejecutar las políticas públicas, y controlar y sancionar su Incumplimiento".

De acuerdo a esto, debido a la cantidad de delitos que se han llevado a cabo se entiende, existe una falta al control de los mismos, por parte del Órgano Legislativo. Estos hechos pasan impunes no en su totalidad, pero sí, en su mayoría, permitiendo que esta nueva denominación de delincuentes, causen inestabilidad económica, pánico e incertidumbre social.

Y por ultimo en su artículo 393 de la Constitución de la Republica del Ecuador:

Art. 393.- "El Estado garantizará la seguridad humana a través de políticas y acciones integradas, para asegurar la convivencia pacífica de las personas, promover una cultura de paz y prevenir las formas de violencia y discriminación y la comisión de infracciones y delitos. La planificación y aplicación de estas políticas se encargará a órganos especializados en los diferentes niveles de gobierno".

Al mencionar estos artículos de la Constitución de la Republica del Ecuador, a lo que quiero llegar, no es a que el Estado no funcione como ente regulador, ni nada por el estilo, tampoco que sus leyes sean obsoletas, sino más bien, a que los derechos y salvaguardas en las cuales los ciudadanos nos deberíamos amparar, no están funcionando, que existe una realidad que avanza a pasos agigantados y es la simple necesidad de regulaciones más completas, con una mayor amplitud, que puedan cubrir, los varios tipos de delitos electrónicos que están apareciendo, que van a afectar jurídica y socialmente, para así hacer efectiva la seguridad en

el ámbito informático, porque en sí, la seguridad de la sociedad se está viendo afectada por la falta de leyes y controles.

## III.K. FIGURAS DELICTIVAS EN NUESTRA LEGISLACIÓN VIGENTE

### III.K.1 ESPIONAJE INFORMÁTICO

Art. 202 innumerado primero del Código Penal

"El que empleando cualquier medio electrónico, informático o afín, violentare claves o sistemas de seguridad, para acceder u obtener información protegida, contenida en sistemas de información: para vulnerar el secreto, confidencialidad y reserva, o simplemente vulnerar la seguridad, será reprimido con prisión de seis meses a un año y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica".

Si la información obtenida se refiere a seguridad nacional, o a secretos comerciales o industriales, la pena será de uno a tres años de prisión y multa de mil a mil quinientos dólares de los Estados Unidos de Norteamérica.

La divulgación o la utilización fraudulenta de la información protegida, así como de los secretos comerciales o industriales, serán sancionadas con pena de reclusión menor ordinaria de tres a seis años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica.

Si la divulgación o la utilización fraudulenta se realiza a partir de la persona o personas encargadas de la custodia o utilización legitima de la información, estas serán sancionadas con pena de reclusión menor de seis a nueve años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica".

Este articulo castiga puntualmente al que violente claves o sistemas de seguridad, con dos fines: 1- acceder u obtener información protegida y 2- Vulnerar el secreto o la seguridad. Lo que este articulo no comprende y exime son las posibilidades de ingreso o traspaso de seguridades por medios pasivos, como los que existen en la actualidad, que al momento de ejecutar, no generan violencia al ingreso del sistema, más que nada por programación específica o permiso inconsciente del usuario que lo permite. (Capitulo IV, Art. 4 del Proyecto).

### III.K.2 DELITO CONTRA LA INTIMIDAD O PRIVACIDAD INFORMÁTICA

Art. 202 innumerado segundo del Código Penal

"La persona o personas que obtuvieren información sobre datos personales para después cederla, publicarla, utilizarla o transferirla a cualquier título, sin la autorización de su titular o titulares, serán sancionadas con pena de prisión de dos meses a dos años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica".

Este articulo castiga puntualmente a los que obtienen información con fin de ceder, publicar, utilizar o transferir, más no previene la simple adjudicación, no se expresa sobre el que realice este acto delictivo sea el responsable o un trabajador público, ya que las personas jurídicas también poseen el derecho a la intimidad (Capitulo IV, Art. 5 del Proyecto).

## III.K.3 SABOTAJE INFORMÁTICO

Art. 262 del Código Penal

"Serán reprimidos de tres a seis años de reclusión menor, todo empleado público y toda persona encargada de un servicio público, que hubiere maliciosa y fraudulentamente, destruido o suprimido, documentos, títulos, programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, de que fueren depositarios, en su calidad de tales, o que les hubieren sido encomendados en razón de su cargo".

Este articulo penaliza a todo servidor público que destruya o suprima información, sin embargo, esto no debería limitarse únicamente a los empleados y servidores públicos, en la actualidad, esto ocurre comúnmente en todos los sectores, tanto financieros, privados, entre otros, incluyendo; a su vez, una serie de actividades además de la destrucción y el suprimir, como dicta el presente articulado. (Capitulo IV, Art. 29 del Proyecto).

## III.K.4 FALSIFICACIÓN ELECTRÓNICA

Este delito se incorpora en el Art. 60 de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos e incluida en el Código Penal, se encuentra en el Capítulo III, "De las Falsificaciones de Documentos en General", que forma parte del Título IV, "De los Delitos Contra la Fe Pública", que en su Art. 353.1.

Art. 353 innumerado primero del Código Penal

"Son reos de falsificación electrónica la persona o personas que con el ánimo de lucro o bien para causar un perjuicio a un tercero, utilizando cualquier medio, alteren o modifiquen mensajes de datos, o la información incluida en estos que se encuentre contenida en cualquier soporte material, sistema de información o telemático, ya sea:

- Alterando un mensaje de datos en algunos de sus elementos o requisitos de carácter formal o esencial.

- Simulando un mensaje de datos en todo o en parte, de manera que induzca a error sobre su autenticidad.

- Suponiendo en un acto la intervención de personas que no la han tenido o atribuyendo a las que han intervenido en el acto, declaraciones o manifestaciones diferentes de las que hubieren hecho.

El delito de falsificación electrónica será sancionado de acuerdo a lo dispuesto en el capítulo III "De la falsificación de documentos en general"."

En este artículo se imputa a las personas que con ánimo de lucro falsifican mensajes de datos para lastimar a un tercero. Primero, la falsificación informática actualmente sobrepasa el simple mensaje de datos, involucra también páginas web, archivos, programación, documentos e identidades cibernéticas, como lo son los IP´s. Por último el lucro no es un factor intrínseco o clave para el cometimiento de este acto delictivo. (Capitulo IV, Art. 24 del Proyecto).

## III.K.5 DAÑO INFORMÁTICO

Art. 415 innumerado primero del Código Penal

"El que dolosamente, de cualquier modo o utilizando cualquier método, destruya, altere, inutilice, suprima o dañe, de forma temporal o definitiva, los programas, datos, bases de datos, información o cualquier mensaje de datos contenidos en un sistema de información o red electrónica, será reprimido con prisión de seis meses a tres años y multa de sesenta a ciento cincuenta dólares de los Estados Unidos de Norteamérica.

La pena de prisión será de tres a cinco años y multa de doscientos a seiscientos dólares de los Estados Unidos de Norteamérica, cuando se trate de programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, destinada a prestar un servicio público o vinculado con la defensa nacional".

Sobre este artículo se puede ver claramente que castiga el daño causado con Dolo con el fin de destruir, alterar, inutilizar, suprimir o dañar definitiva o parcialmente los programas o información. Ahora el daño informático sin Dolo, también causa daños que deberían ser indemnizados y por el que se debería castigar al causante. La propiedad informática consta a su vez de Hardware y medios Telemáticos, que deberían ser considerados, ya que se comprenden como el contenedor, de lo que se entiende, se quiere proteger con este articulado. (Capitulo IV, Art. 9 del Proyecto).

## III.K.6 APROPIACIÓN ILÍCITA

Art. 553 innumerado primero del Código Penal

"Serán reprimidos con prisión de seis meses a cinco años y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, los que utilizaren fraudulentamente sistemas de información o redes electrónicas, para facilitar la apropiación de un bien ajeno, o los que procuren la transferencia no consentida de bienes, valores o derechos de una persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas informáticos, sistema informáticos, telemáticos o mensaje de datos".

Aquí lo que se capta, es que se penara a los que utilizan ilegalmente sistemas de información o redes para la apropiación de un bien ajeno o su transferencia, por alteración, manipulación o modificación de los medios informáticos. De todos los artículos, que corresponden al castigo de ámbito delincuencial informático, este es el más completo, más habría que agregar los medios electrónicos y especificar la información como bien protegido. (Capitulo IV, Art. 6 del Proyecto).

## III.K.7 ESTAFA INFORMÁTICA

Art. 563 del Código Penal.- Estafa.-

"El que, con propósito de apropiarse de una cosa perteneciente a otro, se hubiere hecho entregar fondos, muebles, obligaciones, finiquitos, recibos, ya haciendo uso de nombres falsos, o falsas calidades, ya empleando manejos fraudulentos para hacer creer en la existencia de falsas empresas, de un poder, o de un crédito imaginario, para infundir la esperanza o el temor de un suceso, accidente, o cualquier otro acontecimiento quimérico, o para abusar de otro modo de la confianza o de la credulidad, será reprimido con prisión de seis meses a cinco años y multa de ocho a ciento cincuenta y seis dólares de los Estados Unidos de Norteamérica".

Sera sancionado con el máximo de la pena prevista en el inciso anterior y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, el que cometiere el delito utilizando medios electrónicos o telemáticos.

La pena será de reclusión menor ordinaria de tres a seis años, si la defraudación se cometiera en casos de migraciones ilegales".

En este caso, es peculiar el hecho de que para que este alcanzara a suprimir el delito informático, solo se haya integrado el ultimo inciso a este articulo, está más que demostrada que se requiere, de un articulado más fuerte en cuanto al delito y la acción que se busca encuadrar. (Capitulo IV, Art. 18 y 19 del Proyecto).

Constitución de la Republica del Ecuador:

**Art. 52.-** Las personas tienen derecho a disponer de bienes y servicios de óptima calidad y a elegirlos con libertad, así como a una información precisa y no engañosa sobre su contenido y características.

## III.L ANÁLISIS CÓDIGO ORGÁNICO INTEGRAL PENAL

Artículo 103.- **Atentados sexuales a menores de dieciocho años a través de medios electrónicos.-** "Quien a través de medio electrónico o telemático sedujere o intentare seducir con fines de connotación sexual a una persona menor de dieciocho años de edad y proponga concertar un encuentro con el mismo a fin de cometer cualquiera de las infracciones previstas en este capítulo, siempre que tal propuesta se acompañe de actos materiales encaminados al acercamiento, será sancionado con pena privativa de libertad de tres a cinco años, sin perjuicio de las penas correspondientes a las infracciones en su caso cometidas. Se impondrá el máximo de la pena cuando el acercamiento se obtenga mediante coacción o intimidación.

Quien a sabiendas de que trata con una persona menor de dieciocho años de edad, por medios electrónicos o telemáticos lo indujere a la realización de manifestaciones sexuales y, a partir de aquello, lo intente obligar a realizar conductas por vía de amenazas será sancionado con la misma pena privativa de libertad cinco a siete años.

Quien utilice o facilite el correo tradicional, medios electrónicos o telemáticos o cualquier otro medio de comunicación para ofrecer servicios sexuales con menores de dieciocho años de edad será sancionado con pena privativa de libertad de tres a cinco años".

En cuanto a este delito, no pueda dar referencia de equivocación o falla alguna, sobre este tema en específico, se ha sido muy minucioso y puntual al punto que al momento han sido cubiertos los puntos neurálgicos, que permiten este acto delictual. Más con ánimo de expresar de una forma más sencilla he colocado dentro del proyecto dos articulados, correspondientes al tema, los cuales me parece aseguraran un poco más el cumplimiento de la norma. (Capitulo IV, Art. 34 y 35 del Proyecto).

**Artículo 115.- Violación de la intimidad.- "**Quien viole la intimidad de otra a través de las siguientes conductas, será sancionada con pena privativa de libertad de seis meses a un año:

1. Capte, grabe o divulgue sin consentimiento palabras de otra no emitidas públicamente, mediante cualquier tipo de instrumentos;

2. Capte, grabe o divulgue sin consentimiento imágenes de otra persona, mediante cualquier tipo de instrumentos;

3. Capte, grabe o divulgue las comunicaciones telemáticas de otra sin su consentimiento; o,

4. Acceda a la información contenida en soportes informáticos de otra, sin su consentimiento.

Si las conductas descritas en los numerales anteriores se cometen por una persona en ejercicio de un servicio o función pública, será sancionada con privativa de libertad de uno a tres años.

No son aplicables estas normas entre cónyuges que hagan vida en común; o convivientes; ni a los padres, madres, guardadores o quienes hagan sus veces, en cuanto a las palabras, imágenes, papeles, correspondencia, comunicaciones telemáticas o informaciones contenidas en soportes informáticos del otro cónyuge con quien haga vida en común; o de su conviviente, hijas o hijos o de las personas menores de edad que se hallen bajo su dependencia.

No son aplicables estas normas para quien divulgue grabaciones de audio y video en las que interviene personalmente.

La divulgación de las palabras, imágenes, conversaciones, telecomunicaciones, informaciones o grabaciones que no sean de conocimiento público, obtenidas mediante cualquiera de las conductas descritas en los numerales anteriores, será sancionada con pena privativa de libertad de uno a tres años".

En este articulo, se cubre la captación, la grabación o divulgación de las palabras, imágenes, comunicaciones y accesos a información, esto último muy importante ya que había recalcado que en el articulado vigente, esto hacía falta, pero aun así se dejan cosas de lado como los archivos, documentos, multimedia ajenos a la comunicación telemática (sonido - video - texto - animación). Cada individuo posee el derecho singular y personal a la intimidad sin importar su estado civil, y los mayores de edad dependientes no deberían de estar aplicables. (Capitulo IV, Art. 4 y 5 del Proyecto).

**Artículo 149.- Aprovechamiento ilícito de servicios públicos (Bypass).-** Quien, de manera ilícita, mediante cualquier mecanismo clandestino o alterando los sistemas de control o aparatos contadores, se aproveche de los servicios públicos de energía eléctrica, agua, derivados de hidrocarburos, gas natural, gas licuado de petróleo o señal de telecomunicaciones y otros para destinarlos a asentamientos ilegales, o para provecho personal o de terceros, será sancionado con pena privativa de libertad de uno a tres años y multa de una a cien remuneraciones básicas unificadas del trabajador privado en general.

Igual pena recibirá la servidora o servidor público que permita o facilite la comisión de la infracción u omita efectuar la denuncia de la comisión de la infracción.

Quienes ofrezcan, presten o comercialicen servicios públicos de luz eléctrica, telecomunicaciones o agua potable sin estar legalmente facultados, mediante concesión, autorización, licencia, permiso, convenios, registros o cualquier otra forma de la contratación administrativa, serán sancionados con pena privativa de libertad de tres a cinco años.

En este articulo, en si esta direccionado a evitar y castigar al que busque enriquecerse acosta de la manipulación de los servicios públicos, la intervención informática en el misma es considerada más como un tipo de herramienta para lograr el fin, y en sí, solo cabe el hacer reseña de la servicios públicos informáticos, es decir, todos aquellos que se tramitan por vía web, así como también los alterables por la vía telemática, como lo es el nuevo sistema de energía eléctrica. (Capitulo IV, Art. 18 y 19 del Proyecto).

**Art. 152 Apropiación fraudulenta por medios electrónicos.-**

"Quienes utilicen fraudulentamente un sistema de información o redes electrónicas y de telecomunicaciones, para facilitar la apropiación de un bien ajeno, o los que procuren la transferencia no consentida de bienes, valores o derechos de una persona, en perjuicio de ésta o de un tercero, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos o mensajes de datos y equipos terminales de telecomunicaciones, serán sancionados con pena privativa de libertad de tres a cinco años.

La misma sanción se impondrá si la infracción se hubiese cometido con inutilización de sistemas de alarma o guarda; descubrimiento o descifrado de claves secretas o encriptadas; utilización de tarjetas magnéticas o perforadas; utilización de controles o instrumentos de apertura a distancia; y, violación de seguridades electrónicas, informáticas u otras semejantes.

Quienes alteren los números de serie físicos y electrónicos que identifican un equipo terminal de telefonía móvil, o estén en tenencia de infraestructura para el efecto, quienes activen y comercialicen estos equipos robados o hurtados; serán reprimidos con las penas señaladas. Sin perjuicio de las sanciones administrativas y adopción de medidas cautelares conforme a la Ley Especial de Telecomunicaciones."

Este articulo indica que el que, facilite o procure transferencia de bienes, valores o derechos, alterando, manipulando, modificando, inutilizando, descubrimiento o descifrando medios que permitan la apropiación ilegal de un bien será castigado; honestamente este es el articulo más completo en cuanto al ámbito delictual tecnológico, ya que es amplia, es decir previene varios aspectos, incluyendo uno de los mas importante, acción como la que está tomando Estados Unidos con los proyectos SOPA y PITA, previniendo casos como lo ocurrido con la pagina MEGAUPLOAD.

**Sección Segunda**
**Infracciones contra la información**

**Art. 203 Base ilegal de datos.-**

"Quien obtenga, compile, archive, transfiera, comercialice o procese datos personales sin autorización judicial o de su titular; o quien ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales; o revelare información registrada en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de una ley, será sancionado con pena privativa de libertad de uno a tres años la persona que:

Si las conductas antes descritas se cometen por parte de una persona en ejercicio de un servicio o función pública, será sancionado con pena privativa de libertad de tres a cinco años".

En este articulo, dice que la persona que acceda, obtenga, compile, archive, transfiera,

comercialice o procese datos personales de forma fraudulenta o revele información obligado a preservar por disposición de ley se le sancionará. Ahora si esta base se falsifica, duplica o no tuviese la obligación de preservación por ley, que sucede, quedaría impune, porque si no está descrito como especifica la ley, el delito no existe, por la tanto la acción no es punible. (Capitulo IV, Art. 9 del Proyecto).

**Art. 204 Daño informático.-**

"Quien dolosamente, destruya, altere, inutilice, suprima o dañe, los programas, datos, bases de datos, información o cualquier mensaje de datos contenidos en un sistema de información o red electrónica, de forma temporal o definitiva; será sancionado con pena privativa de libertad de tres a cinco años y multa de diez a veinte remuneraciones básicas unificadas del trabajador privado en general.

Con igual pena serán sancionados en los siguientes casos quienes:

1. Vendan o distribuyan de cualquier manera programas destinados a causar los efectos señalados en el párrafo anterior;

2. Obtengan una contraseña, código de acceso o datos informáticos similares que permitan acceder a todo o parte de un sistema informático, destinados a causar los efectos señalados en el párrafo anterior; o,

3. Destruyan la infraestructura o instalaciones físicas necesarias para la transmisión, recepción o procesamiento de información en general.

Si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o está vinculada con la defensa nacional la pena privativa de libertad será de cinco a siete años".

Como en el articulo vigente, me permito repetirme, al decir que el daño informático no solo debe ser castigado por dolo, sino también por culpa y error, ya que son conceptos que causan perdidas, así como el bloqueo, que ocurre con los bienes y derechos, que también son dañados, como las páginas web o sistemas públicos y privados que interactúan directamente en la red.

Que ocurre con la pena hacia los generadores del daño, como son los arquitectos de los programas destinados al daño informático, sobre los que por negligencia dejan abiertas puertas traseras y por ultimo cinco a seis años si esto es causado dentro de una entidad gubernamental, teniendo en cuenta el daño gravísimo y costoso que se pudiere suscitar, no solo para la entidad vulnerada si no también a los que dependen de las misma, una indemnización, seria a su vez también requerida. (Capitulo IV, Art. 9 del Proyecto).

**Art. 205 De la intrusión indebida a los sistemas informáticos, de información o telemáticos.-**

"Son responsables de intrusión indebida a los sistemas informáticos, de información, o telemáticos quien por cualquier medio o fin, y con el ánimo de apoderarse de la información contenida en dichos sistemas, o para descubrir los secretos comerciales o industriales, o bien para vulnerar la intimidad de una persona natural o jurídica, sin su consentimiento o autorización, interfieran, interrumpan o se apoderen de cualquier mensaje de datos, serán sancionados con pena privativa de libertad de tres a cinco años y multa de diez a veinte remuneraciones básicas unificadas del trabajador privado en general.

Si la divulgación o la utilización fraudulenta de los datos o información reservada, los secretos comerciales o industriales, se realiza por la persona o personas a las cuales se les encomendó su custodia o utilización, serán sancionados con pena privativa de libertad de cinco a siete años".

Para que se adecúe el tipo, el delincuente debe de tener, animo de apoderarse, descubrir secretos o de vulnerar intimidad, mediante la interferencia, interrupción o apoderación de mensajes de datos y se castigará a su vez, al que divulgue o utilicé ilegalmente siendo el responsable. Esto definitivamente tiene ciertas brechas transgredidles, sin ánimo es demostrativo, lucrarse, ceder, doloso, error, culposo, transferencia o de publicación, en este caso quedaría impune ya que la divulgación expresamente trata sobre los custodios, más no sobre el usuario común. (Capitulo IV, Art. 4 y 5 del Proyecto).

**Art. 206 Falsificación electrónica.-**

"Quien utilizando cualquier medio altere, borre o suprima deliberada e ilegítimamente datos informáticos que generen datos no auténticos con la intención que sean tomados o utilizados a afectos legales como auténticos con independencia de que los datos sean legibles o inteligibles será sancionado con pena privativa de libertad de cinco a siete años".

Actualmente existe una serie de métodos y aplicaciones para la falsificación, sin necesidad de alterar, borrar o suprimir, un usuario puede redirigir a una información errónea, puede crear anomalías o mascaras informáticas y aquí se habla de un acto deliberado cuando no solo se da en esa calidad. (Capitulo IV, Art. 24 del Proyecto).

**Art. 207 Falsedad informática.-**

"Quien copie, clone o imite una página web con la finalidad de obtener la información general que el usuario ingrese en ella, será sancionada con pena privativa de libertad de siete a nueve años".

El margen que existe encuadrado en este articulo es incompleto y especifico, dice el que copie, clone o imite una pagina web, con el fin de obtener información que se ingrese en ella, a lo que puedo preguntar, solo las paginas web ¿contienen información?, es decir qué pasa con el que aplique esto con un sistema, con un IP, un usuario o en una nube informática que no solo maneja datos personales, sino también generales e internacionales, es decir que esta falla permite el que exista algunas opciones grandes de impunidad de parte del delincuente o trasgresor al momento de su cometimiento. (Capitulo IV, Art. 24 del Proyecto).

**Art. 208 Estafa informática.-**

“Quien defraudare a otra, modificando o suplantando el sistema informático que altere su normal funcionamiento, transmisión o mensajes de datos, será sancionado con pena privativa de libertad de nueve a once años”.

El articulo en si es simple más no engloba todas las posibilidades delictivas dentro de este cuadro, un articulo más puntual es requerido. (Capitulo IV, Art. 19 del Proyecto).

**Art. 239 Revelación de información reservada.-**

"La servidora o servidor público que sin justa causa, revele, use o se aproveche de información reservada concernientes al servicio público que tenga conocimiento por razón de su oficio o entregue indebidamente documentos o copia de documentos que tenga a su cargo y no deban ser publicados, cualquiera que sea el soporte en que se encuentren, causando daño a un tercero o al Estado, será sancionada con pena privativa de libertad uno a tres años".

Este artículo se dirige directamente, hacia la penalización del servidor público, en cuanto a la revelación de información respecto al servicio público, la violencia de intimidad también es causada por otros agentes, como el desarrollador de Wikileaks, que en su momento liberó información cruzada entre gobiernos y el intercambio de información entre varias autoridades nacionales.

**Artículo 249.- Defraudación Tributaria.-**

"Constituye defraudación todo acto doloso de simulación, ocultación, omisión, falsedad o engaño que induzca a error en la determinación de la obligación tributaria o por los que se deja de pagar en todo o en parte los tributos realmente debidos, en provecho propio o de un tercero; así como aquellas conductas dolosas que contravienen o dificulten las labores de control, determinación y sanción que ejerce la administración tributaria.

9. Alterar, dolosamente, libros o registros informáticos de contabilidad, anotaciones, asientos u operaciones relativas a la actividad económica, así como el registro contable de cuentas, nombres, cantidades o datos falsos;

10. Llevar doble contabilidad, deliberadamente, con distintos asientos en libros o registros informáticos, para el mismo negocio o actividad económica;

11. Ocultar o destruir, de manera dolosa, total o parcialmente, los libros o registros informáticos de contabilidad u otros exigidos por las normas tributarias, o los documentos que los respalden, para evadir el pago o disminuir el valor de obligaciones tributarias.”

A este articulo, en mi apreciación, en su numeral 11, debería de agregarse los registros o bases informáticas no sólo de contabilidad o de documentos sino, a su vez, los archivos estructurales del sistema, las bases de registro de los contribuyentes.

**Art. 286 Infracciones aeronáuticas.-**

"Son infracciones aeronáuticas las siguientes acciones u omisiones:

1. Todo acto de destrucción, cambio, retiro o interferencia contra las señales, equipos, instrumentos, medios de comunicación y demás instalaciones que, con fines aeronáuticos, hubieren sido colocados por la autoridad competente;

2. Toda alteración y falsificación de la matrícula, manuales de a bordo, registro de mantenimiento;

3. Falsificar partes y repuestos de aeronaves;

4. Todo atentado contra la seguridad de los pasajeros y de las aeronaves, que consista en obstaculizar u obstruir las pistas de aterrizaje, calles de rodaje, plataformas de estacionamiento utilizados por aeronaves;

5. Emitir información falsa por parte de los tripulantes o controladores del tránsito aéreo, durante el servicio de tránsito aéreo;

6. No informar o denunciar, en forma inmediata, ante la autoridad competente, la posición de una aeronave o sus partes, que se encuentre accidentada o abandonada;

7. Portar armas, sin la debida autorización a bordo de la aeronave o en el área de abordaje;

8. Colocar artefactos explosivos o incendiarios en las aeronaves e instalaciones aeronáuticas y su tentativa;

9. Cometer o intentar cometer actos de piratería en contra de una aeronave; u,

10. Obstaculizar la ejecución de las funciones del tripulante, esenciales en la conducción de la aeronave.

Los casos previstos en los numerales 1, 2, 3, 4, 5 y 6 serán sancionados con pena privativa de libertad de uno a tres años; y, los casos previstos en los numerales 7, 8, 9, y 10 serán sancionados con pena privativa de libertad dos a cinco años y multa de diez a treinta remuneraciones básicas unificadas del trabajador privado en general".

Al artículo le falta intensificar la pena, ya que fallas cometidas de este tipo crean una responsabilidad social y económica muy grande, agregar otros medios de transporte, ya que solo se está especificando, con enfoque aéreo, pero estas mismas directrices serian importantes, en embarcaciones fluviales y marinas, o en vehículos terrestres.

En el numeral 2 agregar clonación y documentos de funcionamiento.

En el numeral 3 agregar reemplazo injustificado.

En el numeral 4 agregar destrucción parcial o total, alteración de su estado natural y su tentativa.

En el numeral 5 agregar al usuario en general que emita, proporcione o proponga.

En el numeral 8 agregar artefactos electrónicos, magnéticos, telemáticos e informáticos.

En el numeral 9 agregar o cualquier tipo de acto fraudulento.

En el numeral 10 agregar y las funciones de los encargados de transito, autoridades competentes y de cualquiera de la cual dependa la correcta conducción del vehículo.

**Artículo 300.- Infracciones contra la información pública no clasificada legalmente.-**

"La servidora o servidor militar o policial que, utilizando cualquier medio electrónico, informático o afín, obtenga información a la que tenga acceso en su condición de servidora o servidor policial o militar, para después cederla, publicarla, divulgarla, utilizarla o transferirla a cualquier título sin la debida autorización, será sancionado con pena privativa de libertad de seis meses a un año.

A quien destruyere o inutilizare este tipo de información, se le aplicará la misma pena privativa de libertad.

Si la divulgación o la utilización fraudulenta son realizadas por parte de la persona o personas encargadas de la custodia o utilización legítima de la información, éstas serán sancionadas con el máximo de la pena privativa de libertad".

**Art. 307 Infracciones contra la información pública clasificada legalmente.-**

"La servidora o servidor militar o policial que, utilizando cualquier medio electrónico, informático o afín, obtenga información clasificada de conformidad con la Ley, será sancionado con pena privativa de libertad de tres a cinco años.

A quien destruyere o inutilizare este tipo de información, se le aplicará la misma pena privativa de libertad.

La divulgación o la utilización de la información así obtenida, será sancionada con pena privativa de libertad de siete a once años, siempre que no se configure otra infracción de mayor gravedad.

Si la divulgación o la utilización fraudulenta son realizadas por parte de la persona o personas encargadas de la custodia o utilización legítima de la información, éstas serán sancionadas con el máximo de la pena privativa de libertad."

Ahora tanto en los artículos 300 y 307 del proyecto de Código Orgánico Integral Penal, se repiten textualmente es sólo la calidad de clasificado y no clasificado, si bien es cierto que la calidad de la información agraviada es diferente en ambos casos en un mismo artículo podría hacerse esta diferenciación e integración de la pena respectiva. Esto, a su vez, también integra

a la violación de la intimidad informática de la que ya antes se ha mencionado tanto en el Código Orgánico Integral Penal como en el Código Penal vigente, esta redundancia puede afectar al momento de la imputación al delincuente creando su impunidad en cuanto a este delito.

## III.M LEGISLACIÓN INTERNACIONAL

Un punto interesante de revisar es la legislación Internacional, ya que los delitos Informáticos, a medida que se perfeccionan, cada vez es más común que pasen las fronteras de un país.

Al revisar toda la información internacional, vemos el hecho de que los delitos informáticos no han sido una temática conflictiva que nace de la noche a la mañana, sino más bien una figura que se ha ido configurando desde el nacimiento de la computación y fortaleciendo a medida de que han avanzado los medios tecnológicos.

Encontramos también que muchos países se han ido preparando de forma continua ante el avance de los delitos informáticos, que se han hecho acuerdos de colaboración, incluso que el continente europeo lleva más de diez años trabajando, en modo de cooperación entre los países miembros de ese continente.

Con este tipo de delitos, vemos las dificultades que enfrentan muchos países en cuanto a la territorialidad y competencia jurisdiccional internacional, ya que un porcentaje alto de crímenes se realizan de un país a otro, en el caso de Ecuador, esto se reflejó, en un principio con el Skimming o clonación de tarjetas de crédito las cuales eran usadas en las Repúblicas hermanas de Perú y Colombia, debido a esto existe una posibilidad muy grande de que el agresor y la víctima estén sujetos a leyes penales diferentes.

Para este tipo de casos las naciones del mundo han pactado acuerdos, de carácter internacional, como lo es, el Acuerdo de la Ronda Uruguay, en su artículo 10 “Toda información que por su naturaleza sea confidencial o que se suministre con carácter de tal a los efectos de la valoración en aduana será considerada como estrictamente confidencial por las autoridades pertinentes, que no la revelarán sin autorización expresa de la persona o del gobierno que haya suministrado dicha información, salvo en la medida en que pueda ser necesario revelarla en el contexto de un procedimiento judicial”, los datos.

Más sin adoptar una posición inquisidora, ni con ánimo de restar la debida importancia de los mismos, me atrevo a cuestionar la validez de todos estos mencionados, en la actualidad. Es con ahínco que retomo la problemática o dificultad más grande a la que se enfrenta la norma, control y regulación de estos delitos y de este medio, es la extraterritoriedad, el hecho de que no se produzcan o generen solamente a nivel nacional, ha creado una gran barrera para las naciones de todo el mundo, que han tenido que enfrentar con el pasar del tiempo impedimentos como:

- Falta de acuerdos globales acerca de qué tipo de conductas deben constituir delitos informáticos.

- Ausencia de acuerdos multilaterales en la definición legal de dichas conductas delictivas.

- Falta de experticia de la policía, fiscales y otros funcionarios judiciales en el campo de los delitos informáticos.

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

- Carácter transnacional de muchos delitos cometidos mediante el uso de computadoras.

- Ausencia de tratados de extradición, de acuerdos de ayuda mutuos y de mecanismos sincronizados que permitan la puesta en vigor la cooperación internacional.

Mas todos estos impedimentos se han convertido en vacíos, en la lucha de lo que se quiere combatir, en este momento ya no se necesita de más acuerdos, sino más bien, de un solo convenio, mediante el cual, la creación de lo que considero, sería la respuesta adecuada a nivel internacional, conformar una alianza entre diferentes naciones, primero uniéndose países hermanos, los que comparten fronteras y luego por territorios, que se forme un organismo internacional, con representantes de todos los miembros, los cuales deberán trabajar en un marco de regulación y control de los delitos informáticos a nivel mundial.

Cada país al momento incluye dentro de su jurisprudencia, los delitos informáticos, sus clases y castigos, más esto, no es igualitario para todos, van acorde a su legislación, lo que causa, que no exista un apropiado manejo de la justicia internacional.

Ahora con la creación de un organismo mundial las penas, los delitos y el marco legal rector de los mismos, será igual aquí y en la China, lo cual facilitará el castigo y sobre todo el control de los usuarios que busquen vulnerar con el cometimiento de estos delitos nacional e internacionalmente.

Un ejemplo claro de esto, podría ser, el que yo reserve una habitación de un hotel en Londres, a través de una página web y pague la reservación completamente, pero por motivos de fuerza mayor, naturales, los aeropuertos cerraron y no pude viajar, entonces por lógica un porcentaje de la reserva me tiene que ser devuelto, por la página web, que actuó de intermediaria y que, al fin y al cabo realizo la gestión comercial.

Pero si la página se rehusare a hacer esto, ante quien podría presentarme, el caso por lógica debería de presentarse en el país en el que se hizo la transacción o en el país de origen del gestor de la página web y bajo que normas legales se regiría el proceso.

Otro ejemplo más común y sencillo, hubo un usuario que en amazon.com, ofreció y vendió ciertos artículos, mismos que les fueron pagados en su totalidad y nunca fueron entregados, ni se recibió justicia para los cerca de 100 afectados, pues al reclamar no se sabía qué país debía formalizar de estafador al vendedor.

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

Estos ejemplos son sólo unos de las muchas dificultades que se han presentado dentro de la sociedad y que por falta de un ente regulador internacional nunca se pudieron solucionar.

En el contexto internacional son realmente contados los países, que poseen una legislación apropiada, para la penalización de los Delitos Informáticos, de éstos sobresalen Chile y Argentina en América Latina, España, Francia, Holanda, Gran Bretaña, Austria y Alemania en el continente Europeo y Estados Unidos en Norteamérica. Considero importante para este estudio y como base para el proyecto que propongo, el mencionar, aspectos relacionados con la ley, así como los delitos informáticos que persiguen.

## III.L.1 CHILE

"De todos los países latinoamericanos Chile fue el primer país en sancionar una Ley contra delitos informáticos, esta entró en vigencia el 7 de junio de 1993. Refiriéndose a delitos, como:

La destrucción o inutilización de los de los datos contenidos dentro de una computadora, que es castigada con penas de prisión. Asimismo, dentro de esas consideraciones se encuentran los virus.

La conducta maliciosa tendiente a la destrucción o inutilización de un sistema de tratamiento de información o de sus partes componentes o que dicha conducta impida, obstaculice o modifique su funcionamiento.

La conducta maliciosa que altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información."(14)

## III.L.2 ESPAÑA

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

La realización por cualquier medio de destrucción, alteración, inutilización o cualquier otro daño en los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.

La violación de secretos, el espionaje y divulgación, aplicando pena de prisión y multa.

---

(14) Legislación Chilena
(15) Legislación Española

Las estafas con ánimo de lucro valiéndose de alguna manipulación informática, sin detallar las penas a aplicar en el caso de la comisión del delito." (15)

### III.L.3 FRANCIA

"En enero de 1988, este país dictó la Ley relativa al fraude informático, en la que se consideran aspectos como: Intromisión fraudulenta que suprima o modifique datos.

Conducta intencional en la violación de derechos a terceros que haya impedido o alterado el funcionamiento de un sistema de procesamiento automatizado de datos.

Conducta intencional en la violación de derechos a terceros, en forma directa o indirecta, en la introducción de datos en un sistema de procesamiento automatizado o la supresión o modificación de los datos que éste contiene, o sus modos de procesamiento o de transmisión.

Supresión o modificación de datos contenidos en el sistema, o bien en la alteración del funcionamiento del sistema, en si lo que se puede denominar como sabotaje." (16)

### III.L.4 HOLANDA

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

El hacking.

El phreaking.- que es la utilización de servicios de telecomunicaciones evitando el pago total o parcial de dicho servicio.

La ingeniería social, también conocida como el hecho de convencer a la gente de entregar información que en circunstancias normales no entregaría.
La distribución o propagación de virus."(17)

### III.L.5 GRAN BRETAÑA

"Debido a un caso de hacking en 1991, comenzó a regir en este país la Computer Misuse Act (Ley de Abusos Informáticos).

Mediante esta ley el intento, exitoso o no, de alterar datos informáticos es penado con hasta cinco años de prisión o multas.

Esta ley tiene un apartado que específica la modificación de datos sin autorización."(18)

---

(16) Legislación Francia
(17) Legislación Holanda
(18) Legislación Gran Bretaña

## III.L.6 AUSTRIA

"La Ley de reforma del Código Penal, sancionada el 22 de Diciembre de 1987, reprime a aquellos que con dolo causen un perjuicio patrimonial a un tercero influyendo en el resultado de una elaboración de datos automática a través de la confección del programa, por la introducción, cancelación o alteración de datos o por actuar sobre el curso del procesamiento de informacion.

Además contempla sanciones para quienes comenten este hecho utilizando su profesión de especialistas en sistemas."(19)

## III.L.7 ALEMANIA

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

Espionaje de datos.
Estafa informática.
Alteración de datos.
Sabotaje informático." (20)

## III.L.8 ESTADOS UNIDOS

"Este país adoptó en 1994 el Acta Federal de Abuso Computacional que modificó al Acta de Fraude y Abuso Computacional de 1986. Con la finalidad de eliminar los argumentos hipertónicos acerca de qué es y que no es un virus, un gusano, un caballo de Troya y en que difieren de los virus, la nueva acta proscribe la transmisión de un programa, información, códigos o comandos que causan daños a la computadora, a los sistemas informáticos, a las redes, información, datos o programas.

La nueva ley es un adelanto porque está directamente en contra de los actos de transmisión de virus. Asimismo, en materia de estafas electrónicas, defraudaciones y otros actos dolosos relacionados con los dispositivos de acceso a sistemas informáticos, la legislación estadounidense sanciona con pena de prisión y multa, a la persona que defraude a otro mediante la utilización de una computadora o red informática.

En el mes de Julio del año 2000, el Senado y la Cámara de Representantes de Estados Unidos, tras un año largo de deliberaciones, estableció el Acta de Firmas Electrónicas en el Comercio Global y Nacional. La ley sobre la firma digital responde a la necesidad de dar validez a documentos informáticos, mensajes electrónicos y contratos establecidos mediante Internet entre empresas para el B2B (business to business / negocio a negocio) y entre empresas y consumidores para el B2C (businees to consumer / negocio al consumidor)." (21)

Para el entendimiento del párrafo anterior:

---

(20) Legislación Austria
(21) Legislación Alemania
(22) Legislación Norte Americana

**III.L.8.a Business to business:** Es la transmisión de información referente a transacciones comerciales electrónicamente, normalmente utilizando tecnología como la Electronic Data Interchange (EDI), presentada a finales de los años 1970 para enviar electrónicamente documentos tales como pedidos de compra o facturas.

**III.L.8.b Business to consumers;** Este se refiere a la estrategia que desarrollan las empresas comerciales para llegar directamente al cliente o usuario final.

A pesar del sentido amplio de la expresión B2C, en la práctica, suele referirse a las plataformas virtuales utilizadas en el comercio electrónico para comunicar empresas vendedoras de productos o servicios con compradores particulares. Por eso, el uso más frecuente es "Comercio electrónico B2C".

## III.L VISIÓN DEL FUTURO INFORMÁTICO NACIONAL E INTERNACIONAL

El profesor y Profesional Premiado del derecho August Bequai, en su intervención Computer Related Crimes en el Consejo de Europa señala que: "Si prosigue el desorden político mundial, las redes de cómputo globales y los sistemas de telecomunicaciones atraerán seguramente la ira de terroristas y facinerosos. Las guerras del mañana serán ganadas o perdidas en nuestros centros de Informática, más que en los campos de batalla. ¡La destrucción del sistema central de una nación desarrollada podría conducir a la edad del oscurantismo!

En 1984, de Orwell, los ciudadanos de Oceanía vivían bajo la mirada vigilante del Hermano Grande y su policía secreta. En el mundo moderno, todos nos encontramos bajo el ojo inquisidor de nuestros gigantes Sistemas Informáticos y Tecnológicos.

La revolución de la electrónica y la informática, ha dado a un pequeño grupo de tecnócratas un monopolio sobre el flujo de información mundial. En la sociedad informatizada, el poder y la riqueza están convirtiéndose cada vez más en sinónimos de control sobre los bancos de datos. Somos ahora testigos del surgimiento de una elite informática".

Esta reseña hecha por Bequai, por increíble que parezca no ha sido exagerada, ni hecha al azar, ésta realmente, es una visión aterradora de lo que podría ocurrir o que ya está ocurriendo, por tanto es no sólo imperativo, sino mas bien crucial, el crear conciencia social y legal en la nación y en el mundo, así los países, se pueden preparar adecuadamente, para contrarrestar a la criminalidad informática, por la cual, podríamos fácilmente sucumbir, es exorbitante e incontrolable la rapidez del avance de este fenómeno de no ser tratado con la seriedad e importancia que amerita.

## III.M ENCUESTA

Para poder realizar un Proyecto de ayuda a nuestra legislación, sobre las penalizaciones y castigos de los delitos informáticos, a los que al momento somos susceptibles en todo el país.

Me pareció interesante e importante realizar, como una fuente de información adicional, una Encuesta de 9 preguntas dentro del tema Delitos Informáticos, ésta, no se orientó a un grupo específico, al contrario, se entregó en forma general. Es decir a 400 jóvenes, adolecentes, adultos e incluso adultos mayores; de forma directa y por redes sociales, de todo nivel social; de variadas ocupaciones y sectores, con acceso limitado e ilimitado al uso de tecnologías.

Las preguntas se basaron en las situaciones más conocidas, las que se están viviendo frecuentemente, se escuchan en reuniones, en la calle, radio, TV y, se leen en la prensa, pues los delitos Informáticos, están alcanzando a muchos con sus diferentes formas de ataques. El detalle de las preguntas que se hicieron es el siguiente:

**La pregunta 1** ¿Ha escuchado sobre los delitos informáticos?, Me parece importante saber cuánta gente sabe del tema o pone atención a lo que escucha y sabe sobre delito informático;

**La pregunta 2** ¿Sabía usted que el Estado ecuatoriano castiga penalmente sólo los siguientes delitos informáticos? Espionaje o intrusismo informático -Delito contra privacidad informática - Sabotaje informático - Falsificación electrónica - Daño informático - Apropiación ilícita - Estafa informática - Producción, comercialización y distribución de imágenes pornográficas.

La idea de esta pregunta es saber qué opina la gente con respecto a que sólo estos delitos informáticos, son penalizados en nuestro país, y que al momento hay muchos más que deberían tener también un castigo;

**La pregunta 3** ¿Conoce alguna ley que le ampare sobre los mismos? La idea es saber si la gente sabe que en nuestra legislación existen leyes que castigan los delitos informáticos;

**La pregunta 4** ¿Alguna vez ha sido víctima de uno de estos delitos? El propósito es saber cuántos se dan en Ecuador, los ataques de delitos informáticos, saber si la gente tipifica correctamente si un taque sufrido es un delito informático. Como comentario, muchos creen que el que roba por tarjeta de débito es un delito normal de Robo, no lo catalogan como tecnológico;

**La pregunta 5** ¿En caso de que le haya sucedido, recibió justicia sobre el caso? Con esta pregunta, es interesante saber, si la gente ha denunciado el delito, ha buscado culpables y sanciones;

**La pregunta 6** ¿Sabe usted si esto le sucedió a algún conocido? Me interesa saber con esta pregunta cómo se ha diseminado el Delito informático en nuestro país, es decir que si son muchos los conocidos, que han sido víctimas, esto nos muestra cuán rápido está creciendo esta nueva forma de delito;

**La pregunta 7** ¿En ese caso se recibió justicia? En la pregunta 5, quería saber si la persona como víctima había denunciado, sin embargo en esta me interesa saber si el conocido atacado, denunció, logró una penalidad, es importante ya que esto nos muestra que en su mayoría la gente deja pasar el delito.

**La pregunta 8** ¿Le parece que debería haber más difusión sobre las normas que nos defienden y como protegernos de estos delitos? Esta era para saber cuánto interés existe en la gente en saber sobre los delitos informáticos, sus repercusiones y la posibilidad de denunciarlos obteniendo una penalización.

**La pregunta 9** Teniendo en cuenta que hasta el momento sólo existen ocho artículos generales que castigan estos delitos, ¿le parece se deberían crear nuevos tipos de delitos en la ley? Es importante saber qué opina la gente a este respecto, esto nos indicará, lo dañino que se están volviendo los ataques informáticos y la molestia general que existe porque son delitos que normalmente quedan impunes por los vacíos legales.

El resultado general de esta encuesta, es parte de las conclusiones de este proyecto.

# CAPITULO IV: PROYECTO

## PROYECTO DE TIPIFICACIÓN DE ARTÍCULOS LEGALES EN EL ÁMBITO INFORMÁTICO

### TITULO DELITOS INFORMÁTICOS
### CAPÍTULO I
### DE LOS DELITOS CONTRA LA SEGURIDAD DEL ESTADO

**Art. 1.- Extraterritorialidad.-** Cuando alguno de los delitos propios de este título, tenga lugar dentro del territorio ecuatoriano, el victimario, se someterá al correspondiente juzgamiento y penalización, sin importar que tenga su origen en el extranjero.

**Art. 2.- Responsabilidad de los servidores públicos.-** Cuando alguno de los delitos propios de este capítulo, sean efectuados por empleados públicos, sean de rol o contratados deberán responder por su acción delictiva.

### CAPÍTULO II
### DE LOS DELITOS QUE COMPROMETEN LA SEGURIDAD DEL ESTADO

**Art. 3.- Seguridad Nacional.-** Todo el que por medio electrónico, computacional o telemático atente o permita un ataque contra la seguridad interna o externa del Estado ecuatoriano, induciendo, controlando o asesorando a una potencia extranjera o agrupación interna a declarar la guerra al Estado Ecuatoriano, será reprimido con reclusión mayor especial, de doce a dieciséis años, sometido a la vigilancia especial de la autoridad por diez años después de cumplida la pena, e inhabilitado por el mismo tiempo para ejercer los derechos de ciudadanía.

Todo el que atente o permita por medio electrónico, computacional o telemático contra su seguridad interna o externa, induciendo, controlando o asesorando a uno o varios ya sean

extranjeros o nacionales a generar disturbios o violentar las leyes del Estado Ecuatoriano, será reprimido con prisión de seis a ocho años sometido a la vigilancia especial de la autoridad por diez años después de cumplida la pena.

## CAPÍTULO III
## DE LOS DELITOS INFORMÁTICOS

**Art. 4.- Violaciones de comunicaciones electrónicas.-** Será reprimida con pena de prisión de uno a tres años, aquella persona que se valga de cualquier tipo de medio tecnológico, para atentar o permitir el atentado contra el derecho de privacidad, para descubrir secretos personales o transgredir de cualquier forma los frutos recabados, que este acto permita encontrar, sin importar su naturaleza.

**Art. 5.- Acceso indebido.-** El que acceda, intercepte, altere, camufle sin autorización del propietario, mediante algún tipo de medio tecnológico o telemático, para accesar a una información física o digital, cuenta o usuario, sin importar la naturaleza del mismo, sea esta persona natural o jurídica, será penado con prisión de seis meses a dos años, si este acto es cometido por un servidor público será reprimido con prisión de uno a tres años y se aplicara la sujeción a la vigilancia de la autoridad cinco años después de cumplida la pena.

- En concordancia a este articulo, enuncio a la Constitución de la Republica del Ecuador en su artículo 66, numeral 19, dicta:

  Art. 66.- Se reconoce y garantizará a las personas:

  19. El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley.)

**Art. 6.- Apoderamiento informático.-** Aquel que por cualquier medio informático, electrónico, magnético o telemático se apropie, adjudique, adquiera, incaute, usurpe, requise, arrebate o se haga con información, tales como archivos, datos, documentos, mensajes de correo electrónico o cualesquiera otros efectos ajenos a su propiedad y sin debida autorización, será reprimido con prisión de uno a tres años; y, en caso que el delito sea en el sector publico se aplicará la sujeción a la vigilancia de la autoridad cinco años después de cumplir la pena.

**Art. 7.- Uso y transmisión de la información.-** El que con fines fraudulentos, duplique o modifique datos ajenos, ya existentes en un sistema o transmita, difunda o ceda la información duplicada o alterada, será penado con prisión de tres a cinco años, incapacidad perpetua para el desempeño de todo cargo público y en caso que el delito afecte al sector publico se aplicará la sujeción a la vigilancia de la autoridad cinco años después de cumplir la pena de prisión.

**Art.8.- Daños en la propiedad informática, electrónica o telemática.-** El que perjudique, deteriore, corrompa, lesione o hiciese inaccesible la propiedad ajena, privada o restringida, comprendiendo esto la información, el software, hardware y afines de este medio o de cualquier otro modo dañe los datos, programas o documentos electrónicos, contenidos en redes, soportes o sistemas informáticos, con el fin de causar un daño temporal o total. Será reprimido con prisión de tres a cinco años de prisión y en caso que el delito afecte al sector público se aplicará la sujeción a la vigilancia de la autoridad cinco años después de cumplir la pena de prisión.

**Art.9.- Actos parasitarios.-** Todo persona que por cualquier motivo se dedicasen a obstaculizar, interrumpir o denegar las funciones de un sistema, programa o medio online y distribuyan o propaguen para el efecto, bombas lógicas, mailings electrónicos, spams, virus, algoritmos, gusanos informáticos y afines, será reprimido de tres a seis años de prisión y en caso que el delito afecte al sector publico se aplicará la sujeción a la vigilancia de la autoridad cinco años después de cumplir la pena de prisión.

**Art.10.- Uso ilegitimo.-** Todo persona que por cualquier motivo utilice sin autorización equipos, IP y softwares de un sistema informático ajeno para el cumplimiento de acciones fraudulentas será penalizado con dos a cuatro años de prisión y en caso que el delito afecte al sector publico se aplicará la sujeción a la vigilancia de la autoridad cinco años después de cumplir la pena de prisión.

Toda persona que abusando del ámbito de teleproceso o tiempo de uso asignado, se genere un beneficio así misma o un tercero, será penalizado con uno a tres años de prisión.

**Art.11.- Data diddling.-** El que introdujere o presentare por un medio informático, electrónico o telemático datos falsos, con el fin de producir o lograr ilícitos en los procesos o transacciones, a su favor o de un tercero, será penalizado con dos a cinco años de prisión, multado a indemnizar los daños causados y en caso que el delito afecte al sector público, se aplicará la sujeción a la vigilancia de la autoridad cinco años después de cumplir la pena de prisión.

**Art.12.- Sobre el levantamiento de información restringida.-** El que revele, difunda o distribuya información militar, privada, restringida o protegida por los casos de excepción descritos en la Constitución de la Republica de Ecuador, sin el debido consentimiento, se le reprimirá con la pena de tres a seis años de prisión y en caso que el delito afecte al sector publico se aplicará la sujeción a la vigilancia de la autoridad cinco años después de cumplir la pena de prisión.

En concordancia a este articulo, enuncio a la Constitución de la Republica del Ecuador en su artículo 66, numerales 20 y 21, dicta:

Art. 66.- Se reconoce y garantizará a las personas:

20. El derecho a la intimidad personal y familiar.

21. El derecho a la inviolabilidad y al secreto de la correspondencia física y virtual; ésta no podrá ser retenida, abierta ni examinada, excepto en los casos previstos en la ley, previa intervención judicial y con la obligación de guardar el secreto de los asuntos ajenos al hecho que motive su examen. Este derecho protege cualquier otro tipo o forma de comunicación).

**Art.13.- La injuria informática.-** Cualquier persona que ocasione o brinde asistencia, en el cometimiento directo o indirecto de la injuria calumniosa o no calumniosa, a través de medios tecnológicos, tales como televisión, impresos, facsímile, radiodifusión, telemáticos, redes sociales, blogs, internet o por cualquier otro medio o análogo de eficacia semejante, con el fin de lesionar la imagen pública de otra persona, sea esta natural o jurídica, se reprimirá con la pena de uno a tres años de prisión y en caso que el delito afecte al sector publico se aplicará prisión de dos a cuatro años.

En concordancia a este artículo, enuncio al Código Penal Vigente en su artículo 489, dicta:

Art. 489.- La injuria es: Calumniosa, cuando consiste en la falsa imputación de un delito; y, No calumniosa, cuando consiste en toda otra expresión proferida en descrédito, deshonra o menosprecio de otra persona, o en cualquier acción ejecutada con el mismo objeto.

En concordancia a este articulo, enuncio a la Constitución de la Republica del Ecuador en su artículo 66, numeral 7 y 18, dicta:

Art. 66.- Se reconoce y garantizará a las personas:

7. El derecho de toda persona agraviada por informaciones sin pruebas o inexactas, emitidas por medios de comunicación social, a la correspondiente rectificación, réplica o respuesta, en forma inmediata, obligatoria y gratuita, en el mismo espacio u horario.

18. El derecho al honor y al buen nombre. La ley protegerá la imagen y la voz de la persona.).

**Art.14.- Difamación informática.-** Cualquier persona que ocasione o brinde asistencia, en el cometimiento directo o indirecto de la difamación, a través de medios tecnológicos, tales como televisión, impresos, facsímile, radiodifusión, telemáticos, redes sociales, blogs, internet o por cualquier otro medio o análogo de eficacia semejante, con el fin de cobrar deudas, extorsionar o lesionar la imagen pública de otra persona, sea esta natural o jurídica, se reprimirá con la pena de uno a tres años de prisión y en caso que el delito afecte al sector publico se aplicará prisión de dos a cuatro años.

En concordancia a este artículo, enuncio al Código Penal Vigente en su artículo 499-A dicta:

Art. 499-A.- Constituye difamación la divulgación, por cualquier medio de comunicación social u otro de carácter público, excepto la autorizada por la Ley, de los nombres y apellidos de los deudores ya sea para requerirles el pago o ya empleando cualquier forma que indique que la persona nombrada tiene aquella calidad. Los responsables serán sancionados con la pena de prisión de seis meses a dos años.

**Art.15.- Robo de información.-** Todas las personas que sustraigan datos, programas páginas web o sistemas, con el fin de beneficiarse o a un tercero, ejecutando el delito mediante las siguientes circunstancias:

1º.- Uso de algoritmos, virales, spam o bombas electrónicas; serán reprimidos con pena de dos a cuatro años de prisión y en caso que el acceso indebido afecte al sector público se aplicará la sujeción a la vigilancia de la autoridad hasta cinco años después de cumplida la pena de prisión.

2º.- Uso de llaves falsas e inutilización de sistemas específicos de seguridad, alarma o resguardo; serán reprimidos con pena de dos a cinco años de prisión y en caso que el acceso indebido afecte al sector público se aplicará la sujeción a la vigilancia de la autoridad hasta cinco años después de cumplida la pena de prisión.

**Art.16.- Se consideraran llaves falsas.-** Cualquier tipo de herramienta informática, telemática, electrónica, tecnológica o análoga, que se utilice o permita el traspaso a una restricción o cerradura física o virtual.

**Art.17.- Defraudación informática.-** Toda persona que se hubiere hecho entregar cualquier tipo de beneficio proveniente del Estado, para sí mismo o terceros, empleando medios tecnológicos creando una alteración o utilizando una falla existente, con el fin de abusar o lesionar al Estado, será reprimido con prisión de tres a seis años de prisión y se aplicará la sujeción a la vigilancia de la autoridad hasta cinco años después de cumplida la pena de prisión.

**Art.18.- Estafa informática.-** Toda persona que se hubiere hecho entregar cualquier tipo de beneficio para sí mismo o terceros, empleando medios tecnológicos, creando una alteración o utilizando una falla existente, con el fin de abusar o lesionar a una persona natural o jurídica, será reprimido con prisión de tres a seis años de prisión y se aplicará la sujeción a la vigilancia de la autoridad hasta cinco años después de cumplida la pena de prisión.

**Art.19.- Infracciones sistemas públicos.-** El que, física o digitalmente, por medios tecnológicos o telemáticos manipule, altere o evite el normal y original funcionamiento de los sistemas tecnológicos de transportes fluviales, aéreos o terrestres, sistemas públicos informáticos o servicios públicos de energía eléctrica, agua, derivados de hidrocarburos, gas natural, gas licuado de petróleo o señal de telecomunicaciones, para beneficiarse a sí mismo o a un tercero será reprimido con prisión de tres a nueve años y en caso que el delito afecte al sector publico se aplicará la sujeción a la vigilancia de la autoridad hasta cinco años después de cumplida la pena de prisión.

**Art.20.- Infracciones en transporte.-** Son infracciones de transporte las siguientes acciones u omisiones:

1. Todo acto de destrucción, cambio, retiro o interferencia contra las señales, equipos, instrumentos, medios de comunicación y demás instalaciones que, con fines de transporte, hubieren sido colocados por la autoridad competente;

2. Toda alteración, falsificación, clonación de la matrícula, documentos de funcionamiento, manuales de abordo, registro de mantenimiento;

3. Falsificar partes, reemplazo de partes y repuestos a los componentes físicos o digitales de los medios de transporte;

4. Todo atentado contra la seguridad de los pasajeros y de los medios de transporte, que consista en obstaculizar, destruir parcial o totalmente, alterar su estado de funcionamiento correcto y su tentativa, las pistas de aterrizaje, calles de rodaje, plataformas de estacionamiento o puertos utilizados por los medios de transporte;

5. Emitir, proporcionar o proponer información falsa por parte de una persona, los tripulantes o controladores del tránsito de los medios de transporte, durante el servicio activo de transporte;

6. No informar o denunciar, en forma inmediata, ante la autoridad competente, la posición de un medio de transporte o sus partes, que se encuentre accidentada o abandonada;

7. Portar armas, sin la debida autorización a bordo de cualquier medio de transporte o en el área de abordaje;

8. Colocar artefactos electrónicos, magnéticos, telemáticos, explosivos o incendiarios en cualquier tipo de medio de transporte e instalaciones de los mismos y su tentativa de incapacitación del vehículo;

9. Cometer o intentar cometer actos de piratería o cualquier tipo de acto fraudulento en contra de cualquier medio de transporte; u,

10. Obstaculizar la ejecución de las funciones del tripulante, esenciales en la conducción de los medios de transportes y las funciones de los encargados de transito, autoridades competentes y de cualquiera de la cual dependa la correcta conducción del vehículo.

Los casos previstos en los numerales 1, 2, 3, 4, 5 y 6 serán sancionados con pena privativa de libertad de dos a cinco años; y, los casos previstos en los numerales 7, 8, 9, y 10 serán sancionados con pena privativa de libertad tres a seis años y multa de diez a treinta remuneraciones básicas unificadas del trabajador privado en general.

En el caso en el que, lo anterior escrito sea cometido por un servidor público, se reprimirá con prisión de seis a nueve años e incapacidad perpetua para el desempeño de todo cargo público y en caso que el delito afecte al sector publico se aplicará la sujeción a la vigilancia de la autoridad hasta cinco años después de cumplida la pena de prisión.

**Art.21.- Fraude informático.-** Se impondrá pena de prisión de tres a seis años a la persona que, por medio de un artificio físico o digital, tecnológico o telemático, intervenga en el resultado de procesamiento de un sistema, con el objetivo de procurarse un rédito patrimonial para sí o un tercero.

**Art.22.- Hurto informático.-** A la persona que se entregue así mismo o a terceros de forma dolosa, información, de los cuales no posea, goce, propiedad o debida autorización, serán reprimidos con prisión de tres a cinco años y en caso que el delito afecte al sector publico se aplicará la sujeción a la vigilancia de la autoridad hasta cinco años después de cumplida la pena de prisión.

En concordancia a este articulo, enuncio a la Constitución de la Republica del Ecuador, en su artículo 335, dicta:

Art. 335**.-** El Estado regulará, controlará e intervendrá, cuando sea necesario, en los intercambios y transacciones económicas; y sancionará la explotación, usura, acaparamiento, simulación, intermediación especulativa de los bienes y servicios, así como toda forma de perjuicio a los derechos económicos y a los bienes públicos y colectivos).

**Art. 23.- Falsificación Informática.-** Sera penalizado todo aquel que ejecute actos clasificados como Phishing, Skimming y demás formas de suplantación, engaño, clonación, imitación y falsificación de cheques, bonos, datos o afines, todo documento, pagina web, programaciones, sistemas, identificación física o digital, o conjuntos de datos por vía computarizada, digital o telemática, con tres a seis años de prisión y en caso que el delito se realice en el sector publico se aplicará la sujeción a la vigilancia de la autoridad hasta cinco años después de cumplida la pena de prisión.

**Art.24.- Chantaje informático.-** Cualquiera que a través de un medio informático, electrónico o telemático, busque aprovecharse de algún tipo de herramienta para someter o comprometer a otro usuario a actuar en contra de su voluntad, alegando represalias en perjuicio de la persona a la que se dirige o de otro o cualquier otra acción que incida a cumplir con su voluntad, será penalizado con prisión de tres a seis años y en caso que el delito afecte al sector publico se aplicará la sujeción a la vigilancia de la autoridad hasta cinco años después de cumplida la pena de prisión.

**Art.25.- Tapping.-** La persona natural o jurídica, que utilicé bypass, pinche, extraiga o realice cualquier acción que involucre el intervenir, interceptar o receptar contenidos de salida o de entrada a través de medios de comunicación, con la ayuda de cualquier tipo de tecnología, de forma ilegal y sin autorización debida, con la finalidad de obtener y enviar datos; o comandos, incurrirá en la pena de prisión de dos a cinco años y en caso que el delito afecte al sector publico se aplicará la sujeción a la vigilancia de la autoridad hasta cinco años después de cumplida la pena de prisión.

**Art.26.- Planeamiento.-** Todo aquel que gestione, realicé o simule actos fraudulentos tipificados acorde a la ley, en contra de la sociedad utilizando medios tecnológicos o telemáticos será sancionado con una pena de uno a tres años de prisión y en caso que el delito afecte al sector publico se aplicará la sujeción a la vigilancia de la autoridad hasta cinco años después de cumplida la pena de prisión.

**Art. 27.- Rounching.-** Toda persona que se aproveche de las repeticiones automáticas o espacios de oportunidad de los procesos de tecnológicos, con el fin de cometer un acto fraudulento que le genere así mismo o a terceros una ganancia, será reprimido con la pena de prisión de uno a tres años prisión y en caso que el delito afecte al sector publico se aplicará la

sujeción a la vigilancia de la autoridad hasta cinco años después de cumplida la pena de prisión.

**Art.28.- Sabotaje o daño informático.-** La persona que, por cualquier acción altere el estado y las funciones originales establecidas, físicas o sistemáticas, de un dispositivo tecnológico, telemático o a cualquiera de sus componentes, por cualquier medio, será reprimido con prisión de tres a cinco años prisión y en caso que el delito afecte al sector publico se aplicará la sujeción a la vigilancia de la autoridad hasta cinco años después de cumplida la pena de prisión.

**Art.29.- Sabotaje o daño culposo.-** Si en el delito previsto en el artículo anterior, se probara la existencia de culpa, se incurrirá en la misma penalización, con una reducción entre la mitad y dos tercios.

**Art.30.- Sicariato informático.-** La persona que provoque un acto fraudulento por medios informáticos, electrónicos, digitales, magnéticos o telemáticos, a un tercero, afectando a este física o digitalmente por beneficio, precio, pago, recompensa o promesa remuneratoria, será sancionada con pena privativa de libertad de veinticinco a veintiocho años.

Para la imposición de la pena determinada, se sancionará como autores, además del autor material, a quien ofreciere, facilitare o entregare el medio de pago para la comisión de la infracción, o la recompensa que haya sido ofrecida, cualquiera que sea ésta.

Quienes encarguen u ordenen a través de medios informáticos, electrónicos, magnéticos o telemáticos la ejecución de la infracción, así como sus intermediarios y ejecutores, serán sancionados con la misma pena privativa de libertad.

Se entenderá que la infracción fue cometida en territorio y jurisdicción ecuatoriana cuando los actos de preparación, organización y planificación, fueren realizados en el Ecuador, aún cuando su ejecución se lleve a cabo en territorio de otro Estado.

(Esto todavía no se realiza de forma común en la actualidad, la eliminación y estorbo a la competencia o a usuarios simples, el contratar a profesionales o peritos en el área informática, para lacerar o vulnerar a terceras personas naturales o jurídicas, es algo que está muy próximo a suceder, las posibilidades son muy grandes de que esto se convierta en asiduo método delictivo, por ende, es imperativo que antes que esto se vuelva más común y afecte a un mayor número de personas, el anticipo y encuadre penal en cuanto a su sanción).

**Art.31.- Terrorismo informático.-** Toda persona que por medio de verdaderos o falsos nombres o anónimos, remitan consignas, instrumentos y planes de terrorismo a nivel nacional o internacional, serán penalizados con prisión extraordinaria de dieciséis a veinticinco años y multa de veinte salarios mínimos laborales e incapacidad perpetúa para el desempeño de todo cargo público.

**(**En muchos países en la actualidad esto se da mucho, no hay una penalización concreta, para quien incita, hace llamamientos, por medio de una computadora a realizar daños a un determinado lugar como muestra de rechazo a algo, quedan impune, la explicación se juntaron solos).

**Art.32.- Tráfico informático.-** Toda persona que por medio de verdaderos o falsos nombres o anónimos, coordinen acciones o remitan consignas, instrumentos y planes de trafico ilegal a nivel nacional o internacional, concernientes al blanqueo, drogas, personas o de información, con el fin de fabricar, comprar, vender o distribuir, entre otros, serán penalizados con prisión extraordinaria de dieciséis a veinticinco años y multa de veinte salarios mínimos laborales e incapacidad perpetua para el desempeño de todo cargo público.

(Lamentablemente el narcotráfico se masificado gracias a la tecnología, traspasa fronteras a grandes mercados, se realizan grandes negociaciones por internet, e incluso la tecnología les ayuda también al lavado de dinero, pues existen miles de empresas ficticias en línea, cuya finalidad única, es solo esto. cuando se hacen redadas, nunca se capturan computadores o equipos para ser peritados, seria prueba del delito).

**Art.33.- Pornografía infantil.-** Se entiende por esto a cualquier tipo de acción de tipo sexual, real o ficticia, en el que se involucre a menores de edad, que se realicen por medios de tecnología, como sonidos, videos, fotos y afines, que sean divulgados por medios informáticos, electrónicos y telemáticos, a la sociedad.

En concordancia a este artículo, enuncio al Código Penal Vigente, en su Capitulo innumerado y al Código Orgánico Integral Penal, en sus artículos 65 y 100, que dictan:

**Artículo 65.- Pornografía con utilización adolescentes, de niñas o niños.-** Quien utilice adolescente para fotografiar, filmar, grabar, producir, divulgar, ofrecer, vender, comprar, poseer, portar, almacenar, trasmitir o exhibir, por cualquier medio, para uso personal o intercambio, representaciones reales o simuladas de actividad sexual será sancionado con pena privativa de libertad de diecinueve a veinticinco años.

Si la infracción se comete contra una niña o niño menor de doce años de edad o persona discapacitada, será sancionado con pena privativa de libertad de veinticinco a veintiocho años.

Si la víctima es menor de cinco años de edad o cuando la víctima mantenga o haya mantenido una relación afectiva con el agresor; o sea ascendiente, descendiente, hermana o hermano o afines en línea recta o se aprovecharen de una posición de autoridad sobre la víctima, tutoras o tutores, representantes legales, curadoras o curadores o cualquier persona del entorno íntimo de la familia, ministras o ministros de culto o profesionales de la educación o de la salud, la pena se aumentará en un tercio de la pena máxima prevista en esta infracción.

Serán comisados los instrumentos, productos o réditos utilizados u obtenidos del cometimiento de la infracción.

**Artículo 100.- Distribución de material pornográfico e incitación a niños, niñas y adolescentes.-** Quien vende o entregue a menores de edad, material pornográfico, o incite a un menor de edad a la ebriedad, o a la práctica de actos obscenos o le facilitare la entrada a los prostíbulos o lugares donde se exhibe pornografía, será sancionado con pena privativa de la libertad de tres a cinco años.

**Art.34.- Exposición de menores.-** Aquel que obligue o estimule a la realización de actos de exhibición corporal, de uno o más menores de edad y les grave, fotografié o exhiba a terceros,

a través de dispositivos tecnológicos, informáticos o telemáticos, con el ánimo de la obtención de rédito, se le impondrán la pena privativa de libertad no menor de cinco ni mayor de doce años y con cuarenta salarios mínimos laborales de multa.

(Respecto a los artículos 33 y 34, en el mundo del internet existen miles de páginas de toda índole, que contienen exposiciones de menores, están ahí, todos lo sabemos, sin embargo, no se puede penalizar por mirarlas, pero a nivel mundial debiera penalizarse a aquellas redes que permiten que se suba este tipo de información a sus archivos, a nivel país, debiera castigarse a aquellas madres, padres o familiares que exponen a sus hijos a cambio de dinero, sabiendo muchas veces lo que están haciendo, deben ser castigados también aquellos que toman las fotografías).

**Art.35.- Delitos informáticos cometidos por menores con Dolo.-** El que cometa, sea cómplice, instruya o sea instruido para el cometimiento de un delito informático siendo menor de edad, en cuya acción se demuestre dolo, dicho menor o menores se les penalizará con la indemnización de los daños causados, más multa de cinco salarios básicos laborales y de acuerdo a criterio del Juez se le otorgara una de las siguientes medidas:

Uno a tres años en la cárcel de menores
Prestaciones en beneficio de la comunidad que no serán menos 300 horas.
Arresto domiciliario de seis meses a un año.
Internamiento terapéutico (probando que el menor sufre de una adicción informática)
Libertad vigilada

Sea cual sea la determinación del Juez en cuanto a las penalizaciones anteriores, en todas queda terminantemente prohibido el uso de ningún tipo de dispositivo computacional o telemático, durante el tiempo de la sentencia.

(La juventud es una de las mejores herramientas de la tecnología, mientras más pequeño mas experto se vuelven en los sistemas, la curiosidad y la falta de temor a dañar algo los hace ingresar a sistemas, transgrediendo todas las seguridades, al principio lo realizan como una competencia entre amigos, quien mas allá llegue, será el mejor, pero en algunos casos aprovechan el estar dentro, para sacar dinero, hacer compras falsas, usar tarjetas de crédito ajenas, en la actualidad muchos de los autores de estos delitos son menores a 18 años, la excusa de ser menor los hace seguir delinquiendo).

**Art.36.- Atentado contra las pruebas.-** Será reprimido con uno a tres años de prisión, el que por cualquier razón o circunstancia, haya posibilitado la pérdida o inutilización total o parcial de objetos destinados a servir a modo de prueba informática ante la autoridad competente. Si el culpable fuere el mismo depositario, sufrirá la pena de dos a cuatro años de prisión y multa de tres salarios mínimos laborales.

(Respecto a los artículos 34, las pruebas tecnológicas ya son aceptadas al momento de un proceso legal, debe penalizarse a quien, intente dañar, adulterar o las trate de cambiar en contenido y forma).

**DISPOSICIÓN FINAL**

Que los artículos o delitos detallados en este proyecto sean considerados en el medio jurídico y el Código Orgánico Integral Penal.

# CONCLUSIÓN

El derecho tiene como finalidad normar la conducta humana. Los actos del hombre cambian de acuerdo a la época, en la actualidad no existe institución, incluso hogar en el que no se encuentre un computador o un sistema informático.

Dentro de este trabajo de investigación, he podido observar, una serie de aspectos sobre el mundo tecnológico, la delincuencia a la que el Ecuador y el mundo se encuentra sometido, quienes son sus actores, características y herramientas.

Cuando nos mencionan algo sobre delitos informáticos, el primer pensamiento es en Hackers o Crackers, más no se comprende la magnitud de este mundo virtual, en el cual incluso existen terroristas. Los medios tecnológicos nos brindan una serie de comodidades y beneficios, pero así mismo nos atan o encadenan, en un circuito relleno de sistemas interconectados, como un solo cuerpo.

Al momento de iniciar este trabajo, redacté, sobre lo que se esperaba lograr a partir del mismo, sobre los problemas existentes. A su vez procedí a dar una breve y básica conceptualización, sobre lo que es la informática y sus componentes.

El sistema informático, acorde a este trabajo, se revela a sí mismo, como el núcleo del principio de las acciones delictivas. En este caso para el entendimiento del proceso delictivo, encontré que, las tres partes fundamentales, de la informática, son el Hardware, el Software y el Humanware. Ahora ninguno de estos tres es más o menos importante, que el otro, ya que, si cualquiera se encontrase ausente, el sistema deja de existir.

El Hardware comprende básicamente todos los dispositivos físicos. El Software son los datos de funcionamiento y el Humanware es sencillamente, el que permite la existencia y acción de los dos anteriores, es por lógica que entendemos a este grupo, como el corazón, cerebro y pulmones del sistema informático. Importantes son todos y cada uno a un nivel esencial, así también funciona en este circuito tecnológico, si un sistema cae, lo harán todos los demás, los sistemas interconectados pierden su equilibrio y en una fracción de minutos o horas, podría caer el sistema del país entero, caos social, entre muchos imaginables y mencionables, que hacen de este ámbito, un tema de importancia clave.

Existe una amplia gama de sistemas, de tamaño y especialidad varia, acordes a la necesidad por el que fue diseñado. El envase más común y primario fue el computador, debido al avance tecnológico, se desarrollaron otros tipos de variada naturaleza y tamaño, grandes servidores, equipos de escritorio y portátiles, estos últimos facilitando el accionar delincuencial.

Con esto dicho, abarqué el tema correspondiente a la seguridad informática. Con tanta libertad tecnológica, rápidamente se empezó a sentir algunos, por no decir, a los pioneros de lo que hoy entendemos por Delitos Informáticos. Los usuarios empezaron a comprender las posibilidades de los sistemas de información y el navegar “online”, la conectividad aceleró aun más los procesos, al punto qué, aun aquellos que estaban ocupados en las batallas y campañas bélicas, físicas y territoriales, ahora llevan sus conflictos a la web. La informática

ciertamente es un fenómeno mundial, tan importante como lo fueron la rueda, el fuego y la pólvora, en su momento.

Toda la cultura o mentalidad, se ha orientado completamente a la función digital, imponiendo incluso nuevas profesiones, como blogueros, comerciantes, diseñadores e incluso hay profesionales en el estudio del accionar humano en la red, investigadores de las tendencias tecnológicas, definitivamente, la red digital, es un mundo paralelo al nuestro en el cual vuelve a nacer la sociedad, todas sus costumbres se ven afianzadas, repotenciadas, viviendo a gigas por minuto, con una libertad irreal, que no repercute en el medio ficticio, sino en nuestro diario existir, afecta nuestras relaciones, nuestra imagen social, nuestra credibilidad, economía, privacidad, entre otros.

Como se expone en este trabajo, todo lo que comprende a los ámbitos digitales, electrónicos, telemáticos o afines, avanzan de forma irregular y, a su vez, acelerada, desarrollando, nuevos dispositivos, sistemas y programas, que además de brindarnos beneficios, ofrecen también oportunidades nuevas y sumamente complicadas de su uso de una forma delictiva, incluso traspasar la barrera del tipo de delito tradicional, creando nuevos e innovadoras formas no tradicionales, motivo por el cual se suscita la realización de este trabajo de tesis.

El peligro del acceso o intervención de los sistemas, cada día se acrecienta sobre la realidad nacional del país, donde incluso ya se han vulnerado, levemente los sistemas de instituciones públicas, incluyendo la Web de la Presidencia de la República del Ecuador, como una forma de demostrar que lo pueden hacer.

Los métodos de seguridad, por conocimiento personal son muy pobres, sobretodo en el sector privado, cuyo enfoque de protección, hasta hace dos años, consistía meramente en la encriptación y variación de los diferentes antivirus y firewalls. Con el creciente auge de delitos, se ha debido actualizar y mejorar estas defensas y seguridades, al punto que se ha realizado acuerdos con Estados y empresas extranjeras, una de estas empresas fue traída a mediados de Octubre del 2011, trayendo seguridad lógica completa, incluso para ataques causados por el grupo "Anonymous", como los que se dieron a los sistemas gubernamentales durante el 2011, me refiero a esta mejora, con el propósito de demostrar, que la importancia debida, se esta dando recientemente, a las acciones ilegales cometidas en este ámbito.

Para entendimiento del párrafo anterior, considero necesario, dejar claro, que lo que se protege en este tipo de seguridad, se puede clasificar como "lógica" o "digital". El bien que se utiliza y protege es la información, que es el conjunto de datos de cualquier índole.

En este caso la información se convierte en el Bien Jurídico Protegido, sus características y consideraciones son puntuales, es decir se dividen en crítica, valiosa o sensitiva. La Información Critica es aquella totalmente indispensable para la continuidad operativa. La Valiosa, es un activo con valor en sí misma y la Sensitiva es más que nada, aquella que, solo es conocida por las personas que la procesan y solo por ellas.

Las maneras y formas de vulnerar la información, son múltiples e ilimitadas, pero las principales amenazas para la seguridad tecnológica, son las que provienen del "Humanware"

o de los usuarios, pues son ellos, los que idearan diferentes y variadas formas de ataques. El ataque más común es el daño. Este puede ocurrir por dos vías la lógica y la física.

¿De quién nos debemos proteger? Es la pregunta clave, en todo este asunto y es que este tipo de criminal no tiene una edad, o norma de comportamiento, más las puntuales que se han mencionado en este trabajo y la única característica que comparten entre todos, además del manejo de sistemas, es que la persona que comete delitos informáticos, tiene un perfil diferente, al que conocemos del delincuente común, se podría describir en muchos de sus aspectos, como el de un criminal de "cuello blanco". Es una persona con instrucción, muchas veces superior, pues debe conocer de muy buena forma el procedimiento informático. Causan problemas en los sistemas de información, ya sea por satisfacción personal, como una manera de demostrar sus conocimientos técnicos, o lo hace por lograr réditos económicos.

Los ataques a su vez, pueden ser, activos o pasivos. Los ataques pasivos son los accesos sin mayor repercusión, mientras que los ataques activos, involucra de por si acciones como interrupción, intercepción, modificación, fabricación y destrucción de la información.

En lo que concierne al daño físico, se comprende este de dos maneras, una de ellas denominada "sabotaje" y la otra "destrucción", aunque se piense que imparten el mismo fin, son dos acciones completamente diferentes y la diferencia en sí, es muy simple. Aunque la seguridad física comprende muchos aspectos, los principales son los dos antes mencionados, el "sabotaje", es la suspensión, inhabilitación parcial o total de un dispositivo tecnológico o de un sistema computacional, con posible arreglo y la "destrucción", como describe su nombre, se constituye en la eliminación sin posibilidad de recuperación de los equipos o aparatos electrónicos.

Cabe mencionar que en sí, los sistemas y empresas más propensas a los ataques informáticos, ya sean estos físicos o lógicos, son aquellos que, manejan grandes sumas de dinero, transacciones, nominas, entre otros tipos del sector financiero y económico. El mundo de las transferencias y otras facilidades de intercambio comercial "online", es un servicio muy llamativo, pero también es el mundo, con la mayor cabida para los delincuentes informáticos.

Evaluar y controlar permanentemente la seguridad física y lógica del sistema es la base para comenzar a integrar la seguridad como una función primordial dentro de cualquier organismo.

En el tema principal, en lo que se entiende por Delito Informático, es la conducta típica, de generalidad dolosa, que vulnera los derechos y bienes jurídicos protegidos físicos o virtuales, de una o más personas naturales o jurídicas, en la que se utilizan medios tecnológicos, informáticos, electrónicos, telemáticos y afines, como instrumento, medio o fin delictivo.

No basta solo con conocer cómo funciona el mundo informático, electrónico o telemático, sino también es esencial, reconocer quienes y que elementos utilizan, determinar las características y tipos de atacantes, como serán sus intervenciones y cuáles son los principales o al menos los más conocidos utensilios con los que violentan a terceros, a través de este medio.

Es una realidad tangible que en el Ecuador se han preparado y realizado ciertas medidas, en la Ley de Comercio Electrónico, Firma Electrónica y Mensaje de Datos, en la Ley de Propiedad Intelectual y por ultimo reformas en el Código Penal Vigente, para contener el avance y controlar este nuevo ámbito delictivo, marco que hasta hace cinco años podría haber sido seguro, más lo que se ha buscado es crear un entendimiento de lo fundamental, de actualizar e identificar, los nuevos tipos de delito, debido a que la generalidad que se ha implementado hasta ahora, ha vulnerado y debilitado no solo a nuestro sistema judicial, sino a su vez el del Estado y la sociedad, que constantemente y cada día más a menudo son víctimas de estos ataques delictivos, que en una mayoría resultan impunes.

Desde hace algunos años, juristas, han querido o intencionado crear un encasillamiento de los diferentes delitos informáticos, a las figuras típicas de carácter tradicional ya existentes en la ley y no han encontrado todavía una fórmula adecuada que se complemente con los códigos vigentes.

Al momento se aplica una incorrecta restricción de los delitos informáticos, causa de la incorrecta aplicación de la ley penal.

Es muy común que el actor o victimario de estos delitos, no sea ajeno a la escena del crimen, sino más bien que mantengan cierta familiaridad, nexo laboral o personal, siendo esto a su vez un agravante en su contra al momento de realizarse el delito, ya que lo hace con dolo.

Absolutamente todos los delitos informáticos, causan o provocan pérdidas económicas de gran cuantía, ya sea por desvió de fondos, como por sabotaje lógico e incluso alteraciones de procesos en sistemas básicos, como luz y agua. El simple hecho de traspasar la seguridad de un sistema, le cuesta miles de dólares en credibilidad a una empresa, en lo que respecta a su imagen, de entidad segura, sin contar con la información que ha sido sustraída.

Dar y manejarse de acuerdo a un porcentaje de los ataques informáticos que recibe la sociedad o que se denuncian, es no sólo una utopía, sino también caminar a ciegas, ya que no todos los ataques son denunciados o lo que es peor, se los atribuye a un fallo del sistema, a cualquier razón, menos la de un acto delictivo.

Estratégicamente, para que un Estado o sus representantes, tomen una correcta o positiva decisión, se requiere una información lo más precisa posible, por lo mismo decir que el Ecuador tiene un promedio de, tantos ataques informáticos al día, mes o año, simplemente no tiene validez, habría que multiplicar por tres o por cuatro esa cifra, para tener un conocimiento probable, lo propio es concientizar y educar a la sociedad en cuanto a la importancia de la denuncia, ofrecer un sigilo durante la denuncia y proceso, para que estos delitos y sus autores no queden impunes por miedo de represalias o exposición social que les pueda desacreditar.

La norma actual lamentablemente no abarca toda las posibilidades, que en este momento existen en este ámbito delictual, o las que pueden crearse, para poder dar esta aseveración, opinar o determinar esto, durante todo el trabajo se revisó tipos penales que existen en otros países, un poco más adelantados en cuanto al manejo y desarrollo de este tema, como los son Chile y Argentina, que son los más evolucionados en Latinoamérica, así como también, con

países como España, Reino Unido y Alemania, fuertes informáticos en el continente Europeo, entre otros, que brindaron luz al proyecto que se propone en el capítulo 4.

Con respecto al bien jurídico, hay que tener claro, qué es el bien material o inmaterial, que se encuentra guardado y protegido por el derecho, estos bienes son valores legalizados, como la salud, la vida, la propiedad, entre otros. El bien jurídico dentro de los delitos informáticos, asume una protección proveniente de los delitos tradicionales, reinterpretados por supuesto, para así adaptarse a lo que involucra el ámbito tecnológico e informático, subsanando así, las lagunas que se originan debido a los diferentes tipos de comportamientos delictivos.

En cuanto a las auditorias, informes y los peritos, esto es algo realmente esencial, debido a que cumple una multifuncionalidad, de todas las posibles, dos de sus funciones, son las más destacadas. Primero está la aseguración y equipamiento de la seguridad tanto física, como digital, para usuarios e instituciones públicas o privadas. Segundo y quizás la más importante, es la búsqueda "forense" por así decirlo, de cómo se cometió un delito, la recolección de pruebas y la realización de la investigación.

En lo que concierne a los peritos informáticos, en nuestro país contamos con profesionales con preparación y conocimientos superiores a la de los transgresores, que con su potencial pueden encontrar posibles fallas o "leaks", detectar y prevenir el delito, encontrar y recuperar procedimientos, pruebas e ilegalidades acontecidas, el problema no es en si la preparación de los peritos informáticos sino más bien la falta de infraestructura y equipamientos que en la actualidad son deficientes. El ejemplo más claro que tenemos de este tipo de actuación es el caso "Rafael Correa vs Diario El Universo", con la investigación al disco, que se tuvo que llevar a Estados Unidos el disco, que debía ser investigado, pues en el Ecuador, no contamos con laboratorios tecnológicos adecuados para este tipo de análisis.

Además, sobre el tema de los peritos, me gustaría agregar ciertas observaciones, primero es realmente interesante, el hecho de que en Ecuador, habiten un promedio de catorce millones de habitantes, de las cuales más o menos, ocho millones tienen acceso a la tecnología, en diferentes formas, por lo que podrían ser posibles víctimas de estos delitos, y tan sólo tenemos un cuerpo pericial, que abarca, como mucho tres millones de personas a nivel nacional. Como por ejemplo: para la provincia del Guayas sólo existen diez peritos, que no cumplen con la cuota necesaria, para resolver y procesar rápidamente estos delitos, es mi opinión personal el que, el Estado se preocupe de la pronta capacitación de peritos informáticos y de la implementación de laboratorios para análisis de pruebas.

Aunque, es cierto, que los peritos no necesitan ser sólo proporcionados por la función pública, teniendo los medios se puede solicitar los servicios de un perito privado o externo, con el fin de agilitar los procesos, pero, mejores resultados se tendrán, si estos expertos son parte de la función judicial.

Así como tenemos abogados especializados en rama laboral, tributaria, etc., es menester, en la actualidad, tenerlos también en la rama informática, que es un espacio que ha alcanzado un desarrollo vertiginoso en estos tiempos.

La prueba de los delitos, fue un punto muy importante en este trabajo, ya que sin pruebas no hay delito. La prueba es la que dará el soporte al procedimiento para poder establecer la penalización a un delito. Dentro de esto, una de los puntos, también muy importantes, son los diferentes pasos que se debe de seguir, es decir, primero cumplir con los requisitos para que se considere prueba válida ante la justicia, su preservación adecuada hasta el momento de la audiencia y la presentación inalterada.

La tecnología avanza rápidamente, esto es un hecho que no se puede dejar de mencionar, a su vez los delincuentes informáticos avanzan paralelamente, con nuevas técnicas y desarrollos en este ámbito. Lo que sí, es acertado asegurar es que la sociedad, no para de querer mayores adelantos tecnológicos, aun viviendo, la incertidumbre de lo que pueda ocurrir, de lo que aparecerá al siguiente día o inclusive en las próximas horas, es importante decir que, al igual que este trabajo, existen muchas personas tratando de brindar una mayor seguridad tecnológica y justicia para aquellos que han sido victimados, por estas acciones delictuales.

El grado de especialización, conocimientos y las técnicas delictivas se incrementan a grandes pasos, debido a que las personas con este conocimiento ya no sólo actúan culposamente al azar, sino que maliciosamente, maquinan planes y proyectos para delinquir, ya sea a nivel nacional o global, este último, predilecto, de estos delincuentes, ya que brinda mayores opciones de escape con impunidad.

En este investigación se ha puntualizado una serie de ítems muy importantes sobre el mundo informático, la seguridad, entre otros, pero algo, que no se debe pasar por alto, son los tipos de delincuentes informáticos, los programas base que utilizan para sus acciones delictivas y los delitos que se han podido clasificar hasta el momento, de los cuales por increíble o imposible que suene, ningún país a nivel mundial, tiene una protección legal o digital, para todos, cubren la mayoría, pero no todos los clasificados, que se mencionaron en este trabajo de tesis.

Existen diversos tipos de delincuentes informáticos, entre los cuales puntualizo, a los más conocidos, como son los Piratas Informáticos, los Hackers, los Crackers y el Ciber terrorista.

Sobre los Piratas Informáticos, es un tipo de delincuente, que en cada acción que comete señala y demuestra dolo y alevosía, debido a que su única razón de ataque es apropiarse y beneficiarse económicamente, de lo que encuentra.

El hacker, es un usuario sumamente preparado en la informática medular, ellos crean y desarrollan, su delito no radica en robar, ellos sólo están interesados, en cada día saber más. Dentro de lo que comprende el mundo del Hacker, existen una serie de sub-categorías, entre las cuales las más importantes son las siguientes: Script Kiddies, Hacktivistas, Hackers del Estado, Hackers Espía y de Sombrero Blanco.

Cabe recalcar, que sobre los tipos de Hackers antes mencionados, los que existen e interactúan en el Ecuador son los Script Kiddies, Espía y de Sombrero Blanco. Los primeros son los hackers novatos que buscan fama traspasando seguridades de sistemas y deforman o cambian las características de las páginas web, de alguna empresa o institución. Los segundos tienen una trayectoria antigua, muy antigua y que al igual que todo, han evolucionado hasta

ingresar al mundo digital, estos son usuarios que buscan infiltrarse en la competencia de empresas o gobiernos y robar secretos. Los terceros es la clase más común de Hackers, son los investigadores o innovadores, creadores, y en su completa extensión, amantes del conocimiento, algunos de ellos se convierten en peritos o expertos en seguridad informática y se especializan en las pruebas de penetración o metodologías.

Muchos de estos, famosos mundialmente por sus ataques, que incluso han estado presos, ahora son contratados por países, con el fin de precautelar los sistemas de seguridad del estado.

El Cracker, en cambio es un ente dañino que ronda por la web expectante de encontrar oportunidades de beneficiarse así mismo, sin importar el daño que pudiese provocar a los demás. Sus destrezas radican en la invasión de sistemas, descubrir claves y contraseñas con programas, algoritmos o encriptaciones de su autoría, pero sobre todo para el robo de datos, delito que lo sustenta económicamente. Algunos intentan ganar dinero vendiendo la información robada, otros sólo lo hacen por fama o diversión. Entre la comunidad de los Crackers podemos encontrar algunos sub-tipos: Crackers de sistemas, Crackers de Criptografía, Phreaker y Ciberpunk.

De los cuales en el Ecuador solo interactúan los de Sistemas, Phreakers y Ciberpunks. Los primeros son los más comunes y se caracterizan por ser, generadores de programas y alteradores del contenido de un determinado programa. Los segundos se encuentran especializados en las funciones telemáticas, poseen un amplio conocimiento para hacer conexiones gratuitas, reprogramar centrales telefónicas, grabar conversaciones de otros teléfonos para luego poder escuchar la conversación en su propio teléfono. Los últimos son aquellos, que realizan actos de vandalismo electrónico o digital, destruyen y atentan, en contra de las páginas web o sistemas informatizados.

El Ciber Terrorista es un delincuente con otro nivel de peligrosidad en comparación a todos los sujetos que se mencionó anteriormente, es el nombre que se le otorga a todos aquellos que se encuentran motivados por creencias religiosas o políticas, buscan causar el miedo, caos e incertidumbre, por medio de la interrupción de las infraestructuras criticas, incluso en algunos casos pueden causar asesinatos. Estos son categorizados como el tipo más peligroso, con una amplia gama de habilidades y objetivos.

Una vez que tenemos un claro conocimiento de los tipos de transgresores, es importante también conocer las clases de software o programas, que hacen de herramientas y habilitan el acto delictual. En sí, todos son conocidos como Malware, ya que todos producen un daño, más cada uno tiene su característica propia, los básicos son: Adware, Crimeware, Malware, Spyware, Ransom ware y Rogue Software.

Como mencioné en el párrafo anterior, todos estos software o programas, producen daños y afectan a los sistemas, de los miles que existen, estos son la base de todos. El Adware es un software de anuncios que circulan por la Web, es usado para hacer más lento el sistema y sustraer información de un usuario. El Crimeware se encarga de los delitos financieros, roba identidades y accesos al sector económico, comercial y bancario. El Spyware recopila

información y la envía al ordenador que le controla. El Ransom Ware y el Rogue Software mediante engaños de diferente índole, buscan extraer una remuneración consentida al usuario.

El Malware, en sí, es como el nivel máximo del software malicioso y es usado por Crackers y Terroristas Informáticos, debido a su eficacia al momento de infiltrarse y dañar todo dispositivo o sistema, para el cual ha sido diseñado. Es el más complicado de combatir por parte de los Antivirus.

Todos los días se generan ataques y muchas veces no los sabemos identificar, existen diferentes y variadas formas delictivas que atentan constante y diariamente a la sociedad, es muy importante tener muy claras las características de cómo se aplicaran o como se presentaran en un sistema informático lógica o físicamente. Los tipos de ataques son: Bullying Informático, Datos Falsos o Engañosos, Eavesdropping y Packet Sniffing, Snooping y Downloading, Spoofing, Jamming o Flooding, Huevo de Pascua Virtual, Manipulación de Programas o Los Caballos de Troya, La Técnica del Salami, Falsificaciones Informáticas, Entradas Falsas, Manipulación de los Datos de Salida, Phishing, El Sabotaje Informático, Pornografía Infantil En la Web, Bombas Lógicas o Logic Bombs, Gusanos, Virus Informáticos, Ciberterrorismo, Ataques de Denegación de Servicio, Back Doors y Trap Doors, La Llave Maestra o Superzapping, Pinchado de Líneas o Wiretapping, Hijacking, Keylogger, Pharming, Spamming, Carding y Sicariato Informatico.

Cada uno de estos ataques genera a su vez, un delito específico, el hecho de que ataquen a una misma categoría, no los hace iguales o similares, esto es muy importante de comprender al momento de analizarlos.

Es sumamente importante en este ámbito entender, comprender y analizar el accionar del delincuente informático, de lo que realizan actualmente y mucho más, las posibilidades tecnológicas existentes, para anticipar las acciones delictivas que se pudiesen generar en la actualidad, nuestra legislación penal abarca únicamente delitos como: Sabotaje Informático, Espionaje o Intrusismo Informático, Falsificación Electrónica, Daño Informático, Apropiación Ilícita y Estafa Informática. Esto de acuerdo a este trabajo e investigación, simplemente no es suficiente, la generalidad que abarca, cada uno de estos articulados, permite que ciertos delitos, estén quedando impunes o en su defecto, por buscar un castigo muchos abogados suelen tratar de encajar, el delito informático en uno del tipo tradicional, cuando esto no es un funcionamiento correcto, las leyes se aplican de acuerdo a su naturaleza, cumpliendo el propósito para lo que fueron creadas.

Al revisar legislaciones internacionales, vemos el hecho de que los delitos informáticos no ha sido una temática conflictiva que nace de la noche a la mañana, sino más bien una figura, que se ha ido configurando desde el nacimiento de la computación y fortaleciendo a medida que han avanzado los medios tecnológicos.

Es con ahínco que retomo una de las problemáticas o dificultad más grande a la que se enfrenta la norma, control y regulación de estos delitos en este momento, que es, la acción delictiva internacional, el hecho de que no se produzcan o generen solamente a nivel nacional, ha creado una gran barrera para las naciones de todo el mundo.

No es que otros países, no tengan un marco legal sobre los delitos informáticos, la traba se encuentra básicamente en que, cada país se maneja con su propio código y leyes, adecuado a su realidad social. Esto es algo erróneo y equivoco, ya que el medio informático o telemático, no es solamente propio de un país, es decir este medio, no tiene costumbres, ni culturas, ni tradiciones, es la mejor aplicación del término versátil y a la vez esto se da uniformemente. En el medio informático o telemático se habla un solo idioma y sus cambios se aplican de forma global, por lo mismo es claro que las posibilidades de delinquir son iguales en Ecuador y en cualquier otro país del mundo, he ahí el error.

Es menester que todos los países del mundo, en forma general o por regiones, unan sus esfuerzos a fin de evitar la propagación de los delitos informáticos.

Lo que se debería realizar es un consejo u organismo mundial, como por ejemplo el OMPI (Organización Mundial de Propiedad Intelectual), que regula internacionalmente los derechos de la propiedad de autor y tiene sucursales en cada país del mundo. Así mismo puede funcionar, la creación de un organismo mundial, que podría llamarse, OMDI (Organización Mundial de Delitos Informáticos).

Esta organización se debería de componer de un representante, de cada país involucrado, este ente emitiría leyes, que rijan a nivel internacional, en todos los países, que se encargue de tipificar a nivel global los delitos y sanciones, que atraviesan fronteras y que se encargue de velar por la seguridad informática.

Esto sería un paso extremadamente grande, al buscar la penalización apropiada de estos delitos, sería un escalón importantísimo en el desarrollo de un país como el Ecuador, ir a una mesa de discusión y ser el gestor de la idea, la Constitución de la República del Ecuador, dice, que este es un país que busca la unidad mundial, al momento de protegerse, que mejor precedente que este a nivel internacional. El que cada país se maneje con un mismo marco jurídico con respecto a este ámbito, evitará que los delitos, se propaguen y queden sin castigo, facilitará la indemnización por daños, ayudará en la captura puntual de los delincuentes informáticos. Bajo esta fórmula se corregiría y terminaría con la disputa internacional y la cantidad de acuerdos ineficientes, que crean la impunidad.

Sin duda el internet ha generado una revolución en las comunicaciones, pero también en las formas de cometer delitos, porque sabemos que la informática y el internet, se pueden aprovechar para cometer varios tipos de delitos.

Cuando se habla de delitos informáticos y de las cosas que se pueden hacer en el internet, como por ejemplo robar información de otra persona hablamos de cuentas bancarias, claves, números de tarjeta, para poder estafar y aprovechar esos actos para cometer un delito, uno dice y claro es internet y vale todo.

Pero en Ecuador junto a la Ley de Propiedad Intelectual, se ingreso la tipificación penal de delitos puntuales y generales, que esperaban cumplir como freno absoluto y controlador de este ámbito delictivo, pero son simplemente un grupo de reformas que se ingresaron al código penal, la idea de mi proyecto está orientada a incluir las tecnologías como medios comisivos de delitos, como objetos de delito e introducir al Código Orgánico Integral Penal una sección

específica, sobre infracciones informáticas, esto permitirá extender el tipo penal, puntualmente en cuanto a los tipos penales, tenemos claro que un tipo penal, es una conducta, en la que uno hace algo y es castigado, si ese algo, no es exactamente lo que esta descrito en la norma, uno no puede ser castigado.

Que pasa en Ecuador, se hackeo la pagina Web de una serie de entidades de gobierno y que es lo que pasa, aunque hubiesen capturado a los culpables, la propia corte los hubiese tenido que absolver, ya que la pagina Web, no es catalogada como una cosa, en el sentido jurídico, por ende no existe daño, lo que se realizó, fue algo que no se puede calificar jurídicamente hasta el momento y mucho menos penar, porque se cometió un delito que ni siquiera se encontraba descrito en la ley.

En ese caso fue un simple hacking de imagen, pero lo que se podrían haber hecho, era mucho más grave y los resultados de juzgamiento hubiese sido el mismo, esto denota que estamos frente a una legislación pobre aun, para enfrentar delitos de esta naturaleza.

Se ha reaccionado a tiempo, se busca realizar reformas, ahora este proyecto que presento en mi trabajo de tesis está acorde a los avances en la informática, electrónica, telemática y la dinámica del avance de las tecnologías, la idea es que una buena ley sea dictada de forma que pueda adoptar e integrar estos nuevos tipos y conceptos.

Lo que está faltando hasta el momento es la capacitación en Fiscales, Jueces, en los abogados y en la policía que les toca investigar, hay cuerpos especializados, pero no, con todos los recursos que uno pudiera esperar para afrontar este tipo de investigaciones, pero sí, con buena capacidad y por el lado de la justicia, es importantísimo, tener nuevos soportes para legislar adecuadamente a esta nueva generación de delitos.

En sí, serio adecuado que los actores involucrados en la temática del delito tecnológico, aporten a al fortalecimiento de la prevención de los delitos informáticos esto es, la Fiscalía General del Estado, a través de la adecuada formación de Fiscales en temas Informáticos y el ministerio de educación, exigiendo a las Universidades del País, quienes a través de sus Facultades de Derecho deben de estandarizar dentro del pensum correspondiente la materia de Derecho Informático, tal como lo hace la Universidad del Pacifico.

Para esta investigación se hizo una revisión exhaustiva de Derecho Comparado, Constitución de la Republica del Ecuador, Ley de Código Orgánico Integral Penal, que al momento se encuentra en debate en la Asamblea Nacional.

En este trabajo de Tesis, se realizó primero el análisis y observaciones puntuales de las leyes, tanto las vigentes en el Código Penal, como las que se están planteando dentro del Código Orgánico Integral Penal y segundo, un proyecto, en el cual, se han colocado una serie de articulados y figuras legales, cuya misión es ayudar a brindar justicia de forma puntual, rápida y efectiva a una serie de delitos que se están dando y que se pueden dar en un futuro próximo en nuestra sociedad. Es muy importante, el que se empiecen aplicar medidas en este ámbito, en nuestros días, existen una serie de delincuentes dispersos, pero ya sabemos de una agrupación delincuencial fuerte y famosa, como lo es el grupo “Anonymous”, que está sentando un precedente muy fuerte en cada país donde tiene representantes, liberando

información privada, dañando y atacando a los gobiernos, bien podríamos considerar a sus integrantes, como terroristas cibernéticos.

En este momento es una agrupación, cuánto podemos llegar a cegarnos, a creer que no se van a multiplicar, qué, nos hace pensar, que con la impunidad con la que actúan estos delincuentes, otros grupos no van a emular el ejemplo, para beneficiarse de una sociedad sin defensas legales apropiadas para la amplia gama de delitos informáticos posibles.

El proyecto que se plantea en este trabajo de tesis está compuesto por 36 artículos que encuadran delitos en el ámbito informático, que serán enviados a la asamblea, como un aporte ciudadano, de manera que se contemplen para su incorporación en un sección específica del Código Orgánico Integral Penal, este, es en sí, el primer eslabón de una intención superior, con estos artículos podríamos asegurar una legislación completa y efectiva en cuanto a estos delitos, la idea principal, es crear algo totalmente superior y preparar una ley penal completa en relación a las ya existentes, no solo a nivel de Sudamérica, sino también a nivel internacional.

Con una lectura a este proyecto, se puede ver que se proponen figuras, que no, sólo, no existen aquí, sino en ninguna parte del mundo. Que mejor base legal para sentar un precedente en cuanto al derecho en el Ecuador. Mismo precedente que podrá ser utilizado como fundamento para dirigirse ante un foro internacional, con la propuesta de conformar una organización llamada OMDI (Organización Mundial de Delitos Informáticos), a la cual me réferi anteriormente, porqué no darle eso a nuestro país, que sea el Ecuador, el que se dirija al mundo como Republica Soberana e Independiente y anuncie, esto, es lo que hay que hacer, esta es una solución para los problemas internacionales, en cuanto a la actuación sin fronteras limitadas de los delitos informáticos y más que nada lograr que se realice, es justo y apropiado mencionar que con una apropiada y fuerte ley en cuanto a estos delitos, ningún país del mundo podría refutar o negar, la capacidad, experiencia y conocimiento que respaldan esta propuesta.

Finalmente, es con ahincó espero, que con los estudios hechos en este trabajo de tesis, sirvan a mi país a lograr mayores estándares nacionales e internacionales, judicial y socialmente hablando, poseemos una serie de ventajas, que con innovación y emprendimiento nos pueden hacer destacar en todas las ramas. Brindar un sustento o llamado de atención a la vigilancia de los medios informáticos, electrónicos y telemáticos, en aras de una superación social, que sea un primer pasó de lo que va a llegar a ser fundamental, si todavía no se lo ha considerado así. El ecuador y su sistema jurídico, al igual que en otros aspectos debe de destacar y ser ejemplo para otros países.

## GLOSARIO

**Algoritmos:** Conjunto ordenado y finito de operaciones que permite hallar la solución de un problema.

**Antivirus:** Programa informático que detecta la presencia de un virus y lo anula.

**Atipicidad.-** Ausencia del tipo, falta de elementos positivos del tipo, falta de adecuación del tipo penal.

**Biometría:** es la parte de la biología que estudia en forma cuantitativamente la variabilidad individual de los seres vivos utilizando métodos estadísticos.

**Certificado electrónico de información:** Es el mensaje de datos que contiene información de cualquier tipo.

**Comercio electrónico:** Es toda transacción comercial realizada en parte o en su totalidad, a través de redes electrónicas de información.

**Conminar**.- Amenazar [a uno con penas y castigos] el que tiene potestad de hacerlo.

**Criptografía:** Ocultación de la información mediante cifrado.

**Daño.-** Detrimento o destrucción de bienes.

**Dañosidad.-** malo, nocivo, perjudicial, pernicioso, funesto, maligno, dañoso.

**Datos personales autorizados:** Son aquellos datos personales que el titular ha accedido a entregar o proporcionar de forma voluntaria.

**Delito informático**.- Acción delictiva realizada en el ciberespacio o a través de medios informáticos.

**Delito tradicional**.- Acción delictiva típica que atenta a la sociedad.

**Documento:** Registro incorporado en un sistema en forma de escrito, video, audio o cualquier otro medio, que contiene data o información acerca de un hecho o acto capaces de causar efectos jurídicos.

**Dolo.-** En los delitos, voluntad intencional; en los contratos o actos jurídicos, engaño.

**Factura electrónica:** Conjunto de registros lógicos archivados en soportes susceptibles de ser leídos por equipos electrónicos de procesamiento de datos que documentan la transferencia de bienes y servicios.

**Fiabilidad:** la probabilidad de que un sistema se comporte tal y como se espera de él.

**Firmware:** Programa o segmento de programa incorporado de manera permanente en algún componente de hardware.

**Humanware:** El soporte humano, que controla o se desenvuelve en un medio informático.

**Hardware:** Equipos o dispositivos físicos considerados en forma independiente de su capacidad o función, que forman un computador.

**Ilícito.-** Que no está permitido por la ley o la moral.

**Impoluto.-** Limpio, sin mancha.

**Impunidad**.- Falta de castigo merecido.

**Imputar.-** Atribuir a una persona la responsabilidad de un delito, una culpa o una falta.

**Inclusión.-** Acto de incluir o estado de incluido.

**Información:** Significado que el ser humano le asigna a la data utilizando las convenciones conocidas y generalmente aceptadas.

**Instigador.-** Se aplica a la persona que influye en otra para que realice una acción o piense de un modo, especialmente si es con el objetivo, de que haga algo malo o perjudicial

**Intimidad:** El derecho a la intimidad previsto en la Constitución Política de la República, para efectos de esta ley, comprende también el derecho a la privacidad, a la confidencialidad,

**Lesividad.-** Que causa o puede causar lesión:

**Perito legal.-** Persona que pone su conocimiento y experiencia en una ciencia o arte al servicio de la Justicia.

**Punible.-** Que merece castigo.

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

**Red electrónica de información:** Es un conjunto de equipos y sistemas de información interconectados electrónicamente.

**Reputar.-** Estimar o hacer concepto del estado o calidad de una persona o cosa.

**Sellado de tiempo:** Anotación electrónica firmada electrónicamente y agregada a un mensaje de datos.

**Sistema de información:** Es todo dispositivo físico o lógico utilizado para crear, generar, enviar, recibir, procesar, comunicar o almacenar, de cualquier forma, mensajes de datos.

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

**Software:** Información organizada en forma de programas de computación, en cualquier forma, con el objeto de que éstos realicen funciones específicas.

**Tarjeta inteligente:** Rótulo, cédula o carnet que se utiliza como instrumento de identificación, de acceso a un sistema,

**Tecnología de Información:** Rama de la tecnología que se dedica al estudio, aplicación y procesamiento de data, lo cual involucra la obtención, creación, almacenamiento, administración, modificación, manejo, movimiento, control, visualización, distribución, intercambio, transmisión o recepción de información.

**Transgrede.-** Actuar en contra de una ley, norma o costumbre. Infringir, quebrantar, violar.

**Virus:** Programa o segmento de programa indeseado que se desarrolla incontroladamente y que genera efectos destructivos o perturbadores en un programa o componente del sistema.

## BIBLIOGRAFÍA

### LIBROS


- Alvin Toffler, "La tercera ola". Editorial Sudamericana, España. 1998.
  Arazandi, Segunda Edición. 2002.

- CAMACHO LOSA Luis, El Delito Informático, Madrid, España, 1987.

- CASTILLO JIMENEZ, María Cinta, RAMALLO ROMERO, Miguel. El delito informático. Facultad de Derecho de Zaragoza. Congreso sobre Derecho Informático. 22-24 junio 1989.

- COMISIÓN DE LAS COMUNIDADES EUROPEAS**.** Delitos relativos a las Computadoras. Bruselas, 21.11.1996 COM (96) 607 final.

- DAVARA RODRÍGUEZ, Miguel Ángel, Análisis de la Ley de Fraude Informático, Revista de Derecho de UNAM. 1990.

- DAVARA**,** Miguel Ángel, Fact Book del Comercio Electrónico, Ediciones

- Dr. Giovanni Manunta, "Seguridad: una introducción". Consultor y profesor de Seguridad de Cranfield University.

- E. ALCALDE, M. GARCÍA Y S. PEÑUELAS. "Informática Básica". Editorial Mcgraw-Hill-, 1991.

- EDUARDO PÉREZ GOROSTEGUI. "Economía de la Empresa". Editorial Centro de Estudios Ramón Areces; 1989. (Cap. 1. Para las ideas generales de la teoría de Sistemas).

- FRANCISCO SANCHIS. "Planificación y Explotación de Sistemas Informáticos". U. Politécnica de Madrid; 1990.

- GARRIDO MONTT, MARIO. Nociones Fundamentales de la Teoría del Delito Edit. Jurídica de Chile, 1992. Citado por Jijena Leiva Renato, Los Delitos Informáticos y la Protección Penal a la Intimidad, Editorial Jurídica de Chile, 1993.

- GUTIÉRREZ FRANCÉS, María Luz, Fraude Informático y estafa.

- H.D. CLIFTON. "Business Data System". Editorial Prentice – Hali Internacional, Inc; 1983.

- MAGLIONA MARKOVICTH Claudio Paúl, LÓPEZ MEDEL Macarena, Delincuencia y Fraude Informático, Editorial Jurídica de Chile. 1999

- Miguel Gustavo Aldegani, “Seguridad Informática”. MP Ediciones. Argentina. 1997. Página 22.

- MOHRENSCHLAGER, Manfred. El Nuevo Derecho Penal informático en Alemania” (Págs. 99 a 143). “Delincuencia Informática”. (1992, Ed. P.P.U., Colección IU RA-7). Tendencias de Política Jurídica en la lucha contra la Delincuencia “(PÁGS. 47 a 64). “Delincuencia Informática”. (1992, Ed. P.P.U., Colección IURA-7). Citado por Marcelo Huerta y Claudio Líbano, Los Delitos Informáticos. Editorial Cono Sur.

- P. DE MIGUEL. “Fundamentos de los computadores”. Paraninfo; 1990.

- PARKER, D.B, Citado por Romeo Casabona Carlos M. Poder Informático y Seguridad Jurídica.

- PEDRO MAESTRE YENES. "Glosario Informática para uso de la Seguridad Social". Ministerio de Trabajo y Seguridad Social; 1991.

- PÉREZ LUÑO, Antonio Enrique. “Manual de informática y derecho”, Editorial Ariel S.A., Barcelona, 1996.

- REYES ECHANDÍA, Alfonso, La Tipicidad, Universidad de Externado de Colombia, 1981.

- ROGER. S. PRESSMAN. “Ingeniería del Software”. Editorial McGraw-Hill; 1989.

- ROMEO CASABONA, Carlos María, Poder Informático y Seguridad Jurídica, Fundesco, Madrid, España, 1987.

- ROMEO CASABONA, Carlos María. “Poder informático y Seguridad jurídica”. Editorial Fundesco 1987

- SNEYERS, Alfredo. El fraude y otros delitos informáticos. Ediciones T.G.P. Tecnologías de Gerencia y producción, 1990

- TELLEZ VALDÉS, Julio. “Los Delitos informáticos. Situación en México”, Informática y Derecho Nº 9, 10 y 11, UNED, Centro Regional de Extremadura, Mérida, 1996.

- TIEDEMANN, Klaus, Poder informático y delito, Barcelona, España. 1985.

- Ulrich Sieber, “Documentación Para Aproximación Al Delito Informático”, publicado en Delincuencia, Editorial. PPU, Barcelona, España, 1992, Pág. 65.

- Periódico El Comercio 21 de diciembre 2011, Página 17.

- Artículo 9, Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, código vigente.

- Artículo 55, Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, código vigente).

- Diario Hoy, Sección Actualidad, 21 de abril del 2008.

- Legislación Chilena

- Legislación Española

- Legislación Francia

- Legislación Holanda

- Legislación Gran Bretaña

- Legislación Austria

- Legislación Alemania

- Legislación Norte Americana

- Legislación Costa Rica

- Legislación Peru

- Legislación Argentina

- Legislación Venezuela

- Legislación Bolivia


**EBOOKS**


- Ardita, Julio Cesar. Director de Cybsec S.A. Security System y ex Hacker. Entrevista online realizada el día 19 de Mayo de 2011. http://www.cybsec.com.

- CALLEGARI, Nidia, Citada por Julio Telles Valdés. Ob. Cita. Calvo, Rafael Fernández. Glosario Básico Ingles-Español para usuarios de Internet. 1994-2000. http://www.ati.es/novatica/2000/145.

- Howard, John D. Thesis: Analysis of security on the internet 1995-2006. Carnegie Institute of Technology. Carnegie Mellon University. 1995. EEUU. http://www.cert.org. Capitulo 6 – Pagina 59

- Huerta, Antonio Villalón. "Seguridad en Unix y Redes". Versión 1.2 Digital – Open Publication License v.10. 2 de Octubre de 2000. http://www.kriptopolis.com.

- LARA RIVERA, Jorge, Los Delitos Informáticos. www.jusrismática.com.

- RESA NESTARES CARLOS: Crimen Organizado Transnacional: Definición, Causas Y Consecuencias, Editorial Astrea, 2005. Revista "Seguridad Corporativa". http://www.seguridadcorporativa.org


**WEB**


- http://wwwisis.ufg.edu.sv/wwwisis/documentos/EB/005.8-B644s-Seguridad%20informatica.pdf
- http://en.wikipedia.org/wiki/File:Adventure_Box_Front.jpg
- http://es.wikipedia.org/wiki/Inform%C3%A1tica
- http://www.monografias.com/trabajos11/curinfa/curinfa.shtml
- http://www.ciberhabitat.gob.mx/museo/historia/
- http://www.informatica.gob.ec/index.php/noticias/7-nacional/528-gobierno-conformo-comision-para-la-seguridad-informatica
- http://es.wikipedia.org/wiki/Business-to-business
- http://es.wikipedia.org/wiki/B2C
- http://www.bibliojuridica.org/libros/1/172/21.pdf
- http://members.nbci.com/segutot/delitos.htm
- http://www.fas.org/irp/congress/1996_hr/s960605l.htm
- http://digitaldesign.bariloche.net.ar/xiijovenab/ComDerPen%20-%20DelitosInfor.htm
- http://www.npa.go.jp/hightech/antai_repo/ereport.htm
- http://www.monografias.com/trabajos/legisdelinf/legisdelinf.shtml
- http://www.govnews.org/mhonarc/gov/us/fed/congress/gao/reports/_msg00533.html
- http://www.dtj.com.ar/publicaciones.htm
- http://margay.fder.uba.ar/centro/juridicas/Juridica11/salt.html
- http://www.gocsi.com/
- http://www.ecomder.com.ar
- http://www.bilbaoweb.com/hackuma/guidel1.htm
- http://arnal.es/free/noticias/free2_08.html#T12
- http://www.bilbaoweb.com/hackuma/guidel1.htm
- http://www.inei.gob.pe/cpi/bancopub/cpi008.htm
- http://margay.fder.uba.ar/centro/juridicas/Juridica11/salt.html
- http://www.monografias.com/trabajos/legisdelinf/legisdelinf.shtml
- http://www.onnet.es/04001001.htm
- http://legal.infosel.com/Legal/EnLinea/Articulos/articulo/0001/
- http://www.delitosinformaticos.com/delitos/delitosinformaticos.shtml
- http://www.taringa.net/posts/info/6980126/Todo-sobre-la-informatica-y-computacion.html, 1 y 2

- http://es.wikipedia.org/wiki/Sistema_inform%C3%A1tico
- http://www.alegsa.com.ar/Dic/hardware.php
- http://books.google.com.ec/books?id=SUjFswQk1_4C&pg=PA47&lpg=PA47&dq
- http://guindo.pntic.mec.es/~pold0000/apuntes/ut01/tema01/tema01.htm
- http://desarrollodesoftware.fullblog.com.ar/sistemas-informaticos.html
- http://www.institutojandula.com/RET/SistemasInformaticos.pdf, página 6
- http://www.institutojandula.com/RET/SistemasInformaticos.pdf, página 7
- http://www.institutojandula.com/RET/SistemasInformaticos.pdf, página 5
- http://es.wikipedia.org/wiki/Sistema_inform%C3%A1tico
- http://es.answers.yahoo.com/question/index?qid=20090812082615AAgZEjO
- http://computacioneinformatica.blogspot.es/1258315020/
- http://es.wikipedia.org/wiki/Inform%C3%A1tica
- http://definicion.de/datos/
- http://definicion.de/sistema-de-informacion/
- http://definicion.de/seguridad-informatica/
- http://www.buenastareas.com/ensayos/Seguridad-Informatica/383903.html
- http://members.fortunecity.es/elizmer68/analisis_del_objetivo_de_la_segu.htm
- http://dspace.espoch.edu.ec/bitstream/123456789/93/1/18T00369.pdf, página 27
- http://dspace.espoch.edu.ec/bitstream/123456789/93/1/18T00369.pdf, página 27
- http://www.cybsec.com
- http://dspace.espoch.edu.ec/bitstream/123456789/93/1/18T00369.pdf, página 28
- http://dspace.espoch.edu.ec/bitstream/123456789/93/1/18T00369.pdf, página 29
- http://dspace.espoch.edu.ec/bitstream/123456789/93/1/18T00369.pdf, página 30
- http://www.oocities.org/es/kagutierbcv/tinfo/t3/ii.html
- http://www.segu-info.com.ar/fisica/seguridadfisica.htm
- http://www.segu-info.com.ar/fisica/incendios.htm
- http://www.segu-info.com.ar/fisica/clima.htm
- http://www.segu-info.com.ar/fisica/instalacioneselectricas.htm
- http://dspace.espoch.edu.ec/bitstream/123456789/93/1/18T00369.pdf, página 33
- http://dspace.espoch.edu.ec/bitstream/123456789/93/1/18T00369.pdf, página 34
- http://www.segu-info.com.ar/logica/seguridadlogica.htm
- http://www.mailxmail.com/curso-delitos-informaticos/sistemas-empresas-mayor-riesgo
- http://www.segu-info.com.ar/delitos/delitos.htm
- http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf, página 11
- http://www.angelfire.com/la/LegislaDir/Carac.html
- http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf, página 15
- http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf, página 18
- http://www.mailxmail.com/curso-delitos-informaticos/delitos-perspectiva
- http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf, página 20
- http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf, Página 21
- http://es.wikipedia.org/wiki/Auditor%C3%ADa_inform%C3%A1tica
- http://crimenescyberneticos.blogspot.com/2011/08/auditor-versus-delitos-informaticos-es.html

- http://www.monografias.com/trabajos67/pruebas-penales-salvador/pruebas-penales-salvador.shtml
- http://www.monografias.com/trabajos6/delin/delin2.shtml
- http://www.monografias.com/trabajos16/seguridad-informatica/seguridad-informatica.shtml
- http://es.wikipedia.org/wiki/Cracker
- http://www.informatica-hoy.com.ar/aprender-informatica/Que-es-un-Cracker.php
- http://www.cabinas.net/informatica/ciberterrorismo_informatico.asp
- http://es.wikipedia.org/wiki/Adware
- http://es.wikipedia.org/wiki/Crimeware
- http://es.wikipedia.org/wiki/Malware
- http://es.wikipedia.org/wiki/Spyware
- http://es.wikipedia.org/wiki/Ransomware
- http://es.wikipedia.org/wiki/Rogue_software
- http://es.wikipedia.org/wiki/Scareware
- http://es.wikipedia.org/wiki/Coerci%C3%B3n
- http://www.monografias.com/trabajos16/seguridad-informatica/seguridad-informatica.shtml
- http://es.wikipedia.org/wiki/Huevo_de_pascua_(virtual)
- http://es.wikipedia.org/wiki/Troyano_(inform%C3%A1tica)
- http://www.channelinsider.es/2011/03/16/se-incrementa-el-numero-de-troyanos-descargadores-de-malware/
- http://dmi.uib.es/~dmiamp/TEGP/Tema%202/Delito%20informatico%20I%20pres.pdf, página 5, 7
- http://dmi.uib.es/~dmiamp/TEGP/Tema%202/Delito%20informatico%20I%20pres.pdf, página 5, 6)
- http://www.alambre.info/2004/08/09/los-delitos-informaticos/
- http://es.wikipedia.org/wiki/Phishing
- http://www.monografias.com/trabajos6/delin/delin.shtml
- http://dmi.uib.es/~dmiamp/TEGP/Tema%202/Delito%20informatico%20I%20pres.pdf, página 10
- http://dmi.uib.es/~dmiamp/TEGP/Tema%202/Delito%20informatico%20I%20pres.pdf, página 10
- http://dmi.uib.es/~dmiamp/TEGP/Tema%202/Delito%20informatico%20I%20pres.pdf, página 9
- (http://www.cabinas.net/informatica/ciberterrorismo_informatico.asp).
- (http://es.wikipedia.org/wiki/Ataque_de_denegaci%C3%B3n_de_servicio).
- (http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/argueta_a_a/capitulo1.pdf, página 5).
- (http://dmi.uib.es/~dmiamp/TEGP/Tema%202/Delito%20informatico%20I%20pres.pdf, página 7, 8).
- (http://www.buenastareas.com/ensayos/Wiretapping/551908.html).
- (http://es.wikipedia.org/wiki/Hijacking).
- (http://es.wikipedia.org/wiki/Keylogger).
- (http://es.wikipedia.org/wiki/Pharming).
- (http://es.wikipedia.org/wiki/Spam).

- (http://dmi.uib.es/~dmiamp/TEGP/Tema%202/Delito%20informatico%20I%20pres.pdf, páginas 8 y9)
- (http://www.taringa.net/posts/noticias/6832432/Legislacion-informatica.html).
- (http://www.elnotariado.com/images_db/noticias_archivos/DelitosInformaticos.pdf, página 9,10,11).