UNIVERSIDAD NACIONAL DE LOJA

ÁREA JURÍDICA, SOCIAL Y ADMINISTRATIVA

NIVEL DE POSTGRADO
MAESTRÍA EN CIENCIAS PENALES

TESIS PREVIA A OPTAR POR EL GRADO DE MAGISTER EN CIENCIAS PENALES.

TÍTULO:

"LOS OPERADORES DE JUSTICIA FRENTE A LOS DELITOS INFORMÁTICOS"

AUTOR:

DR. JORGE IVÁN PAZ MONTEROS

DIRECTOR:

DR. NORMAN JARAMILLO VIVANCO MG. SC.

LOJA – ECUADOR

2013

CERTIFICACIÓN

Dr. Norman Jaramillo Vivanco, Docente de la Carrera de Derecho del Área Jurídica Social y Administrativa de la Universidad Nacional de Loja,

CERTIFICO:

Que el trabajo de investigación intitulado: "LOS OPERADORES DE JUSTICIA FRENTE A LOS DELITOS INFORMÁTICOS", presentado por el señor Dr. Jorge Iván Paz Monteros, para optar por el grado de Magíster en Ciencias Penales, ha sido dirigido, orientado y debidamente revisado, por lo que autorizo su presentación y sustentación pública.

Loja, 18 de octubre de 2013

Atentamente,

Dr. Norman Jaramillo Vivanco

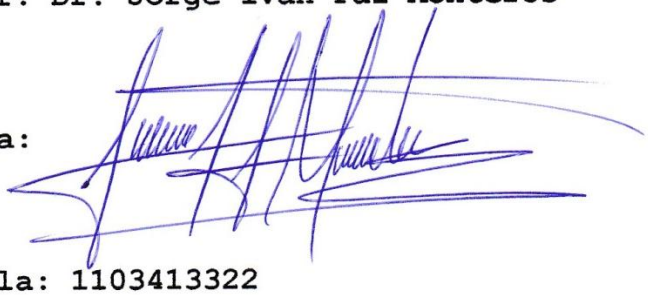
DIRECTOR DE TESIS

AUTORÍA

Yo, Dr. Jorge Iván Paz Monteros, declaro ser autor del presente trabajo de tesis y eximo expresamente a la Universidad Nacional de Loja y a sus representantes jurídicos de posibles reclamos o acciones legales por el contenido de la misma.

Adicionalmente acepto y autorizo a la Universidad Nacional de Loja, la publicación de mi tesis en el Repertorio Institucional-Biblioteca Virtual.

Autor: Dr. Jorge Iván Paz Monteros

Firma: 

Cédula: 1103413322

Fecha: 18 de octubre de 2013

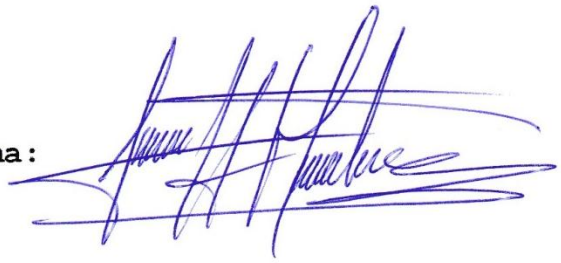
CARTA DE AUTORIZACIÓN DE TESIS POR PARTE DEL AUTOR, PARA LA CONSULTA, REPRODUCCIÓN PARCIAL O TOTAL Y PUBLICACIÓN ELECTRÓNICA DEL TEXTO COMPLETO

Yo, Dr. Jorge Iván Paz Monteros, declaro ser autor de la tesis titulada "Los operadores de justicia frente a los delitos informáticos", como requisito para optar al grado de Magister en Ciencias Penales; autorizo al Sistema Bibliotecario de la Universidad Nacional de Loja para que con fines académicos, muestre al mundo la producción intelectual de la Universidad, a través de la visibilidad de su contenido de la siguiente manera en el Repertorio Digital Institucional:

Los usuarios pueden consultar el contenido de este trabajo en el RDI, en las redes de información del país y del exterior, con las cuales tenga convenio la Universidad.

La Universidad Nacional de Loja, no se responsabiliza por el plagio o copia de la tesis que realice un tercero.

Para constancia de esta autorización, en la ciudad de Loja, a los dieciocho días del mes de octubre del dos mil trece, firma su autor.

Firma: 

Autor: Dr. Jorge Iván Paz Monteros

Cédula: 1103413322

Dirección: Av. Eduardo Kingman y Gobernación de Mainas

Correo electrónico: jorgep498@hotmail.com

Teléfono: 2584225 **Celular:** 0997230995

DATOS COMPLEMENTARIOS

Director de Tesis: Dr. Norman Jaramillo Vivanco Mg Sc

Tribunal de Grado: Dr. Adolfo Moreno Sánchez Mg. Sc.

Presidente

Dr. Gabriel Paz Costa Mg. Sc.

Miembro del H. Tribunal de Grado

Dr. Shandry Armijos Fierro Mg. Sc.

Miembro del H. Tribunal de Grado

DEDICATORIA

Hay hombres que luchan un día y son buenos.
Hay otros que luchan un año y son mejores.
Hay quienes luchan muchos años, y son muy buenos.
Pero hay los que luchan toda la vida, esos son los imprescindibles.
Bertolt Brecht / 1898-1956.

A Dios, quien me dio la fe, la fortaleza, la salud y la esperanza para terminar este trabajo, a la vida por lo aprendido y para aquellas personas que son especiales en mi vida y que me enseñaron lo más hermoso, el querer, a no confiar y luchar por lo se quiere, y que hoy lo siguen haciendo de la mejor manera con su ternura y cariño.

A mi padre ejemplo de vida y amigo incondicional, quien con sus consejos y principios morales me supo guiar por el buen camino. Gracias por haberme educado así. Estoy orgulloso de ser como soy y eso te lo debo a ti, aunque me falta mucho para llegar a ser como tú. Te quiero papá.

A mi madre quien participó directamente en mi formación, por ser una mujer excepcional, que ayudó en mi crianza y en mis primeras letras, que fomentó los mas altos valores del ser humano, por enseñarme el

compromiso absoluto con lo que uno hace. Ya no estás físicamente con nosotros, pero la presencia de tu ausencia, cada día me vuelve más capaz.

A mi amada compañera de vida, mi esposa Gioconda, mil gracias sobre todo por tu amor, tu comprensión, paciencia y fortaleza. Como en todo lo que escribo, estás presente en mi mente y en el alma. "Te amo vida mía, porque eres mi amor, mi cómplice y todo, y en la calle codo a codo, somos mucho más que dos". (Benedetti)

A mis hijos Iván Darío, Hugo Ernesto y Ana María, que son el amor de mi vida, por quienes cada día tiene sentido, testigos silenciosos de mis luchas cotidianas en busca de un mejor futuro, a ellos mi esperanza, mi alegría, mi vida y la culminación de este trabajo y lo que representa. Recuerden que cuentan conmigo y siempre los voy a amar.

A mis hermanas, Gabriela, Lorena, Anabelle, quienes siempre me apoyaron y nunca dudaron que lograría este triunfo. Sin ustedes esto tampoco habría sido posible.

No puedo dejar pasar esta oportunidad sin decirles que las amo y que gracias por su apoyo incondicional.

A mi tía Magali, por haberme brindado su ayuda en todo momento, sobre todo en los más difíciles, por tus consejos, valores, por la motivación constante que me ha permitido ser una persona de bien, pero más que nada, por su amor.

Jorge Paz Monteros

AGRADECIMIENTO

Quiero dejar constancia de mi especial agradecimiento a la Universidad Nacional de Loja, especialmente al Nivel de Postgrado del Área jurídica, Social y Administrativa, representadas tan dignamente por sus Autoridades, por el apoyo brindado a los estudiantes para realizarse académicamente, a todos y cada uno de los maestros por sus conocimientos impartidos y su ardua labor de formación de nosotros sus estudiantes.

Dentro de mis años de preparación académica, he recibido el apoyo incondicional de los seres que forman parte de mi existir sin el cual hubiera sido imposible culminar mis estudios de cuarto nivel, por lo tanto debo manifestar mi gratitud, de manera muy especial a mi padre quien con su sabiduría supo orientar el desarrollo de este trabajo académico.

Un agradecimiento especial al Director de Tesis, el Dr. Norman Jaramillo Vivanco, por su dedicación, responsabilidad, apoyo y orientaciones, que han permitido culminar el presente trabajo de investigación.

Y en general a todas las personas que de alguna manera supieron darme fuerzas para llegar hasta esta parte culminante de mi carrera.

A todos ellos muchas gracias.

Dr. Jorge Iván Paz Monteros

ESQUEMA DE TESIS

1.- Título "Los operadores de justicia frente a los delitos informáticos"

2.- Resumen

Abstract

3.- Introducción

4.- Revisión de literatura

4.1.- El Delito.- Conceptos

4.2.- El Delito Informático.- Conceptualización y características

4.3.- La Historia del Delito Informático

4.4.- Elementos del Delito Informático

4.4.1.- Objetividad jurídica o bien jurídico protegido

4.4.2.- Sujeto activo

4.4.2.1.- Sujeto activo general o indeterminado

4.4.2.2.- Sujeto activo especial o cualificado

4.4.3.- Sujeto pasivo

4.4.3.1.- Sujeto pasivo general

4.4.3.2.- Sujeto pasivo especial

4.4.4.- Aspecto subjetivo

Índice

1.- TITULO:

"LOS OPERADORES DE JUSTICIA FRENTE A

LOS DELITOS INFORMÁTICOS"

2.- RESUMEN

Al igual que ocurre con otras profesiones, los agentes de la ley se están transformando por culpa de la tecnología de la información. El Centro Nacional de Información sobre el Crimen del FBI, ofrece a la policía de todo el país información casi instantánea sobre delitos y delincuentes. Los investigadores utilizan bases de datos para almacenar y cruzar pistas en casos complejos. A través de la tecnología de reconocimiento de patrones, los sistemas de identificación de huellas dactilares automatizados tardan minutos en las tareas que antes llevaban meses.

Las computadoras comprueban rutinariamente los mercados de acciones de Nueva York y Londres para detectar posibles fraudes. La policía de Tejas utiliza una intranet para cruzar bases de datos de fotografías, huellas dactilares y otra información relacionada con delitos y crímenes.

Los forenses informáticos usan software especial para escanear los discos duros de los criminales para localizar "huellas dactilares" digitales o lo que es

igual rastros de ficheros borrados que contienen evidencias de actividades ilegales.

Todas estas herramientas ayudan a los oficiales de la ley a descubrir actividades ilegales y a detener a criminales.

Como las armas, las personas utilizan las computadoras para quebrantar la ley y para hacerlas respetar. Las computadoras son potentes instrumentos en manos de criminales, por lo que éste es un problema en continuo crecimiento en nuestra sociedad.

El "delito informático", se lo puede definir así: "cualquier crimen llevado a cabo a través del conocimiento o uso de la informática".

Con exactitud no se sabe la extensión que tiene el delito informático pues la mayor parte de las veces no se publican, por la simple razón que más grave sería para una compañía el dar a relucir las falencias existentes en su sistema informático que el delito mismo.

Desde 1999 en el Ecuador se puso en discusión el proyecto de Ley de Comercio Electrónico, Mensajes de Datos y Firmas Electrónicas, conformándose comisiones para la discusión de la Ley por parte de los organismos directamente interesados en el tema CONATEL, Superintendencia de Bancos, Cámaras de Comercio y puedan realizar las observaciones a la misma.

Las falencias que presentó al inicio este proyecto fueron puliéndose hasta que por fin en abril del 2002 fue aprobado el texto definitivo de la Ley de Comercio Electrónico, Mensajes de Datos y Firmas Electrónicas y en consecuencias las reformas al Código Penal que daban a la luz los denominados Delitos Informáticos.

Ahora bien el problema de esta investigación radica en que las instituciones llamadas a realizar el control social formal sobre estas infracciones informáticas, llámese Fiscalía o Policía Judicial, no cuentan con una preparación técnica adecuada, que permita hacer frente al problema, además de eso no cuentan siquiera con la infraestructura adecuada, como centros de vigilancia computarizada, el software necesario y demás implementos necesarios para combatir los Delitos

Informáticos. Falta también la preparación de Jueces y Magistrados en estos temas, ya que en ocasiones se ven confundidos frente a este tipo de delitos confundiéndolos con delitos tradicionales.

La Fiscalía debería contar con una Unidad Especializada, como existe en países como Estados Unidos donde el FBI cuenta con el Computer Crime Unit, o como en España que también tienen un departamento especializado en esta clase de investigaciones.

ABSTRACT

As with other professions, the law enforcers are becoming because of information technology. The National Crime Information FBI provides police around the country almost instant information on crimes and criminals. Researchers use databases to store and cross tracks in complex cases. Through the technology of pattern recognition systems, automated fingerprint identification tasks take minutes that used to take months.

Computers routinely check stock markets in New York and London to detect fraud. Texas police used an intranet to cross databases photographs, fingerprints and other information related to crimes and offenses.

The computer forensic use special software to scan hard drives to locate criminals 'fingerprints' digital or what is the same traces of deleted files that contain evidence of illegal activity.

All these tools help law enforcement officials to discover illegal activities and arrest criminals.

Like the weapons, people use computers to break the law and enforce them. Computers are powerful tools in the hands of criminals, so this is an ever growing problem in our society.

The "computer crime", it can be defined as: "any crime carried out through knowledge or use of information."

Not exactly know the extension that has the computer crime because most of the times are not published, for the simple reason that most serious would be for a company to give to light the shortcomings existing in the computer system that the crime itself.

Since 1999 in Ecuador was put into discussion the draft Law on Electronic Commerce, Data Messages and Electronic Signatures, conforming committees for discussion of the Act by agencies directly interested in the subject CONATEL Superintendency of Banks, Chambers of Trade and observations can be made to it.

The failures that presented at the beginning this project was polishing until finally in April 2002 approved the final text of the Law of Electronic

Commerce, Data Messages and Electronic Signatures and consequences Penal Code reforms that opened to light Cybercrime called.

But the problem of this research is that the institutions responsible for making formal social control over these breaches computer, be it prosecutor or judicial police do not have adequate technical training that allows to address the problem, besides that do not have even with adequate infrastructure, such as computerized surveillance centers, the necessary software and other equipment needed to combat computer crime. Lack also preparing Judges on these issues, and are sometimes confused against this type of crime mistaking traditional crimes.

The prosecution should have a special unit, as exists in countries like the U.S. where the FBI has the Computer Crime Unit, or as in Spain that also have a department specializing in this kind of research.

3.- INTRODUCCIÓN

El avance de la tecnología ha permitido el desarrollo de una serie de elementos, que se podrían considerar como necesarios hoy en día para el desenvolvimiento de las actividades de los seres humanos, principalmente en el aspecto científico, técnico. La información automatizada o informática constituye hoy en día una herramienta, necesaria para cumplir un sinnúmero de actividades gubernativas, judiciales, militares, laborales, económicas, educativas, etc.

Junto al avance de la tecnología informática y su influencia en casi todas las áreas de la vida social, ha surgido una serie de conductas ilícitas denominadas, de manera genérica, «delitos informáticos».

Generalmente los delitos informáticos están orientados a atacar informaciones, datos, archivos, por medio de virus, spamming, etc., y pueden ir desde una simple intromisión, sin consentimiento, en los datos o archivos de una persona, hasta la destrucción de todo un sistema informático de una entidad pública o privada.

Pese al hermetismo que referente al cometimiento de delitos informáticos mantienen las grandes empresas, bancos, etc., en la actualidad es muy común escuchar en medios de comunicación el alarmante incremento de esta clase de delitos que se cometen ya no solo a nivel internacional sino en nuestro país.

Con la presente investigación y enmarcado en la apertura del conocimiento, pretendo dar a conocer una serie de delitos informáticos que en la actualidad se perpetran, pero principalmente centrar mi trabajo en la preparación que deben tener los operadores de justicia en cuanto conocimientos informáticos tanto en el derecho penal como en la informática aplicada a la investigación de esta clase de infracciones.

Existe una gran motivación en estudiar este tema por cuanto se encuentra en apogeo y es de gran interés de la ciudadanía para evitar la posibilidad de que en determinado momento puedan constituirse en sujeto pasivo o víctima de estos delitos.

El trabajo investigativo se ha empezado con la revisión de literatura, que en primer lugar contempla una

definición general del delito, dentro de este el delito informático, los elementos del tipo penal como sujeto activo, pasivo, el bien jurídico protegido, etc., su clasificación. Realizo también un análisis de la investigación preprocesal y procesal penal relacionada a la aplicación de la informática. Estudio aquellas conductas emergentes en el sistema informático que atentan contra la intimidad personal y contra la propiedad; analizo también la prueba procesal penal informática, los delitos informáticos y su tipificación en el régimen penal ecuatoriano y en el Derecho comparado.

Luego de la revisión de la literatura, hago un análisis referente a la metodología y técnicas que se emplearon en el desarrollo del trabajo investigativo y presento los resultados obtenidos del trabajo de campo mediante la aplicación de las encuestas. En base a toda la información obtenida realizo la verificación de los objetivos propuestos y la contrastación de la hipótesis planteada en el proyecto de tesis.

Para culminar mi trabajo de tesis expongo las conclusiones a las que llegué como resultado de esta

labor, así mismo las recomendaciones, que personalmente considero que pueden contribuir para el mejoramiento de la actividad de los operadores de justicia y abogados en general, sugiriendo además posibles soluciones al problema.

4.- REVISIÓN DE LITERATURA

4.1.- EL DELITO.- CONCEPTOS

La Real Academia de la Lengua define el vocablo delito, como la acción u omisión voluntaria castigada por la ley con pena grave.

En latín delito, es "delictum" palabra que sugiere un hecho contra la ley, un acto doloso que se castiga con una pena.

A lo largo de la historia los pensadores y juristas han dado su propia definición de lo que es el delito.

El jurisconsulto y profesor italiano Francisco Carrara, (Lucca, 1805 - 1888), nos da una definición clara acerca del delito, al expresar: "es la infracción de la ley del estado, promulgada para proteger la seguridad de los ciudadanos, y que resulta de un acto externo del hombre, positivo o negativo, moralmente imputable y socialmente dañoso"[1].

[1] Carrara, Francisco, "Programa de Derecho Criminal", parte general, volumen I, Editorial Temis, Bogotá, Pág. 43.

En este concepto, el autor deja señaladas las características propias que integran el delito, haciendo una explicación clara y objetiva, refiriéndose a la acción (acto externo del hombre), tipicidad (promulgada para proteger la seguridad de los ciudadanos), antijurídico (infracción de la ley del estado), culpable (moralmente imputable y socialmente dañoso) y por lo tanto punible, una vez reunidas todas estas condiciones. De esta manera, es inevitable llegar a tener una comprensión concreta y asimismo se verifica que las conceptualizaciones del delito, se han mantenido y rigen hasta la actualidad, a pesar de ser una conceptualización de hace más de un siglo.

Luis Jiménez de Asúa dice que delito es "el acto típico antijurídico, imputable, culpable, sancionado con una pena y conforme a las condiciones objetivas de publicidad"[2].

Guillermo Cabanellas, da su explicación cuando comienza diciendo que la palabra acto, abarca tanto a lo que uno hace como a lo que deja de hacer (acción y omisión). En las dos formas se expresa la voluntad.

[2] Revista judicial derechoecuador.com.- El Delito.- 24 noviembre de 2005

Como criterio propio puedo conceptualizar al delito, como un acto humano de acción u omisión, típico, antijurídico, culpable y punible.

Digo que es una **acción**, pues se origina de una actividad humana, de los movimientos corporales, encaminados a un fin determinado. Se considera también que un delito puede ser resultado de una conducta inactiva, entonces hablamos ya no de acción sino de omisión.

La acción debe ser **típica**, y decimos que es así cuando está claramente definida por la ley penal, para que ésta pueda ser penada. El Código Penal ecuatoriano claramente establece en el Art. 2. **"Nadie puede ser reprimido por un acto que no se halle expresamente declarado infracción por la ley penal, ni sufrir una pena que no esté en ella establecida"[3].**

Se dice que la acción que realiza el ser humano es **antijurídica**, cuando es lesiva a las garantías y derechos jurídicamente establecidos. Lo antijurídico es la esencia del delito, lo que lo caracteriza.

[3] Régimen Penal ecuatoriano.- Código Penal del Ecuador.- Ediciones Legales.- Art. 2

Culpable, es decir que el acto humano debe ser consciente y voluntario, elementos que configuran el dolo, o también puede originarse en una conducta culposa la que se caracteriza por la negligencia, impericia, imprudencia. Es atribuir o hacer penalmente responsable a una persona por el hecho injusto llevado a cabo, es un juicio de valor sobre la relación entre autor - hecho, que se ha entendido como un reproche dirigido al autor por el hecho realizado.

Punible, cuando los elementos anteriores se encuentran concatenados, estamos frente al acto punible que es sancionado con una pena determinada.

4.2.- EL DELITO INFORMÁTICO.- CONCEPTUALIZACIÓN Y CARACTERISTICAS

A fin de fundamentar mi trabajo de tesis procederé a transcribir algunas definiciones que referentes al delito informático he recopilado y que a continuación las expongo:

En el artículo denominado "El Delito Informático", de autoría de Arturo Oswaldo Huilcapi Peñafiel, se cita

algunos criterios sobre el delito informático, entre los cuales tomo los siguientes: "Nidia Callegari define al delito informático como "aquel que se da con la ayuda de la informática o de técnicas anexas"; 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"; María de Luz Lima dice que el "delito informático 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"[4].

Considero que la definición dada por Callegari, es muy general, pues en la misma únicamente se menciona que la informática es un instrumento para el cometimiento de un delito. Sarzana va más allá al señalar que es un comportamiento criminal en el cual se encuentra involucrada una computadora.

[4] HUILCAPI Arturo.- El Delito Informático.- Pagina Judicial de Diario La Hora

Luz Lima por su parte da un concepto más abarcativo al decir que es un acto ilícito penal, lo cual es indudables, sumándole a esto el papel que cumplen los medios, "método, medio o fin", en este caso la computadora para ser utilizada con fines defraudatorios y depredatorios.

Existen varias opiniones y criterios entorno al concepto del delito informático. Algunos autores sostienen que es un delito común cometido bajo el empleo de medios informáticos, es decir, que se encuentran ya tipificados en el Código Penal, por lo cual niegan la existencia de un bien jurídico específico para esta clase de delitos; otros autores otorgan al delito informático un contenido propio que afecta un nuevo interés social y por ende un novísimo bien jurídico; y, finalmente, una tercera vertiente, postulada por la doctrina norteamericana y británica, que señala que diferencia a la informática como un medio para cometer delitos tradicionales, como fin en sí misma y como medio de prueba.

Entre los primeros se encuentran autores como Guibourg, Alende, Campanella, Parker y Viega Rodríguez.

Según Guibourg, Alende, Campanella: "El llamado delito informático no constituye una nueva categoría delictiva. Los hechos ilícitos que se cometen (o se facilitan) mediante el empleo del ordenador son, en principio, los mismos que desde hace milenios las sociedades han castigado de una forma o de otra"[5].

Referente al delito informático Parker señala que es: "cualquier acto criminoso relacionado con la tecnología informática, por el cual una víctima ha sufrido una pérdida y un autor ha obtenido intencionalmente una ganancia"[6].

María José Viega Rodríguez menciona: "Los llamados delitos informáticos no constituyen una nueva categoría delictivas, 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"[7].

Otros autores diferencian el uso de la informática como medio para afectar bienes jurídicos protegidos ya existentes, de aquellas conductas que afectan un nuevo

[5] GUIBOURG, Ricardo A. SOBRE LA TÉCNICA EN EL DERECHO, EN GUIBOURG (RECOPILADOR), INFORMÁTICA JURÍDICA DECISORIA, Pág. 273.
[6] Citado por: GUIBOURG, Ricardo A. Ibid. Pág. 274.
[7] VIEGA RODRÍGUEZ, María José. Delitos Informáticos, Nº 009.

interés social. Es por ello que hablan del delito computacional, que se define como aquella conducta que empleando tecnología de la información vulnera bienes jurídicos ya existentes; por ejemplo las ofensas que a través de redes sociales pueden proferirse a determinada persona, que afecta el bien jurídico tradicionalmente conocido como honor.

Se habla también de delito informático en un sentido estricto y lo definen como aquella conducta que afecta un nuevo interés social que se encuentra íntimamente ligado al tratamiento de la información.

Autores como Pérez Luño, Jijena Leiva, María de la Luz Lima, Tellez Valdez, Davara Rodríguez, etc., han manifestado que si bien existe diferencia entre delito computacional y delito informático, en ambos se emplea las computadoras para cometer las infracciones.

Pérez Luño, haciendo énfasis en aquella diferenciación, nos indica que la criminalidad mediante computadoras comprende "aquel conjunto de conductas criminales que se realizan a través de un ordenador electrónico, o que

afectan el funcionamiento de los sistemas informáticos"[8].

Para Jijena Leiva la "criminalidad mediante computadoras" se define así: "… toda acción típica, antijurídica y culpable, para cuya consumación se usa la tecnología computacional o se afecta a la información contenida en los sistemas de tratamiento automatizado de la misma (delito informático propiamente tal)"[9].

La autora citada anteriormente María de la Luz Lima, considera que el crimen mediante computadoras es "cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñen un papel ya sea como método, medio o fin"[10].

Como ejemplos de esta clasificación, la autora señala: **como método**: el fraude, robo, robo de servicios no autorizados; **como medio**: el acceso no autorizado para extorsionar con la información; y, **como fin**: la destrucción de programas, daños a la memoria, entre otros.

[8] PÉREZ LUÑO, Antonio - Enrique. MANUAL DE INFORMATICA Y DERECHO, Ariel S.A, (1996) Pág. 69
[9] JIJENA LEIVA, Renato Javier. LA CRIMINALIDAD INFORMATICA, Pág. 508.
[10] Citado por: LEVENE, Ricardo (hijo) & CHIARAVALLOTI, Alicia. DELITOS INFORMATICOS, Pág. 19.

Por su parte, Julián Tellez Valdez, emite una definición sencilla en la que considera el delito informático como aquellas conductas, típicas o no, en las que se tiene a la computadora como instrumento o fin"[11].

Acotando de manera sensata, el profesor Ramiro Salinas Siccha, nos da una definición acerca del delito informático, señalando, "son aquellas conductas típicas, antijurídicas, culpables y punibles, en las que la computadora, sus técnicas y funciones desempeñan un papel trascendente, ya sea como método, medio o fin en el logro de los objetivos indebidos del agente, cual es el logro de algún perjuicio de tipo patrimonial a su víctima. Agrega el citado autor, que también se le podría definir a los delitos informáticos como aquella conducta típica, antijurídica, culpable y punible en la que el agente hace uso de cualquier medio informático para obtener un beneficio indebido en perjuicio del sujeto pasivo"[12].

El Catedrático de Derecho Penal y Criminología Klaus Tiedemann, manifiesta que por criminalidad mediante

[11] TELLEZ VALDEZ, Julio. "DERECHO INFORMÁTICO". Instituto de Investigaciones Jurídicas de la Diversidad Nacional Autónoma de México, México 2008 .Pág. 104.
[12] SALINAS SICCHA, Ramiro. DERECHO PENAL PARTE ESPECIAL. Segunda Edición. Editora Jurídica Grijley, mayo de 2007. Pág. 1187.

computadoras, ha de entenderse "a todos los comportamientos antijurídicos según la ley vigente (o socialmente perjudiciales y por eso punibles en el futuro) realizados merced al empleo de un equipo automático de procesamiento de datos"[13].

La doctrina norteamericana y británica coinciden al expresar que el uso del ordenador en la comisión de delitos se puede manifestar de tres maneras: primero, cuando el computador es objeto de la ofensa; segundo, cuando la computadora es la "herramienta" del delito, el sujeto activo la utiliza para facilitar la comisión de delitos tradicionales; y, tercero, las computadoras resultan incidentales en la comisión de delitos, en la medida que contienen evidencias de los delitos.

Teniendo como referente lo antes analizado podríamos concluir en el sentido que el delito informático, es toda acción típica, antijurídica, culpable, punible, caracterizada por el uso de información automatizada, utilizando un ordenador y la tecnología de la informática para tal cometido.

[13] TIEDEMANN, klaus. CRIMINALIDAD MEDIANTE COMPUTADORAS. Pág. 334.

Entre las características principales de los Delitos Informáticos, se puede señalar las siguientes:

a) Son cometidos a través de un ordenador;
b) Pueden ocupar un programa informático para cometer el ilícito;
c) Son rápidos en su cometimiento y fáciles de ocultar;
d) Difíciles al momento de identificar a su autor;
e) Fáciles para borrar las pruebas de su ejecución;
f) Generan pérdidas económicas;
g) Son pocos o casi nulos en ser denunciados;
h) Son de carácter doloso, por la malicia e intencionalidad con que se cometen; y,
i) Son prolíferos, de acuerdo a las estadísticas y casos que cada día se presentan en un mayor grado.

Las personas que cometen esta clase de delitos, poseen características propias, que los diferencia de la delincuencia común, debido a su alto grado de preparación, a saber:

a) Son personas jóvenes;

b) Poseen suficientes conocimientos en el área de la Informática.
c) Ocupan lugares estratégicos en su trabajo, en donde tienen acceso a información confidencial, archivos o bases de datos.
d) Son personas "inteligentes, imaginativos, activos;
e) Se debe claramente identificar al delincuente informático, pues no es lo mismo el joven que entra a un sistema informático por curiosidad, por investigar, que el empleado de una institución financiera que desvía los fondos de las cuentas de sus clientes.

En suma, se puede considerar a los delincuentes informáticos como personas con amplios conocimientos de Informática, capaces de causar un funcionamiento inapropiado de sistemas informáticos.

4.3.- LA HISTORIA DEL DELITO INFORMÁTICO

"En 1760 Wolfgang Kempelen, un inventor húngaro de 49 años de edad, además de un ingeniero y consejero en la corte emperatriz austriaca María Teresa, construyó un jugador de ajedrez mecánico. Este sorprendente

artilugio derrotó a los más renombrados jugadores internacionales de la época e hizo ganar a su inventor fama mundial.

Un autómata con aspecto de turco se sentaba tras la enorme caja que soportaba el tablero y las piezas. El operador de la máquina podía abrir la caja para demostrar que no había nada dentro de ella excepto una red de ruedas dentadas, engranajes y cilindros giratorios. Cada 12 movimientos, Kempelen debía "dar cuerda" al aparato con una enorme llave. Desde luego, ahora se sabe que esta máquina era realmente una gran broma. El auténtico jugador era un enano que controlaba el mecanismo desde dentro y que estaba oculto por espejos cuando la caja se abría. El pequeño jugador no podía ver el tablero, pero podía determinar las piezas a mover vigilando una serie de imanes que se encontraban bajo el mismo"[14].

Con este ingenioso invento, Kempelen ha sido considerado por muchos como el precursor de lo que en la época moderna se conoce como "delito informático".

[14] BEEKMAN George.- Introducción a la Informática.- Sexta Edición.- Pearson Educación S.A.- Madrid.- 2005.- Pág. 356

Han pasado más de dos siglos y los seres humanos seguimos siendo impresionados por maquinas inteligentes.

En 1997 el mundo se quedó impresionado cuando observó como la computadora denominada Deep Blue fabricada por la multinacional IBM ganaba una partida de ajedrez al campeón mundial de aquella época Gary Kasparov.

Las computadoras en la actualidad no solo juegan ajedrez o nos ayudan a procesar textos sino que han traspasado esas barreras y hoy en día controlan nuestro dinero, la educación, medicina, nuestros automotores, se han constituido en el instrumento esencial para ganar o perder batallas, y en definitiva en todas las actividades que realice el ser humano, se encuentra involucrado un ordenador.

Confiamos nuestras fortunas, nuestra salud e inclusive nuestras vidas a la tecnología de la información, pero debemos estar conscientes también que la fe ciega en esa tecnología puede ser muy peligrosa si sabemos tomar las debidas precauciones.

4.4.- ELEMENTOS DEL DELITO INFORMÁTICO

El estudio de los tipos penales a partir de su formulación en el Código Penal, permiten distinguir los elementos básicos que los integran y por otro lado circunstancias que pueden presentarse en su comisión, como las agravantes, atenuantes y otras disposiciones que pueden presentarse con el delito.

Los aspectos que se detalla a continuación, vendrían a constituir los elementos básicos o partes integrantes de la estructura del tipo penal:

- Objetividad jurídica o bien jurídico protegido
- Sujeto Activo
- Sujeto pasivo
- Aspecto subjetivo
- Aspecto objetivo, el que se descompone en: a) verbo nuclear o rector y b) otros aspectos
- Objeto de la acción
- Resultado
- Precepto legal
- Sanción

4.4.1.- La objetividad jurídica o bien jurídico protegido

Todo tipo penal protege relaciones de interés para la sociedad, relaciones expresadas a través de los derechos personales, patrimoniales, entre otros, como son: la vida, la fe pública, etc.

La objetividad jurídica o bien protegido a que se refiere el contenido de cada tipo penal es el elemento o aspecto que en la codificación moderna sirve para agrupar los delitos en los diferentes títulos del Libro II del Código Penal.

Roxin Claus, en su obra Derecho Penal define al bien jurídico como "las circunstancias dadas o finalidades que son útiles para el individuo y su libre desarrollo en el marco de un sistema global estructurado sobre la base de esa concepción de los fines o para el funcionamiento del propio sistema"[15].

Una definición amplia, refiere al bien jurídico protegido como "El patrimonio, en el caso de la amplia

[15] MÁRQUEZ, Carlos. El Delito Informático. La Información y la Comunicación en la Esfera Penal. Editorial Leyer. Bogotá Colombia. 2002. Pág.97

gama de fraudes informáticos y las manipulaciones de datos que da a lugar; La reserva, la intimidad y confidencialidad de los datos, en el caso de las agresiones informáticas a la esfera de la intimidad en forma general, especialmente en el caso de los bancos de datos; La seguridad o fiabilidad del tráfico jurídico y probatorio, en el caso de falsificaciones de datos o documentos probatorios vía medios informáticos; El derecho de propiedad, en este caso sobre la información o sobre los elementos físicos, materiales de un sistema informático, que es afectado por los daños y el llamado terrorismo informático"[16].

En el caso de los delitos informáticos, los bienes jurídicos protegidos podrían ser diversos en atención hacia aquellos a los que está dirigido el acto lesivo, valiéndose a través o por medio del ordenador que permite el acceso a información que se procesa en un sistema informático.

4.4.2.- Sujeto activo

[16] ACURIO DEL PINO, Santiago. Ruptura 2001. Delitos Informáticos. F&R Gráficas. Quito. 2001. Pág. 303

Según Guillermo Cabanellas, el sujeto activo del delito es **"el autor, cómplice o encubridor; el delincuente en general"[17].**

El sujeto activo es el elemento del tipo que expresa la persona que puede ser autor, o quien puede cometer los hechos previstos en el tipo penal.

En un tipo penal, el sujeto activo puede ser: sujeto activo general o indeterminado; y, sujeto activo especial o cualificado.

4.4.2.1.- Sujeto activo general o indeterminado

La denominación empleada por nuestro código para expresar el sujeto activo general y mediante la cual podemos identificarlo, pueden ser los vocablos "el que", "quien", lo cual significa que determinado acto delictivo puede ser cometido por cualquier persona; es decir no existe ninguna condición o circunstancia especial para la ejecución de esa acción. Sin embargo para identificar bien si se trata de un sujeto activo general, debemos siempre leer detenidamente toda la frase donde se estipula el tipo penal, pues puede que

[17] CABANELLAS Guillermo.- Diccionario Jurídico Elemental.- Pág. 374

nos encontremos con una expresión como "el que tenga la administración de los bienes de propiedad estatal", ante lo cual dejaría de ser un sujeto activo general.

4.4.2.2.- Sujeto activo especial o cualificado

A diferencia del sujeto activo general, el sujeto activo especial es determinado, se limita a ciertas personas que pueden ejecutar el tipo penal; podemos identificarlo en nuestro código por frases como "el funcionario público", "la autoridad", "la madre", "los abuelos", etc., con lo cual se limita exclusivamente a que sean este tipo de personas quienes puedan cometer determinado delito.

En los delitos informáticos, el sujeto activo, sin lugar a dudas es especial o cualificado, pues se necesita de tener conocimientos en informática para poder cometerlos y dependiendo del nivel de conocimientos se cometerá el delito, que será de menor o mayor gravedad.

4.4.3.- Sujeto pasivo

El jurista Guillermo Cabanellas al respecto señala que el sujeto pasivo es el "que recibe la acción del agente, y no coopera en ella"[18].

Otra definición refiere que el sujeto pasivo "es la persona natural o jurídica titular del bien jurídico que el legislador protege y sobre la cual recae la actividad típica del sujeto activo"[19].

El sujeto pasivo viene a ser el sujeto o titular del derecho vulnerado, del bien dañado o puesto en peligro y tiene similares características que el sujeto activo, en cuanto a su clasificación; de tal modo que puede ser sujeto pasivo general o especial, según el caso.

4.4.3.1.- Sujeto pasivo general

Se considera que el sujeto pasivo es general, cuando el titular del derecho que se lesiona o se pretende lesionar, puede ser cualquier persona, en cuyo caso encontramos en el Código Penal frases como: "quien mate a otra persona" o "quien hiriere a otra persona"; las palabras "otra persona", identifican a un sujeto pasivo

[18] CABANELLAS Guillermo.- Diccionario Jurídico Elemental. Pág. 296
[19] ACURIO, Santiago. Ruptura por la legalidad. F&R Gráficas. Quito Ecuador. 2001. Pág.309

general, que también al igual que el sujeto activo, puede considerarse como indeterminado.

4.4.3.2.- Sujeto pasivo especial

El sujeto pasivo es especial, cuando se limita la posibilidad de ser perjudicado por la comisión de cierto tipo penal y lo encontramos en enunciados como "la madre que mate al hijo".

Igual como manifesté anteriormente al referirme al sujeto activo, en algunos tipos se hace necesario leer todo el contenido del precepto, para identificar el tipo de sujeto pasivo.

En el caso de los delitos informáticos, el sujeto pasivo es aquella persona natural o jurídica que se ve afectada por el acto ilícito que vulnera alguno o algunos de sus bienes jurídicos protegidos.

Ampliando esta definición, se distingue que el sujeto pasivo del delito es el ente o la víctima sobre la cual recae la conducta de acción u omisión que realiza el sujeto activo, y en el caso de los delitos

informáticos, las víctimas pueden ser cualquier individuo o persona natural, así también personas jurídicas como instituciones bancarias, gobiernos, etc., **mismos que usan sistemas automatizados de información, por lo cual considero que el sujeto pasivo en tratándose de delitos informáticos es especial.**

En general, se estima como sujeto pasivo mediato a la sociedad entendida en su conjunto; como sujeto pasivo inmediato al titular del bien jurídico lesionado, quien es la víctima directa del delito informático, denominado también como ofendido o agraviado.

4.4.4.- Aspecto subjetivo

El aspecto subjetivo del tipo penal, en la mayoría de las legislaciones, se formula como formas de la culpabilidad, entiéndase por éstas al dolo o la culpa. Entonces al hablar del aspecto subjetivo de determinado delito o tipo penal, diríamos que es un delito doloso o culposo.

Por ejemplo en el delito de peculado contemplado en nuestro Código Penal, el aspecto subjetivo sería el

dolo, pues se comete a sabiendas, con intención y en las infracciones de tránsito el aspecto subjetivo sería la culpa, porque se cometen por imprudencia, impericia o inobservancia.

El aspecto subjetivo cuando se trata de los delitos informáticos, es el dolo, no podría a mi entender configurarse como un delito culposo, pues el sujeto activo al tener altos conocimientos de informática, está consciente del daño que puede ocasionar a los sistemas de información y lo realiza a sabiendas, por lo cual existe intención manifiesta de causar daño en su accionar.

Debo recalcar lo que en páginas anteriores se señaló que no es lo mismo el joven que entra a un sistema informático por curiosidad, por investigar, que el empleado de una institución financiera que a sabiendas desvía los fondos de las cuentas de los clientes, aquí claramente se distingue el dolo de la culpa.

4.4.5.- Aspecto Objetivo

El aspecto objetivo es una parte fundamental del tipo penal, es la razón de ser de éste, es la acción u omisión peligrosa, descrita en forma breve y clara. Lo integran dos elementos, el verbo rector o nuclear y los otros aspectos de la parte objetiva.

4.4.5.1.- Verbo rector o nuclear

El verbo nuclear, constituye como su palabra lo dice el núcleo, el centro del aspecto objetivo, porque expresa la acción u omisión socialmente peligrosa, por ejemplo "matare", "lesionare", "sustraiga", etc. En un mismo tipo penal, puede existir más de un verbo rector.

Por ejemplo en el artículo 130 del Código Penal del Ecuador, se establece que "El que en cualquier forma o por cualquier medio se alzare en contra del gobierno, con el objeto de desconocer la Constitución de la República, deponer al gobierno constituido, impedir la reunión del congreso o disolverlo, o provocar la guerra civil, será reprimido con reclusión mayor de cuatro a ocho años. El acto existe desde que hay tentativa punible"[20].

[20] Régimen Penal ecuatoriano.- Código Penal del Ecuador.- Ediciones Legales.- Art. 130

En este ejemplo, encontramos algunos verbos nucleares, como "alzare", "desconocer", "deponer", "impedir", "disolverlo" y "provocar".

El artículo… (415.1) de nuestro Código Penal, referente a los daños informáticos, se estipula: "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 contenido 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….[21]"

En este delito de daños informáticos, encontramos algunos verbos rectores, como "destruir", "alterar", "inutilizar" "suprimir" y "dañar".

4.4.5.2.- Otros aspectos de la parte objetiva

Para determinar exactamente en qué consiste la acción u omisión socialmente peligrosa, hay que completar la idea dada por el verbo rector con información que

[21] Régimen Penal ecuatoriano.- Código Penal del Ecuador.- Ediciones Legales.- Art. 415

permita determinar exactamente el hecho, a esto es lo que se conoce como otros aspectos de la parte objetiva.

A continuación veremos un ejemplo.

En el primer inciso del artículo 197 de nuestro Código Penal, se establece que "serán sancionados con penas de dos meses a un año de prisión, quienes interceptaren sin orden judicial, conversaciones telefónicas o realizadas por medios afines y quienes se sustrajeran o abrieran sobres de correspondencia que pertenecieren a otro sin autorización expresa"[22].

En el presente ejemplo, los otros aspectos de la parte objetiva, están determinados por ejemplo en la frase "sin orden judicial, conversaciones telefónicas".

En el caso del delito de daño informático analizado recientemente, los otros aspectos de la parte objetiva están determinados por la expresión "de forma temporal o definitiva".

4.4.6.- Objeto de la acción u omisión

[22] Régimen Penal ecuatoriano.- Código Penal del Ecuador.- Ediciones Legales.- Art. 197

El objeto de la acción u omisión es un elemento del tipo penal, consistente en la cosa material o persona sobre la que recae la acción u omisión del verbo nuclear.

Por ejemplo, el artículo 240 del Código Penal del Ecuador, referente a la violación de sellos y documentos, establece que "cuando hubieren sido rotos los sellos puestos por orden de la autoridad pública, los guardianes serán reprimidos, por simple negligencia, con prisión de ocho días a seis meses".

En este ejemplo, el objeto de la acción está determinado por una cosa material, que son "los sellos", porque es precisamente sobre ellos que recae el verbo nuclear de romper.

En el delito de daños informáticos analizado, el objeto de la acción recae en los "programas, datos, bases de datos, información o cualquier mensaje de datos", pues sobre ellos recaen los verbos "destruir", "alterar", "inutilizar" "suprimir" y "dañar".

4.4.7.- Resultado

El resultado es el aspecto del tipo penal que consiste en el cambio que se opera en la realidad, producto de la acción u omisión del hecho delictivo. Este resultado puede ser de peligro o de daño.

4.4.7.1.- Resultado de peligro

Se dice que un tipo penal es de resultado de peligro, cuando el hecho peligroso, es una acción u omisión que pone en peligro bienes jurídicamente protegidos, sin necesidad que se llegue a materializar el peligro o el daño.

Ejemplo:

El artículo 474 del Código Penal ecuatoriano, establece que "serán reprimidos con prisión de un mes a un año y multa de seis dólares de los Estados Unidos de Norte América, los que hubieren abandonado o hecho abandonar un niño en un lugar no solitario; y los que lo hubieren expuesto o hecho exponer, siempre que no sea en un hospicio o en casa de expósitos"[23].

[23] Régimen Penal ecuatoriano.- Código Penal del Ecuador.- Ediciones Legales.- Art. 474

En el ejemplo propuesto, el hecho de "abandonar o hecho abandonar a un niño en un lugar solitario", constituye el peligro, por ello se considera que su resultado es de peligro.

El artículo (202.2) de nuestro Código Penal al referirse a la obtención y utilización no autorizada de información, señala que "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". En este caso, nos encontramos frente a un delito de resultado de peligro porque la información obtenida es cedida, transferida, publicada, etc., pero no destruida.

4.4.7.2.- Resultado o de daño

El tipo penal es de resultado cuando exige la producción de un resultado dañoso a la vida, la integridad de las personas o los bienes.

Voy a tomar como ejemplo el caso del delito denominado infanticidio honoris causa.

El artículo 453 del Código Penal, en su primer inciso, dispone que "la madre que por ocultar su deshonra matare al hijo recién nacido, será reprimida con la pena de reclusión menor de tres a seis años"[24].

En este ejemplo el resultado es de daño, la muerte del hijo recién nacido.

El artículo 262 del Código Penal en relación a la destrucción o supresión de documentos, programas, etc., dispone: "Serán reprimidos con 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"[25].

[24] Régimen Penal ecuatoriano.- Código Penal del Ecuador.- Ediciones Legales.- Art. 453
[25] Régimen Penal ecuatoriano.- Código Penal del Ecuador.- Ediciones Legales.- Art. 262

En este caso, se configura un delito de resultado daño, por cuanto los documentos, programas, información, etc., es destruida o eliminada por el empleado público.

4.4.8.- Precepto legal

El precepto legal es la ubicación que la conducta como delito tiene en el ordenamiento del código, libro, título, capítulo, sección, artículo.

El mismo delito de daños informáticos, se encuentra previsto en el artículo 415.1, del Capítulo VII, del Título V, del Libro Segundo del Código Penal.

4.4.9.- Sanción

A cada acto delictivo, le corresponde una sanción, que es adecuada por los legisladores, de acuerdo a la valoración social y gravedad del hecho.

Como ejemplo citaré la disposición sobre los daños informáticos Art. 415.1 del Código Penal, que sanciona con **prisión de seis meses a tres años y multa de**

sesenta a ciento cincuenta dólares de los Estados Unidos de Norteamérica al 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 contenido en un sistema de información o red electrónica.

4.5.- ALGUNOS DELITOS INFORMÁTICOS

Se considera que el robo de dinero, noticias, información y recursos informáticos, es lo más común cuando de delitos informáticos se trata. Veamos algunos ejemplos:

"• Un estudiante a tiempo parcial utilizó su teléfono y su PC para engañar a la computadora de la Pacific Telephone para que el equipamiento telefónico le fuera entregado a él. Inició un negocio, contrató a varios empleados y estafó alrededor de un millón de dólares en equipamiento antes de ser delatado por un empleado disgustado (tras dos meses en prisión, se convirtió en consultor de seguridad informático).

- Un antiguo reparador de cajeros automáticos obtuvo ilegalmente unos 86.000 dólares espiando a los clientes cuando éstos introducían sus contraseñas para crear después tarjetas de crédito ficticias que utilizaba con esas contraseñas"
- En 1988, varios millones de dólares de uno de los mayores bancos norteamericanos fueron transferidos ilegalmente a una cuenta privada de un banco suizo. La transferencia se detectó porque un error informático que se produjo ese día en particular obligo a los empleados a comprobar las operaciones manualmente: el procedimiento automatizado que se utilizaba a diario no se habla dado cuenta del delito.
- En 1999, el London Times revelo que varios bancos londinenses habían pagado millones de libras a varios hackers que habían amenazado con dejar inutilizados sus sistemas si no pagaban. En este caso, los bancos prefirieron pagar a admitir públicamente que sus sistemas no eran seguros.
- En 1999, dos hermanos chinos fueron sentenciados a muerte por utilizar computadoras para desviar alrededor de 30.000 dólares a cuentas bancarias que ellos controlaban.

- En 1999, un empleado de PairGain, un vendedor de productos a través de Internet de alta velocidad, puso un anuncio anónimo en un tablón de acciones de Yahoo; el mensaje decía que PairGain iba a ser adquirida por otra compañía por un valor dos veces superior al de su cotización en bolsa. Los inversores hicieron que el precio de la acción subiera alrededor de un 40 por ciento antes de darse cuenta de que habían perdido miles de dólares por culpa de un mensaje ficticio. Un equipo de investigación del FBI trazó la huella electrónica del delincuente y le detuvo una semana más tarde acusándole de manipulación del mercado de acciones. Desde entonces, este tipo de manipulación se ha cometido docenas de veces.
- En el año 2000, varios intrusos entraron en Creditcards.com, robaron 55.000 números de tarjetas de crédito y pidieron un rescate por ellos. Cuando su intento de extorsión falló, publicaron todos estos números en la Red. Desde aquel la compañía dispone de un sitio web mucho más seguro.
- En 2001, dos jóvenes rusos fueron arrestados por burlar las redes de varias compañías norteamericanas, robar información importante y pedir un rescate por ella. El FBI los capturó empleando como cebo una falsa

compañía de seguridad. Cuando solicitaron el pago, los agentes del FBI accedieron. Ambos jóvenes fueron arrestados cuando aterrizaron en Estados Unidos para cobrar su botín.

• Durante la Operation Cyber Loss de mayo de 2001, el departamento de control del fraude en Internet del FBI examinó a 88 personas en 10 días. Según este organismo, 56.000 personas fueron defraudadas durante la investigación por una cantidad superior a 117 millones de dólares"[26].

4.5.1.- La piratería del software

La piratería de software se refiere al uso del mismo (software) sin contar con la respectiva licencia y se ha convertido en una práctica descontrolada, que puede enmarcarse en las siguientes situaciones:

- Copiar e instalar en más de un computador un programa adquirido;
- Quemar CD´s u otro medio con fines de instalación y distribución;
- Instalar actualizaciones de programas sin contar con la licencia respectiva;

[26] BEEKMAN George.- Introducción a la Informática.- Sexta Edición.- Pearson Prentice Hall.- Madrid 2005.- Pág. 358 -359

- Descargar programas desde Internet sin contar con la licencia;
- Comprar copias no autorizadas de software.

"La piratería es un delito a escala mundial, y sus tasas están en aumento principalmente en los países en desarrollo. En China, aproximadamente el 95 por ciento de todas las nuevas instalaciones de software son piratas; en Vietnam, este valor aumenta hasta el 97 por ciento. Algunos países del Tercer Mundo rechazan las leyes internacionales de copyright con el pretexto de que esas leyes protegen a los países ricos a expensas de las naciones sin desarrollar. En 1998, la Corte Suprema de Argentina determinó que las leyes de copyright del país no se aplicaban al software. La información quiere ser libre. La información también es cara. En 1999, la policía de Moscú intentó dar un golpe al mercado del software ilegal destruyendo montañas de estos productos. Sin embargo, sus esfuerzos no tuvieron éxito. En la actualidad, Rusia tiene una de las tasas de piratería más altas del mundo, superada solamente por China"[27].

[27] BEEKMAN George.- Introducción a la Informática.- Sexta Edición.- Pearson Prentice Hall.- Madrid 2005.- Pág. 361

El derecho de autor se conceptualiza como el "conjunto de normas jurídicas y principios que regulan los derechos morales y patrimoniales que la ley concede a los autores (los derechos de autor), por el solo hecho de la creación de una obra literaria, artística, musical, científica o didáctica, esté publicada o inédita"[28].

La Declaración Universal de los Derechos Humanos, reconoce y garantiza como uno de los derechos humanos fundamentales el derecho de autor, es así que el numeral 2 del artículo 27, establece que toda persona tiene derecho a la protección de los intereses morales y materiales que le correspondan por razón de las producciones científicas, literarias o artísticas de que sea autora.

La Constitución de la República del Ecuador, en la sección cuarta del capítulo segundo, título II contempla el artículo 22, en virtud del cual las personas tienen derecho a desarrollar su capacidad creativa, al ejercicio digno y sostenido de las actividades culturales y artísticas, y a beneficiarse de la protección de los derechos morales y

[28] http://es.wikipedia.org/wiki/Derecho_de_autor.- 02/10/2012

patrimoniales que les correspondan por las producciones científicas, literarias o artísticas de su autoría.

"En el derecho anglosajón se utiliza la noción de copyright (traducido literalmente como "derecho de copia") que —por lo general— comprende la parte patrimonial de los derechos de autor (derechos patrimoniales).

Una obra pasa al dominio público cuando los derechos patrimoniales han expirado. Esto sucede habitualmente trascurrido un plazo desde la muerte del autor (post mortem auctoris). El plazo mínimo, a nivel mundial, es de 50 años y está establecido en el Convenio de Berna. Muchos países han extendido ese plazo ampliamente. Por ejemplo, en el Derecho europeo, son 70 años desde la muerte del autor. Una vez pasado ese tiempo, dicha obra entonces puede ser utilizada en forma libre, respetando los derechos morales"[29].

"Muchas veces, estas leyes consiguen cumplir sus objetivos. Un novelista puede tardar dos o tres años de su vida en escribir una obra maestra seguro de que no encontrará copias piratas de su obra vendiéndose por

[29] http://es.wikipedia.org/wiki/Derecho_de_autor.- 02/10/2012

las esquinas. Un estudio cinematográfico puede invertir millones de dólares en una película, sabiendo que recuperará su inversión, en un periodo de tiempo más o menos corto, a través de las entradas de los cines y los alquileres posteriores de esa película. Un inventor puede trabajar muchas horas para crear una ratonera más efectiva sabiendo que el MegaMousetrap City no robará su idea.

Pero hay veces en las que las leyes de propiedad intelectual se aplican de un modo que puede llegar a ahogar la innovación y la creatividad que buscan proteger. En 1999, Amazon.com obtuvo una controvertida patente para <<las compras con un-clic>>, evitando así que otros sitios de comercio electrónico ofrecieran a sus clientes una experiencia similar. Análogamente, SightSound patentó todas las descargas de pago «señales de audio o video digital deseadas», mientras que RealNetworks hizo lo mismo con el streaming de audio y video..."[30]

4.5.2.- El sabotaje informático

La palabra sabotaje proviene del francés sabotage, que significa "fabricar zapatos" y puede definirse como

[30] BEEKMAN George.- Introducción a la Informática.- Sexta Edición.- Pearson Prentice Hall.- Madrid 2005.- Pág. 361

una acción meditada tendiente a debilitar al enemigo mediante la subversión, la obstrucción, la interrupción o la destrucción de material.

En la época de la revolución industrial, el sabotaje consistía en que los trabajadores rebeldes apagaban las máquinas dando patadas en los engranajes con sus zapatos de madera llamados "sabots".

En la actualidad el sabotaje se realiza de otra manera, se emplea para ello software mal intencionado (virus, gusanos, troyanos) en lugar "sabots".

4.5.3.- Troyanos

Del latín Troiānus, troyano es un adjetivo que hace referencia a aquel o aquello perteneciente o relativo a la antigua ciudad de Troya. La aplicación del término está vinculada a la leyenda del Caballo de Troya.

Este ardid es utilizado por un tipo de software malicioso conocido justamente como troyano. Se trata de una aplicación que, en apariencia inofensiva, es ejecutada por el usuario y termina permitiendo el

acceso remoto a la computadora sin que el propio usuario lo advierta.

"Este tipo de programas suele estar disponible en sitios web con material shareware bajo nombres que suenan a juegos o utilidades. Cuando un descuidado usuario descarga y ejecuta uno de estos programas, el resultado puede ser la perdida de ficheros, la modificación de datos o cualquier otro daño. Algunos saboteadores de redes usan troyanos para pasar datos secretos a otros usuarios no autorizados.

Un tipo especial de troyano, conocido como bomba lógica, está programado para atacar en respuesta a un evento o a una combinación de ellos. Por ejemplo, un programador podría plantar una bomba lógica diseñada para lanzarse en el momento de que cierto usuario accediera al sistema, cuando se introdujera un código especial en una base de datos o cuando el usuario llevara a cabo una cierta secuencia de acciones"[31].

4.5.4.- Virus

[31] BEEKMAN George.- Introducción a la Informática.- Sexta Edición.- Pearson Prentice Hall.- Madrid 2005.- Pág. 363

Biológicamente hablando, un virus es un agente infeccioso microscópico que sólo puede multiplicarse dentro de las células de otros organismos. Los virus infectan todos los tipos de organismos, desde animales y plantas, hasta bacterias y arqueas.

"Un virus software trabaja de un modo similar: se propaga de programa en programa, o de disco a disco, y utiliza cada programa o disco infectado para hacer copias de sí mismo. Un virus software suele esconderse en el sistema operativo de la computadora o en una aplicación"[32].

Los virus pueden desplazarse adjuntos a los correos electrónicos. Melissa (1999) fue uno de los más conocidos, cuyo método fue el siguiente:

A determinado usuario le llega un archivo adjunto a un mensaje electrónico, enviado por alguien conocido. Dicho mensaje, incluye en asunto "Mensaje importante de..." y en el cuerpo del mensaje se indica que dicho documento fue solicitado por el usuario en mención y que no se lo muestre a nadie más.

[32] BEEKMAN George.- Introducción a la Informática.- Sexta Edición.- Pearson Prentice Hall.- Madrid 2005.- Pág. 363

Cuando se abra el archivo de Word, el virus macro se activará y abrirá el Outlook en la computadora. En el Outlook, selecciona los primeros cincuenta nombres de la libreta de direcciones y les enviará a esas personas 50 mensajes con documentos de Word infectados. Todos recibirán un documento infectado de alguien conocido y puede ser cualquier archivo Word, incluso confidencial, que se tenga en el computador; además de la infección, se estará revelando documentos privados.

4.5.5.- Gusanos

"Al igual que los virus, los gusanos (conocidos también como tapeworms) utilizan computadoras para auto reproducirse. Pero a diferencia de aquéllos, los gusanos viajan por las redes de computadoras de forma independiente buscando estaciones limpias a las que poder infectar. Un gusano puede reproducirse hasta que la maquina se colapsa por falta de memoria o de espacio en disco. Un segmento de gusano típico reside en memoria en lugar de hacerlo en disco, por lo que puede ser eliminado reiniciando todas las máquinas de la red"[33].

[33] BEEKMAN George.- Introducción a la Informática.- Sexta Edición.- Pearson Prentice Hall.- Madrid 2005.- Pág. 365

Es algo usual detectar la presencia de gusanos en un sistema cuando, debido a su incontrolada replicación, los recursos del sistema se consumen hasta el punto de que las tareas ordinarias del mismo son excesivamente lentas o simplemente no pueden ejecutarse.

4.5.6.- Hacking y cracking

"A finales de los 70, las computadoras de tiempo compartido de Stanford y del MIT llamaban la atención de comunidades informales de fanáticos de las computadoras que se llamaban a sí mismos hackers. En esos días, un hacker era una persona que disfrutaba aprendiendo los entresijos del funcionamiento de un sistema informático y que escribía inteligentes programas llamados hacks. Los hackers eran, en la mayoría de casos, curiosos, entusiastas, inteligentes, idealistas, excéntricos e inofensivos. Tanto es así que muchos de ellos fueron los arquitectos de la revolución de las micro computadoras"[34].

¿Qué es hacking?

[34] BEEKMAN George.- Introducción a la Informática.- Sexta Edición.- Pearson Prentice Hall.- Madrid 2005.- Pág. 367

Hacking es la búsqueda permanente de conocimientos en todo lo relacionado con sistemas informáticos, sus mecanismos de seguridad, las vulnerabilidades de los mismos, la forma de aprovechar estas vulnerabilidades y los mecanismos para protegerse de aquellos que saben hacerlo.

¿Qué es cracking?

Tiene dos definiciones, según se hable de seguridad informática o de crackeo de programas. En el caso de seguridad informática es el permanente intento de violación de seguridad de los sistemas informáticos, con fines justificados o no. En el caso de crackeo de programas la definición es la de creador de cracks, literalmente romper, que son programitas destinados a la desprotección de programas comerciales para que puedan ser usados sin límite y gratis.

4.6.- LA INVESTIGACIÓN PREPROCESAL Y PROCESAL PENAL

4.6.1.- La investigación preprocesal

El artículo 195 de la Constitución de la República del Ecuador, preceptúa que la Fiscalía dirigirá, de oficio o a petición de parte, la investigación preprocesal y procesal penal; durante el proceso ejercerá la acción pública con sujeción a los principios de oportunidad y mínima intervención penal, con especial atención al interés público y a los derechos de las víctimas. De hallar mérito acusará a los presuntos infractores ante el juez competente, e impulsará la acusación en la sustanciación del juicio penal.

El artículo 215 de nuestro Código de Procedimiento Penal refiriéndose a la indagación previa, señala:

"Art. 215.- Indagación previa.- Antes de resolver la apertura de la instrucción, si lo considera necesario, la Fiscal o el Fiscal con la colaboración de la policía judicial que actuará bajo su dirección, investigará los hechos presumiblemente constitutivos de infracción penal que por cualquier medio hayan llegado a su conocimiento.

Si durante la indagación previa tuvieran que adoptarse medidas para las cuales se requiere de autorización

judicial, la fiscal o el Fiscal deberá previamente obtenerla.

De no existir fundamentos para deducir la imputación, la indagación no podrá mantenerse abierta por más de un año, y transcurrido este plazo el fiscal dispondrá el archivo provisional del expediente o solicitará al juez su archivo definitivo, según fuera el caso; este plazo se contará desde la fecha en la cual el fiscal dio inicio a la indagación previa.

Sin embargo, si llegaren a poder de la fiscal o el fiscal elementos que le permitan imputar la autoría o participación en el delito a persona determinada, iniciará la instrucción aunque el plazo hubiere fenecido, siempre que la acción penal no hubiere prescrito según las reglas generales.

Sin perjuicio de las garantías del debido proceso y del derecho a la defensa; las actuaciones de la Fiscalía, de la Función Judicial, de la Policía Judicial y de otras instituciones y funcionarios que intervengan en la indagación previa, se mantendrán en reserva de terceros ajenos a ésta y del público en general, sin

perjuicio del derecho del ofendido, y de las personas a las cuales se investiga y de sus abogados, de tener acceso inmediato, efectivo y suficiente de las investigaciones. El personal de las instituciones mencionadas que habiendo intervenido en estas actuaciones, las divulguen o pongan de cualquier modo en peligro el éxito de la investigación o las difundan atentado contra el honor y al buen nombre de las personas en general, serán sancionados conforme a lo previsto en el Código Penal."[35]

Esta disposición exige al Fiscal la investigación de los hechos que se presume constituyen una infracción de la ley, para que de esta manera cuente con los elementos necesarios que le permitan contar con los elementos de convicción referentes a la existencia en primer lugar de una infracción penal y luego sobre la presunta participación del o los responsables de la misma.

En base a esta indagación, la Fiscal o el Fiscal podrá determinar si el hecho ha ocurrido o no, si hay lugar o no al ejercicio de la acción penal, identificar al presunto responsable, conocer su nombre, residencia,

[35] Régimen Penal ecuatoriano.- Código de procedimiento penal del Ecuador.- Ediciones Legales.- Art. 215

etc. Además debe observar el cumplimiento de las garantías constitucionales y el respeto a los derechos humanos.

El Art. 80 del Código de Procedimiento Penal ecuatoriano, señala: "Toda acción, preprocesal o procesal que vulnere garantías constitucionales carecerá de eficacia probatoria alguna"[36].

Como derechos de protección la Constitución de la República del Ecuador Art. 76 señala que: "Nadie podrá ser interrogado, ni aún con fines de investigación, por la Fiscalía General del estado, por autoridad policial o por cualquier otra, sin la presencia de un abogado particular o un defensor público, ni fuera de los recintos autorizados para el efecto. Cualquier diligencia judicial o administrativa, que no cumpla con este precepto, carecerá de eficacia probatoria"[37].

De igual manera el Art.77 numeral. 7 literal c de la Constitución de la República del Ecuador dispone que "nadie podrá ser forzado a declarar en contra de sí

[36] Régimen Penal ecuatoriano.- Código de procedimiento penal del Ecuador.- Ediciones Legales.- Art. 80
[37] Constitución de la República del Ecuador.- Art. 76, numeral 7, literal e)

mismo, sobre asuntos que puedan ocasionar su responsabilidad penal"[38].

4.6.2.- La investigación procesal penal

El cuarto libro del Código de Procedimiento Penal ecuatoriano contempla las etapas del proceso penal y concretamente el artículo 206 establece las siguientes:

1. La Instrucción Fiscal;
2. La Etapa Intermedia;
3. El Juicio; y,
4. La Etapa de Impugnación.

4.6.2.1.- La instrucción fiscal

Con los elementos de convicción obtenidos en la indagación previa, el Fiscal en uso de la facultad que confiere los artículos 33 y 217 del Código de Procedimiento Penal, en audiencia convocada por el Juez, puede resolver iniciar instrucción fiscal contra determinada persona imputando su presunta participación como responsable en el cometimiento de un delito de acción pública. En caso de delito flagrante, esta etapa

[38] Constitución de la República del Ecuador.- Art. 77, numeral 7, literal c)

dura treinta días y en los delitos no flagrantes dura noventa días, salvo vinculaciones posteriores en cuyo caso se dilata por treinta días más en cada vinculación. En esta diligencia puede el juez de la causa como garantista de los derechos constitucionales dictar medidas cautelares de carácter real y personal.

4.6.2.2.- La etapa intermedia

La conclusión de la instrucción fiscal en audiencia se escucha al procesado, al acusador particular de haberlo, al Fiscal de acuerdo con lo que dispone el artículo 226.1 del Código de Procedimiento Penal sobre competencia, aspectos de perjudicialidad, de procedibilidad. Se analizan aspectos sobre acuerdos probatorios en la denominada preparación del juicio, luego de lo cual el Fiscal de la causa pronuncia dictamen. Concluido el mismo se escucha al acusador particular y después al abogado del procesado. Concluidas las intervenciones el juez de la causa dicta su resolución que puede ser un auto de llamamiento a juicio o un auto de sobreseimiento.

4.6.2.3.- El juicio

Esta etapa se iniciará con la sustanciación del proceso ante el presidente del Tribunal Penal, quien estaría obligado en primera instancia, a designar un defensor para el sindicado en caso de que éste se encuentre imposibilitado para contratarlo. Además deberá convocar a la Audiencia para el juzgamiento y solicitar a las partes que le entreguen la lista de los testigos, ya que estará encargado e dictar las órdenes respectivas para la comparecencia de los mismos. Como se había señalado anteriormente en la instrucción fiscal solo se investiga pero no se prueba, para que todas las indagaciones realizadas por el fiscal alcancen el valor de prueba, estas deberán ser presentadas ante el tribunal penal.

Propósitos de esta etapa

Esta etapa, a criterio del Dr. Guerrero tendrá tres propósitos fundamentales:

a) la prueba de la existencia del delito
b) La prueba de la culpabilidad del infractor; y,

c) La imposición de la pena correspondiente al delito cometido, de las medidas de seguridad y del pago del daño causado al ofendido.

Audiencia de Juicio

Se observarán los principios de: contradicción, oralidad, publicidad, inmediación y concentración. Se realiza la sustanciación ante el Tribunal Penal y comprende la intervención de los sujetos procesales, la declaración de los testigos y peritos y la exhibición de pruebas.

Desde el art. 291 al 313, se desarrolla el procedimiento a seguir, el mismo que se ha dividido en dos partes. La primera inicia con la intervención del fiscal quien plantea la teoría del caso y solicita que se practiquen las pruebas que se consideren necesarias. Una vez presentado el testimonio, los miembros del Tribunal y los otros sujetos, procesales podrán interrogar observando para el efecto las normas constitucionales y procesales sobre la procedibilidad del interrogatorio.

A continuación, vendrá la exposición del acusador particular o de su defensor, quien realizará una exposición del motivo de su acusación y solicitará la práctica de las pruebas que considere necesarias.

Continuando luego la audiencia, el acusado puede rendir su testimonio, luego de lo cual, podrá ser interrogado por los miembros del Tribunal y las otras partes (art.301).

Realizado el reconocimiento, el defensor del acusado hará una exposición detallada de los hechos y circunstancias favorables para su defendido y pedirá que se practiquen las pruebas de descargo (art.303), luego de lo cual, el Tribunal procederá a tomar testimonios de los testigos presentados por el acusado, quienes también podrán ser interrogados por las partes (art. 304).

Concluida la prueba se dará lugar al debate en el que las partes podrán exponer sus alegatos, luego de lo cual los miembros del Tribunal deberán deliberar y finalmente anunciar su resolución en forma oral para

posteriormente expedir la sentencia a que hubiere lugar.

4.6.2.4.- La etapa de impugnación

Los recursos procesales vigentes son: Nulidad, Apelación, Casación, Revisión y de Hecho. Mientras los recursos de Nulidad y Apelación se interponen ante la Corte Provincial, los recursos de Casación y Revisión se interponen ante la Corte Nacional de Justica, el Recurso de Hecho por lógica jurídica se interpone ante el Juez o jueza que negó el recurso interpuesto en primera instancia.

4.7.- LA INFORMÁTICA APLICADA A LA INVESTIGACIÓN DE CONDUCTAS DELICTIVAS

El Dr. Santiago Acurio del Pino, define a la Informática Forense como "la ciencia forense que se encarga de la preservación, identificación extracción, documentación e interpretación de la evidencia digital, para luego ésta ser presentada en una Corte de Justicia"[39].

[39] ACURIO DEL PINO Santiago Dr.- Introducción a la informática Forense.- Pag. 7

Según el mismo autor, el objetivo de la Informática Forense es el de "recobrar los registros y mensajes de datos existentes dentro de un equipo informático, de tal manera que toda esa información digital, pueda ser usada como prueba ante un tribunal"[40].

4.7.1.- Principios básicos

En el manual de manejo de evidencias de la Fiscalía General del Estado se prevé que el funcionario de la Fiscalía o de la Policía Judicial no debe acudir solo al lugar de los hechos, este tipo de actividad debe ser realizada como mínimo por dos personas, contando además con miembros de seguridad; que deben planear y coordinar sus acciones.

Ninguna acción debe tomarse por parte de la Policía Judicial, la Fiscalía o por sus agentes y funcionarios que cambie o altere la información almacenada dentro de un sistema informático o medios magnéticos, a fin de que esta sea presentada fehacientemente ante un tribunal.

[40] ACURIO DEL PINO Santiago Dr.- Introducción a la informática Forense.- Pag. 8

En circunstancias excepcionales una persona competente puede tener acceso a la información original almacenada en el sistema informático objeto de la investigación, siempre que después se explique detalladamente y de manera razonada cual fue la forma en la que se produjo el acceso, su justificación y las implicaciones de dichos actos.

Se debe llevar una bitácora de todos los procesos adelantados en relación a la evidencia digital. Cuando se hace una revisión de un caso por parte de una tercera parte ajena al mismo, todos los archivos y registros del caso y el proceso aplicado a la evidencia que fue recolectada y preservada, deben permitir a esa parte recrear el resultado obtenido en el primer análisis.

El Fiscal del Caso y/o el oficial a cargo de la investigación son responsables de garantizar el cumplimiento de la ley, y del apego a estos principios en el caso del Fiscal y la conservación de la evidencia a partir de la aprehensión y hasta la presentación como prueba con la debida cadena de custodia en el caso del miembro de la Policía Nacional.

De igual forma debe asegurar que cualquier persona que acceda a o copie dicha información cumpla con la ley y estos principios.

4.7.2.- Principios del peritaje

1.- Objetividad

El perito debe ser objetivo, debe observar los códigos de ética profesional.

2.- Autenticidad y conservación

Durante la investigación, se debe conservar la autenticidad e integridad de los medios probatorios.

3.- Legalidad

El perito debe ser preciso en sus observaciones, opiniones y resultados, conocer la legislación respecto de su actividad pericial y cumplir con los requisitos establecidos por ella.

4.- Idoneidad

Los medios probatorios deben ser auténticos, ser relevantes y suficientes para el caso.

5.- Inalterabilidad

En todos los casos, existirá una cadena de custodia debidamente asegurada que demuestre que los medios no han sido modificados durante la pericia.

6.- Documentación

Deberá establecerse por escrito los pasos dados en el procedimiento pericial.

4.7.3.- Incautación de equipos informáticos o electrónicos

Si se presume que existe algún tipo de evidencia digital se debe pedir autorización judicial para incautar los equipos y se debe contar además con igual autorización para acceder al contenido de dichos aparatos.

A efecto de realizar un allanamiento e incautación de equipos informáticos o electrónicos se deben considerar circunstancias como las siguientes:

Se debe efectuar en el momento oportuno, esto a fin de evitar la destrucción de equipos, datos, o evidencia

contenida en esta, etc.; o el sospechoso puede estar conectado al internet.

Hay que tener preparado el material que se empleará al momento de incautar los equipos como cintas de embalajes, etiquetas, discos, cámaras fotográficas, etc.

Si los datos o archivos se encuentran en más de un lugar, en una red o conexión remota, hay que realizar simultáneamente los allanamientos e incautación en los diferentes sitios.

Se debe contar con la autorización judicial para duplicar, reproducir datos encontrados, fijar y grabar la escena, obtener códigos, claves de acceso, contraseñas, buscar documentos que contienen información de acceso, conexiones en redes, etc.

La falta de una orden de allanamiento e incautación que ampare las actuaciones (sobre los equipos y sobre la información) de la Policía Judicial y la Fiscalía puede ocasionar la exclusión de los elementos probatorios por

violación de las Garantías Constitucionales. Art. 66 de la Constitución de la República del Ecuador.

4.7.4.- En la escena del delito

Se prevé en el Manual de Manejo de Evidencias de la Fiscalía General del Estado que los investigadores que llegan primero a una escena del crimen tienen ciertas responsabilidades, las cuales se resumen así:

"**Observe y establezca los parámetros de la escena del delito**: El primero en llegar a la escena, debe establecer si el delito está todavía en progreso, luego tiene que tomar nota de las características físicas del área circundante. Para los investigadores forenses esta etapa debe ser extendida a todo sistema de información y de red que se encuentre dentro de la escena. En estos casos dicho sistema o red pueden ser blancos de un inminente o actual ataque como por ejemplo uno de denegación de servicio (DoS).

Inicie las medidas de seguridad: El objetivo principal en toda investigación es la seguridad de los investigadores y de la escena. Si uno observa y

establece en una condición insegura dentro de una escena del delito, debe tomar las medidas necesarias para mitigar dicha situación. Se deben tomar las acciones necesarias a fin de evitar riesgos eléctricos, químicos o biológicos, de igual forma cualquier actividad criminal.

Esto es importante ya que en una ocasión en una investigación de pornografía infantil en Estados Unidos un investigador fue muerto y otro herido durante la revisión de una escena del crimen.

Facilite los primeros auxilios: Siempre se deben tomar las medidas adecuadas para precautelar la vida de las posibles víctimas del delito, el objetivo es brindar el cuidado médico adecuado por el personal de emergencias y el preservar las evidencias.

Asegure físicamente la escena: Esta etapa es crucial durante una investigación, se debe retirar de la escena del delito a todas las personas extrañas a la misma, el objetivo principal es el prevenir el acceso no autorizado de personal a la escena, evitando así la contaminación de la evidencia o su posible alteración.

Asegure físicamente las evidencias: Este paso es muy importante a fin de mantener la cadena de custodia de las evidencias, se debe guardar y etiquetar cada una de ellas. En este caso se aplican los principios y la metodología correspondiente a la recolección de evidencias de una forma práctica. Esta recolección debe ser realizada por personal entrenado en manejar, guardar y etiquetar evidencias.

Entregar la escena del delito: Después de que se han cumplido todas las etapas anteriores, la escena puede ser entregada a las autoridades que se harán cargo de la misma. Esta situación será diferente en cada caso, ya que por ejemplo en un caso penal será a la Policía Judicial o al Ministerio Público; en un caso corporativo a los Administradores del Sistema. Lo esencial de esta etapa es verificar que todas las evidencias del caso se hayan recogido y almacenado de forma correcta, y que los sistemas y redes comprometidos pueden volver a su normal operación.

Elaborar la documentación de la explotación de la escena: Es indispensable para los investigadores documentar cada una de las etapas de este proceso, a

fin de tener una completa bitácora de los hechos sucedidos durante la explotación de la escena del delito, las evidencias encontradas y su posible relación.

La cadena de custodia es un sistema de aseguramiento que, basado en el principio de la "mismidad", tiene como fin garantizar la autenticidad de la evidencia que se utilizará como "prueba" dentro del proceso. La información mínima que se maneja en la cadena de custodia, para un caso específico, es la siguiente: a) Una hoja de ruta, en donde se anotan los datos principales sobre descripción de la evidencia, fechas, horas, custodios, identificaciones, cargos y firmas de quien recibe y quien entrega; b) Recibos personales que guarda cada custodio y donde están datos similares a los de la hoja de ruta; c) Rótulos que van pegados a los envases de las evidencias, por ejemplo a las bolsas plásticas, sobres de papel, sobres de Manila, frascos, cajas de cartón, etc.; d) Etiquetas que tienen la misma información que los rótulos, pero van atadas con una cuerdita a bolsas de papel kraft, o a frascos o a cajas de cartón o a sacos de fibra; e) Libros de registro de entradas y salidas, o cualquier otro sistema

informático que se deben llevar en los laboratorios de análisis y en los despachos de los fiscales e investigadores con los sospechosos. Un investigador puede encontrar buenas referencias sobre los hechos ocurridos en las notas recopiladas en la explotación de la escena del Delito"[41].

En el Manual de Manejo de Evidencias de la Fiscalía General del Estado, de igual manera se realiza las siguientes recomendaciones que deben tenerse presentes al momento de encontrar cualquier dispositivo informático o electrónico:

"No tome los objetos sin guantes de hule, podría alterar, encubrir o hacer desaparecer las huellas dactilares o adeníticas existentes en el equipo o en el área donde se encuentra residiendo el sistema informático.

Asegure el lugar.

Asegure los equipos. De cualquier tipo de intervención física o electrónica hecha por extraños.

[41] Manual de Manejo de Evidencias de la Fiscalía General del Estado

Si no está encendido, no lo encienda (para evitar el inicio de cualquier tipo de programa de autoprotección.

Verifique si es posible el Sistema Operativo a fin de iniciar la secuencia de apagado a fin de evitar pérdida de información.

Si usted cree razonablemente que el equipo informático o electrónico está destruyendo la evidencia, debe desconectarlo inmediatamente.

Si está encendido, no lo apague inmediatamente (para evitar la pérdida de información "volátil").

No use el equipo informático que está siendo investigado, ni intente buscar evidencias sin el entrenamiento adecuado.

Si tiene un "Mouse", muévalo cada minuto para no permitir que la pantalla se cierre o se bloqueé.

Si una computadora portátil (Laptop) no se apaga cuando es removido el cable de alimentación, localice y remueva la batería, esta generalmente se encuentra

debajo del equipo, y tiene un botón para liberar la batería del equipo. Una vez que está es removida debe guardarse en un lugar seguro y no dentro de la misma máquina, a fin de prevenir un encendido accidental.

Si el aparato está conectado a una red, anote los números de conexión, (números IP).

Fotografíe la pantalla, las conexiones y cables.

Usar bolsas especiales antiestática para almacenar diskettes, discos rígidos, y otros dispositivos de almacenamiento informáticos que sean electromagnéticos (si no se cuenta, pueden utilizarse bolsas de papel madera). Evitar el uso de bolsas plásticas, ya que pueden causar una descarga de electricidad estática que puede destruir los datos.

Coloque etiquetas en los cables para facilitar reconexión posteriormente.

Anote la información de los menús y los archivos activos (sin utilizar el teclado), cualquier movimiento del teclado puede borrar información importante.

Si hay un disco, un disquete, una cinta, un CD u otro medio de grabación en alguna unidad de disco o grabación, retírelo, protéjalo y guárdelo en un contenedor de papel.

Bloqueé toda unidad de grabación con una cinta, un disco o un disquete vacío aportado por el investigador (no del lugar de los hechos), pues al utilizar algún elemento del lugar del allanamiento o de los hechos, se contamina un elemento materia de prueba con otro.

Selle cada entrada o puerto de información con cinta de evidencia.

De igual manera debe sellar los tornillos del sistema a fin de que no se puedan remover o reemplazar las piezas internas del mismo.

Desconecte la fuente de poder.

Quite las baterías y almacénela de forma separada el equipo (si funciona a base de baterías o es una computadora portátil).

Mantenga el sistema y medios de grabación separados de cualquier tipo de imán, o campo magnético.

Al llevar aparatos, anote todo número de identificación, mantenga siempre la cadena de custodia.

Lleve todo cable, accesorio, conexión.

Lleve, si es posible, manuales, documentación, anotaciones.

Tenga en cuenta que es posible que existan otros datos importantes en sistemas periféricos, si el aparato fue conectado a una red, por tanto desconecte el cable de poder de todo hardware de Red (Router, modem, Swich, Hub).

Si el equipo es una estación de trabajo o un Servidor (conectado en red) o está en un negocio, el desconectarla puede acarrear daño permanente al equipo; responsabilidad civil para la Policía Judicial y la Fiscalía General del Estado".[42]

[42] Manual de Manejo de Evidencias de la Fiscalía General del Estado

4.8.- LOS DELITOS INFORMÁTICOS Y SU TIPIFICACIÓN EN EL RÉGIMEN PENAL ECUATORIANO

El avance tecnológico como se ha analizado en temas anteriores, ha traído consigo además de beneficios para la sociedad, un sinnúmero de problemas manifestados en conductas inadecuadas que en ocasiones adoptan las personas que tienen vastos conocimientos en el área informática y que justamente han tenido que ser regulados por el Código Penal, determinado sus tipos penales, y las sanciones respectivas.

A continuación analizaré cada uno de estos tipos penales previstos en nuestro Código Penal.

Los delitos informáticos que el Código Penal contempla son los siguientes: Delitos contra la Información Protegida: Violación de claves o sistemas de seguridad; Delitos contra la Información Protegida: Destrucción o supresión de documentos, programas; Falsificación Electrónica; Daños Informáticos; Fraude Informático; Violaciones al Derecho a la Intimidad y Pornografía Infantil, a saber:

4.8.1.- Delitos contra la información protegida: Violación de claves o sistemas de seguridad.

En el capítulo V del título II referente a los delitos contra las garantías constitucionales y la igualdad racial, se contempla los delitos contra la inviolabilidad del secreto, al respecto el artículo (202.1) dispone: "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 por parte de la persona o personas encargadas de la custodia o utilización legítima de la información, éstas 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"[43].

Este artículo fue agregado por la Ley No. 67, que fuera publicada en Registro Oficial, Suplemento No. 557 de 17 de Abril de 2002.

Según se puede apreciar, el acto delictivo está dado por el hecho de acceder u obtener información protegida en sistemas de información, para lo cual deben violentar claves o sistemas de seguridad, empleando cualquier medio informático, lo cual únicamente puede ser cometido por una persona con un nivel muy elevado de conocimientos informáticos.

[43] Régimen Penal ecuatoriano.- Código penal del Ecuador.- Ediciones Legales.- Art. 202.1

Además la pena que se impone para este tipo de delito va acorde a la gravedad del daño o de quien sea la posible víctima. Es así que si el delito informático, provoca una situación alarmante en la seguridad del país, la sanción establecida en un inicio se incrementa considerablemente.

"Artículo... (202.2).- Obtención y utilización no autorizada de Información.- 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"[44].

Hay que tener claro que no cualquier persona accede a los datos personales de un sujeto, sino que son personas que por su situación laboral, tienen acceso a la base de datos y pueden manipularla y de darse el caso que utilicen esa información sin consentimiento de su titular, recibirán la sanción correspondiente.

[44] Régimen Penal ecuatoriano.- Código Penal del Ecuador.- Ediciones Legales.- Art. 202.2

4.8.2.- Delitos contra la información protegida: Destrucción o supresión de documentos, programas.

El Título III. "De los Delitos contra la Administración Pública", en su capítulo V "De la Violación de los deberes de Funcionarios Públicos, de la Usurpación de Atribuciones y de los Abusos de Autoridad", contempla el artículo 262 que dice: "Serán reprimidos con 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"[45].

Muchos empleados públicos en razón del cargo que ocupan, manejan información reservada, es por ello que se ha previsto en el Código Penal una sanción para posibles acciones maliciosas, que pudieren cometer los funcionarios públicos, al destruir datos, programas, mensajes por su propia autoría o en complicidad con

[45] Régimen Penal ecuatoriano.- Código Penal del Ecuador.- Ediciones Legales.- Art. 262.2

otros sujetos. Se trata de un sujeto activo cualificado.

4.8.3.- Falsificación electrónica

En el título IV, "De los delitos contra la fe pública", Capítulo III, "De las falsificaciones de documentos en general", luego del artículo 353, se agrega el siguiente artículo innumerado:

"Artículo… (353.1).- Falsificación electrónica.- Son reos de falsificación electrónica la persona o personas que con 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 éstos, que se encuentre contenida en cualquier soporte material, sistema de información o telemático, ya sea:

1.- Alterando un mensaje de datos en alguno de sus elementos o requisitos de carácter formal o esencial;

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

3.- 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 este capítulo"[46].

Este artículo fue agregado por la Ley No. 67, publicada en el Registro Oficial, Suplemento No. 557 de 17 de Abril del 2002.

En este tipo penal, claramente se puede evidenciar la falta de una sanción contra quienes cometen este delito, únicamente se menciona que las sanciones estarán de acuerdo a lo que dispone ese capítulo. Hay que señalar que cada norma debe tener sus preceptos y conceptos bien establecidos y regulados, destinando a cada ilícito una respectiva sanción.

4.8.4.- Daños informáticos

El título V "De los delitos contra la seguridad pública", Capítulo VII "Del incendio y otras destrucciones, de los deterioros y daños", contempla los siguientes artículos innumerados que fueran

[46] Régimen Penal ecuatoriano.- Código penal del Ecuador.- Ediciones Legales.- Art. 353.1

agregados por Ley No. 67, publicada en Registro Oficial, Suplemento No. 557 del 17 de Abril de 2002:

"Artículo… (415.1).- Daños informáticos.- 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 contenido 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"[47].

Según esta disposición, se sanciona con pena de prisión y multa a la persona que destruya, altere, inutilice, suprima o dañe, temporal o definitivamente, programas, datos, bases de datos, información o cualquier mensaje

[47] Régimen Penal ecuatoriano.- Código Penal del Ecuador.- Ediciones Legales.- Art. 415.1

de datos contenido en un sistema de información o red electrónica, sin importar la finalidad que se persiga, la forma como lo haga o el método que emplee, basta únicamente la mala fe con la que se actúa; y si esos datos, programas, etc., han sido destinados a prestar un servicio público o se encuentra vinculado con la defensa nacional, las penas son más severas.

"Artículo... (415.2).- Si no se tratare de un delito mayor, la destrucción, alteración o inutilización de la infraestructura o instalaciones físicas necesarias para la transmisión, recepción o procesamiento de mensajes de datos, será reprimida con prisión de ocho meses a cuatro años y multa de doscientos a seiscientos dólares de los Estados Unidos de Norteamérica"[48].

Aquí se advierte que debido a la magnitud e impacto de la destrucción, no va a ser sancionada con una pena severa, por la sencilla razón que su consecuencia no repercute a nivel general de una población, sino es un daño simple y tal vez susceptible de arreglo.

4.8.5.- Fraude informático

[48] Régimen Penal ecuatoriano.- Código Penal del Ecuador.- Ediciones Legales.- Art. 415.2

En el titulo X. "De los delitos contra la propiedad", Capítulo V "De las estafas y otras defraudaciones", se añaden dos artículos innumerados a continuación del artículo 553, y que igualmente fueran agregados por la Ley No. 67, publicada en el Registro Oficial, Suplemento No. 557 del 17 de Abril de 2002:

"Artículo… (553.1).- Apropiación ilícita.- 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, 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 informáticos, sistemas informáticos, telemáticos o mensajes de datos"[49].

"Artículo… (553.2).- La pena será de prisión de uno a cinco años y multa de mil a dos mil dólares de los

[49] Régimen Penal ecuatoriano.- Código Penal del Ecuador.- Ediciones Legales.- Art. 553.1

Estados Unidos de Norteamérica, si el delito se hubiere cometido empleando los siguientes medios:

1.- Inutilización de sistemas de alarma o guarda;

2.- Descubrimiento o descifrado de claves secretas o encriptadas;

3.- Utilización de tarjetas magnéticas o perforadas;

4.- Utilización de controles o instrumentos de apertura a distancia;

5.- Violación de seguridades electrónicas, informáticas u otras semejantes"[50].

El artículo 563 del Código Penal señala que se reprimirá con prisión de seis meses a cinco años y multa de ocho a ciento cincuenta y seis dólares a la persona que con propósito de apropiarse de una cosa perteneciente a otro, se hubiere hecho entregar fondos, muebles, obligaciones, finiquitos, recibos, haciendo uso de nombres falsos o de todas las circunstancias que allí se indican. Si tal delito se hubiere cometido utilizado medios electrónicos o telemáticos, se sancionará con el máximo de la pena prevista en el inciso anterior y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica.

[50] Régimen Penal ecuatoriano.- Código Penal del Ecuador.- Ediciones Legales.- Art. 553.2

El delito que se ha detallado en estos tres artículos se enmarca en la apropiación de bienes ajenos, especialmente dineros de cuentas bancarias, y se configura cuando una persona se introduce ilegalmente en el sistema informático de una institución bancaria para desviar cantidades grandes o pequeñas de dinero a cuentas bancarias a las que tienen acceso, ocasionando perjuicio en el patrimonio de la víctima del delito. Vale aquí recordar a los dos hermanos chinos a los que me referí anteriormente, que fueron sentenciados a muerte por emplear computadoras para desviar cerca de 30.000 dólares a sus cuentas bancarias, lo que contrasta en cuanto a la severidad de la sanción con la pena prevista en nuestro sistema punitivo que contempla pena de prisión solamente.

4.8.6.- Violaciones al derecho a la intimidad (contravención)

El Capítulo III denominado "De las contravenciones de tercera clase", que se encuentra en el Título I del Libro III del Código Penal, contempla el artículo 606 que luego del numeral 19 establece que serán reprimidos con multa de siete a catorce dólares de los Estados Unidos de Norteamérica y con prisión de dos a cuatro

días, o con una de estas penas solamente los que violaren el derecho a la intimidad, en los términos establecidos en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.

En la comisión de esta clase de delitos, la informática es un medio idóneo. Esta disposición tipifica como contravención a la violación al derecho a la intimidad, por consiguiente la pena establecida es una multa y prisión insignificante por esta acción ilícita.

4.8.7.- Pornografía infantil

Este ilícito se encuentra tipificado en el Título VIII, Capítulo III, "De los delitos de explotación sexual", al respecto en el artículo 528.7 se manifiesta: "Quien produjere, publicare o comercializare imágenes pornográficas, materiales visuales, audiovisuales, informáticos, electrónicos o de cualquier otro soporte físico o formato u organizare espectáculos en vivo, con escenas pornográficas en que participen los mayores de catorce y menores de dieciocho años será reprimido con la pena de seis a nueve años de reclusión menor ordinaria, el comiso de los objetos y de los bienes

productos del delito, la inhabilidad para el empleo profesión u oficio.

Con la misma pena incurrirá quien distribuyere imágenes pornográficas cuyas características externas hiciere manifiesto que en ellas se ha grabado o fotografiado la exhibición de mayores de doce y menores de dieciocho años al momento de la creación de la imagen.

Con la misma pena será reprimido quien facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico en cuyas imágenes participen menores de edad.

Cuando en estas infracciones, la víctima sea un menor de doce años o discapacitado, o persona que adolece enfermedad grave incurable, la pena será de reclusión mayor extraordinaria de doce a dieciséis años, al pago de la indemnización, el comiso de los objetos y de los bienes producto del delito, a la inhabilidad del empleo, profesión u oficio; y, en caso de reincidencia, la pena será de veinticinco años de reclusión mayor especial.

Cuando el infractor de estos delitos sea el padre, la madre, los parientes hasta el cuarto grado de consanguinidad y segundo de afinidad, los tutores, los representantes legales, curadores o cualquier persona

del contorno íntimo de la familia, los ministro de culto, los maestros y profesores y, cualquier otra persona por su profesión u oficio hayan abusado de la víctima, serán sancionados con la pena de dieciséis o veinticinco años de reclusión mayor extraordinaria, al pago de la indemnización, el comiso de los objetos y de los bienes producto del delito de inhabilidad del empleo u oficio.

Si la víctima fuere menor de doce años se aplicará el máximo de la pena"[51].

Es una infracción concebida, producida y comercializada a través de dispositivos electrónicos, cámara de video, fotográfica, ordenador, etc., donde se practican actos obscenos con la participación de menores de edad, inclusive discapacitados, es por ello que este delito totalmente indeseable conlleva una sanción drástica, que implica inclusive el pago de indemnizaciones, inhabilidad del empleo, el comiso de los bienes producto del delito, llegando inclusive a establecer una pena agravada contra los sujetos cualificados que incluye a los progenitores y más familiares que están en relación directa con las víctimas y que cometieren este delito.

[51] Régimen Penal ecuatoriano.- Código Penal del Ecuador.- Ediciones Legales.- Art. 528.7

4.9.- LA TIPIFICACIÓN Y PUNICIÓN DE LOS DELITOS INFORMÁTICOS EN EL DERECHO COMPARADO

En el contexto internacional, son pocos los países que cuentan con una legislación apropiada. Entre ellos, se destacan, Estados Unidos, Alemania, Austria, Gran Bretaña, Holanda, Francia, España, Argentina y Chile.

Dado lo anterior a continuación se mencionan algunos aspectos relacionados con la ley argentina y española, así como con los delitos informáticos que persigue.

4.9.1.- Legislación argentina

En Argentina en base a la Ley Nacional N° 26.3889, sancionada el 4 de junio de 2008, se reformó el Código Penal para comprender las modalidades delictivas vinculadas con la informática, a continuación realizo un enfoque de las normas que se relacionan con el delito informático:

La ley citada modifica el artículo 77 del Código Penal incorporando algunas definiciones para precisar el alcance de los vocablos incluidos en las normas, como

«documento» comprende toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión; **«firma» y «suscripción»** comprenden la firma digital, la creación de una firma digital o firmar digitalmente; **«instrumento privado» y «certificado»** comprenden el documento digital firmado digitalmente.

Se sustituye también el artículo 128 del Código Penal, por el siguiente:

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

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

Será reprimido con prisión de un (1) mes a tres (3) años el que facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico a menores de catorce (14) años"[52].

Claramente se distinguen de la norma transcrita, tres figuras delictivas orientadas a proteger la intimidad sexual de los menores de edad.

Como revisamos anteriormente este ilícito también se encuentra tipificado y sancionado con mayor rigurosidad en el Código Penal ecuatoriano, en el Título VIII, Capítulo III, "De los delitos de explotación sexual", Art. 528.7.

La inclusión de estos tipos penales es plenamente justificada ante la proliferación de casos de pornografía infantil que en los últimos tiempos viene teniendo lugar en el medio internacional y local y que han hecho del internet la vía principal para su difusión sin que las fronteras estatales signifiquen obstáculo alguno para tal accionar.

[52] Código Penal de la Nación Argentina.- http://www.codigopenalonline.com.ar

Relativo a la violación de secretos y de la privacidad, el artículo 153 contempla: "Será reprimido con prisión de quince (15) días a seis (6) meses el que abriere o accediere indebidamente a una comunicación electrónica, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, que no le esté dirigido; o se apoderare indebidamente de una comunicación electrónica, una carta, un pliego, un despacho u otro papel privado, aunque no esté cerrado; o indebidamente suprimiere o desviare de su destino una correspondencia o una comunicación electrónica que no le esté dirigida.

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

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

Si el hecho lo cometiere un funcionario público que abusare de sus funciones, sufrirá además, inhabilitación especial por el doble del tiempo de la condena.

(Artículo sustituido por art. 4° de la Ley N° 26.388, B.O. 25/6/2008)

Artículo 153 bis. - Será reprimido con prisión de quince (15) días a seis (6) meses, si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido.

La pena será de un (1) mes a un (1) año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros."[53].

La comunicación electrónica está asociada con los mensajes de datos, correos electrónicos, etc., que se envían y/o receptan por medio de un computador o en base a un sistema informático. Aquí tiene singular y relevante importancia la autorización del titular, pues sin ella ninguna persona puede acceder o desviar de su destino tales comunicaciones.

Referente al delito de indebida publicación de información, el artículo 155 del Código Penal

[53] Código Penal de la Nación Argentina.- http://www.codigopenalonline.com.ar/

argentino, dispone: "Será reprimido con multa de pesos un mil quinientos ($ 1.500) a pesos cien mil ($ 100.000), el que hallándose en posesión de una correspondencia, una comunicación electrónica, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, no destinados a la publicidad, los hiciere publicar indebidamente, si el hecho causare o pudiere causar perjuicios a terceros.
Está exento de responsabilidad penal el que hubiere obrado con el propósito inequívoco de proteger un interés público."[54].

El artículo 157 del Código Penal en mención, sanciona a los funcionarios públicos que revelen secretos de hechos, datos protegidos por la ley, secretos que pudieren causar alarma social o perjudicar a personas inocentes, con prisión de un mes a dos años e inhabilitación especial de uno a cuatro años.

Al tipificar tales conductas como delictivas, se ha pretendido en Argentina criminalizar las actuaciones de instituciones públicas que manejan y procesan datos personales, y que al igual como ocurre en nuestro país,

[54] Código Penal de la Nación Argentina.- http://www.codigopenalonline.com.ar/

sus empleados muchas veces han cometido actos delictivos, a sabiendas del perjuicio causado.

4.9.2.- Legislación española

El Código Penal español, respecto de la violación al derecho a la intimidad, imagen y domicilio de una persona, establece en el artículo 197 lo siguiente:

"1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales, intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o

telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.

3. El que por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo, acceda sin autorización a datos o programas informáticos contenidos en un sistema informático o en parte del mismo o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años.

4. Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores.

Será castigado con las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior.

5. Si los hechos descritos en los apartados 1 y 2 de este artículo se realizan por las personas encargadas o

responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros, se impondrá la pena de prisión de tres a cinco años, y si se difunden, ceden o revelan los datos reservados, se impondrá la pena en su mitad superior.

6. Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o un incapaz, se impondrán las penas previstas en su mitad superior"[55].

"Artículo 198.- La autoridad o funcionario público que, fuera de los casos permitidos por la ley sin mediar causa legal por delito, y prevaliéndose de su cargo, realizare cualquiera de las conductas descritas en el artículo anterior, será castigado con las penas respectivamente previstas en el mismo, en su mitad superior y, además, con la de inhabilitación absoluta por tiempo de seis a doce años"[56].

La legislación española determina toda una estructura jurídica para proteger el derecho a la privacidad

[55] Código Penal Español.- http://abogadospenal.fullblog.com.ar/codigo-penal-espanol---texto-integro-actualizado-2-121244071996.html

[56] Código Penal español.- http://abogadospenal.fullblog.com.ar/codigo-penal-espanol---texto-integro-actualizado-2-121244071996.html

personal, mientras que nuestro Código Penal lo tipifica como una mera contravención.

Refiriéndose a las estafas, el mismo Código en el artículo 248 establece:

"1. Cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno.

2. También se consideran reos de estafa:

a) Los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro.

b) Los que fabricaren, introdujeren, poseyeren o facilitaren programas informáticos específicamente destinados a la comisión de las estafas previstas en este artículo.

c) Los que utilizando tarjetas de crédito o débito, o cheques de viaje, o los datos obrantes en cualquiera de ellos, realicen operaciones de cualquier clase en perjuicio de su titular o de un tercero"[57].

[57] Código Penal español.- http://abogadospenal.fullblog.com.ar/codigo-penal-espanol---texto-integro-actualizado-2-121244071996.html

Las disposiciones transcritas tipifican y sancionan conductas que se adecuan a los elementos de tipo penal de la estafa. A pesar de que no esté titulada como informática, son claros sus elementos, al señalar la existencia de la manipulación informática, la cual produce un delito informático que como ya lo hemos estudiado constituye la estafa informática, esta es la denominada técnica de salami, que el literal "a" la prevé. Igualmente el literal "b", se lo relaciona con el delito informático conocido como técnica de salami, que son la introducción de programas informáticos con el fin mismo de estafar a los sujetos pasivos. Y el último literal, es el uso de un instrumento privado para hacerle un daño a su titular, el denominado skimming. Aquí, a la hora de sancionar a los culpables se implantan parámetros punibles, consistentes en fijar la respectiva pena de acuerdo al daño ocasionado, es decir al perjuicio económico, a las circunstancias y a los medios utilizados en la perpetración del delito. Esta normativa contempla que las estafas informáticas, se generan mediante un proceso lógico, sistematizado y consciente de la generación de grandes daños en la economía y patrimonio de las posibles víctimas.

En la sección tercera del Código Penal español, que se refiere a los delitos relativos al mercado y a los consumidores, encontramos el Artículo 278, que textualmente dice:

"1. El que, para descubrir un secreto de empresa se apoderare por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mismo, o empleare alguno de los medios o instrumentos señalados en el apartado 1 del art. 197, será castigado con la pena de prisión de dos a cuatro años y multa de doce a veinticuatro meses.

2. Se impondrá la pena de prisión de tres a cinco años y multa de doce a veinticuatro meses si se difundieren, revelaren o cedieren a terceros los secretos descubiertos.

3. Lo dispuesto en el presente artículo se entenderá sin perjuicio de las penas que pudieran corresponder por el apoderamiento o destrucción de los soportes informáticos"[58].

Esta sección es similar con lo previsto sobre la divulgación de informaciones reservadas o secretos en

[58] Código Penal español.- http://abogadospenal.fullblog.com.ar/codigo-penal-espanol---texto-integro-actualizado-2-1212440719 96.html

el Código Penal ecuatoriano, similitud que comprende además la respectiva sanción.

En el Código objeto del análisis comparativo en primer lugar, se ha puesto de manifiesto que este delito consiste en apoderarse de un documento informático y en segundo lugar, se impone una pena contra quienes difundan o revelen tales secretos. Muchas veces con la intención de apoderarse de un secreto de algún producto, se incurre en violentar las seguridades de un sistema para buscar y obtener la información reservada y así poder utilizarla a su beneficio o cederla a favor de terceros, produciendo un grave perjuicio en los autores de la misma, a este delito se lo conoce como acceso indebido a un sistema informático, y en el caso de que el autor no reciba retribución alguna por su autoría, se le conoce como piratería informática, y al difundirse tal producto en el mercado, el daño ocasionado es de mayor significancia aún para los consumidores, al no recibir un producto de calidad.

Continua el Código Penal español y en el artículo 286, prevé:

"1. Será castigado con las penas de prisión de seis meses a dos años y multa de seis a 24 meses el que, sin consentimiento del prestador de servicios y con fines comerciales, facilite el acceso inteligible a un servicio de radiodifusión sonora o televisiva, a servicios interactivos prestados a distancia por vía electrónica, o suministre el acceso condicional a los mismos, considerado como servicio independiente, mediante:

1° La fabricación, importación, distribución, puesta a disposición por vía electrónica, venta, alquiler, o posesión de cualquier equipo o programa informático, no autorizado en otro Estado miembro de la Unión Europea, diseñado o adaptado para hacer posible dicho acceso.

2° La instalación, mantenimiento o sustitución de los equipos o programas informáticos mencionados en el párrafo 1°.

2. Con idéntica pena será castigado quien, con ánimo de lucro, altere o duplique el número identificativo de equipos de telecomunicaciones, o comercialice equipos que hayan sufrido alteración fraudulenta.

3. A quien, sin ánimo de lucro, facilite a terceros el acceso descrito en el apartado 1, o por medio de una comunicación pública, comercial o no, suministre

información a una pluralidad de personas sobre el modo de conseguir el acceso no autorizado a un servicio o el uso de un dispositivo o programa, de los expresados en ese mismo apartado 1, incitando a lograrlos, se le impondrá la pena de multa en él prevista.

4. A quien utilice los equipos o programas que permitan el acceso no autorizado a servicios de acceso condicional o equipos de telecomunicación, se le impondrá la pena prevista en el art. 255 de este Código con independencia de la cuantía de la defraudación.

Las conductas descritas en este articulado, el Código Penal ecuatoriano no las tipifica, están dirigidas a resguardar los servicios de radio y televisión prestados a través de vía electrónica o informática, es decir que la norma lo ampara para dar un servicio óptimo y castigar a quienes lo intervienen o acceden para provocar un daño. Pero esta situación no se la lleva a cabo con la simple presencia del sujeto activo de la infracción, es menester una herramienta, equipo o programa informático que faculte un delito completo. Es por esto que en esta norma jurídica, a más de sancionar a quienes acceden a violentar las telecomunicaciones, se castiga además a los sujetos que fabrican y ponen en

comercialización estos aparatos. Los aspectos últimamente detallados son importantes, en ellos encontramos el origen de la infracción y por consiguiente hay que castigar a los responsables de la producción de tales materiales que son usados ilegalmente.

Al analizar el Código Penal español, en el título XVIII, de las falsedades, capítulo II. de las falsedades documentales, sección primera, De la falsificación de documentos públicos, oficiales y mercantiles y de los transmitidos por servicios de telecomunicación en cuanto a las falsificaciones, se encuentra que nuestro Código Penal, a diferencia del español, tipifica las conductas que se refieren a la falsificación electrónica o informática.

Nuestro Código Penal tiene un texto similar a lo previsto en los numerales del artículo 390 del Código Penal español, no obstante nuestros legisladores lo encaminaron al ámbito informático.

La disposición que transcribo a continuación, tomada del Código Penal español, no se refiere a nuestro tema de estudio, y sirve para fundamentar lo aseverado:

Artículo 390

1. Será castigado con las penas de prisión de tres a seis años, multa de seis a veinticuatro meses e inhabilitación especial por tiempo de dos a seis años, la autoridad o funcionario público que, en el ejercicio de sus funciones, cometa falsedad:

1°) Alterando un documento en alguno de sus elementos o requisitos de carácter esencial.

2°) Simulando un documento en todo o en parte, de manera que induzca a error sobre su autenticidad.

3°) Suponiendo en un acto la intervención de personas que no la han tenido, o atribuyendo a las que han intervenido en él declaraciones o manifestaciones diferentes de las que hubieran hecho.

4°) Faltando a la verdad en la narración de los hechos.

Se puede catalogar como rescatable lo que los legisladores adaptaron de este texto, al tipificar esta conducta. No obstante omitieron lo relativo a la pena.

La sección cuarta, referente a la falsificación de tarjetas de crédito y débito y cheques de viaje, del Código Penal español, en el artículo 39 dispone:

"1. El que altere, copie, reproduzca o de cualquier otro modo falsifique tarjetas de crédito o débito o cheques de viaje, será castigado con la pena de prisión de cuatro a ocho años. Se impondrá la pena en su mitad superior cuando los efectos falsificados afecten a una generalidad de personas o cuando los hechos se cometan en el marco de una organización criminal dedicada a estas actividades.

Cuando de acuerdo con lo establecido en el art. 31 bis una persona jurídica sea responsable de los anteriores delitos, se le impondrá la pena de multa de dos a cinco años.

2. La tenencia de tarjetas de crédito o débito o cheques de viaje falsificados destinados a la distribución o tráfico será castigada con la pena señalada a la falsificación.

3. El que sin haber intervenido en la falsificación usare, en perjuicio de otro y a sabiendas de la falsedad, tarjetas de crédito o débito o cheques de viaje falsificados será castigado con la pena de prisión de dos a cinco años"[59].

[59] Código Penal español.- http://abogadospenal.fullblog.com.ar/codigo-penal-espanol---texto-integro-actualizado-2-121244071996.html

Esta sección tiene trascendencia en el ámbito de la falsificación informática, es sabido que la alteración, copia y reproducción de una tarjeta de crédito o débito, se la hace a través de un sistema informático o con el uso de aparatos idóneos y propicios creados para tal particular. Si bien es cierto que no se lo menciona como lo señalamos, pero es fácil deducir y concluir que a este delito se lo conoce a manera de falsificación informática de instrumento privado.

En nuestro ordenamiento penal, no existe normativa alguna acerca de este tema, no obstante que es conocido que los ilícitos producidos durante los últimos años tienen índices alarmantes. El Código Penal español tipifica tales conductas como delitos. Las sanciones establecidas en el numeral uno, se enfocan a castigar individual y colectivamente, en general al grupo de individuos que forman una organización delictiva, siendo estos los sujetos que obtienen la tarjeta de crédito o débito de un titular y quienes con la ayuda de aparatos electrónicos configuran como tal la falsificación de ese instrumento. A más de las personas indicadas anteriormente, en el numeral tres se penaliza a los individuos que ya utilizan o ponen en

funcionamiento tales documentos falsos, sin tener participación directa en el cometimiento de la falsificación.

En muchos casos, surgen delincuentes informáticos que sin tener la intención de provocar un daño financiero en la economía de una persona, tal vez ingenuamente ponen en manifiesto su deseo de utilizar un documento falso, sin tener en cuenta las repercusiones que mediata o inmediatamente acarrean. Es así que con el ánimo de sacar un provecho, utilizan estas tarjetas para una compra por ejemplo, e incurren en delito. Esta situación tiene una diferente concepción, pero las legislaciones estudiadas y más la nuestra, hasta el momento no las han tipificado en sus normativas penales.

CAPÍTULO III. DISPOSICIONES GENERALES

Artículo 400.- La fabricación o tenencia de útiles, materiales, instrumentos, sustancias, máquinas, programas de ordenador o aparatos, específicamente destinados a la comisión de los delitos descritos en los Capítulos anteriores, se castigarán con la pena señalada en cada caso para los autores.

Artículo 536.- La autoridad, funcionario público o agente de éstos que, mediando causa por delito, interceptare las telecomunicaciones o utilizare artificios técnicos de escuchas, transmisión, grabación o reproducción del sonido, de la imagen o de cualquier otra señal de comunicación con violación de las garantías constitucionales o legales, incurrirá en la pena de inhabilitación especial para empleo o cargo público de dos a seis años.

Si divulgare o revelare la información obtenida, se impondrán las penas de inhabilitación especial, en su mitad superior y, además, la de multa de seis a dieciocho meses.

Dentro de las disposiciones generales, he tomado dos artículos se relacionan o refieren a los delitos informáticos, precisamente a los objetos o medios con los cuales se lleva a cabo un ilícito penal, el artículo 400, pone de manifiesto que la fabricación o tenencia de programas de ordenador para el cometimiento de cualquiera de los delitos señalados en el Código Penal español, es castigado con la respectiva pena a sus autores. En nuestro Código Penal, se debería advertir que todo ese proceso que abarca la fabricación

y uso de esos aparatos, y en este caso de esos programas que cuando se los introduce en un sistema, dañan el normal funcionamiento o van dirigidos a sacar un provecho económico.

En el artículo 536 del Código que he transcrito, lo denominaremos intervención o pinchado de las líneas de comunicación, delito informático que la doctrina lo menciona y que dicho cuerpo legal también lo contempla; se sanciona a la autoridad, funcionario público o agente de éstos, y a personas comunes y corrientes, anteriormente ya se los ha revestido de aplicación y ejecución en sus actos. Ahora se castiga a estos sujetos que dentro de sus actividades, llegan a transgredir las leyes, la misma Constitución y en concreto el libre funcionamiento de las telecomunicaciones. No sabemos las intenciones reales de sus posibles actos, pero sí las consecuencias que generarían dentro de una sociedad, o dentro de una persona en específico.

5.- MATERIALES Y METODOS

En el desarrollo del presente trabajo de investigación, apliqué el método científico que me permitió lograr un conocimiento en relación con el problema objeto de estudio y a la vez posibilitó el planteamiento de una solución alternativa al mismo, que sea confiable y con el nivel de certeza producto de la investigación.

Así también se aplicaron los métodos inductivo y deductivo, que permitieron partir de un conocimiento general, para ir a lo particular e identificar el grado de conocimiento que tienen nuestros operadores de justicia a cerca del tema.

Los datos obtenidos en el proceso de investigación fueron sometidos a los métodos analítico - sintético a través de los que se procedió a sistematizar la información teórica lograda para el análisis correspondiente.

La investigación fue de tipo documental y de campo; participativa, transversal.

Como técnicas de investigación se aplicaron las siguientes: la observación, que durante el proceso investigativo constituyó una técnica que posibilitó el acercamiento directo del investigador con el problema planteado, tomando contacto con los protagonistas del mismo; se elaboraron fichas bibliográficas, fichas mnemotécnicas, fichas de transcripción, para recolectar los elementos teórico doctrinarios que permitieron ilustrarnos respecto a la temática planteada y que constituyeron luego el fundamento de la sugerencia de las alternativas de solución; así también se elaboraron las fichas documentales correspondientes; se aplicaron cuarenta encuestas a abogados entre magistrados, jueces, agentes fiscales, agentes de la policía judicial y profesionales del derecho en libre ejercicio, en el distrito judicial de Loja.

Los datos así recopilados fueron ordenados sistemáticamente para el análisis pertinente y constituyeron como ya se ha dicho, el fundamento para la redacción del informe final y además para la alternativas de solución o recomendaciones que se plasma en este trabajo investigativo.

6.- RESULTADOS

6.1.- PRESENTACIÓN E INTERPRETACIÓN DE LOS RESULTADOS OBTENIDOS MEDIANTE LA APLICACIÓN DE ENCUESTAS

Concluida la aplicación de las encuestas, mismas que cumpliendo con lo establecido en el proyecto de investigación se dirigieron a cuarenta profesionales, entre magistrados, jueces, fiscales y abogados en libre ejercicio, se procedió a la tabulación de las respuestas y sus resultados se presentan de manera sistemática en cuadros y gráficos estadísticos, considerando las frecuencias con sus respectivos porcentajes, los cuales permiten visualizar de manera numérica la información. La interpretación de los resultados se realizó de manera cuantitativa y cualitativa.

PREGUNTA No. 1

1.- ¿Verdad que los delitos cometidos a través de medios informáticos son emergentes en nuestro país?

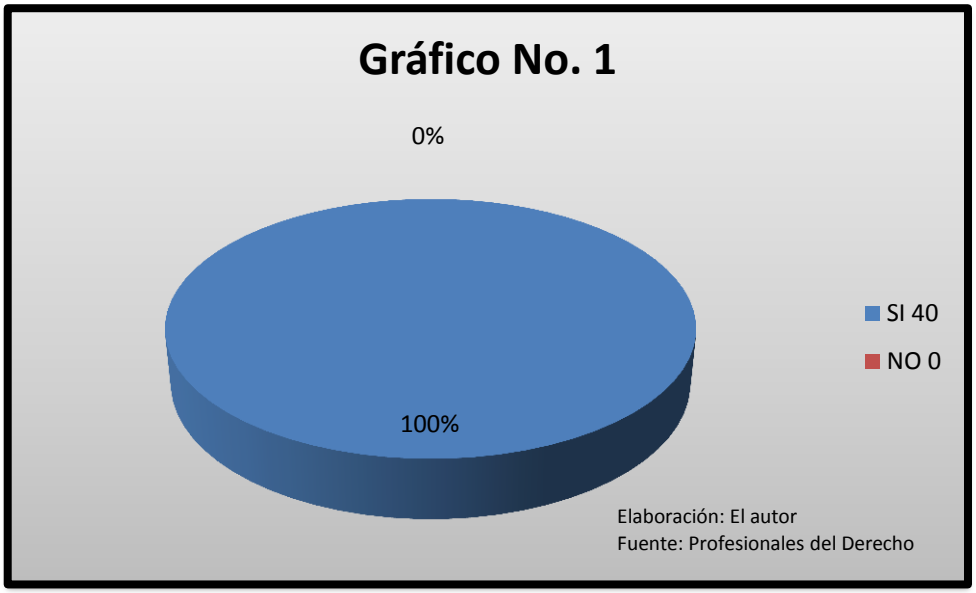
Si ( )

No ( )

CUADRO No. 1

ALTERNATIVA	FRECUENCIA	PORCENTAJE
SI	40	100%
NO	0	0%
TOTAL	**40**	**100%**

Elaboración: El autor
Fuente: Profesionales del Derecho



INTERPRETACION

A esta interrogante 40 personas que representan el 100% del universo encuestado, responden de manera afirmativa, señalando que los delitos que se comenten a través de medios electrónicos o informáticos en nuestro país, tienen el carácter de emergentes.

Los primeros tipos penales informáticos que se incluyeron en nuestra legislación fueron en el año 2002 con la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.

De lo que se tiene conocimiento el primer delito informático que se cometió en el Ecuador fue en el año 1996 y consistió en redondear los valores de las planillas de consumo telefónico emitidas por (en aquel entonces) EMETEL, y que nunca se supo a donde se dirigieron esos recursos, que por cada planilla era mínimo pero que en conjunto era una cantidad de dinero considerable.

PREGUNTA No. 2

2.- Está usted de acuerdo en que la tipificación de los delitos informáticos contiene algunos elementos constitutivos como:

Dolo ( )

Sujeto activo cualificado ( )

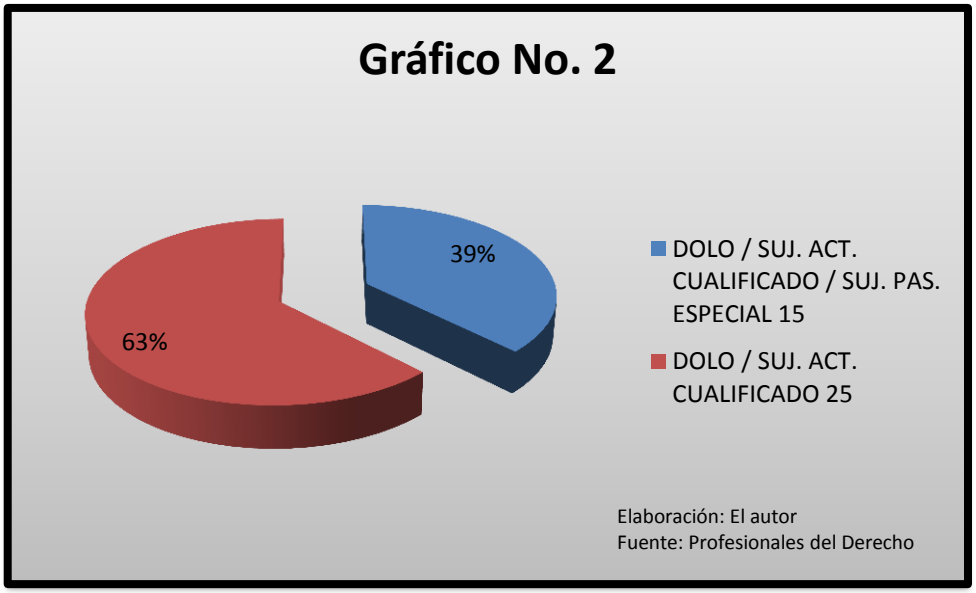
Sujeto pasivo especial ( )

Otros ( )

CUADRO No. 2

ALTERNATIVA	FRECUENCIA	PORCENTAJE
DOLO Y SUJETO ACTIVO CUALIFICADO	25	62,50%
DOLO SUJETO ACTIVO CUALIFICADO SUJETO PASIVO ESPECIAL	15	37,50%
OTROS	0	0%
TOTAL	40	100%

Elaboración: El autor
Fuente: Profesionales del Derecho



INTERPRETACIÓN

Veinticinco profesionales que representan el 62,50% del universo encuestado, señalan como principales elementos constitutivos de este tipo penal al dolo, el sujeto activo cualificado.

El resultado referido pone de manifiesto que algunos sectores de profesionales del Derecho, si bien conocen del delito informático, por lo emergente de la conducta aún no se tiene el suficiente dominio del tema en cuanto a los elementos que lo constituyen.

Quince encuestados que representan el 37,50% se pronuncian señalando tres de los elementos constitutivos del delito informático; constituye entonces una minoría con relación al universo investigado.

El dolo es una característica o el elemento esencial del delito informático. Por dolo se entiende como la actitud positiva de causar daño, la voluntad de cometer un delito, los delitos cometidos por dolo son más graves, no existe ningún delito informático culposo,

pues en todos existe el ánimo de causar daño a una persona natural o jurídica, de ahí que no se puede hablar de delitos informáticos culposos.

Los sujetos activos en esta clase de delitos poseen ciertas características que los diferencian del común de los delincuentes, esto es, las habilidades que poseen para el manejo de los sistemas informáticos.

El sujeto pasivo o víctima del delito, es el ente sobre el cual recae el acto delictivo y pueden ser individuos, instituciones financieras, instituciones militares, gobiernos, etc. que usan sistemas automatizados de información.

PREGUNTA No. 3

3.- ¿Los miembros de la Policía Judicial que intervienen en la investigación preprocesal y procesal penal, deberían tener suficiente conocimiento de los sistemas informáticos a fin de contribuir positivamente en el proceso?

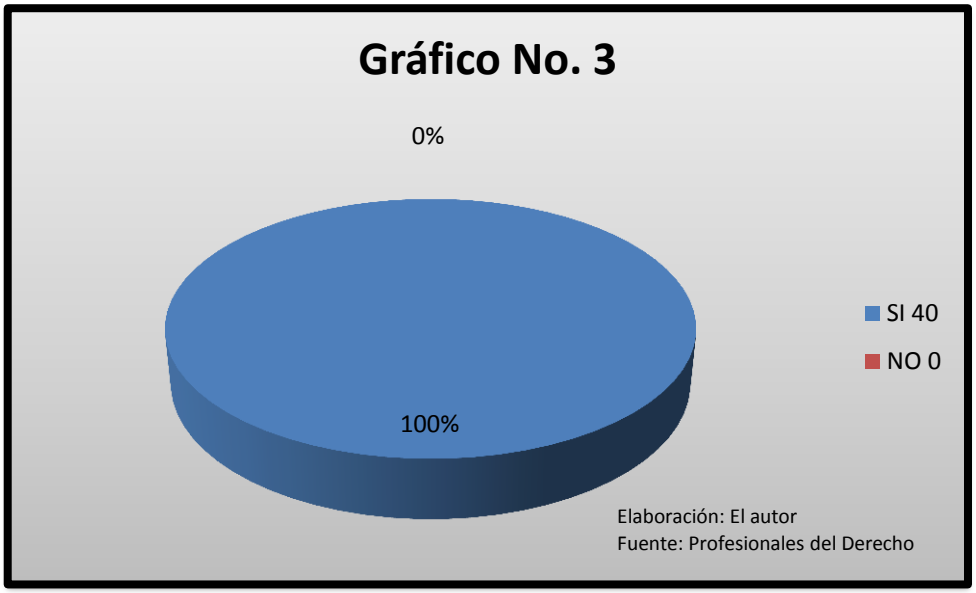
Si ( )

No ( )

CUADRO No. 3

ALTERNATIVA	FRECUENCIA	PORCENTAJE
SI	40	100%
NO	0	0%
TOTAL	**40**	**100%**

Elaboración: El autor
Fuente: Profesionales del Derecho



INTERPRETACIÓN

Cuarenta personas que corresponden al 100% del universo encuestado, manifiestan que los agentes investigadores de la Policía Judicial deberían tener amplio conocimiento respecto de sistemas informáticos a fin de

contribuir positivamente en el proceso de investigación de los delitos informáticos.

Considero que ante el importante aumento y la rápida evolución de los delitos informáticos, el elemento humano de la Policía Judicial debe capacitarse permanentemente y así contribuyan de mejor manera a lograr el objetivo de investigar y combatir los delitos relacionados con internet y las nuevas tecnologías.

PREGUNTA No. 4

4.- ¿Los funcionarios de la Fiscalía General deberían tener el conocimiento necesario respecto de los sistemas informáticos, a fin de aportar la prueba sobre la existencia del delito y la responsabilidad penal?

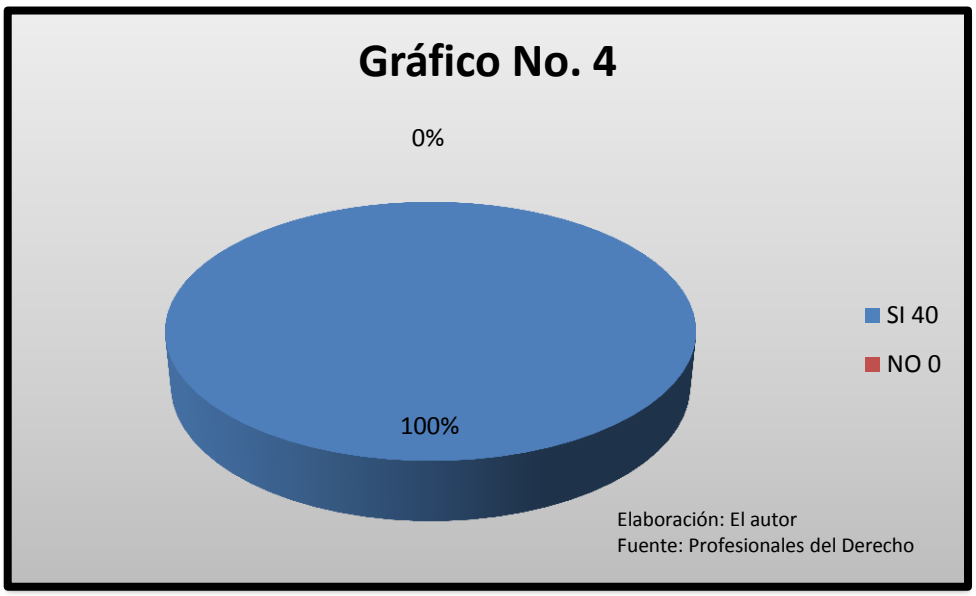
Si ( )

No ( )

CUADRO No. 4

ALTERNATIVA	FRECUENCIA	PORCENTAJE
SI	40	100%
NO	0	0%
TOTAL	**40**	**100%**

Elaboración: El autor
Fuente: Profesionales del Derecho



INTERPRETACIÓN

El 100% del universo encuestado, señala que los funcionarios de la Fiscalía General deben conocer sobre sistemas informáticos a fin de que esos conocimientos contribuyan para que el Fiscal aporte prueba en la investigación para determinar la existencia del delito y de la responsabilidad penal.

Los elementos de convicción en la investigación preprocesal y procesal penal y la prueba en la etapa de juicio es de singular importancia, pues es en base a ella que se resolverá la situación jurídica de un caso concreto que implica además de intereses económicos, garantías y derechos de las. Solo de esta manera se

confirmará o negará la existencia de la infracción y la responsabilidad de quienes han sido considerados como presuntos responsables, todo esto servirá para que los fiscales tengan el conocimiento necesario y resuelvan el asunto sometido a su decisión.

PREGUNTA No. 5

5.- ¿Los jueces con la finalidad de apreciar y valorar la prueba y resolver los casos relacionados con esta clase de delitos, deberían tener conocimiento sobre los sistemas informáticos?

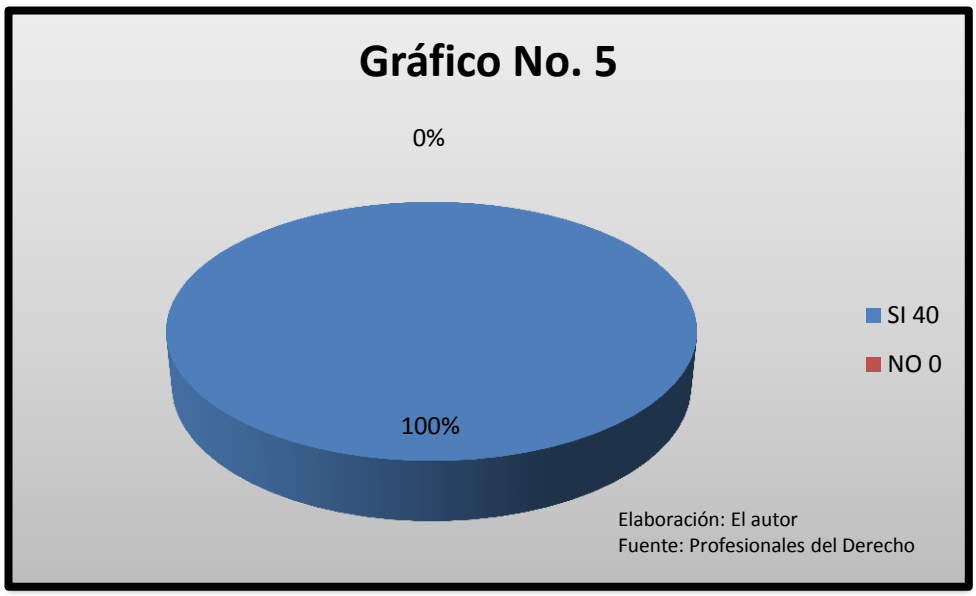
Si ( )

No ( )

CUADRO No. 5

ALTERNATIVA	FRECUENCIA	PORCENTAJE
SI	40	100%
NO	0	0%
TOTAL	**40**	**100%**

Elaboración: El autor
Fuente: Profesionales del Derecho



INTERPRETACIÓN

Los cuarenta profesionales que representan el 100% del universo encuestado, señalan al igual que la interrogante anterior que los jueces deben conocer sobre sistemas informáticos con la finalidad que puedan de mejor manera apreciar y valorar la prueba y en base a la misma resolver los casos puestos a su conocimiento.

Como ya se indicó la prueba dentro del procesal penal es importante. El juez en virtud del principio dispositivo, no aporta elementos probatorios sobre los hechos sometidos a su conocimiento, sino que verifica los elementos de prueba aportados por la fiscalía, la

acusación particular de haberla y el procesado. Averiguar los hechos y probarlos es carga de la fiscalía, apreciar los hechos probados es deber del juez, por lo tanto deben tener el conocimiento necesario para que resuelvan el asunto sometido a su resolución.

PREGUNTA No. 6

6.- ¿Considera usted importante que los peritos a designarse para que contribuyan en la investigación preprocesal y procesal penal de los delitos informáticos, acredite conocimientos teóricos – prácticos, experiencia y habilidades en la aplicación de los procedimientos de investigación?

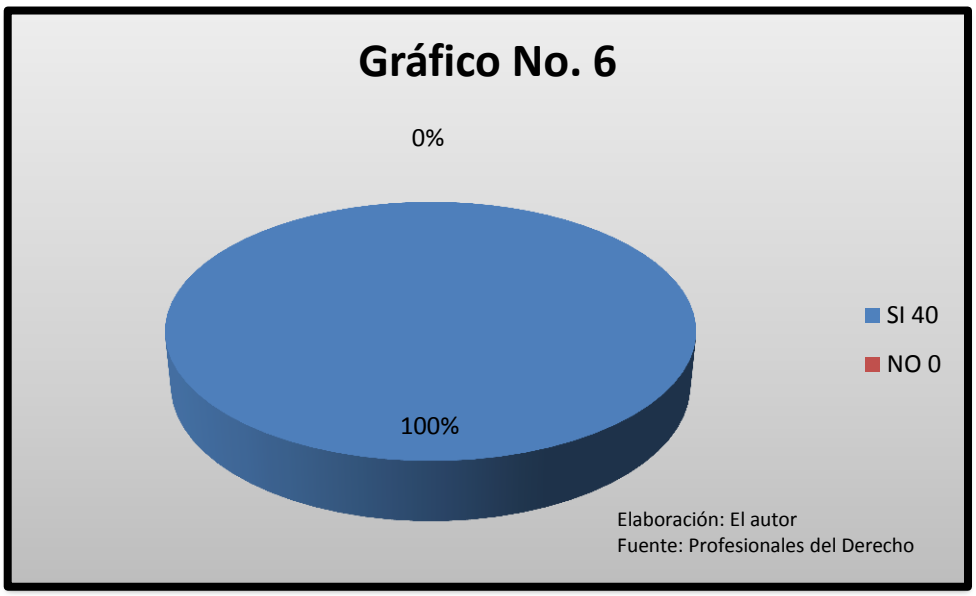
Si ( )

No ( )

CUADRO No. 6

ALTERNATIVA	FRECUENCIA	PORCENTAJE
SI	40	100%
NO	0	0%
TOTAL	**40**	**100%**

Elaboración: El autor
Fuente: Profesionales del Derecho



INTERPRETACIÓN

El 100% de los profesionales encuestados, señalan que las personas que intervienen como peritos en la investigación preprocesal y procesal penal de los delitos informáticos deben acreditar conocimientos teóricos – prácticos, experiencia y habilidades en la investigación de delitos informáticos.

PREGUNTA No. 7

7.- ¿En su calidad de servidor de la Fiscalía General del Estado o miembro de la Policía Judicial, qué procedimientos deben observarse al momento de aprehender o incautar equipos informáticos?

Asegurar el lugar ( )

Preservar los equipos informáticos ( )

Aprehender los equipos informáticos ( )

Buscar evidencias en el sistema informático ( )

Encender los equipos apagados ( )

Anotar los números de la dirección ip ( )

Fotografiar pantallas, cables, conexiones, etc. ( )

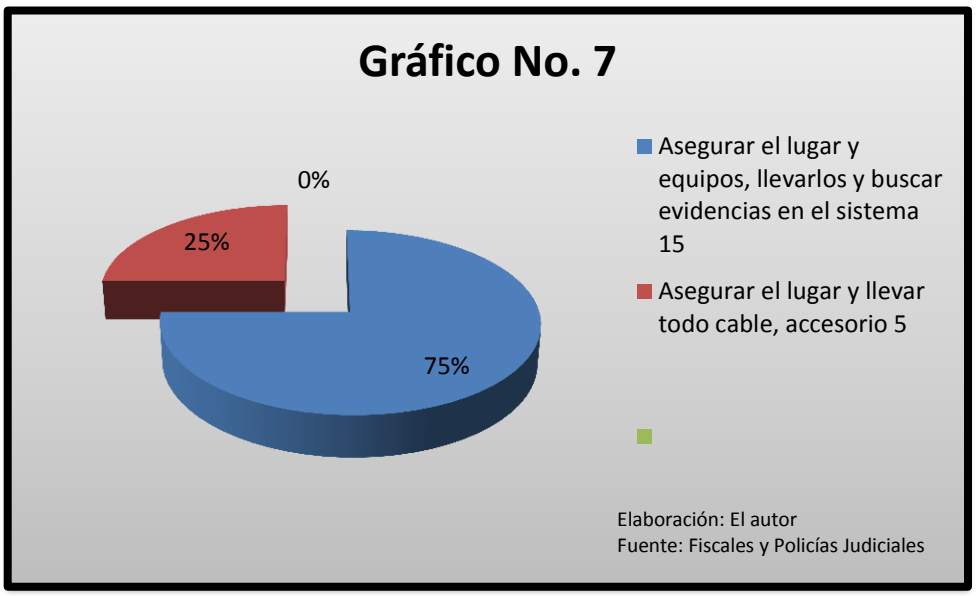
Llevar todo cable, accesorio, conexión ( )

Anotar la información de archivos activos ( )

CUADRO No. 7

ALTERNATIVA	FRECUENCIA	PORCENTAJE
ASEGURAR EL LUGAR, PRESERVAR LOS EQUIPOS, APREHENDER LOS EQUIPOS INFORMÁTICOS, BUSCAR EVIDENCIAS EN EL SISTEMA INFORMATICO	15	75%
ASEGURAR EL LUGAR Y LOS EQUIPOS LLEVAR TODO CABLE, ACCESORIO, CONEXIÓN	5	25%
TOTAL	**20**	**100%**

Elaboración: El autor
Fuente: Fiscales y Policías Judiciales



INTERPRETACION

Quince de los encuestados que representan el 75% del universo, señalan que al momento de incautar un equipo informático o electrónico, se debe asegurar el lugar, preservar los equipos, aprehender los equipos informáticos y buscar evidencias en el sistema informático.

Cinco encuestados que representan el 25% se pronuncian señalando que al momento de incautar un equipo informático, deben asegurar el lugar, preservar los equipos, aprehender todo cable, accesorio, conexión, etc.

Los resultados obtenidos mediante la aplicación de esta pregunta en particular, evidencian el desconocimiento que existe respecto a los procedimientos que deben emplearse para incautar un equipo informático, pues son los encuestados mismo quienes han manifestado, entre otras cosas que lo que hay que hacer es buscar evidencias en el sistema informático, o aprehender los equipos, pero tales acciones si no se las ejecuta de la manera adecuada, lejos de contribuir a la investigación de determinado hecho delictivo, van a terminar entorpeciendo el procedimiento pudiendo inclusive borrar o destruir datos de suma importancia para su esclarecimiento.

PREGUNTA No. 8

8.- Una vez que se hubieren aprehendido o incautado equipos informáticos, ¿de qué manera se deben resguardar las evidencias digitales?

Mantener la cadena de custodia ( )

Almacenar las baterías aparte ( )

Usar bolsas antiestática para almacenar ( )

Bloquear toda unidad de grabación ( )

Sellar cada entrada o puerto de información ( )

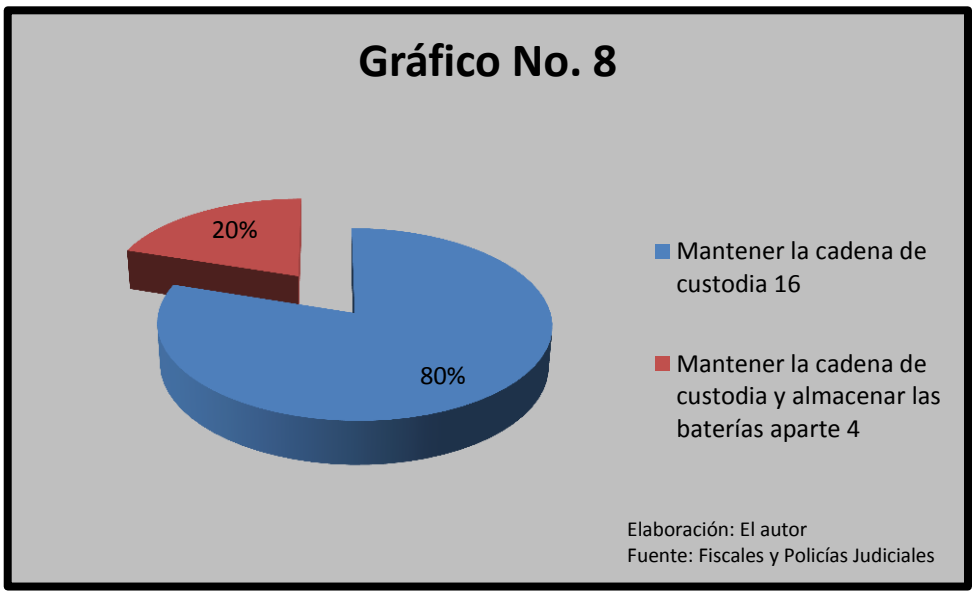
Sellar los tornillos del sistema ( )

Mantener los periféricos lejos de un campo magnético ( )

CUADRO No. 8

ALTERNATIVA	FRECUENCIA	PORCENTAJE
MANTENER LA CADENA DE CUSTODIA	16	80%
MANTENER LA CADENA DE CUSTODIA Y ALMACENAR LAS BATERIAS APARTE	4	20%
TOTAL	20	100%

Elaboración: El autor
Fuente: Fiscales y Policías Judiciales



INTERPRETACION

El 80% del universo encuestado, señala que para resguardar las evidencias digitales que pudieren existir en un equipo informático que fuere incautado, se debe mantener la cadena de custodia.

Cuatro encuestados que representan el 20% se pronuncian señalando que a más de mantener la cadena de custodia, para preservar las evidencias se debe almacenar las baterías en forma separada del equipo.

El pronunciamiento efectuado por los encuestados, determina algunos de los aspectos que deben tenerse en cuenta si se quiere preservar evidencias digitales que pudieran existir en un equipo informático que hubiese sido incautado a consecuencia del cometimiento de un ilícito; sin embargo se evidencia que existe desconocimiento, pues no se han señalado aspectos como usar bolsas antiestática para almacenar, lo cual es sumamente importante, porque mantiene alejado y protegido al periférico de cualquier agente de contaminación externo que pudiere estropear la información que se pueda encontrar en su interior; además no se indica tampoco que hay que bloquear toda unidad de grabación, pues es importante proteger estas

unidades empleando por ejemplo cintas de protección, para evitar daños en el equipo, por ejemplo un disco de arranque que formatee el computador; otro aspecto importante entre los otros que no se han mencionado, es el hecho de mantener los periféricos lejos de cualquier magnetismo, puesto que los dispositivos son muy sensibles a campos magnéticos estáticos de los imanes permanentes; algunos dispositivos pueden ser afectados temporalmente, pero otros pueden estropearse para siempre.

PREGUNTA No. 9

9.- ¿Se cuenta en las dependencias de la Policía Judicial, con los medios materiales apropiados para preservar las evidencias digitales que se hubieren encontrado en una escena del delito?

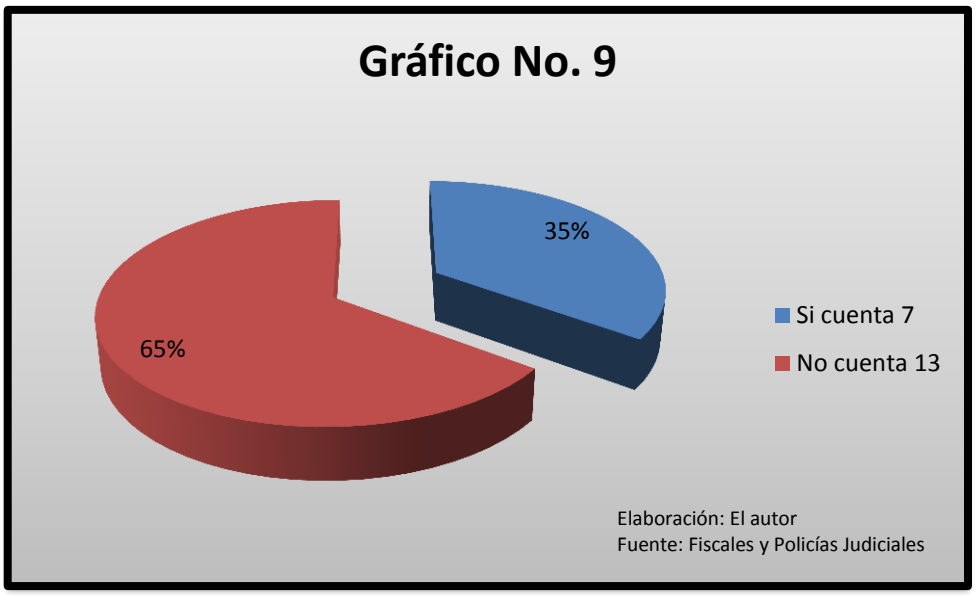
Si ( )

No ( )

CUADRO No. 9

ALTERNATIVA	FRECUENCIA	PORCENTAJE
SI	7	35%
NO	13	65%
TOTAL	**20**	**100%**

Elaboración: El autor
Fuente: Fiscales y Policías Judiciales



INTERPRETACIÓN

Siete encuestados, que representan el 35% del universo manifiestan que la Policía Judicial si cuenta con los medios materiales apropiados para preservar las evidencias digitales.

Trece encuestados, que representan el 65% del universo, manifiestan que la Policía Judicial no cuenta con los materiales en referencia.

De las respuestas obtenidas se demuestra que la Policía Judicial no cuenta con los materiales necesarios para preservar las evidencias digitales. Consecuentemente podíamos deducir que es una limitante para realizar técnicamente un trabajo de incautación de equipos informáticos, con la correspondiente preservación de evidencias.

6.2.- Estudio de casos

CASO No. 1

INDAGACION PREVIA 215-2011

Fiscalía Dr. Rodrigo Galván Calderón

Denunciante: NN

Delito contra la información protegida

Hechos:

Con fecha quince de julio de 2011, el Lic. NN informa sobre la vulneración al sistema informático de admisiones que ha existido desde terminales

informáticos de la Universidad Nacional de Loja, específicamente desde el Ciber café del Departamento de Bienestar Universitario. Adjuntan informes que determinan el número de cédula, direcciones IP, máquinas y lugares a los que se accedieron.

Se inicia la Indagación Previa y la Fiscalía dispone:

1.- Que se reciban las versiones del Dr. NN, Lic. NN, Ing. NN, Ing. NN, entre otros.

2.- Que se realice un análisis a los tres CPU a fin de determinar si se vulneró el sistema informático de admisiones de la UNL e identificar a las personas que lo efectuaron; para ello delega al Ing. NN.

3.- Que se oficie al Registro Civil a fin que confiera copia de la tarjeta índice de algunos estudiantes.

4.- Que se realice el reconocimiento del lugar de los hechos.

Durante la etapa preprocesal se han practicado las diligencias ordenadas por la Fiscalía, a excepción de la más importante que era el análisis o peritaje a las computadoras.

Posteriormente, la UNL justifica la propiedad de las computadoras y solicita su devolución, para lo cual se hace su reconocimiento, a cargo del Cbop. NN, que al igual que la entrega recepción inicial, nunca se observó ni tomó en cuenta ningún procedimiento para el manejo de evidencias informáticas.

La Fiscalía señala que no se ha podido determinar concretamente las personas que tuvieron acceso, ni tampoco la existencia de la infracción o la participación de ninguna persona, por lo cual con fecha 08 de mayo de 2013 solicita al Juez la desestimación de la denuncia presentada.

CASO No. 2

INDAGACION PREVIA 112-2013

Fiscalía Dr. Alonso Rodríguez Ordóñez

Denunciante: NN

Delito contra la información protegida

Hechos:

El dos de marzo de dos mil trece, a eso de las 22H00, mientras se encontraba navegando en internet, en su computadora portátil, apareció una página que decía: "Policía Nacional del Ecuador" que indicaba que se había violado políticas de seguridad y que se lo iba a sancionar conforme el Código Criminal del Ecuador, quedando bloqueada la computadora hasta la actualidad y la única forma de desbloquearla era de adquirir en rapipagos el producto "ukash", que tiene un valor de cien dólares.

Se inicia la Indagación Previa y la Fiscalía dispone:

1.- Que se reciba la versión del ofendido

2.- Que se practique el reconocimiento del lugar de los hechos

3.- Que el denunciante realice el reconocimiento de la denuncia

4.- Que se practique un peritaje al computador, para lo cual designa al Cbop. NN, a fin de que determine el autor del hecho, lugar y fecha en que se cometió y daños causados

5.- Que ingrese a la cadena de custodia el computador portátil

El ofendido ha rendido su versión y ha reconocido su denuncia.

El reconocimiento del lugar de los hechos no se ha podido realizar, por cuanto según se indica, el mismo no se ha podido determinar.

La cadena de custodia solo detalla las características del computador como marca, modelo, color, número de serie y cargador, además de mencionar nombres, apellidos, número de cédula de quien entrega y recibe, etc., pero al igual que en el caso anterior, nunca se observaron los procedimientos contenidos en el manual de manejo de evidencias de la Fiscalía General del Estado.

El perito designado Cbop. NN, mediante oficio contesta a la Fiscalía indicando que ese peritaje lo debe efectuar un perito en Informática y que la Policía Judicial de Loja no cuenta con ese personal calificado, por lo cual sugiere que se solicite tal pericia al Departamento de Criminalística de las ciudades de Quito o Guayaquil.

Luego del procedimiento correspondiente, el Director de Investigaciones de la Fiscalía General del Estado, hace conocer que el único perito acreditado en el Consejo de la Judicatura de Loja, es la Ing. NN, por lo cual la Fiscalía la designa para que realice la experticia en el presente caso.

El informe pericial emitido por la Ing. NN, en antecedentes se limita a mencionar aspectos como designación, posesión, etc., y no menciona nada sobre aspectos de seguridad.

Como ámbito de acción del peritaje se indica el de constatar la existencia del mensaje informático, capturar pantallas con datos, custodiar la información extraída; y, exponer la información mediante informe.

El objetivo del peritaje consistía en determinar el autor del mensaje, así como la dirección del lugar donde se remitió y fechas del mismo, además de los eventuales daños que pudieron ocasionarse al computador.

Ya en el procedimiento, la perito indica que por cuanto el mensaje (que por cierto nunca fue capturado) no le permite encender la computadora, decide arrancar en modo seguro con símbolo de sistema, para desde allí ingresar en un disco extraíble que contiene un programa que elimina el virus, para poder trabajar en el computador. Al efecto así lo realiza y ejecuta el programa denominado Polifix 2.0.7.

Según la información contenida en el informe pericial, se capturan pantallas de información del equipo, opciones de arranque en modo seguro; y, unidades de disco existentes, pero nunca se captura la pantalla que contenía el mensaje que causó el daño al computador.

La perito concluye que la computadora tenía "virus malicioso" que se pudo haber infectado por conexión de disco, cd, usb o navegar en internet.

Indica además que para localizar el software se utilizó Polifix 2.0.7, **"un programa que borra absolutamente todos los archivos de este tipo de virus, por este motivo no se puede determinar el autor del mensaje, ni su dirección, ni la fecha de envío del mismo".**

Se señala también que no se han detectado daños de ningún tipo en la computadora portátil y no se ha borrado ninguna información **"solo el virus malicioso".**

Una vez efectuado este procedimiento y cumplidas las formalidades del caso, la Fiscalía devuelve el computador a su propietario.

CASO No. 3

INDAGACION PREVIA 144-2011

Fiscalía Dra. Lorgia González Jaramillo

Denunciante: NN

Delito de hurto

Hechos:

De la cuenta del Banco de Guayaquil No. 1-800-533-11041-32871-51 el 3 de enero de 2011, ha sido retirados ciento cincuenta dólares que a su vez habían sido depositados en dicha cuenta el 27 de diciembre de 2010, por concepto de pensiones alimenticias.

Indica en su denuncia verbal que ese dinero nunca fue retirado por ella ni por ningún familiar suyo y que esta es la cuarta ocasión que lo realizan, las tres anteriores fueron en los meses de febrero, marzo y abril de 2010, con un perjuicio de setecientos cincuenta dólares.

Se inicia la Indagación Previa y la Fiscalía dispone:

1.- Que se reciba la versión de la ofendida

2.- Que se practique el reconocimiento del lugar de los hechos

3.- Que la denunciante realice el reconocimiento de la denuncia

4.- Que se practiquen las demás diligencias tendientes al esclarecimiento de la denuncia

El policía delegado para la práctica de las diligencias, mediante oficio informa, que no se ha podido realizar las diligencias dispuestas por cuanto no ha comparecido la denunciante.

La Fiscalía oficia al Banco de Guayaquil, a fin de que certifique sobre el movimiento de la cuenta bancaria de la denunciante, el cual nunca obtuvo respuesta.

Con estos antecedentes, la Dra. Fiscal con fecha 11 de abril del 2012 informa que se han dispuesto varias diligencias, pero no se ha logrado obtener elementos de convicción que permitan justificar la existencia de la infracción o imputar responsabilidad a alguna persona, por lo que solicita el archivo definitivo de la denuncia.

6.3.- Datos estadísticos sobre delitos informáticos

Fraude informático se multiplica en tres años es el titular del Diario El Telégrafo, que se publicara el 17 de septiembre de 2012, en el cual se menciona que desde el 2009 el aumento de denuncias referente a delitos informáticos es dramático, en ese año (2009) se reportaron solamente 168 casos, mientras que en lo que va del 2012 llegan a 1.564.

De acuerdo a la misma fuente, en julio de 2011 la presidenta del Consejo de Participación Ciudadana y Control Social (Cpccs), Marcela Miranda, denunció el desvío de 20 mil dólares de las cuentas bancarias de 47 funcionarios de esa entidad. Los afectados posteriormente señalaron que las cuentas de los

funcionarios estaban en diez bancos distintos, entre ellos, Guayaquil, Pacífico, Pichincha, Amazonas, Machala y Produbanco, cuyos montos retirados fueron entre los dos mil y cincuenta mil dólares.

Posterior a esta denuncia, según el Diario El Telégrafo, la Fiscalía recibió otras 15 denuncias por un delito similar, por parte de empleados de la Secretaría Técnica de Capacitación y Formación Profesional y de la Contraloría General, cuyo perjuicio ascendía a los ocho mil dólares.

Agrega además: "Desde entonces, (2009) las autoridades han registrado un incremento de denuncias hasta situarse en 4.287 casos. Esa cifra contempla los robos denunciados hasta junio del presente año (2012), pero existiría un subregistro de aquellas personas que no reportaron la pérdida"[60].

Las empresas: GMS y Kaspersky, presentaron el estudio Delitos informáticos en el Ecuador ¿Por qué los criminales te quieren tanto?, dictada por el especialista en seguridad informática Dmitry Bestuzhev. Sobre el mismo se manifiesta:

[60] http://www.telegrafo.com.ec/noticias/judicial/item/fraude-informatico-se-multiplica-en-tres-anos.html

"El estudio presentado por GMS y Kaspersky incluyó datos sobre el incremento de los ataques informáticos en el país en los últimos años, las causas principales de los ataques a entidades bancarias, las aplicaciones más vulnerables en las computadoras de los ecuatorianos y se demostró de manera gráfica las múltiples formas en que los hackers hacen uso de estos virus.

El estudio demuestra que entre el 2009 y 2010 el Ecuador tuvo un incremento del 360% de crimen cibernético. Dmitry Bestuzhev, Senior Regional Researcher de América Latina de Kaspersky Lab, indica que "el 94% de todos los programas de código malicioso hospedados en los servidores Web del Ecuador se encuentran en la provincia del Pichincha. Además está previsto para el presente año el delito informático incrementará en un porcentaje incluso mayor al 100%. El Ecuador cuenta con el 61% de ataques cibernéticos son en Pichincha y las provincias que reflejan menor grado de violaciones de seguridad informática son Guayas y Azuay con el 20% y 7% respectivamente"[61].

[61] http://www.gms.com.ec/index.php?option=com_content&view=article&id=91&Itemid=153

7.- DISCUSION

7.1.- Verificación de objetivos

Al plantear el desarrollo del presente trabajo de investigación, los objetivos propuestos, para ser verificados dentro del trabajo investigativo son los que a continuación se detallan:

Primer objetivo general

- Medir el grado de conocimiento de los operadores de justicia, referente a la tipicidad de los delitos informáticos y la informática aplicada a la investigación de los mismos.

Verificación del primer objetivo general.- El objetivo general planteado al inicio del presente trabajo de investigación, se verifica en forma total y satisfactoria para el presente estudio, especialmente con el trabajo de campo realizado, con la aplicación de las encuestas, el estudio de casos y con el correspondiente sustento bibliográfico, doctrinario que me ha posibilitado desarrollar un estudio analítico y

crítico, que se lo ha determinado en el contenido del trabajo realizado en nuestra legislación penal, en lo relacionado a los delitos informáticos.

Segundo objetivo general

- Fundamentar la necesidad de capacitar en el orden técnico en el conocimiento de la informática aplicada a la investigación pre procesal y procesal penal en los delitos informáticos.

Verificación del segundo objetivo general.- El objetivo general planteado al inicio del presente trabajo de investigación, se verifica. Se establece la necesidad de capacitar en el orden técnico sobre el conocimiento de la informática aplicada a la investigación preprocesal y procesal penal.

Objetivos específicos

- Identificar las deficiencias en el orden técnico jurídico de la formación de los operadores de justicia sobre la investigación de delitos informáticos.

Se ha evidenciado que hay falencias en el conocimiento y manejo técnico de medios informáticos en la investigación de delitos en dicha materia en los operadores de justicia en general.

- Demostrar la existencia de casos de impunidad que se han presentado en la práctica judicial ante conductas típicas atribuibles a actos cometidos a través de medios informáticos.

A través del estudio de casos realizado, se ha puesto de manifiesto el estado de impunidad en el que han quedado las conductas delictivas que han sido denunciadas y en las cuales se ha empleado medios informáticos para su cometimiento.

- Caracterizar las conductas emergentes que pueden constituir manifestaciones delictivas a través de la informática.

Siendo el delito informático una conducta emergente, tiene diversas manifestaciones que se identifican por ser dirigidas de manera directa contra el patrimonio de las personas sean estas naturales o jurídicas. Es

eminentemente doloso pues hay el ánimo manifiesto de causar daño; el delincuente informático tiene conocimiento amplio y suficiente desde el punto vista técnico de los sistemas informáticos lo que hace que se lo pueda catalogar como un sujeto activo cualificado; en cuanto a la parte ofendida también es un sujeto pasivo especial si se toma en cuenta que el ataque está dirigido al patrimonio de las personas, condición que no es común.

- Realizar un estudio comparativo sobre la tipificación y punición de delitos informáticos en el Derecho comparado

En el decurso del presente trabajo, este objetivo se ha cumplido, pudiendo verificar que la legislación española, la argentina, tipifican y sancionan conductas relativas a delitos informáticos en tanto que la nuestra es insuficiente ante estas nuevas manifestaciones delictivas.

- Presentar los indicadores estadísticos referentes a éstos actos delictivos.

Objetivo que de igual manera que los anteriores ha sido cumplido al presentar datos que demuestran el incremento inusitado de esta clase de delitos en nuestro país.

7.2.- Contrastación de hipótesis

A efecto de orientar el proceso de investigación, se planteó la hipótesis siguiente:

"La deficiente capacitación de los operadores de justicia y miembros de policía judicial en conocimientos técnicos relativos a la informática, es uno de los factores para que se produzca un estado de impunidad".

La hipótesis planteada en el proyecto de investigación, se ha contrastado positivamente a través del presente estudio, pues como se ha manifestado, los operadores de justicia y miembros de la Policía Judicial no están suficientemente capacitados en el conocimiento de sistemas informáticos a los que pueden recurrir los sujetos activos en delitos que se cometen por estos

medios lo que ha determinado ciertos niveles de impunidad en esta materia.

8.- CONCLUSIONES

1. La Informática tiene gran significancia y amplitud en la actualidad, puesto que abarca varios campos de las actividades que el ser humano realiza constantemente, sea en el ámbito educativo, profesional, laboral, financiero, administrativo.

2. El tema de la delincuencia informática, no ha tenido la suficiente difusión en la ciudadanía, razón por lo cual la mayor parte de la población no tiene conocimiento de su incidencia en la actualidad.

3. La insuficiente cultura informática en nuestra sociedad, es un elemento crítico en el impacto de los delitos informáticos, cada día se requieren mayores conocimientos en tecnologías de la información, que permitan manejar estas situaciones.

4. Se producen en nuestro país un sinnúmero de delitos informáticos y la mayoría de tales delitos, son difíciles de investigar por cuanto,

las huellas de los mismos son borradas con cierta facilidad, evadiendo las investigaciones y controles de las autoridades.

5. La incidencia creciente de los delitos informáticos en nuestro país y la necesidad de indagar y resolver los mismos, establece la importancia de contar con profesionales plenamente capacitados en este ámbito que den respuesta a la necesidad de la sociedad de contar con una excelente administración de justicia.

6. Si bien se ha tipificado y sancionado conductas que se adecúan a ilícitos informáticos, seguimos siendo vulnerables ante este tipo de delitos. Más aún la carencia de control, hace de la Informática y la Telemática, un lugar sin fronteras, en el que la gestión de los gobiernos del mundo, no lo pueden regir.

7. Un factor concurrente para la impunidad ante las conductas delictivas que se adecúan a los medios informáticos y telemáticos es sin lugar a duda la carencia de personal especializado en los órganos

jurisdiccionales y de investigación preprocesal y procesal penal.

9.- RECOMENDACIONES

En el Ecuador ya se ha manifestado la importancia de una investigación y sanción de los delitos informáticos, por lo que es preciso mejorar los mecanismos de investigación, empleando inclusive la tecnología apropiada por parte los involucrados en la Administración de Justicia. Por lo que se recomienda lo siguiente:

1. Que los órganos de administración de Justicia se los mantenga dotados a la vanguardia en tecnologías, técnicas y procedimientos informáticos.

2. Las Universidades e Instituciones Tecnológicas Superiores tanto en carreras como Derecho o Sistemas, Escuela de Fiscales, Escuela de Formación de Policías, deben incluir en su malla curricular el tema de los delitos informáticos y las formas de prevención.

3. Mantener informada a la comunidad, a través de los medios de comunicación y de información sobre los

distintos tipos de delitos informáticos que existen, su modo de operación y mecanismos de control.

4. Que los operadores de justicia durante la investigación preprocesal y procesal penal tratándose de delitos informáticos se rijan de acuerdo a las recomendaciones que en el presente trabajo investigativo se formulan, con lo cual espero generar un aporte significativo a la administración de justicia de nuestro país.

5. Las personas, instituciones u organizaciones que se vieran afectadas por la presencia de delitos informáticos, no debe impedir o dejar de lado los beneficios de todo lo que proveen las tecnologías de información, más bien por el contrario dicha situación debe tomarse como un reto, de manera que se realicen esfuerzos encaminados a robustecer los aspectos de seguridad, controles, integridad de la información, etc., en los sistemas informáticos.

Como recomendaciones generales a fin de evitar un índice mayor de estos ilícitos, propongo las siguientes:

- ✓ Únicamente se debe proporcionar datos personales, claves y contraseñas vía internet, si se está absolutamente seguro de la procedencia de la página web que se está empleando.
- ✓ Hay que cambiar constantemente las claves y contraseñas para el acceso a un computador personal, cuenta bancaria, correo electrónico, etc.
- ✓ No se debe usar como contraseñas fechas de nacimiento o la edad, o utilizarlas combinadas con otros caracteres.
- ✓ Para evitar la falsificación de tarjetas de crédito/débito, hay que exigir la exhibición de las máquinas rastrilladoras al momento de realizar el pago.
- ✓ Verificar constantemente los saldos de la cuenta y tarjeta.
- ✓ En lo posible no realizar transacciones bancarias vía internet desde computadoras públicas o de alquiler.

- ✓ Al momento de retirar dinero de un cajero automático, no recibir la ayuda de personas desconocidas y verificar que no se encuentre instalado ningún dispositivo extraño, de presentarse esta situación, debe retirarse de inmediato del lugar.
- ✓ No se deje engañar con los supuestos premios o regalos que en la actualidad se ofrecen vía correo electrónico o mensajes de datos y abundan en la red.
- ✓ Denuncie en forma inmediata ante las autoridades si conoce o sospecha del cometimiento de estas infracciones.
- ✓ Verifique los dispositivos conectados a un ordenador de uso público o de alquiler, si encuentra algo fuera de lo común, no usarlo.

10.- BIBLIOGRAFÍA

1. ACURIO DEL PINO Santiago Dr.- Ruptura 2001. Delitos Informáticos. F&R Gráficas. Quito. 2001.
2. ACURIO DEL PINO Santiago Dr.- Introducción a la informática Forense.
3. BEEKMAN George.- Introducción a la Informática.- Sexta Edición.- Pearson Educación S.A.- Madrid.- 2005.
4. CABANELLAS Guillermo.- Diccionario Jurídico Elemental.
5. CARRARA Francisco.- Programa de Derecho Criminal, parte general, volumen I, Editorial Temis, Bogotá.
6. EDICIONES LEGALES.- Régimen Penal ecuatoriano.- Código Penal del Ecuador.
7. EDICIONES LEGALES.- Régimen Penal ecuatoriano.- Código de Procedimiento Penal del Ecuador.
8. EDICIONES LEGALES.- Constitución de la República del Ecuador.
9. FISCALÍA GENERAL DEL ESTADO.- Manual de Manejo de Evidencias Digitales.
10. GUIBOURG, Ricard; Aliende, Jorge; Campanella, Elena A. Manual de Informática Jurídica. Astrea. Buenos Aires, Argentina. 1996.

11. http://es.wikipedia.org/wiki/Derecho_de_autor .- 02/10/2012

12. http://www.codigopenalonline.com.ar Código Penal de la Nación Argentina.

13. http://abogadospenal.fullblog.com.ar/codigo-penal-espanol---texto-integro-actualizado-2-121244071996.html Código Penal Español.

14. http://www.telegrafo.com.ec

15. http://www.gms.com.ec/

16. HUILCAPI Arturo.- El Delito Informático.- Pagina Judicial de Diario La Hora.

17. JIJENA LEIVA, Renato Javier. Comercio Electrónico. Editorial Andrés Bello. Santiago de Chile, Chile. 2002.

18. LEVENE, Ricardo (hijo) & CHIARAVALLOTI, Alicia. DELITOS INFORMATICOS.

19. MÁRQUEZ ESCOBAR, Carlos Pablo. El Delito Informático conforme con el nuevo Código Penal: la Información y la Comunicación en la Esfera Penal. Leyer. Bogotá, Colombia. 2002.

20. PÉREZ LUÑO, Antonio – Enrique. MANUAL DE INFORMATICA Y DERECHO, Ariel S.A, (1996).

21. REVISTA JUDICIAL derechoecuador.com.- El Delito.- 24 noviembre de 2005.

22. SALINAS SICCHA, Ramiro. DERECHO PENAL PARTE ESPECIAL. Segunda Edición. Editora Jurídica Grijley, mayo de 2007.

23. TÉLLEZ VALDÉZ, Julio. Derecho Informático. McGraw- Hill. Tercera Edición. México, México. 2003.

24. TIEDEMANN, klaus. CRIMINALIDAD MEDIANTE COMPUTADORAS.

25. VIEGA RODRÍGUEZ, María José. Delitos Informáticos, N° 009.

ANEXOS

FORMULARIO DE ENCUESTA

UNIVERSIDAD NACIONAL DE LOJA

AREA JURIDICA, SOCIAL Y ADMINISTRATIVA

NIVEL DE POSTGRADO

MAESTRÍA EN CIENCIAS PENALES

Señores (Jueces, Fiscales, Policías, Abogados) me encuentro desarrollando mi tesis de maestría intitulada: "Los operadores de justicia frente a los delitos informáticos" y requiero sus ilustrados criterios a efecto de tener mejores elementos de juicio para fundamentar mi trabajo investigativo, por este motivo en forma comedida le solicito se sirva dar contestación a las siguientes interrogantes:

PREGUNTA No. 1

1.- ¿Verdad que los delitos cometidos a través de medios informáticos son emergentes en nuestro país?

Si ( )

No ( )

PREGUNTA No. 2

2.- Está usted de acuerdo en que la tipificación de los delitos informáticos contiene algunos elementos constitutivos como:

Dolo ( )

Sujeto activo cualificado ( )

Sujeto pasivo especial ( )

Otros ( )

Indique:

PREGUNTA No. 3

3.- ¿Los miembros de la Policía Judicial que intervienen en la investigación preprocesal y procesal penal, deberían tener suficiente conocimiento de los sistemas informáticos a fin de contribuir positivamente en el proceso?

Si ( )

No ( )

PREGUNTA No. 4

4.- ¿Los funcionarios de la Fiscalía General deberían tener el conocimiento necesario respecto de los sistemas informáticos, a fin de aportar la prueba sobre la existencia del delito y la responsabilidad penal?

Si ( )

No ( )

PREGUNTA No. 5

5.- ¿Los jueces con la finalidad de apreciar y valorar la prueba y resolver los casos relacionados con esta clase de delitos, deberían tener conocimiento sobre los sistemas informáticos?

Si ( )

No ( )

PREGUNTA No. 6

6.- ¿Considera usted importante que los peritos a designarse para que contribuyan en la investigación preprocesal y procesal penal de los delitos informáticos, acredite conocimientos teóricos – prácticos, experiencia y habilidades en la aplicación de los procedimientos de investigación?

Si ( )

No ( )

PREGUNTA No. 7 (Exclusiva para Fiscales y Policías Judiciales)

7.- ¿En su calidad de servidor de la Fiscalía General del Estado o miembro de la Policía Judicial, qué procedimientos deben observarse al momento de aprehender o incautar equipos informáticos?

Asegurar el lugar ( )

Preservar los equipos ( )

Aprehender los equipos informáticos ( )

Buscar evidencias en el sistema informático ( )

Encender los equipos apagados ( )

Anotar los números de la dirección ip ( )

Fotografiar pantallas, cables, conexiones, etc. ( )

Llevar todo cable, accesorio, conexión ( )

Anotar la información de archivos activos ( )

PREGUNTA No. 8 (Exclusiva para Fiscales y Policías Judiciales)

8.- Una vez que se hubieren aprehendido o incautado equipos informáticos, ¿de qué manera se deben resguardar las evidencias digitales?

Mantener la cadena de custodia ( )

Almacenar las baterías aparte ( )

Usar bolsas antiestática para almacenar ( )

Bloquear toda unidad de grabación ( )

Selle cada entrada o puerto de información ( )

Sellar los tornillos del sistema ( )

Mantener los periféricos lejos de un campo magnético ( )

PREGUNTA No. 9 (Exclusiva para Fiscales y Policías Judiciales)

9.- ¿Se cuenta en las dependencias de la Policía Judicial, con los medios materiales apropiados para preservar las evidencias digitales que se hubieren encontrado en una escena del delito?

Si ( )

No ( )

Gracias

INDICE