UNIVERSIDAD NACIONAL DE LOJA

UNIDAD DE EDUCACIÓN A DISTANCIA
CARRERA DE DERECHO

TÍTULO

"LOS DELITOS INFORMÁTICOS EN EL SISTEMA FINANCIERO NACIONAL"

TESIS PREVIA A LA OBTENCIÓN DEL TÍTULO DE ABOGADA

AUTORA: Tamy Ghislaine Izaguirre García

DIRECTOR DE TESIS: Dr. Augusto Astudillo Ontaneda, Mg. Sc.

Loja – Ecuador

2017

CERTIFICACIÓN

Dr. Augusto Astudillo Ontaneda, Mg. Sc., DOCENTE DE LA CARRERA DE DERECHO, DE LA UNIDAD DE EDUCACIÓN A DISTANCIA DE LA UNIVERSIDAD NACIONAL DE LOJA.

CERTIFICA:

Haber revisado prolijamente el trabajo de tesis intitulado: "**LOS DELITOS INFORMÁTICOS EN EL SISTEMA FINANCIERO NACIONAL",** realizado por la estudiante Tamy Ghislaine Izaguirre García y autorizo su presentación para la defensa y sustentación, por cumplir los lineamientos metodológicos y sujetarse al Reglamento para la aprobación de tesis en la **UNIVERSIDAD NACIONAL DE LOJA.**

Loja, septiembre de 2016.

Dr. Augusto Astudillo Ontaneda, Mg. Sc.

DIRECTOR DE TESIS

AUTORIA

Yo, **Tamy Ghislaine Izaguirre García,** declaro ser la autora 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 Repositorio Institucional-Biblioteca Virtual.

Autora: Tamy Ghislaine Izaguirre García

Firma: Tamy G. Izaguirre G.....

Cédula: 1307770097

Fecha: Loja, 21 de abril de 2017

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

Yo, Tamy Ghislaine Izaguirre García, declaro ser autora de la tesis titulada: **"LOS DELITOS INFORMÁTICOS EN EL SISTEMA FINANCIERO NACIONAL"**, como requisito para optar al título de Abogada; 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 su visibilidad de su contenido de la siguiente manera en el Repositorio Digital Institucional.

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

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 21 días del mes de Abril del dos mil diecisiete, firma la autora.

Firma: Tamy G. Izaguirre G.
Autora: Tamy Ghislaine Izaguirre García
Cedula: 1307770097
Dirección: Portoviejo, Av. Reales Tamarindos y Tennis Club
Correo Electrónico: tamy_ghis_5@hotmail.com
Teléfono: 052636711 Celular: 0993056752

DATOS COMPLEMENTARIOS:

Director de Tesis: Dr. Augusto Astudillo Ontaneda, Mg. Sc.

Tribunal de Grado:

Dr. Felipe Neptalí Solano Gutiérrez, Mg. Sc.	PRESIDENTE
Dr. Marco Vinicio Ortega Cevallos, Mg. Sc.	VOCAL
Dr. Marcelo Armando Costa Cevallos, Mg. Sc	VOCAL

AGRADECIMIENTO

Dejo, por este medio constancia de mi imperecedero agradecimiento a la Universidad Nacional de Loja, en la modalidad de estudios a Distancia y su Carrera de Derecho.

En especial al doctor Augusto Astudillo Ontaneda, ilustre catedrático de la Carrera de Derecho.

A cada una de las personas que han aportado con sus conocimientos, para la culminación de mi tesis.

Tamy Ghislaine Izaguirre García

DEDICATORIA

Al **CREADOR DEL UNIVERSO Y LA VIDA**, a quien siempre doy gracias por cada día que me brinda la oportunidad para disfrutar de su hermosa creación; a la memoria de mi padre jurisconsulto a carta cabal, a mi madre y hermosa familia que amo.

Tamy Ghislaine Izaguirre García

1. TÍTULO

“LOS DELITOS INFORMÁTICOS EN EL SISTEMA FINANCIERO NACIONAL”

2. RESUMEN

El presente trabajo de investigación tuvo como objetivo general, realizar un análisis de los delitos informáticos en el Sistema Financiero Nacional, investigación que se justifica debido al incremento de estos delitos en Ecuador y ante la necesidad de abordar de una forma profunda y objetiva en este tema para establecer las falencias existentes en la Legislación Ecuatoriana en cuanto a la pena de los delitos informáticos con respecto a la Seguridad Informática, la defensa y preservación integral de los sistemas informáticos en contra de los cyber-delincuentes. Durante el proceso de investigación se utilizó los métodos inductivo, deductivo, analítico-sintético, comparativo y dialéctico, los que a través de técnicas como la encuesta y la entrevista permitieron obtener la información requerida para llegar al alcance de los objetivos, la verificación y la contrastacion de la hipótesis, determinándose en esta investigaciòn que, las penas que establece el Código Orgánico Integral Penal, no guardan concordancia con los tipos de delitos informáticos que se presentan en el Sistema Financiero Nacional. Ante los resultados obtenidos y el respectivo análisis respaldados en el marco doctrinario y las legislaciones comparadas, se concluye que la actual normativa jurídica establecida en el Código Integral Penal (COIP) no establece penas de forma específica, de acuerdo a la gravedad del delito informático cometido y su penalización está establecida de forma general, se la considera insuficiente tanto en los años de privación de libertad, así como en los valores que debe retribuir quien comete un delito de esta naturaleza. En respuesta a dar una solución tentativa a esta problemática jurídica analizada, se plantea una Reforma Jurídica al Código Integral Penal, específicamente en el artículo 234 a fin de agravar las penas para salvaguardar a los usuarios del Sistema Financiero Nacional, que sean perjudicados por los delitos informáticos.

ABSTRACT

This research had as general objective, an analysis of cybercrime in the National Financial System research is justified due to the increase of these crimes in Ecuador and the need exists to address a thorough and objective in this topic to establish the existing shortcomings in the Ecuadorian legislation regarding the punishment of cybercrime with regard to security, defense and preservation of integrated computer systems against cyber-criminals. inductive, deductive, analytic-synthetic, comparative and dialectical methods used during the research process, the same as through techniques such as encuenta and interview allowed to obtain the information required to reach the achievement of objectives and verification and the testing of the hypothesis, the same as that determined that the penalties established in the Code of Criminal Integral does not keep consistent with the type of the crime, when it comes to cybercrime in the National Financial System. Given the findings and analysis of the data backed up on the respective doctrinal framework and comparative legislation, it is concluded that the current legal rules established in the Comprehensive Code of Criminal Procedure (COIP), does not establish penalties specifically according to the seriousness of computer crime, criminalization of these is generally established and is considered very flexible both in the values that should remunerate who commits a crime of this nature, until the years of imprisonment for these people. In response to a tentative solution to this legal issues analyzed, a Legal Reform Integral Penal Code arises specifically in Article 234 to prevent the users of the National Financial System, are affected by cybercrime.

3. INTRODUCCIÓN

Para nadie es desconocido la enorme influencia que ha alcanzado la informática en la vida diaria de las personas, empresas y organizaciones, la importancia que tiene su progreso para el desarrollo de un país. Las transacciones comerciales, la comunicación, los procesos industriales, las investigaciones, la seguridad, etc., son todos estos aspectos que requieren cada día más de un adecuado desarrollo de la tecnología informática.

Junto al avance de la tecnología informática y su influencia en casi todas las áreas de la vida social, ha surgido una serie de comportamientos ilícitos denominados, de manera genérica, “delitos informáticos”.

Debido a lo expuesto, se desarrolla el presente estudio que contiene una investigación sobre la temática de los delitos informáticos en el Sistema Financiero Nacional, de manera que mediante la metodología utilizada se logró realizar un análisis objetivo, tomando como bases de sustento de este análisis la respectiva doctrina jurídica existente tanto a nivel nacional como internacional.

En la primera parte de la presente tesis, se establecen y definen las principales conceptualizaciones relacionadas con las variables de estudio, se establecen así definiciones de acuerdo a diferentes autores, con el objetivo de tener un enfoque más amplio tanto de las variables como de las categorías de las mismas.

Consecutivamente, en el presente estudio se aborda el marco doctrinario para el análisis de los referentes teóricos relacionados con las variables de investigación, se exponen conceptos teóricos y jurídicos que sustentan los resultados del estudio. Concluye este apartado del informe, con la exposición de la legislación comparada de varios países de la región y de otros a nivel internacional.

En el apartado número cinco, se presentan los materiales y métodos que se utilizaron en el desarrollo de la investigación, se describen además las técnicas como entrevista y encuesta que se aplicaron a los involucrados en la población de estudio.

En el apartado seis, se describen y analizan los resultados de la investigación, los mismos que se sustentan con el respectivo marco doctrinario y enfoques jurídicos de los diferentes autores que fueron citados en la respectiva bibliografía que se utilizó como referente.

En los numerales siete y ocho, se presentan las conclusiones y recomendaciones, las misma que se plantean de acuerdo a los objetivos específicos, estableciendo como principal que que la actual normativa jurídica establecida en el Código Integral Penal (COIP), no establece penas de forma específica de acuerdo a la gravedad del delito informático cometido, por lo tanto se recomienda que una Reforma Jurídica al Código Integral Penal.

Finalmente en el apartado nueve, se presenta la propuesta de reforma al Código Integral Penal, específicamente en el artículo 234 a fin de agravar la pena para evitar que los usuarios del Sistema Financiero Nacional, se vean perjudicados por los delitos informáticos.

.

4. REVISIÓN DE LA LITERATURA

4.1 MARCO CONCEPTUAL

4.1.1 Delito

Caballenas en su Diccionario Jurídico pp 326, presenta la definición etimológica de este término, estableciendo; *"la palabra delito proviene del latín delictum, expresión también de un hecho antijurídico y doloso castigado con una pena. En general, culpa, crimen, quebrantamiento de una ley imperativa."* [1]

Para Carrancá y Trujillo, delito es *"Todo hecho que lesione, dañe o ponga en peligro las condiciones de vida individual o social, más o menos importantes, determinadas por el Poder Público*" [2]

Según Navarrete en su obra sobre Derecho Penal, *"El delito es definido como una conducta típica, antijurídica y culpable, sometida a una sanción penal y a veces a condiciones objetivas de punibilidad. Supone una conducta infraccional del Derecho penal, es decir, una acción u omisión tipificada y penada por la ley*". [3]

[1] CABANELLAS G, "DICCIONARIO JURIDICO ELEMENTAL, editorial Eliasta edición actualizada 1014, pp 326
[2] CARRANCA Y TRUJILLO RAÚL, *DERECHO PENAL* MEXI- CANO (parte general), 7a. ed., *México*, Antigua Librería Robredo
[3] POLAINO NAVARRETE, "DERECHO PENAL, PARTE GENERAL", editorial Bosch Colección: 1ª Edición,

Ernst Beling define el delito como *"la acción típica antijurídica y culpable sometida a una adecuada sanción penal y que llena las condiciones objetivas de penalidad"* [4]

4.1.2 Delito Informático

Para María de la Luz Lima**,** el delito informático o electrónico en un sentido amplio es *"cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin", y que en un sentido estricto, el delito informático, es "cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin*" [5]

Julio Tellez Valdés, define al delito informático de acuerdo a dos formas típica y atípica, de acuerdo a la forma típica define al delito como *"las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumentos o fin*" y en forma atípica como "*actitudes ilícitas en que se tienen a las computadoras como instrumento o fin"* [6]

De acuerdo al Convenio de Cyber-Delincuencia del Consejo de Europa, los delitos informáticos son "*los actos dirigidos contra la confidencialidad, la*

[4] ERNST BELING "INTRODUCCIÓN A LA TEORÍA DEL DELITO", artículo jurídico publicado en diposit.ub.edu/dspace/bitstream/2445/41555/1/TOL77.pdf
[5] DE LA LUZ LIMA MARIA, "DELITOS ELECTRÓNICOS", Ediciones Porrúa- México,. Pág100, 1984
[6] JULIO TELLEZ VALDEÉS, "DERECHO INFORMÁTICO", 2da edición Mc Graw Hill-México 1996

integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas redes y datos" [7]

Según María de Lourdes Delgado Granados, los *"delitos informáticos, llamados también delitos cibernéticos, delitos electrónicos, delitos relacionados con las computadoras, delincuencia relacionada con el ordenador, computer related crimes, entre otros"*. [8]

Otra de las definiciones que es importante señalar, es la que hace la Organización para la Cooperación Económica y el Desarrollo, como: "*Cualquier conducta ilegal, no ética o no autorizada que involucra el procesamiento automatizado de datos y/o la transmisión de datos*"[9]

4.1.3 Fraude Informático

De acuerdo a Solano, *"Es la manipulación que puede realizarse a través de la utilización de un sistema (imputa) en los programas en la salida de datos del sistema (output) y las manipulaciones a distancia, mediante conexión telemática vía módem a un computador.*" [10]

[7] CONVENIO DE CYBER-DELINCUENCIA DEL CONSEJO DE EUROPA ESTADOS MIEMBROS DEL CONSEJO DE EUROPA Y OTROS ESTADOS-BUDAPEST 2001 http://www.coe.int/

[8] DELGADO GRANADOS MARÍA LOURDES, "DELITOS INFORMÁTICOS DELITOS ELECTRÓNICOS", recuperado en www.ordenjuridico.gob.mx/Congreso/pdf/120.pdf

[9] ORGANIZACIÓN PARA LA COOPERACIÓN ECONÓMICA Y EL DESARROLLO,

[10] SOLANO BARCENAS, ORLANDO: "Manual de Informática Jurídica". Ediciones Jurídicas Gustavo Ibáñez.

4.1.4 Falsificaciones informáticas o fraude informático

Para Solano Barcenas, las **falsificaciones informáticas son** *"la incorrecta modificación del resultado de un procesamiento automatizado de datos, mediante alteración de los datos que se introducen o ya contenidos en el ordenador en cualquiera de las fases de su procesamiento o tratamiento informático, con ánimo de lucro y en perjuicio de terceros.* [11]

4.1.5 Sabotaje informático:

Para Líbano Manssur Carlos, "*es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema*". [12]

4.1.6 Hurto informático

Para Camacho el hurto informático *"es toda interrupción, uso indebido, modificación, o fabricación de datos ajenos que se encuentren en sistemas de computación, sin autorización expresa o implícita de su dueño y/o de quien ostente la propiedad intelectual, con el objeto de obtener un provecho económico o no."* [13]

[11] SOLANO BARCENAS, ORLANDO: "Manual de Informática Jurídica". Ediciones Jurídicas Gustavo Ibáñez.
[12] LÍBANO MANSSUR, CLAUDIO. "LOS DELITOS DE HACKING EN SUS DIVERSAS MANIFESTACIONES". Revista Electrónica de Derechos informáticos, bajados de Internet.
[13] CAMACHO LOSA, L: "EL DELITO INFORMÁTICO". Graficas Cóndor, Madrid.

4.1.7 Falsificación informática

La Dra. Cristina Vallejo, en un artículo de su autoría define a la falsificación informática como, *"Falsedad Vía Computarizada, porque a través de la misma, se pueden elaborar tarjetas de crédito, cheques, títulos valores, en general todo tipo de documentos públicos y privados, o se pueden alterar todo el sistema contable de una Empresa, facilitando a las Sociedades Comerciales llevar la doble contabilidad, todo esto con miras a evadir impuestos"*[14]

4.1.8 Hacker informático

En un artículo publicado sobre programación informática, Raimont, Erick, define a un Hacker informático como *"una persona experta en informática que pertenece a una comunidad que está relacionada directamente con el mundo de la programación informática"* [15]

4.1.9 Seguridad Informática

Para Núñez Ponce, experto en derecho informático, "*seguridad informática es un término que concierne principalmente a entradas remotas no autorizadas por medio de redes de comunicación como Internet ("Black hats"). Pero también incluye a aquellos que depuran y arreglan errores en los sistemas ("White hats") y a los de moral ambigua como son los "Grey hats"*[16]

---

[14] VALLEJO CRISTINA, FALSIFICACIÓN INFORMÁTICA, recuperado en http://www.derechoecuador.com/articulos/detalle/archive/doctrinas/derechoinformatico/2005/11/24/falsificacioacuten-informaacutetica

[15] RAYMOND, ERIC (2003). "THE ART OF UNIX PROGRAMMING". pp. 87-91. Consultado el 9 de febrero de 2015.

[16] NÚÑEZ PONCE, J: "DERECHO INFORMÁTICO. UNA NUEVA DISCIPLINA JURÍDICA PARA UNA SOCIEDAD MODERNA". Perú, Editores S.A, 1996.

4.1.10 Sistema de seguridad informática

Manual de Naciones Unidas para la Prevención y Control de Delitos Informáticos manifiesta que: "*Un sistema de seguridad informática, se refiere a las "características y condiciones de sistemas de procesamiento de datos y su almacenamiento, para garantizar su confidencialidad, integridad y disponibilidad. Considerar aspectos de seguridad significa: conocer el peligro; clasificarlo y protegerse de los impactos o daños de la mejor manera posible"*

4.1.11 Sistema Financiero

En un sentido general, el sistema financiero (sistema de finanzas) de un país "*está formado por el conjunto de instituciones, medios y mercados, cuyo fin primordial es canalizar el ahorro que generan los prestamistas o unidades de gasto con superávit hacia los prestatarios o unidades de gasto con déficit, así como facilitar y otorgar seguridad al movimiento de dinero y al sistema de pagos"*. [17]

Sistema Financiero Ecuatoriano

Para la Superintendencia de Bancos, el Sistema Financiero del Ecuador, es:

> *"El conjunto de instituciones que tiene como objetivo canalizar el ahorro de las personas. Esta canalización de recursos permite el desarrollo de la actividad económica (producir y consumir) haciendo que los fondos lleguen desde las personas que tienen recursos monetarios excedentes hacia las personas que necesitan estos recursos. Los intermediarios financieros crediticios se encargan de captar depósitos del público y, por otro, prestarlo a los demandantes de recursos".* [18]

[17] CALVO, ANTONIO; CUERVO, ÁLVARO; PAREJO, JOSÉ ALBERTO; RODRÍGUEZ, LUIS (2008). "MANUAL DEL SISTEMA FINANCIERO ESPAÑOL", Ariel. ISBN 9788434445536. recuperado en http://www.uv.es/~fcliment/Actualidad_Financiera.pdf

[18] SUPER INTENDENCIAS DE BANCOS DEL ECUADOR, Portal del Usuario http://portaldelusuario.sbs.gob.ec/contenido.php?id_contenido=23

4.1.12 Delitos financieros

Para María de los A. Pérez, el término delito financiero se refiere, en términos generales, a *"cualquier delito, no violento que da lugar a una pérdida económica. Estos delitos, por lo tanto, comprenden una amplia gama de actividades ilegales, incluidos el fraude, pánico financiero, información privilegiada, entre otras*". [19]

4.1.13 Transacción Bancaria

De acuerdo a la Superintendencia de Bancos del Ecuador: "*Una transacción bancaria es un movimiento de flujo de efectivo, ya sea abono al banco o retiro del banco, el retiro puede darse en efectivo a depósito o a cuenta; cheque: cobrado o como abono a alguna cuenta; transferencia a alguna cuenta; cheque de caja: para poder retirar dinero en efectivo del banco*". [20]

4.1.14 Transacciones Electrónicas

De acuerdo a Carreño "*Una transacción electrónica es cualquier actividad que involucra la transferencia de información digital para propósitos específicos. Sin embargo, a pesar de ser electrónicas conservan su esencia original, por lo tanto aún conservan ciertas reglas de origen que las rigen*". [21]

---

[19]. PÉREZ MARÍA DE LOS A, DELITOS FINANCIEROS http://resources.lawinfo.com/es/Preguntas-Frecuentes/delitos-financieros/Federal/qu-son-delitos-financieros.html

[20]. SUPER INTENDENCIA DE INTENDENCIA, recuperado en Portal del Usuario http://portaldelusuario.sbs.gob.ec/contenido.php?id_contenido=23

[21]. CARREÑO, J. "USO DE MEDIOS ELECTRÓNICOS EN LA BANCA", recuperado en http://blogtelecomunicaciones.ramonmillan.com/2008/03/tipos-transacciones-electrnicas.html

4.1.15 Software

Según la Real Academia Española, "*el software es un conjunto de programas, instrucciones y reglas informáticas que permiten ejecutar distintas tareas en una computadora."* [22]

4.1.16 Hardware.-

De acuerdo a la definición que expone:

> "*Son todos los dispositivos y componentes físicos que realizan las tareas de entrada y salida, también se conoce al hardware como la parte dura o física del computador. La mayoría de las computadoras están organizadas de la siguiente forma: Los dispositivos de entrada (Teclados, Lectores de Tarjetas, Lápices Ópticos, Lectores de Códigos de Barra, Escáner, Mouse, etc.) y salida (Monitor, Impresoras, Plotters, Parlantes, etc.) y permiten la comunicación entre el computador y el usuario*." [23]

[22]. REAL ACADEMIA DE LA LENGUA ESPAÑOLA , La 23.ª edición (2014) · El Diccionario en el BRAE
[23]. Periféricos de computadores - Memorias Flash USB». Periféricos - "Introducción a la Informática", A. Prieto (c) McGraw-Hill Interamericana. Archivado desde el original el 25 de noviembre de 2015.

4.2 MARCO DOCTRINARIO

4.2.1 Delitos Informáticos. Definiciones

Emitir una definición sobre delitos informáticos no es una labor sencilla, debido a la razón de que su misma denominación es alusiva a una situación muy especial, ya que para hablar de "delitos" en el sentido de acciones tipificadas o contempladas en textos jurídico penales, se requiere que la expresión "delitos informáticos "esté consignada en los códigos penales, hecho que en Ecuador país se dio a partir del 2002 de la Ley de Comercio Electrónico, Mensajes de Datos y Firmas Electrónicas, y en consecuencia las reformas al Código Penal que daban la luz a los llamados Delitos Informáticos. Sin embargo, muchos especialistas en derecho informático emplean esta alusión a los efectos de una mejor conceptualización.

De esta manera, el autor mexicano Julio Téllez Valdez señala que los delitos informáticos son "*actitudes ilícitas en que se tienen a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin (concepto típico)*".[24]

Por su parte, el tratadista penal italiano Carlos Sarzana sostiene que los delitos informáticos son *"cualquier comportamiento criminal en que la computadora está involucrada como material, objeto o mero símbolo*".[25]

[24]. JULIO TELLEZ VALDEÉS, "DERECHO INFORMÁTICO", 2da edición Mc Graw Hill-México 1996
[25]. SARNAZA, C." CRIMINALITÁ E TECNOLOGÍA", COMPUTER CRIMES, RASEGNA PENITENZIARIA E CRIMINOLOGIA", Nos 1-2, Anno 1, Gennaio €" Giugno, 1979, Roma, Italia. Página 59.

Otra de las definiciones que amerita ser expuesta, es la del Dr. Orlando Solano Bárcenas define quien define al delito informático desde dos conceptos: uno restringido que tiene como *"aquel hecho en el que independientemente del perjuicio que puede causarse a otros bienes jurídicamente tutelados y que eventualmente puedan concurrir en forma real o ideal, se atacan elementos puramente informáticos*"[26]. Y el otro en el sentido amplio lo define como, "*la acción típica, antijurídica y culpable para cuya consumación se utiliza o se afecta a una computadora o sus accesorios". [27.]*

Otra, de las definiciones relacionadas directamente con el contexto de la investigación es la que hace la Organización para la Cooperación y Desarrollo Económico (OCDE) la misma que lo define como "*toda conducta ilegal, no ética o no autorizada, que involucra un proceso automático de datos y / o la transmisión de datos". [28]*

El Departamento de Justicia Norteamericano, lo describe como "*cualquier acto ilegal en relación con el cual el conocimiento de la tecnología informática es esencial para su comisión, investigación y persecución*". [29]

El doctor Rodrigo Medina Jara, agregando algunos aspectos a la definición de Marcel Huertas y Claudio Líbano, dice:

---

[26]. SOLANO BÁRCENAS "MANUAL DE INFORMÁTICA JURÍDICA". Ediciones Jurídicas Gustavo Ibáñez.
[27]Ibid.,Pag.7
[28]Organización para la Cooperación y Desarrollo Económico (OCDE).", recuperado en http://www.eumed.net/rev/cccss/14/ecra.html
[29]. DEPARTAMENTO DE JUSTICIA NORTEAMERICANO, "DELITOS INFORMÁTICOS", recuperado en http://www.eumed.net/rev/cccss/14/ecra.html

"El delito informático "…son todas aquellas acciones u omisiones típicas, antijurídicas y dolosas, trátese de hechos aislados o de una serie de ellos, cometidos contra personas naturales o jurídicas, realizadas en uso de un sistema de tratamiento de información y destinadas a producir un perjuicio en la víctima a través de atentados a la sana técnica informática, lo cual generalmente, producirá de manera colateral lesiones a distintos valores jurídicos, reportándose, muchas veces, un beneficio ilícito en el agente, sea o no de carácter patrimonial, actúe con o sin ánimo de lucro". [30]

A la luz de las definiciones de los diferentes autores que se han abordado y considerando lo que expone el ilustre Cuello Calón, donde afirma que "*El delito es un acto humano, es una acción (acción u omisión) Dicho acto humano ha de ser antijurídico, debe lesionar o poner en peligro un interés jurídicamente protegido, debe corresponder a un tipo legal (figura de delito), definido por la Ley, ha de ser un acto típico"*.[31]

El acto ha de ser culpable, imputable o dolo (intención) o a culpa (negligencia), y una acción es imputable cuando puede ponerse a cargo de una determinada persona. La ejecución u omisión del acto debe estar sancionada con una pena.

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

---

[30]. MEDINA, R "DISEÑO DE POLÍTICAS PÚBLICAS PARA ENFRENTAR EL DELITO EN DEMOCRACIA", Instituto de Ciencia Política de la Universidad de Chile (2001).

[31]. CUELLO CALÓN", "GUÍA PRACTICA DE DERECHO" recuperado en http://derecho911.blogspot.com/2013/06/que-es-la-antijuricidad.html

Según Téllez Valdés, este tipo de acciones presentan las siguientes características principales:

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

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

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

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

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

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

g) Son muy sofisticados y relativamente frecuentes en el ámbito militar.

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

i) En su mayoría son imprudenciales y no necesariamente se cometen con intención.

j) Ofrecen facilidades para su comisión a los menores de edad.

k) Tienden a proliferar cada vez más, por lo que requieren una urgente regulación.

l) Por el momento siguen siendo ilícitos impunes de manera manifiesta ante la ley. [32].

[32]. JULIO TELLEZ VALDEÉS, “DERECHO INFORMÁTICO”, 2da edición Mc Graw Hill-México 1996

Es preciso mencionar que actualmente se han establecido diferentes denominaciones para nombrar las conductas ilícitas en las que se usa la computadora para cometer estos delitos, tales como delitos informáticos, delitos electrónicos, delitos relacionados con las computadoras, crímenes por computadora, delincuencia relacionada con el ordenador.

Los delitos Informáticos constituyen actualmente un tema que debe ser abordado de forma objetiva y profunda, debido a que cada vez más la delincuencia informática se apoya en el delito instrumentado por el uso de la computadora a través de redes telemáticas y la interconexión de la computadora, aunque no es el único medio.

Las ventajas y las necesidades del flujo nacional e internacional de datos, que aumenta de modo creciente, conlleva también a la posibilidad creciente de estos delitos; por eso puede señalarse que la criminalidad informática constituye un reto considerable tanto para los sectores afectados de la infraestructura crítica de un país, como para los legisladores, las autoridades policiales encargadas de las investigaciones y los funcionarios judiciales.

4.2.2 Características de sujetos que cometen delitos informáticos

4.2.2.1 Características del Sujeto Activo

Las personas que cometen los delitos informáticos son aquellas que

> "*poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, los sujetos activos tienen habilidades para el*

manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, aun cuando en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos". [33].

Con el tiempo, se ha podido comprobar que los autores de los delitos informáticos son muy diversos y que lo que los diferencia entre sí es la naturaleza de los delitos cometidos. De esta forma, la persona que "entra" en un sistema informático sin intenciones delictivas es muy diferente del empleado de una institución financiera que desvía fondos de las cuentas de sus clientes.

El nivel típico de aptitudes del delincuente informático, es tema de controversia ya que para algunos el nivel de habilidades no es indicador de delincuencia informática en tanto que otros aducen que los posibles delincuentes informáticos son personas listas, decididas, motivadas y dispuestas a aceptar un reto tecnológico, características que pudieran encontrarse en un empleado del sector de procesamiento de datos.

Sin embargo, teniendo en cuenta las características ya mencionadas de las personas que cometen los delitos informáticos, estudiosos en la materia los han catalogado como delitos de cuello blanco, término introducido por primera vez por el criminólogo norteamericano Edwin Sutherland en el año de 1943.

[33]. SEGU.INFO "LEGISLACIÓN Y DELITOS INFORMÁTICOS - EL DELINCUENTE Y LA VÍCTIMA", recuperado en http://www.segu-info.com.ar/delitos/delincuenteyvictima.htm

Efectivamente, este conocido criminólogo señala un sin número de conductas que considera como “delitos de cuello blanco”. [34]

Aun, cuando muchas de estas conductas no están tipificadas en los ordenamientos jurídicos como delitos, y dentro de las cuales cabe destacar las violaciones a las leyes de patentes y fábrica de derechos de autor, el mercado negro, el contrabando en las empresas, la evasión de impuestos, las quiebras fraudulentas, corrupción de altos funcionarios, entre otros.

Asimismo, este criminólogo estadounidense manifiesta que “*tanto la definición de los delitos informáticos como la de los delitos de cuello blanco no son de acuerdo al interés protegido, como sucede en los delitos convencionales, sino de acuerdo al sujeto activo que los comete*”. [35]

Entre las características en común que poseen ambos delitos, se puede identificar que el sujeto activo del delito, es una persona de cierto status socioeconómico, su condición no puede explicarse por pobreza ni por mala habitación, ni por carencia de recreación, ni por baja educación, ni por poca inteligencia, ni por inestabilidad emocional.

Es difícil elaborar estadísticas sobre ambos tipos de delitos. La "cifra negra" es muy alta; no es fácil descubrirlo y sancionarlo en razón del poder económico de quienes los cometen, pero los daños económicos son altísimos; existe una gran indiferencia de la opinión pública sobre los daños ocasionados a la sociedad; generalmente la sociedad no considera delincuentes a los sujetos que cometen este tipo de delitos, no los segrega, no los desprecia, ni los desvaloriza, por el

[34]. EDWIN SUTHERLAND”, EL DELITO DE CUELLO BLANCO, Madrid: La Piqueta, 1999I. Título II. Serie Pág. 339
[35]. *Ibid* pág. 340

contrario, el autor o autores de este tipo de delitos se considera a sí mismos "respetables".

Otra coincidencia que tienen estos tipos de delitos es que, generalmente, son objeto de medidas o sanciones de caracteres administrativos y no privativos de la libertad. Este nivel de criminalidad se puede explicar por la dificultad de reprimirla en forma internacional, ya que los usuarios están esparcidos por todo el mundo y, en consecuencia, existe una posibilidad muy grande de que el agresor y la víctima estén sujetos a leyes nacionales diferentes.

Actualmente si bien los acuerdos de cooperación internacional y los tratados de extradición bilaterales intentan remediar algunas de las dificultades ocasionadas por los delitos informáticos, sus posibilidades son limitadas.

4.2.2.2 Características del Sujeto Pasivo

De acuerdo al enfoque de Pecoy, en su obra sobre delitos informáticos, en primer término se tiene que distinguir que *"sujeto pasivo o víctima del delito es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo, y en el caso de los delitos informáticos las víctimas pueden ser individuos, instituciones crediticias, gobiernos, etc., que usan sistemas automatizados de información, generalmente conectados a otros*". [36]

El sujeto pasivo del delito, es sumamente importante para el estudio de los delitos informáticos, ya que mediante él se puede conocer los diferentes ilícitos

[36]. PECOY, MARTÍN. CONCEPTO DE DELITO INFORMÁTICO. EN "DELITOS INFORMÁTICOS". Universidad de Montevideo. (2012). pp.29-32

que cometen los delincuentes informáticos con objeto de prever las acciones antes mencionadas, debido a que muchos de los delitos son descubiertos casuísticamente por el desconocimiento del modus operandi de los sujetos activos.

Dado lo anterior, ha sido imposible conocer la verdadera magnitud de los delitos informáticos, ya que la mayor parte de los delitos no son descubiertos o no son denunciados a las autoridades responsables y si a esto se suma la falta de leyes que protejan a las víctimas de estos delitos, la falta de preparación por parte de las autoridades para comprender, investigar y aplicar el tratamiento jurídico adecuado a esta problemática.

Paralelo a lo antes expuesto, se suma el temor por parte de las empresas de denunciar este tipo de ilícitos por el desprestigio que esto pudiera ocasionar a su empresa y las consecuentes pérdidas económicas, entre otros más, trae como consecuencia que las estadísticas sobre este tipo de conductas se mantengan bajo la llamada "cifra oculta" o "cifra negra".[37]

Por lo anterior, se reconoce que para conseguir una prevención efectiva de la criminalidad informática se requiere, en primer lugar, un análisis objetivo de las necesidades de protección y de las fuentes de peligro. Una protección eficaz contra la criminalidad informática presupone ante todo que las víctimas potenciales conozcan las correspondientes técnicas de manipulación, así como sus formas de encubrimiento.

[37]. MANUEL BAJO FERNÁNDEZ, LOS DELITOS INFORMÁTICOS, Editorial Juristas, Enero 2012.

En el mismo sentido, se puede decir que mediante la divulgación de las posibles conductas ilícitas derivadas del uso de las computadoras, y alertando a las potenciales víctimas para que tomen las medidas pertinentes a fin de prevenir la delincuencia informática, y si a esto se suma la creación de una adecuada legislación que proteja los intereses de las víctimas y una eficiente preparación por parte del personal encargado de la procuración, administración e impartición de justicia para atender e investigar estas conductas ilícitas, se estaría avanzando mucho en el camino de la lucha contra la delincuencia informática, que cada día tiende a expandirse más.

Además, se debe destacar que los organismos internacionales han adoptado resoluciones similares en el sentido de que educando a la comunidad de víctimas y estimulando la denuncia de los delitos se promovería la confianza pública en la capacidad de los encargados de hacer cumplir la ley y de las autoridades judiciales para detectar, investigar y prevenir los delitos informáticos**.**

4.2.3 Manipulación indebida de datos a través de la utilización de un sistema de tratamiento de la información.

4.2.3.1 El fraude informático

El fraude informático puede concebirse, como “la manipulación que puede realizarse a través de la utilización de un sistema (imputa) en los programas en

la salida de datos del sistema (output) y las manipulaciones a distancia, mediante conexión telemática vía módem a un computador". [38]

El caso más común es el fraude que se hace en los cajeros automáticos mediante la falsificación de instrucciones para el ordenador, en la fase de adquisición de datos. Tradicionalmente esos fraudes se hacen a partir de tarjeta bancarias robadas, sin embargo, hoy también se usan equipos y programas de computador especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.

4.2.3.2 Falsificaciones informáticas o fraude informático

Siendo éste la "incorrecta modificación del resultado de un procesamiento automatizado de datos, mediante alteración de los datos que se introducen o ya contenidos en el ordenador en cualquiera de las fases de su procesamiento o tratamiento informático, con ánimo de lucro y en perjuicio de terceros". [39] Pueden consumarse como:

Objeto: Es cuando se alteran datos de documentos que se encuentran almacenados en forma computarizada. Pueden falsificarse o adulterarse también micro formas, micro duplicados y microcopias; esto puede llevarse a cabo en el proceso de copiado o en cualquier otro momento.

---

[38]. CORREA, C. - BATTO, H. - CZAR DE ZALDUENDO, S. & NAZAR ESPECHE, F. (1987). Cap. El derecho ante el desafío de la informática. En "Derecho informático"(p. 295). Buenos Aires: Depalma. ISBN 950 14 0400 5

[39]. CUERVO, JOSÉ. "DELITOS INFORMÁTICOS: PROTECCIÓN PENAL DE LA INTIMIDAD". Publicado en http://www.INFORMÁTICA-jurídica.com/trabajos/delitos.asp (2008)

Instrumentos: Los computadores pueden utilizarse para realizar falsificaciones de documentos de uso comercial. Las fotocopiadoras computarizadas en color a partir de rayos láser han dado lugar a nuevas falsificaciones. Estas fotocopiadoras pueden hacer copias de alta resolución, modificar documentos, crear documentos falsos sin tener que recurrir a un original y los documentos que producen son de tal calidad que sólo un experto puede diferenciarlos de los documentos auténticos.

Así mismo, el autor Téllez Valdez clasifica a estos delitos, de acuerdo a dos criterios:

a. Como instrumento o medio

En esta categoría se encuentran las conductas criminales que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito, por ejemplo: Falsificación de documentos vía computarizada (tarjetas de crédito, cheques, etc.)

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

Planeamiento y simulación de delitos convencionales (robo, homicidio, fraude, etc.) Lectura, sustracción o copiado de información confidencial.

b. Modificación de datos tanto en la entrada como en la salida.

En esta categoría se asocian las siguientes alteraciones:

- *Aprovechamiento indebido o violación de un código para penetrar a un sistema introduciendo instrucciones inapropiadas.*

- *Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa.*
- *Uso no autorizado de programas de cómputo.*
- *Introducción de instrucciones que provocan "interrupciones" en la lógica interna de los programas.*
- *Alteración en el funcionamiento de los sistemas, a través de los virus informáticos.*
- *Obtención de información residual impresa en papel luego de la ejecución de trabajos.*
- *Acceso a áreas informatizadas en forma no autorizada.*
- *Intervención en las líneas de comunicación de datos o teleproceso. Como fin u objetivo. En esta categoría, se enmarcan las conductas criminales que van dirigidas contra las computadoras, accesorios o programas como entidad física, por ejemplo: Programación de instrucciones que producen un bloqueo total al sistema. Destrucción de programas por cualquier método. daño a la memoria. Atentado físico contra la máquina o sus accesorios.*
- *Sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centros neurálgicos computarizados.*
- *Secuestro de soportes magnéticos entre los que figure información valiosa con fines de chantaje (pago de rescate, etc.*). [40]

[40]. TÉLLEZ VALDÉS, J, DERECHO INFORMÁTICO, Universidad Autónoma de. México ...

4.2.4. Legislación de la Organización de Naciones Unidas sobre el delito informático

Por su parte, el Manual de la Naciones Unidas para la Prevención y Control de Delitos Informáticos señala que cuando "*el problema se eleva a la escena internacional, se magnifican los inconvenientes y las insuficiencias, por cuanto los delitos informáticos constituyen una nueva forma de crimen transnacional y su combate requiere de una eficaz cooperación internacional concertada"*. [41]

Asimismo, la ONU resume de la siguiente manera a los problemas que rodean a la cooperación internacional en el área de los delitos informáticos:

- *Falta de acuerdos globales acerca de qué tipo de conductas deben constituir delitos informáticos. Ausencia de acuerdos globales en la definición legal de dichas conductas delictivas.*
- *Falta de especialización de las policías, fiscales y otros funcionarios judiciales en el campo de los delitos informáticos.*
- *No armonización entre las diferentes leyes procesales nacionales acerca de la investigación de los delitos informáticos.*
- *Carácter transnacional de muchos delitos cometidos mediante el uso de computadoras.*
- *Ausencia de tratados de extradición, de acuerdos de ayuda mutuos y de mecanismos sincronizados que permitan la puesta en vigor de la cooperación internacional.* [42]

En síntesis, es destacable que la delincuencia informática se apoya en el delito instrumentado por el uso de la computadora a través de redes telemáticas y la interconexión de la computadora, aunque no es el único medio.

Las ventajas y las necesidades del flujo nacional e internacional de datos, que

[41].ORGANIZACIÓN DE LAS NACIONES UNIDAS, MANUAL PARA LA PREVENCIÓN Y CONTROL DE DELITOS INFORMÁTICOS
[42]. ORGANIZACIÓN DE LAS NACIONES UNIDAS, MANUAL PARA LA PREVENCIÓN Y CONTROL DE DELITOS INFORMÁTICOS

aumenta de modo creciente aún en países como la Argentina, conlleva también a la posibilidad creciente de estos delitos; por eso puede señalarse que la criminalidad informática constituye un reto considerable tanto para los sectores afectados de la infraestructura crítica de un país, como para los legisladores, las autoridades policiales encargadas de las investigaciones y los funcionarios judiciales.

4.2.4.1 Tipos de delitos informáticos reconocidos por Las Naciones Unidas

Entre los delitos informáticos que la Organización de las Naciones Unidas reconoce se encuentran los que a continuación se detallan:

4.2.4.2 Fraudes cometidos mediante manipulación de computadoras

En esta categoría se encuentran los siguientes:

Manipulación de los datos de entrada: Este tipo de fraude informático conocido también como sustracción de datos, representa el delito informático más común ya que es fácil de cometer y difícil de descubrir. Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos.

La manipulación de programas: Es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente debe tener conocimientos técnicos

concretos de informática. Este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas. Un método común utilizado por las personas que tienen conocimientos especializados en programación informática es el denominado Caballo de Troya, que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.

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

Fraude efectuado por manipulación informática: aprovecha las repeticiones automáticas de los procesos de cómputo. Es una técnica especializada que se denomina "técnica del salchichón" en la que "rodajas muy finas" apenas perceptibles, de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra.

4.2.4.3 Falsificaciones informáticas

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

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

4.2.5 Daños o modificaciones de programas o datos computarizados

Sabotaje informático

Es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema.

4.2.5.1 Antecedentes de la Tipificación de los delitos informáticos en la Legislación Ecuatoriana

En Ecuador, desde 1999 se puso en el tapete la discusión del proyecto de Ley de Comercio Electrónico, Mensajes de Datos y Firmas Electrónicas, desde ese tiempo se puso de moda el tema, se realizaron cursos, seminarios, encuentros. También se conformó comisiones para la discusión de la Ley, para que

formulen observaciones a la misma por parte de los organismos directamente interesados en el tema como el CONATEL, la Superintendencia de Bancos, las Cámaras de Comercio y otros, que ven el Comercio Telemático como una oportunidad de negocios y de paso lograr que nuestro país entre en el boom de la llamada Nueva Economía.

Cuando la ley se presentó en un principio, tenía una serie de falencias, que con el tiempo se fueron puliendo, una de ellas era la parte penal de dicha ley, ya que las infracciones a la misma es decir a los llamados Delitos Informáticos, como se los conoce, se sancionarían de conformidad a lo dispuesto en nuestro Código Penal, situación como comprenderán era un tanto forzada, esto si se toma en cuenta los 80 años de dicho Código, en resumen los tipos penales ahí existentes, no tomaban en cuenta los novísimos adelantos de la informática y la telemática por tanto les hacía inútiles por decirlo menos, para dar seguridad al Comercio Telemático ante el posible asedio de la criminalidad informática.

Por fin en abril del 2002 y luego de largas discusiones los honorables diputados por fin aprobaron el texto definitivo de la Ley de Comercio Electrónico, Mensajes de Datos y Firmas Electrónicas, y en consecuencia las reformas al Código Penal, que daban luz a los llamados Delitos Informáticos.

De acuerdo a la Constitución Política de la República, en su Título IV, Capitulo 4to, en la sección décima al hablar de la Fiscalía General del Estado, en su Art. 195 señala que: "*La Fiscalía dirigirá, de oficio o a petición de parte la*

investigación pre procesal y procesal penal…"[43]*. Esto en concordancia con el Art. 33 del Código de Procedimiento Penal que señala que "el ejercicio de la acción pública corresponde exclusivamente al fiscal*" [44]. De lo expuesto se puede concluir que el dueño de la acción penal y de la investigación tanto pre procesal como procesal de hechos que sean considerados como delitos dentro del nuevo Sistema Procesal Penal Acusatorio es el Fiscal.

4.2.6 El Sistema Financiero

En un sentido general, el sistema financiero (sistema de finanzas) de un país está formado por el conjunto de instituciones, medios y mercados, cuyo fin primordial es canalizar el ahorro que generan los prestamistas o unidades de gasto con superávit, hacia los prestatarios o unidades de gasto con déficit.

Esta labor de intermediación es llevada a cabo por las instituciones que componen el sistema financiero, y se considera básica para realizar la transformación de los activos financieros, denominados primarios, emitidos por las unidades inversoras (con el fin de obtener fondos para aumentar sus activos reales), en activos financieros indirectos, más acordes con las preferencias de los ahorradores.

[43]. CONSTITUCIÓN DE LA REPUBLICA DEL ECUADOR. TÍTULO IV, CAPITULO 4TO, EN LA SECCIÓN DÉCIMA, Asamblea Constituyente 2008
[44]. CÓDIGO DE PROCEDIMIENTO PENAL, Quito-Ecuador

Siendo, responsabilidad del Fiscal llevar la investigación de esta clase de infracciones de tipo informático para lo cual contara como señala el Art. 208 del Código de Procedimiento Penal con su órgano auxiliar la Policía Judicial, quien realizará la investigación de los delitos de acción pública y de instancia particular bajo la dirección y control de la Fiscalía, en tal virtud cualquier resultado de dichas investigaciones se incorporaran en su tiempo ya sea a la Instrucción Fiscal o a la Indagación Previa, esto como parte de los elementos de convicción que ayudaran posteriormente al representante de la Fiscalía a emitir su dictamen correspondiente.

Este sistema financiero está conformado por "*el conjunto de Instituciones bancarias, financieras y demás empresas e instituciones de derechos público o privado, debidamente autorizadas por la Superintendencia de Bancos, que operan en la intermediación financiera (actividad habitual desarrollada por empresas e instituciones autorizada a captar fondos del público y colocarlos en forma de créditos e inversiones*". [45]

Es el conjunto de instituciones encargadas de la circulación del flujo monetario y cuya tarea principal es canalizar el dinero de los ahorristas hacia quienes desean hacer inversiones productivas. Las instituciones que cumplen con este papel se llaman "Intermediarios Financieros" o "Mercados Financieros.

[45]. SUPERINTENDENCIA DE BANCOS DEL ECUADOR. "SISTEMA FINANCIERO", recuperado en http://portaldelusuario.sbs.gob.ec/contenido.php?id_contenido=23

4.2.6.1 El Sistema Financiero Ecuatoriano

De acuerdo a la definición que presenta Superintendencia de Bancos del Ecuador, el Sistema Financiero Ecuatoriano (SFE), "*es aquel que está constituido por un conjunto de principios y normas jurídicas que se basan en un instrumento y documentos especiales que nos permiten canalizar el ahorro y la inversión de los diferentes sectores hacia otros que lo necesitan y esto conlleva al apoyo y desarrollo de la economía*" [46]

Entre las principales instituciones que están dentro del SFE son las siguientes:

- Bancos privados y públicos
- Cooperativas de ahorro y crédito
- Mutualistas
- Casas de Cambio
- Sociedades Financieras
- Compañías de Servicios

Estas instituciones que forman el Sistema Financiero Ecuatoriano (SFE) se caracterizan por ser las encargadas de la intermediación financiera entre el público y la entidad, captando recursos del público a través del ahorro para luego utilizar dichas captaciones en operaciones de crédito e inversión en los pueblos más olvidado.

[46]. *Ibid.,* p. 2

4.2.6.2 Funciones del Sistema Financiero Ecuatoriano

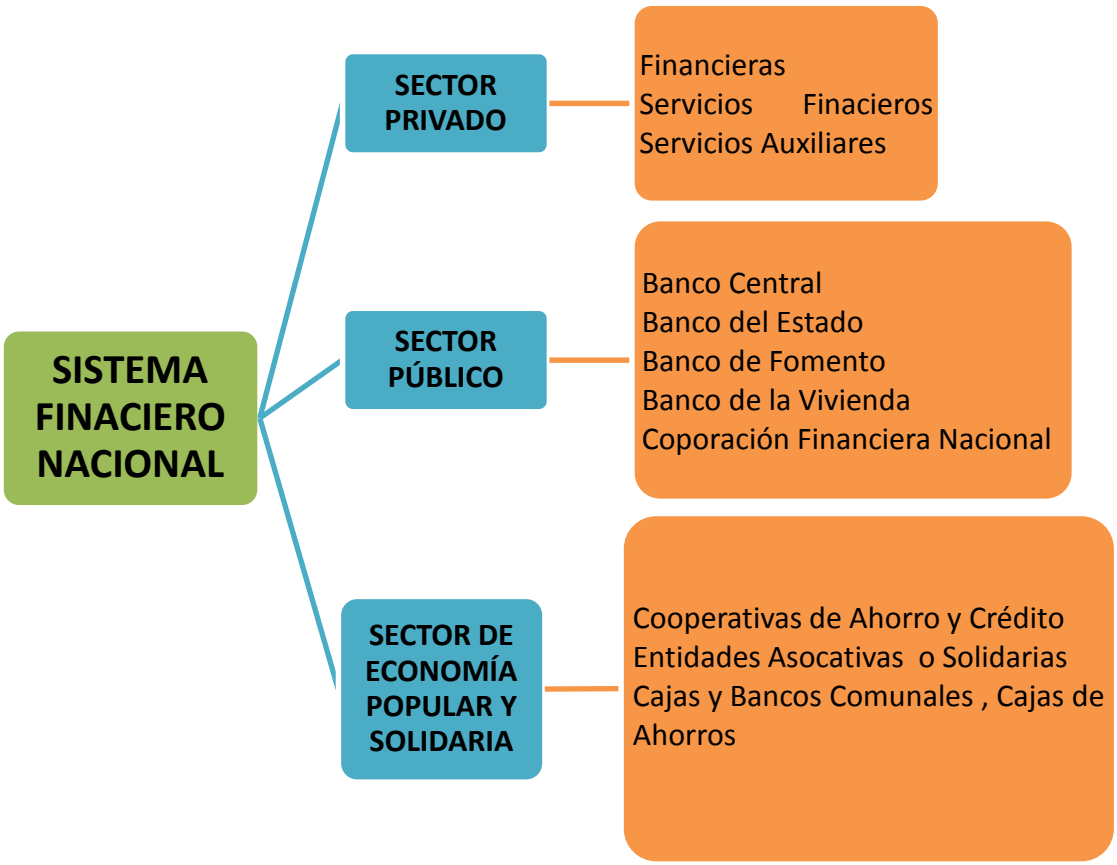
El sistema financiero es los más importantes dentro de la economía, ya que cumple múltiples funciones entre ellas las siguientes:

- *"Captar y promover el ahorro para luego canalizarlo de una forma correcta hacia los diferentes agentes económicos*
- *Facilitar el intercambio de bienes y servicios a sus asociados., de tal forma que lo permitan ser más eficiente*
- *Buscar el crecimiento económico de la población Apoyar de una u otra manara para que la política monetaria sea más efectiva, y de esta manera contribuir al desarrollo local"* [47]

4.2.6.3 Estructura del Sistema Financiero Ecuatoriano

La estructura del Sistema Financiero Nacional (SFE), se basa en el régimen designado por el Banco Central del Ecuador, en donde intervienen varios organismos autónomas reguladores como el Directorio del Banco Central, organismo autónomo y supervisado por el estado ecuatoriano, también se encuentra la Superintendencia de Bancos del Ecuador, entidad autónoma encargada de controlar y supervisar las funciones de varias instituciones financieras y finalmente se encuentran entidades financieras públicas y privadas y de economía popular y solidaria.

[47]. *Ibid.,* p. 2



Fuente: Art. 2 Ley General de Instituciones del Sistema Financiero

Artículo 309 de Constitución del Ecuador 2008

Banco Central del Ecuador

Es una de las entidades autónomas de derecho público, es decir esta manejada y supervisada por el Estado, de duración indefinida y con patrimonio propio, entre sus funciones principales se encuentra las siguientes:

- *Establecer, controlar y aplicar políticas monetarias para la circulación de la moneda de nuestro país*
- *Establecer y aplicar políticas financieras, crediticias, y cambiaria del Estado*

- *Otorgar créditos a las instituciones financieras privadas en casos especiales*
- *Mantener el encaje bancario y excedentes de dicho sistema*
- *Reponer monedas y billetes que no pueden ser utilizados*
- *Proveer de dinero al sistema financiero*
- *Manejar la cámara de compensación*

4.2.7 Principales delitos informáticos en el Sistema Financiero del Ecuador

Con el rápido avance de la tecnología en los últimos 30 años cada vez a pasos más acelerados y la democratización del acceso al Internet en casi todo el planeta, podemos decir sin lugar a dudas que el mundo se ha digitalizado. Desde los aspectos más humanos y sensibles como la música o el cine, hasta los más especializados procesos y actividades desarrolladas por el hombre, como son las complejas transacciones financieras que hoy en día atraviesan el mundo en fracciones de segundo se manejan hoy a través de computadores y redes globales.

Desafortunadamente los estafadores también han dado pasos en paralelo en este universo digital, perjudicando a personas de toda clase color y credo, por medio de engaños de las más variadas clases para que ingresen su información personal en cajeros automáticos, páginas web falsas y otros ingeniosos métodos, para a través del uso de su información despojarlo de sus valores, sin que el perjudicado se dé cuenta.

Debido a la alta incidencia de los crímenes tecnológicos en el ámbito financiero a nivel mundial, la SB alerta al público acerca de las modalidades más utilizadas que los delincuentes utilizan en la actualidad para robar información personal y así realizar todo tipo de actividades ilegales como por ejemplo, pedir créditos con su nombre, hacer compras y suplantar identidades, entre muchas otras más. Preste atención y no se convierta en una víctima más de estos delitos. Más que en los complicados nombres de estos métodos, fíjese en las técnicas que los criminales utilizan para así poder evitarlas.

De acuerdo a la Superintendencia de Bancos del Ecuador, los delitos informáticos más comunes que se cometen en el Sistema financiero del Ecuador son:

Lavado de Dinero: Es el dinero que se ha obtenido por actividades ilegales y que necesita ser incorporado al sistema bancario de manera que pueda ser movilizado eficientemente de un lugar a otro y guardado en forma segura. Efectivo (dinero en efectivo, órdenes de pago, cheques de viajero, etc.) Una variedad sin fin de esquemas se ha desarrollado con el propósito de "estructurar" y "lavar" dinero en el proceso de convertir los fondos de "sucios" a "limpios". El mayor riesgo para un banco está en el potencial para la complicidad y violación de los requerimientos de la Ley del Secreto Bancario.

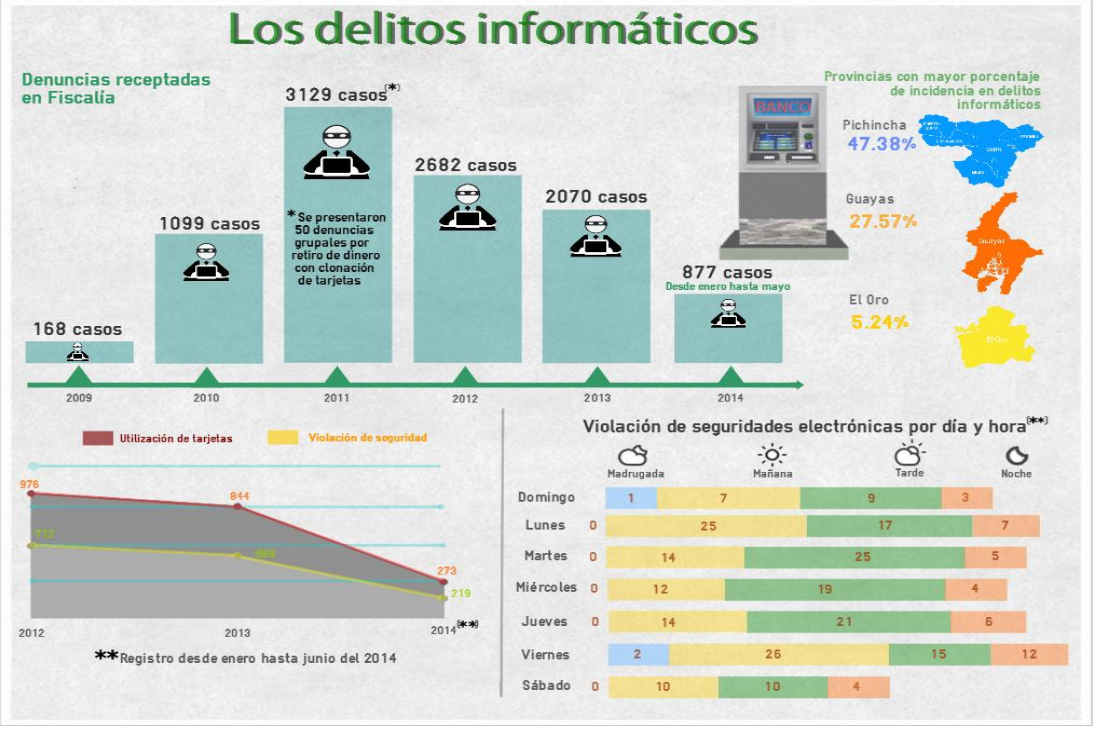
Fraudes con Cuentas Nuevas: Las cuentas corrientes se abren fácilmente debido a que la mayoría de los bancos están ansiosos de captar más clientes. La facilidad con la que los documentos de identidad pueden ser falsificados, las

limitaciones impuestas por las disposiciones de la Ley de Privacidad y el costo de investigar los antecedentes o la confiabilidad de los cheques contribuyen a facilitar que se lleven a cabo las fraudes con cuentas nuevas. Una vez que una nueva cuenta es abierta y se establece un bajo perfil de riesgo de esta actividad, el delincuente defraudador puede llevar a cabo una amplia variedad de diferentes esquemas de fraudes.

Malversación: Cualquiera que tenga un fácil acceso a las cuentas financieras tiene el potencial para llevar a cabo la malversación. Las cuentas del banco o la cuenta de los clientes del banco pueden ser atacadas. Los métodos usados para la malversación. Las cuentas del banco o la cuenta de los clientes del banco pueden ser atacadas. Los métodos usados para la mal. [48]

A continuación se presenta en cifras estadísticas los delitos informáticos que se han dado en el sistema financiero del Ecuador, durante los años 2014 y 2015.

[48]. *Ibid.,* p. 2



Categoría: Boletines
Publicado el Sábado, 13 Junio 2015 09:02

Actualmente el COIP sanciona los delitos informáticos, cuyos actos se comenten con el uso de tecnología para violentar la confidencialidad y la disponibilidad de datos personales. Estos actos que se registran a través de la Internet son: fraude, robo, falsificaciones, suplantación de identidad, espionaje, clonación de tarjetas de crédito, entre otros.

Según las autoridades competentes, las investigaciones referentes a los delitos informáticos se realizan de forma técnica y demanda tiempo para establecer la responsabilidad de aquellos que quebrantan la ley sentados frente a un monitor.

Para el fiscal Edwin Pérez, especialista en delitos informáticos, en Ecuador existen dificultades durante la investigación de delitos propiciados por

el uso de la tecnología, por cuanto la información cruzada a nivel de redes sociales o cuentas de correos electrónicos no se encuentra en el país.

Según Pérez (2015), "Los grandes proveedores de las redes sociales y generadores de los sistemas informáticos como Google, Facebook, Yahoo, entre otros, tienen los bancos de datos de sus usuarios en Estados Unidos, y solicitar esa información puede demorar meses". [49]

Otro de los inconvenientes que se presenta para la investigación radica en que Ecuador no cuenta con convenios internacionales que faciliten el cruce de datos informáticos -como los que existe entre Estados Unidos y Europa-. Por ello, hay complicaciones en detectar las cuentas o las direcciones IP desde las que se habría realizado el ataque o la sustracción de información personal ante las formalidades y la virtualidad de los procesos puede tardarse meses.

Para el fiscal Pérez, "*el robo o interceptación ilegal de datos por el uso de redes sociales, es una de las varias modalidades delito que ahora se investigan, pero la menos denunciada. Este consiste en que otra persona se hace pasar por la víctima para desprestigiarla. Para cometer este hecho no se necesita ser experto, solo tener conocimientos básicos de la informática*".[50]

El delito de interceptación ilegal de datos consta en el artículo 230 del COIP. Que sanciona con tres a cinco años de pena privativa de libertad a quienes utilicen estos datos y los difundan.

[49]. PÉREZ EDWIN, DELITOS INFORMÁTICOS EN ECUADOR, Diario el Universo, 2015
[50]. *Ibid.*, p. 2

4.2.8 Seguridad Informática

La seguridad informática consiste en asegurar en que los recursos del sistema de información de una organización se utilizan de la manera que se planificó y que el acceso a la información allí contenida así como su modificación solo sea accesible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

4.2.8.1 Fiabilidad, Confidencialidad, Integridad y Disponibilidad

Si bien es cierto que todos los componentes de un sistema informático están expuestos a un ataque, son los datos y la información los sujetos principales de protección de las técnicas de seguridad. La seguridad informática se dedica principalmente a proteger la confidencialidad, la integridad y la disponibilidad de la información, por tanto, actualmente se considera que la seguridad de los datos y la información comprende 3 aspectos fundamentales: Confidencialidad; Integridad (seguridad de la información) y Disponibilidad.

Hay que tener en cuenta que tanto las amenazas como los mecanismos para contrarrestarla suelen afectar a estas 3 características de forma conjunta por tanto un fallo del sistema que haga que la información no sea accesible puede llevar consigo una pérdida de integridad. Generalmente tiene que existir los 3 aspectos descritos para que haya seguridad.

Dependiendo del entorno en el que trabaje un sistema, a sus responsables les interesara dar prioridad a un cierto aspecto de la seguridad. Junto a estos 3 conceptos fundamentales se suele estudiar conjuntamente la autenticación y el

no repudio. Suele referirse al grupo de estas características como CIDAN, nombre sacado de la inicial de cada característica.

Los diferentes servicios de seguridad dependen unos de otros jerárquicamente, así si no existe el primero no puede aplicarse el siguiente.

Disponibilidad: Se trata de la capacidad de un servicio de unos datos o de un sistema a ser accesible y utilizable por los usuarios o procesos autorizados cuando lo requieran. También se refiere a la capacidad de que la información pueda ser recuperada en el momento que se necesite.

Confidencialidad: Se trata de la cualidad que debe poseer un documento o archivo para que éste solo se entienda de manera comprensible o sea leído por la persona o sistema que esté autorizado.

Un ejemplo de control de la confidencialidad sería el uso cifrado de clave simétrica en el intercambio de mensajes.

Integridad: Es la cualidad que posee un documento o archivo que no ha sido alterado y que además permite comprobar que no se ha producido manipulación alguna en el documento original.

4.2.8.2 Alta disponibilidad (Hight Availability)

Son sistemas que están disponibles las 24 horas al día, 7 días a la semana, 365 días al año, esta disponibilidad se presenta en niveles:

Base: Se produce paradas previstas e imprevistas.

Alta: Incluyen tecnologías para disminuir el número y la duración de interrupciones imprevistas aunque siempre existe alguna interrupción imprevista.

Operaciones continuas: Utilizan tecnologías para asegurar que no hay interrupciones planificadas

4.2.8.3 Sistemas de disponibilidad continúa

Se incluyen tecnologías para asegurarse que no habrá paradas imprevistas ni previstas.

Sistemas de tolerancia al desastre: requieren de sistemas alejados entre sí para asumir el control en una interrupción provocada por un desastre.

Autenticación: Es la situación en la cual se puede verificar que un documento ha sido elaborado o pertenece a quien el documento dice. La autenticación de los sistemas informático se realizan habitualmente mediante nombre y contraseña.

No repudio: El no repudio o irrenunciabilidad es un servicio de seguridad estrechamente relacionado con la autenticación y que permite probar la participación de las partes en una comunicación, existen dos posibilidades:

No repudio en origen: el emisor no puede negar el envío porque el destinatario tiene pruebas del mismo el receptor recibe una prueba infalsificable del envío.

No repudio de destino: el receptor no puede negar que recibió el mensaje porque el emisor tiene pruebas de la recepción. Si la autenticidad prueba quien es el autor y cuál es su destinatario, el no repudio prueba que el autor envió la comunicación (en origen) y que el destinatario la recibió (en destino)

Elementos vulnerables en un S.I.: Hw, Sw, Datos.

Seguridad es un concepto asociado a la certeza, falta de riesgo o contingencia conviene aclarar que no siendo posible la certeza absoluta el elemento de riesgo está siempre presente independientemente de las medidas que tomemos por lo que debemos hablar de niveles de seguridad, la seguridad absoluta no es posible y en adelante se debe entender que la seguridad informática es un conjunto de técnicas encaminadas a obtener niveles altos de seguridad, la seguridad es un problema integral, los problemas de seguridad informática no pueden ser tratados aisladamente ya que la seguridad de todo el sistema es igual a su punto más débil.

El uso de sofisticados algoritmos y métodos es inútil si no garantizamos la confidencialidad de las estaciones de trabajo, por otra parte, existe algo que los hackers llaman ingeniería asociada que consiste simplemente en conseguir mediante un engaño que los usuarios autorizados revelen sus passwords, por lo tanto la educación de los usuarios es fundamental para que la tecnología de seguridad pueda funcionar.

Los tres elementos principales a proteger en cualquier sistema informático son el software, el hardware y los datos. Por hardware entendemos el conjunto de todos los elementos físicos de un sistema informático como CPU, terminales,

cableados, medios de almacenamiento secundarios, tarjeta de red, etc... Por software se entiende, el conjunto de programas lógicos que hacen funcionar el hardware tanto sistemas operativos como aplicaciones y por datos el conjunto de información lógica que3 Amenazas Física maneja el software y el hardware como por ejemplo paquetes que circulan por un cable de red o entradas de una base de datos.

Habitualmente los datos constituyen los 3 principales elementos a escoger ya que es el más amenazado y seguramente el más difícil de recuperar. También tenemos que ser conscientes de que las medidas de seguridad que deberán establecerse comprenden el hardware el sistema operativo, las comunicaciones, medidas de seguridad física, controles organizativos y legales.

4.3 MARCO JURÍDICO

El Capítulo cuarto de la Constitución del Ecuador; Título Soberanía económica; Sección octava, establece el marco jurídico sobre el Sistema Financiero Nacional, reza:

Art. 308.- Las actividades financieras son un servicio de orden público, podrán ejercerse, previa autorización del Estado, de acuerdo con la ley; tendrán la finalidad fundamental de preservar los depósitos y atender los requerimientos de financiamiento para la consecución de los objetivos de desarrollo del país. Las actividades financieras intermediarán de forma eficiente los recursos captados para fortalecer la inversión productiva nacional, y el consumo social y ambientalmente responsable.

El Estado fomentará el acceso a los servicios financieros y a la democratización del crédito. Se prohíben las prácticas colusorias, el anatocismo y la usura. La regulación y el control del sector financiero privado no trasladarán la responsabilidad de la solvencia bancaria ni supondrán garantía alguna del Estado. Las administradoras y administradores de las instituciones financieras y quienes controlen su capital serán responsables de su solvencia.

Se prohíbe el congelamiento o la retención arbitraria o generalizada de los fondos o depósitos en las instituciones financieras públicas o privadas.

Art. 309.- El sistema financiero nacional se compone de los sectores público, privado, y del popular y solidario, que intermedian recursos del público. Cada uno de estos sectores contará con normas y entidades de control específicas y diferenciadas, que se encargarán de preservar su seguridad, estabilidad, transparencia y solidez. Estas entidades serán autónomas. Los directivos de las entidades de control serán responsables administrativa, civil y penalmente por sus decisiones.

Art. 310.- El sector financiero público tendrá como finalidad la prestación sustentable, eficiente, accesible y equitativa de servicios financieros. El crédito que otorgue se orientará de manera preferente a incrementar la productividad y competitividad de los sectores productivos que permitan alcanzar los objetivos del Plan de Desarrollo y de los grupos menos favorecidos, a fin de impulsar su inclusión activa en la economía.

Art. 311.- EI sector financiero popular y solidario se compondrá de cooperativas de ahorro y crédito, entidades asociativas o solidarias, cajas y bancos comunales, cajas de ahorro. Las iniciativas de servicios del sector financiero popular y solidario, y de las micro, pequeñas y medianas unidades productivas, recibirán un tratamiento diferenciado y preferencial del Estado, en la medida en que impulsen el desarrollo de la economía popular y solidaria.

Art. 312.- Las entidades o grupos financieros no podrán poseer participaciones permanentes, totales o parciales, en empresas ajenas a la actividad financiera.

Se prohíbe la participación en el control del capital, la inversión o el patrimonio de los medios de comunicación social, a entidades o grupos financieros, sus representantes legales, miembros de su directorio y accionistas.

Cada entidad integrante del sistema financiero nacional tendrá una defensora o defensor del cliente, que será independiente de la institución y designado de acuerdo con la ley [51]

De acuerdo marco legal y jurídico establecido en la Constitución de la República del Ecuador, la finalidad principal del Sistema Financiero Nacional es cuidar o preservar los depósitos del público y atender las necesidades de financiamiento de los sectores de desarrollo del país fortaleciendo la inversión productiva nacional y el consumo social ambientalmente responsable.

Determina de una forma general las normas generales de la actividad financiera en el país. La ley general de instituciones de instituciones del sistema financiero, regula, la creación, organización, de actividades y funcionamiento del sistema financiero. La codificación de resoluciones de la Superintendencia de Bancos del Ecuador y la Junta Bancaria. Son normas específicas para el correcto funcionamiento de las instituciones financieras.

En relación a la tipificación del delito en Ecuador, en el Sistema Jurídico Ecuatoriano actual, está tipificado en el Código Orgánico Integral Penal, las conductas ilícitas, acceso ilegal a sistemas informáticos, interceptación ilegal

[51]. *Ibid.,* p. 2

de los comunicadores, daños en sistemas informáticos, fraude electrónico, fraude en telecomunicaciones, entre otros. Este cuerpo jurídico establece:

> *Artículo 190.- Apropiación fraudulenta por medios electrónicos.- La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años. La misma sanción se impondrá si la infracción se comete con inutilización de sistemas de alarma o guarda, descubrimiento o descifrado de claves secretas o encriptadas, utilización de tarjetas magnéticas o perforadas, utilización de controles o instrumentos de apertura a distancia, o violación de seguridades electrónicas, informáticas u otras semejantes.*
>
> *Artículo 191.- Reprogramación o modificación de información de equipos terminales móviles.- La persona que reprograme o modifique la información de identificación de los equipos terminales móviles, será sancionada con pena privativa de libertad de uno a tres años.*
>
> *Artículo 192.- Intercambio, comercialización o compra de información de equipos terminales móviles.- La persona que intercambie, comercialice o compre bases de datos que contengan Código Orgánico Integral Penal 85 información de identificación de equipos terminales móviles, será sancionada con pena privativa de libertad de uno a tres años.*
>
> *Artículo 193.- Reemplazo de identificación de terminales móviles.- La persona que reemplace las etiquetas de fabricación de los terminales móviles que contienen información de identificación de dichos equipos y coloque en su lugar otras etiquetas con información de identificación falsa o diferente a la original, será sancionada con pena privativa de libertad de uno a tres años. Artículo*
>
> *194.- Comercialización ilícita de terminales móviles.- La persona que comercialice terminales móviles con violación de las disposiciones y procedimientos previstos en la normativa emitida por la autoridad competente de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años.*

En concordancia con este cuerpo legal, el mismo COIP desde el artículo 229 hasta el 234, establece la legislación siguiente:

Artículo 229 nos habla sobre la revelación ilegal de base de datos, en la cual estipula que la persona que revela información para su propio provecho o de terceras personas, la cual es información registrada y calificada como secreta, en la cual se viole la intimidad y privacidad de uno o más individuos. A este delito se le da una pena privativa de libertad de uno a tres años.

Si el delito fuere cometido por un servidor público, o algún empleado bancario o de institución de economía popular la pena será de tres a cinco años. En el artículo 92 inciso 2 de la Constitución nos indica: "Las personas responsables de los bancos o archivos de datos personales podrán difundir la información archivada con autorización de su titular o de la ley." Es decir con autorización de su titular o en su defecto de la Ley.

Artículo 230 "Interceptación ilegal de datos" en este artículo ya nos indica que la pena será de tres a cinco años cuando una persona para su beneficio propio o de tercero, se apropie, grabe, intercepte u observe cualquier tipo de dato informático, así como la que diseñe, venda, promocione todo tipo páginas electrónicas, enlaces y todo tipo de mecanismos para que incite al usuario a acceder a una dirección o sitio de internet diferente a la que desea acceder. La persona responsable de clonar, que comercialicen tipos de bandas magnéticas como los las tarjetas de crédito, débito o pago así como los chips u algún otro dispositivo así como las que se encargan en fabricar, producir, distribuir este tipo de instrumentos para poder cometer el delito ya descrito.

Articulo 92 incisos 3 "En el caso de datos sensibles, cuyo archivo deberá estar autorizado por la ley o por la persona titular, se exigirá la adopción de las medidas de seguridad necesarias. Si no se atendiera su solicitud, ésta podrá acudir a la jueza o juez. La persona afectada podrá demandar por los perjuicios ocasionados."

La transferencia electrónica de activo patrimonial no es más que apropiarse de un activo patrimonial de otra persona sin el consentimiento de la misma, en la cual se perjudique a esta o a terceros, por medio de modificación, manipulación del programa informático, o mensaje de datos, para apropiarse. Este delito será penado con libertad privativa de tres a cinco años, y si la persona diere su consentimiento para enriquecer su activo patrimonial por medio de una transferencia electrónica será sancionado con la misma pena. Esto se encuentra tipificado en el artículo 231 del COIP.

La persona que cause y provoque el mal funcionamiento, suprima datos informáticos, destruya, deteriore, borre, mensajes de correos electrónicos, de sistemas de tratamiento de información, o de telecomunicaciones, ya sea a todo o partes de los componentes que lo rigen, la persona que diseñe, programe, envié, adquiera, venda, distribuye de cualquier manera los programas maliciosos destinados a causar el daño ya indicado será sancionada con una pena de tres a cinco años de privativa de libertad.

Esto lo encontramos en el COIP en el artículo 232. Si fuera cometida esta infracción sobre bienes informáticos de algún servicio público o vinculado con la seguridad ciudadana la pena será de cinco a siete años de privación de libertad.

Artículo 233.- Delitos contra la información pública reservada legalmente.- "La persona que destruya o inutilice información clasificada de conformidad con la Ley, será sancionada con pena privativa de libertad de cinco a siete años. La o el servidor público que, utilizando cualquier medio electrónico o informático, obtenga este tipo de información, será sancionado con pena privativa de libertad de tres a cinco años.

Cuando se trate de información reservada, cuya revelación pueda comprometer gravemente la seguridad del Estado, la o el servidor público encargado de la custodia o utilización legítima de la información que sin la autorización correspondiente revele dicha información, será sancionado con pena privativa de libertad de siete a diez años y la inhabilitación para ejercer un cargo o función pública por seis meses, siempre que no se configure otra infracción de mayor gravedad".

En el Artículo 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.- "La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años". [52]

Concatenante, con el cuerpo legal expuesto en el Código Integral Penal (COIP) en relación a la Normativa de seguridad que establece la Superintendencia de Bancos del Ecuador para la instituciones del Sistema Financiero en el Ecuador, se estable en el LIBRO I.- NORMAS GENERALES PARA LAS INSTITUCIONES DEL SISTEMA FINANCIERO TITULO X.- DE LA GESTIÓN Y ADMINISTRACIÓN DE RIESGOS CAPÍTULO V.- DE LA GESTIÓN DEL RIESGO OPERATIVO (incluido con resolución No JB-2005-834 de 20 de octubre del 2005

El artículo 4 se establece que con el propósito de que se minimice la probabilidad de incurrir en pérdidas financieras atribuibles al riesgo

[52]. *Ibid.*, p. 2

operativo, deben ser adecuadamente administrados los siguientes aspectos, los cuales se interrelacionan entre sí:

4.3.5 Medidas de seguridad en canales electrónicos.- Con el objeto de garantizar que las transacciones realizadas a través de canales electrónicos cuenten con los controles, medidas y elementos de seguridad para evitar el cometimiento de eventos fraudulentos y garantizar la seguridad y calidad de la información de los usuarios

4.3.5.1. Las instituciones del sistema financiero deberán adoptar e implementar los estándares y buenas prácticas internacionales de seguridad vigentes a nivel mundial para el uso y manejo de canales electrónicos y consumos con tarjetas, los cuales deben ser permanentemente monitoreados para asegurar su cumplimiento; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.5.2. Establecer procedimientos y mecanismos para monitorear de manera periódica la efectividad de los niveles de seguridad implementados en hardware, software, redes y comunicaciones, así como en cualquier otro elemento electrónico o tecnológico utilizado en los canales electrónicos, de tal manera que se garantice permanentemente la seguridad y calidad de la información; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.5.3. Canales de comunicación seguros mediante la utilización de técnicas de encriptación acorde con los estándares internacionales vigentes; (incluido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.5.4. El envío de información de sus clientes relacionada con al menos números de cuentas y tarjetas, debe ser realizado bajo condiciones de seguridad de la información, considerando que cuando dicha información se envíe mediante correo electrónico o utilizando algún otro medio vía Internet, ésta deberá ser enmascarada; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012 y reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.5.5. La información confidencial que se transmita entre el canal electrónico y el sitio principal de procesamiento de la entidad, deberá estar en todo momento protegida mediante el uso de técnicas de encriptación acordes con los estándares internacionales vigentes y deberá evaluarse con regularidad la efectividad del mecanismo utilizado; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012 y reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.5.6. Las instituciones del sistema financiero deberán contar en todos sus canales electrónicos con software antimalware que esté permanentemente actualizado, el cual permita proteger el software instalado, detectar oportunamente cualquier intento o alteración en su código, configuración y/o funcionalidad, y emitir las alarmas

correspondientes para el bloqueo del canal electrónico, su inactivación y revisión oportuna por parte de personal técnico autorizado de la institución; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.5.7. Las instituciones del sistema financiero deberán utilizar tecnología de propósito específico para la generación y validación de claves para ejecutar transacciones en los diferentes canales electrónicos y dicha información en todo momento debe estar encriptada; (incluido con resolución No. JB- 2012-2148 de 26 de abril del 2012 y reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.5.8. Establecer procedimientos para monitorear, controlar y emitir alarmas en línea que informen oportunamente sobre el estado de los canales electrónicos, con el fin de identificar eventos inusuales, fraudulentos o corregir las fallas; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.5.9. Ofrecer a los clientes los mecanismos necesarios para que personalicen las condiciones bajo las cuales desean realizar sus transacciones que impliquen movimiento de dinero a través de los diferentes canales electrónicos y tarjetas, dentro de las condiciones o límites máximos que deberá establecer cada entidad. (reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

Entre las principales condiciones de personalización por cada tipo de canal electrónico, deberá constar: el registro de las cuentas a las cuales desea realizar transacciones monetarias, números de suministros de servicios básicos, números de telefonía fija y móvil, montos máximos por transacción diaria, semanal y mensual, entre otros. (sustituido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

Para el caso de consumos con tarjetas, se deberán personalizar los cupos máximos, principalmente para los siguientes servicios: consumos nacionales, consumos en el exterior, compras por internet, entre otros; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.5.10. Requerir a los clientes que el registro y modificación de la información referente a su número de telefonía móvil y correo electrónico, se realicen por canales presenciales, además no se debe mostrar esta información por ningún canal electrónico; (incluido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.5.11. Las instituciones del sistema financiero deben registrar las direcciones IP y números de telefonía móvil desde las que se realizan las transacciones. Para permitir transacciones desde direcciones IP y telefonía móvil de otros países se debe tener la autorización expresa del cliente; (incluido con resolución No. JB- 2014-3066 de 2 de septiembre del 2014)

4.3.5.12. Incorporar en los procedimientos de administración de seguridad de la información la renovación de por lo menos una vez (1) al año de las claves de acceso a los canales electrónicos, la clave de banca electrónica debe ser diferente de aquella por la cual se accede a otros canales electrónicos

4.3.5.13. Las instituciones deberán establecer procedimientos de control y mecanismos que permitan registrar el perfil de cada cliente sobre sus comportamientos transacciones que impliquen movimiento de dinero en el uso de canales electrónicos y tarjetas y definir procedimientos para monitorear en línea y permitir o rechazar de manera oportuna la ejecución de transacciones que impliquen movimiento de dinero que no correspondan a sus hábitos, lo cual deberá ser inmediatamente notificado al cliente mediante mensajería móvil, correo electrónico, u otro mecanismo; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012 y reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.5.14. Incorporar en los procedimientos de administración de la seguridad de la información, el bloqueo de los canales electrónicos o de las tarjetas cuando se presenten eventos inusuales que adviertan situaciones fraudulentas o después de un número máximo de tres (3) intentos de acceso fallido. Además, se deberán establecer procedimientos que permitan la notificación en línea al cliente a través de mensajería móvil, correo electrónico u otro mecanismo, así como su reactivación de manera segura; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.5.15. Asegurar que exista una adecuada segregación de funciones entre el personal que administra, opera, mantiene y en general accede a los dispositivos y sistemas usados en los diferentes canales electrónicos y tarjetas; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.5.16. Las entidades deberán establecer procedimientos y controles para la administración, transporte, instalación y mantenimiento de los elementos y dispositivos que permiten el uso de los canales electrónicos y de tarjetas; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.5.17. Las instituciones del sistema financiero deben mantener sincronizados todos los relojes de sus sistemas de información que estén involucrados con el uso de canales electrónicos; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.5.18. Mantener como mínimo durante doce (12) meses el registro histórico de todas las transacciones que se realicen a través de los canales electrónicos, el cual deberá contener como mínimo: fecha, hora, monto, números de cuenta (origen y destino en caso de aplicarse), código de la institución del sistema financiero de origen y de destino, número de

transacción, código del dispositivo: para operaciones por cajero automático: código del ATM, para transacciones por internet: la dirección IP, para transacciones a través de sistemas de audio respuesta - IVR y para transacciones de banca electrónica mediante dispositivos móviles: el número de teléfono con el que se hizo la conexión.

4.3.5.19. Incorporar en los procedimientos de administración de la seguridad de la información, controles para impedir que funcionarios de la entidad que no estén debidamente autorizados tengan acceso a consultar información confidencial de los clientes en ambiente de producción. En el caso de información contenida en ambientes de desarrollo y pruebas, ésta deberá ser enmascarada o codificada. Todos estos procedimientos deberán estar debidamente documentados en los manuales respectivos. Además, la entidad deberá mantener y monitorear un log de auditoría sobre las consultas realizadas por los funcionarios a la información confidencial de los clientes, la cual debe contener como mínimo: identificación del funcionario, sistema utilizado, identificación del equipo (IP), fecha, hora, e información consultada. Esta información deberá conservarse por lo menos por doce (12) meses; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.5.20. Las instituciones del sistema financiero deberán poner a disposición de sus clientes un acceso directo como parte de su centro de atención telefónica (call center) para el reporte de emergencias bancarias, el cual deberá funcionar las veinticuatro (24) horas al día, los siete (7) días de la semana; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.5.21. Mantener por lo menos durante seis (6) meses la grabación de las llamadas telefónicas realizadas por los clientes a los centros de atención telefónica (call center), específicamente cuando se consulten saldos, consumos o cupos disponibles; se realicen reclamos; se reporten emergencias bancarias; o, cuando se actualice su información. De presentarse reclamos, esa información deberá conservarse hasta que se agoten las instancias legales; (incluido con resolución No. JB-2012-2148 de 26 abril del 2012)

4.3.5.22. Las entidades deberán implementar los controles necesarios para que la información de claves ingresadas por los clientes mediante sistemas de audio respuesta IVR), estén sometidas a técnicas de encriptación acordes con los estándares internacionales vigentes; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.5.23. Las instituciones del sistema financiero deberán enviar a sus clientes mensajes en línea a través de mensajería móvil, correo electrónico u otro mecanismo, notificando el acceso y la ejecución de transacciones realizadas mediante cualquiera de los canales electrónicos disponibles, o por medio de tarjetas

4.3.5.26. Informar y capacitar permanentemente a los clientes sobre los procedimientos para el bloqueo, inactivación, reactivación y cancelación de los canales electrónicos ofrecidos por la entidad; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012 y reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.5.27. Es función de auditoría interna verificar oportunamente la efectividad de las medidas de seguridad que las instituciones del sistema financiero deben implementar en sus canales electrónicos; así también deberán informar sobre las medidas correctivas establecidas en los casos de reclamos de los usuarios financieros que involucren debilidades o violación de los niveles de seguridad; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.5.28. Implementar técnicas de seguridad de la información en los procesos de desarrollo de las aplicaciones que soportan los canales electrónicos, con base en directrices de codificación segura a fin de que en estos procesos se contemple la prevención de vulnerabilidades; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.5.29. En todo momento en donde se solicite el ingreso de una clave, ésta debe aparecer enmascarada[53]

En relación al cuerpo legal en el que se sustentan los actuales sistemas de seguridad que se utilizan en Ecuador para prevenir los delitos informáticos en el sector financiero**,** la Superintendencia de Bancos se establecen en el LIBRO I.- NORMAS GENERALES PARA LAS INSTITUCIONES DEL SISTEMA FINANCIERO: SECCIÓN VII.- DE LAS MEDIDAS DE SEGURIDAD (incluida con Resolución No. JB-2011- 1851 de 11 de enero del 2011)

ARTÍCULO 33.- Sin perjuicio de la instalación de aquellas medidas de seguridad y protección que por propia iniciativa estimen convenientes y adecuadas, toda institución financiera deberá adoptar en cada uno de sus establecimientos las medidas mínimas de seguridad que se detallan a continuación:

33.1 Medidas generales de seguridad.- Las instituciones financieras deberán establecer medidas mínimas de seguridad, que:

[53]. T LIBRO I.- NORMAS GENERALES PARA LAS INSTITUCIONES DEL SISTEMA FINANCIERO ITULO X.- DE LA GESTIÓN Y ADMINISTRACIÓN DE RIESGOS CAPÍTULO V.- DE LA GESTIÓN DEL RIESGO OPERATIVO (incluido con resolución No JB-2005-834 de 20 de octubre del 2005

33.1.1. Incluyan la instalación y funcionamiento de dispositivos, mecanismos y equipos, con el objeto de contar con la protección requerida en los establecimientos, para clientes, empleados, público y patrimonio, estableciendo parámetros de acuerdo a la ubicación del establecimiento;

33.1.2. En todo tiempo cuenten con sistemas de seguridad acordes con las disponibilidades técnicas del momento;

33.1.3. Cuenten con áreas seguras de iluminación adecuada y suficiente. En los lugares en donde se maneje efectivo, como bóvedas, cajas, cajeros automáticos, autobancos y consignatarios nocturnos, deberá reforzarse la iluminación y seguridad, debiendo asegurar la iluminación permanente de estos puntos ante un eventual corte de suministro eléctrico;

33.1.4. Mantengan controles de acceso al establecimiento, en caso de que presten servicio al público;

33.1.5. Las puertas de entrada a la entidad financiera deben estar equipadas con dos cerraduras con llaves codificadas o de seguridad, a fin de requerir la presencia de dos personas al momento de la apertura y cierre de sus operaciones;

33.1.6. Establezcan efectivos sistemas de seguridad y vigilancia en el interior de sus instalaciones, con guardias de empresas de seguridad privada, efectivos de la Policía Nacional o personal de seguridad de la propia entidad; (sustituido con resolución No. JB-2011-1923 de 26 de abril del 2011)

33.1.7. El área de cajas deberá ser de acceso restringido al público, al personal no autorizado de la entidad y estar ubicada de tal forma que se minimicen los

33.1.7. El área de cajas deberá ser de acceso restringido al público, al personal no autorizado de la entidad y estar ubicada de tal forma que se minimicen los riesgos de que terceras personas realicen sustracciones de dinero u otras actividades ilícitas; y, (reformado con resolución No. JB-2011-1923 de 26 de abril del 2011)

33.1.8. Garanticen el cumplimiento de la prohibición de que los funcionarios del área de cajeros porten teléfonos celulares, localizadores o beepers de uso personal. Se permite el uso de medios de comunicación bajo el control y supervisión de la entidad.

ARTICULO 34.- Las instituciones financieras contarán con "Manuales y políticas de seguridad y protección", que deben ser aprobados por el directorio u organismo que haga sus veces y que deben contener por lo menos los siguientes aspectos fundamentales para la seguridad de las instituciones, en particular de sus empleados y usuarios,

establecimientos, bienes y patrimonio, así como para el resguardo en el transporte de efectivo y valores:

34.1 Las políticas, normas, principios y procesos básicos conforme a los cuales las entidades bancarias deben formular sus medidas de seguridad y protección;

34.2 Las medidas mínimas de seguridad contenidas en el presente capítulo, precisando sus características, y en su caso, dimensiones y calidad de los materiales;

34.3 Las demás medidas de seguridad que las entidades deseen adoptar como adicionales a las contenidas en el presente capítulo;

34.4 Los criterios para el diseño y construcción de sus establecimientos, incluyendo la instalación, funcionamiento y control de dispositivos, mecanismos, centros de procesos de datos y de comunicación y equipo técnico de protección para la prestación de los servicios que le corresponda;

34.5 Los procesos, sistemas y controles operativos para la prevención y detección de irregularidades en la realización de sus operaciones y en el manejo de los recursos, efectivo y valores que tengan bajo su responsabilidad;

34.6 Las características que deberán reunir los sistemas de monitoreo y alarma, incluyendo los índices de calidad y disponibilidad, así como las demás características técnicas o tecnológicas necesarias para la efectiva emisión y transmisión de las señales e imágenes;

34.7 Los aspectos relativos a la seguridad de la información, tales como la seguridad Física, lógica de redes y comunicación, entre otros;

34.8 Los criterios para la selección, reclutamiento y capacitación del recurso humano, así como para la contratación de servicios profesionales para brindar seguridad y protección a los establecimientos;

34.9 Los lineamientos y planes de capacitación e información al personal que labora en sus entidades, específicamente respecto del entrenamiento en caso de siniestros o durante la comisión de un delito, estos deberán actualizarse por lo menos una (1) vez al año;

34.10 Los dispositivos, sistemas y procedimientos para controlar la entrada y salida de los empleados de la entidad; [54]

[54]. SUPERINTENDENCIA DE BANCOS DEL ECUADOR, LIBRO I.- NORMAS GENERALES PARA LAS INSTITUCIONES DEL SISTEMA FINANCIERO: *SECCIÓN VII.- DE LAS MEDIDAS DE SEGURIDAD (incluida con resolución No. JB-2011- 1851 de 11 de enero del 2011)*

De la exposición y análisis, se infiere que en el COIP se han tipificado delitos informáticos no solo buscando la protección de derechos constitucionales y bienes jurídicos conocidos tradicionalmente, como es por ejemplo el derecho a la propiedad, sino también el derecho de información, que se lo cataloga como un “derecho del buen vivir”. En esta línea, los delitos que afectan a los clientes de la banca como en el caso de investigación, resultan no solo delitos contra la propiedad sino también delitos contra la información, ya que como se advertirá actualmente la simple interceptación de datos así no tenga el ánimo de lucro constituyen delito. Esta idea no es nueva, como Rovira del Canto nos recuerda:

“Los ilícitos informáticos en este campo se han venido considerando, por tanto, como delitos económicos, con todas sus características fundamentales comunes, incluido el elemento subjetivo del ánimo de lucro, en los que lo informático era el calificativo de aquéllos, atendidas, normalmente, las peculiaridades de su medios comisivos y en cuanto afectaban a elementos no corpóreos: la información y los datos.

Sin embargo, en la estructuración actual de los delitos de riesgo informático y de la información, sobre la base de su caracterización y conceptualización en torno a los nuevos bienes jurídicos requeridos de protección jurídico penal (la información en sí misma, los datos informáticos, y la seguridad y fiabilidad en los sistemas informáticos y telemáticos), es al término actual del delito informático a la que debemos aplicar el calificativo de económico, y no al revés, y que comprenden aquellos comportamientos ilícitos informáticos en el ámbito económico/patrimonial, y referirnos consecuentemente a los mismos como delitos informáticos económicos patrimoniales.

En cuanto a la al Marco legal para el proceso y penalización de los delitos informáticos la Constitución Política de la República, en su Título IV, Capitulo 4to, en la sección décima al hablar de la Fiscalía General del Estado, en su Art. 195 señala que:

> *"La Fiscalía dirigirá, de oficio o a petición de parte la investigación pre procesal y procesal penal……". Esto en concordancia con el Art. 33 del Código de Procedimiento Penal que señala que "el ejercicio de la acción pública corresponde exclusivamente al fiscal". De lo dicho podemos concluir que el dueño de la acción penal y de la investigación tanto preprocesal como procesal de hechos que sean considerados como delitos dentro del nuevo Sistema Procesal Penal Acusatorio es el Fiscal. Es por tanto el Fiscal quien deberá llevar como quien dice la voz cantante dentro de la investigación de esta clase de infracciones de tipo informático para lo cual contara como señala el Art. 208 del Código de Procedimiento Penal con su órgano auxiliar la Policía Judicial quien realizará la investigación de los delitos de acción pública y de instancia particular bajo la dirección y control de la Fiscalía, en tal virtud cualquier resultado de dichas investigaciones se incorporaran en su tiempo ya sea a la Instrucción Fiscal o a la Indagación Previa, esto como parte de los elementos de convicción que ayudaran posteriormente al representante de la Fiscalía a emitir su dictamen correspondiente.* [55]

Respecto a la penalización de los delitos informáticos en el Código Orgánico Integral Penal (COIP), en el Titulo X. De los Delitos contra la Propiedad. Cap. II. Del Robo. Cap. V De las Estafas y otras defraudaciones, establece

> *"Utilización fraudulenta de sistemas de información o redes electrónicas. n PRISION 6 MESES A 5 AÑOS n MULTA 500 A 1000 USD Y SI EMPLEA LOS SIGUIENTES MEDIOS: n Inutilización de sistemas de alarma o guarda n Descubrimiento o descifrado de claves secretas o encriptadas n Utilización de tarjetas magnéticas o perforadas n Utilización de controles o instrumentos de apertura a distancia, y, Violación de seguridades electrónicas.*
>
> *Artículo 63.- A continuación del artículo 553 del Código Penal, añádanse los siguientes artículos innumerados: Art. Apropiación Ilícita.- Serán*

[55]LIBRO I.- NORMAS GENERALES PARA LAS INSTITUCIONES DEL SISTEMA FINANCIERO: *SECCIÓN VII.- DE LAS MEDIDAS DE SEGURIDAD (incluida con resolución No. JB-2011- 1851 de 11 de enero del 2011)*

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.

Art. 64.- La pena será de prisión de uno a cinco años y multa de mil a dos mil dólares de los 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. [56]

A la luz de lo expuesto en el Marco Jurídico que sustentan el procesamiento y penalización de los Delitos Informáticos que se cometen en el Sistema Financiero del Ecuador, aún no se establece en el Código Orgánico Integral Penal (COIP), la penalización de forma específica de acuerdo al delito sino que se establece una pena de forma general que va de uno a cinco años de cárcel y de uno a dos mil dólares americanos, pena que en la mayoría de los casos es irrisoria si se analiza objetivamente el caso, especialmente cuando el delito cometido ha generado cuantiosas pérdidas de dinero, quiebra de negocios, y en caso extremos hasta pérdidas de vidas humanas.

[56]. CÓDIGO ORGÁNICO INTEGRAL PENAL (COIP), EN EL TITULO X. DE LOS DELITOS CONTRA LA PROPIEDAD. Cap. II. Del Robo. Cap. V De las Estafas y otras defraudaciones

Es importante resaltar también que en algunos casos esta falta de formación por parte de los Fiscales que dirigen las investigaciones como del cuerpo policial que lo auxilia en dicha tarea, es un componente que no abona a la resolución exitosa de estos delitos. En este sentido, recién en el año 2011 se pudo lograr el objetivo de tener aprobado por el Consejo Nacional de Policía Judicial un departamento de policía especializada en esta clase de infracciones así como en la Fiscalía se creó el Departamento de Investigación y Análisis Forense en el año 2008.

Otro aspecto que es importante analizar, es que en la Función Judicial también falta la suficiente preparación por parte de Jueces y Magistrados en tratándose de estos temas, ya que en algunas ocasiones por no decirlo en la mayoría de los casos los llamados a impartir justicia se ven confundidos con la especial particularidad de estos delitos y los confunden con delitos tradicionales que por su estructura típica son incapaces de subsumir a estas nuevas conductas delictivas que tiene a la informática como su medio o fin; así mismo todo lo que tiene que ver con el reconocimiento de la llamada evidencia digital.

Estos Departamentos tanto en la Fiscalía General del Estado como en la Policía Judicial sirven de puntos de contacto nacionales para una cooperación internacional formal o una cooperación informal basada en redes transnacionales de confianza entre los agentes de aplicación de la ley. Lo cual es posible aplicando la Constitución en su artículo 226 y la Ley de Comercio Electrónico Firmas Electrónicas y Mensajes de Datos.

La cooperación multilateral de los grupos especiales multinacionales pueden resultar ser particularmente útiles y ya existen casos en que la cooperación internacional ha sido muy efectiva. De hecho, la cooperación puede engendrar emulación y éxitos adicionales.

De otro lado en los últimos tiempos la masificación de virus informáticos globales, la difusión de la pornografía infantil, los casos de fraudes informáticos e incluso actividades terroristas son algunos ejemplos de los nuevos delitos informáticos y sin fronteras que presentan una realidad difícil de controlar. Con el avance de la tecnología digital en los últimos años, ha surgido una nueva generación de delincuentes que expone a los gobiernos, las empresas y los individuos a estos peligros.

4.4 LEGISLACIÓN COMPARADA

"*Las actividades informáticas delictivas están en crecimiento a nivel global, incluyendo a América Latina*"[57]. "*El incremento de la delincuencia informática encuentra algunas de sus respuestas en una gran variedad de factores, cuyo desarrollo ya ha sido trabajado ampliamente por la doctrina*" [58]. .

El incremento de tecnología disponible, tanto para el delincuente como las víctimas, combinado con el escaso conocimiento o información sobre cómo protegerse de los posibles delitos que se pueden sufrir a través de las nuevas

[57]. NORTON, INFORME SOBRE DELITOS INFORMÁTICOS 2011, URL: http://norton.com/cybercrimereport. - Las víctimas de los delitos informáticos aumentaron de un 10% a un 13% este año entre 2011 a 2012.

[58]. PALAZZI, PABLO ANDRÉS, DELITOS INFORMÁTICOS, AD-HOC, Buenos Aires, 2000.

tecnologías, otorga a los delincuentes las llaves a las puertas de un inmenso campo fértil de potenciales víctimas de ataques. Por otro lado, *el crecimiento sostenido del mercado negro de la información"* [59], funciona como motor que impulsa una importante masa de ataques informáticos, principalmente destinados a obtener bases de datos con información personal. De acuerdo a uno de los estudios de mayor relevancia mundial en delitos informáticos, en el cuál se han entrevistado más de 13.000 adultos en 24 países, para el año 2012, se calculó que los costos directos asociados con los delitos informáticos que afectan a los consumidores en el mundo ascendieron a US$ 110.000 billones en doce meses.

El mismo estudio revela que por cada segundo 18 adultos son víctimas de un delito informático, lo que da como resultado más de un millón y medio de víctimas de delitos informáticos cada día, a nivel mundial. Entre los desafíos citados anteriormente, uno de los más importantes es el hecho que este tipo de delitos pueden ser cometidos sin respetar barreras geográficas o jurisdiccionales.

En este sentido, cualquier delincuente informático puede operar acciones desde un determinado lugar, conectarse a sistemas o equipos en otra parte y finalmente atacar datos o sistemas ubicados en otro lugar. La cadena puede tener indeterminadas variables dependiendo de la complejidad del ataque y de los conocimientos del delincuente. Si bien esta situación no sucede en todos los casos, es relativamente sencillo realizar estos ataques en la actualidad para

[59]. PALAZZI, PABLO ANDRÉS, DELITOS INFORMÁTICOS, AD-HOC, Buenos Aires, 2000.

personas con conocimientos en informática. Esto representa para el Derecho un verdadero desafío a vencer

En este contexto se establece comparación de esta variable objeto de estudio: Delitos informáticos, con otras legislaciones de otros países del Contexto Regional e internacional.

A partir de Junio de 2008, la Ley 26.388 conocida como la “ley de delitos informáticos” ha incorporado y realizado una serie de modificaciones al Código Penal argentino. Es decir, la misma no regula este tipo de delitos en un cuerpo normativo separado del Código Penal (CP) con figuras propias o independientes, sino que dicha ley modifica, sustituye e incorpora figuras típicas a diversos artículos del CP actualmente en vigencia. Se modificó el Epígrafe del Capítulo III cuyo nuevo título es *"Violación de Secretos y de la Privacidad",* Los artículos que modifica o agrega son: 128, 153, 153 bis, 155, 157, 157 bis, 173, 183, 184, 197, 255. El art. 157 bis ya había sido incorporado por la Ley 25.326 de Protección de Datos Personales (2000) pero fue modificado por la Ley 26.388.[60]

La Ley 1.768 realiza una reforma general al Código Penal. Allí incorpora como Capítulo XI, del Título XII, del Libro Segundo del Código Penal, el de "DELITOS INFORMÁTICOS". Dentro de este capítulo, se incorporan 2 artículos: 363 bis y ter, en cuyos textos se tipifica algunos delitos informáticos. [61]

[60] Argentina Código Penal, Ley 26.388 (2008), Ley 25.326 (2000)
[61] Bolivia Código Penal, Ley 1.768 (1997), Ley 3325 (2006)

La Ley 12.737 es una ley reciente (año 2012), en la cual se dispone la tipificación criminal de los delitos informáticos y otras providencias. En su regulación incorpora modificaciones para los artículos 154-A, 154-B, 266 y 298. Por su parte, la Ley 11.829 regula el Estatuto de la Niñez y la Adolescencia, para mejorar la lucha contra la producción, venta y distribución de pornografía infantil, así como tipificar como delito la adquisición y posesión de dicho material y otros comportamientos relacionados con la pedofilia en Internet. [62]

La Ley 19.223 es una ley "Relativa a Delitos Informáticos" de acuerdo a su propio título, donde regula cuatro artículos, desde los cuáles se tipifican varios delitos informáticos. La Ley 20.009 regula la responsabilidad para el caso de robo, hurto o extravío de tarjetas de crédito, en cuyo texto se sancionan algunas conductas relacionadas con estos aspectos. La Ley 18.168 (modificada por diferentes normativas) regula de manera general las telecomunicaciones, incorporando algunos tipos penales sobre la interferencia o captación ilegítima de señales de comunicación. [63]

La ley 1.273, de reciente sanción legislativa (año 2009), modifica el Código Penal, creando un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos". Se afirma que dicha normativa busca preservar integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones. A través de esta incorporación, suma el CAPITULO I, titulado "De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos", a partir del cual

[62] Brasil Ley 12.737 (2012), Ley 11.829 (2008)
[63] Chile Ley 19.223 (1993), Ley 20.009 (2005), Ley 18.168 (2002)

regula una serie de artículos penales que van desde el artículo 269A hasta el artículo 269J. Adicionalmente se incorpora el artículo 58, considerando como agravante general “si la realización de alguna de las conductas punibles, se realicen utilizando medios informáticos, electrónicos o telemáticos”. [64]

La Ley 9048 es una modificación importante del Código Penal de este país. Inicialmente reforma los artículos 167, 196, 196 bis, 214, 217 bis, 229 bis y 288 de la Ley Nº 4573. Por otro lado adiciona el inciso 6) al artículo 229 y un artículo 229 ter. Finalmente modifica la sección VIII del título VII del Código Penal, titulándolo "Delitos informáticos y conexos", donde regula desde el art. 230 hasta el art. 236. En esta modificación bastante integral, agrega una importante cantidad de delitos informáticos al Código Penal, desde los más tradicionales hasta algunos más modernos como la Suplantación de Identidad (art. 230) o el espionaje cibernético (art. 231)[65]

No se ha encontrado legislación especial en la materia. No obstante, posee la adaptación de ciertos delitos clásicos a las nuevas modalidades informáticas. Entre ellos pueden citarse los artículos 162 a 165, 180, 184, 185, 220, 237, 260, 283 a 286 y 421. Adicionalmente posee la Ley 51/2008 de Firma Electrónica, en la cual se regula penalmente sobre la falsificación de documentos. [66]

No se ha encontrado legislación especial referida a la materia. Sin embargo, a partir de distintas reformas al Código Penal Paraguayo, se han adaptado

[64] Colombia Ley 1.273 (2009), Ley 1366 (2009)
[65] Costa Rica Ley 9.048 (2012)
[66] Panamá Código Penal y sus reformas; Ley 51 (2008)

algunos delitos para la posibilidad de comisión a través de las nuevas tecnologías y en otros casos se ha incorporado tipos penales específicos (como el caso del art. 175 de Sabotaje de Computadoras). Los artículos son 144, 146, 173 a 175, 188, 189, 220, 239, 248 y 249. [67]

La Ley 27309 incorpora al Código Penal del Perú los Delitos Informáticos, a través de un artículo único que modifica el Título V del Libro Segundo del Código Penal, promulgado por Decreto Legislativo No 635, introduciendo allí los artículos 207 – A – B y C y 208. En otro orden, la Ley 28.251 actualizó e incorporó distintos delitos contra la integridad sexual, entre ellos, tipificando la pornografía infantil, a través de la modificación del art 183-A. Además Perú posee la Ley 28.493 (2005) que regula el uso del correo electrónico no solicitado (spam), sin embargo en la misma no incluye ningún tipo de sanción penal.[68]

No se ha encontrado legislación especial al respecto. Sin embargo, Puerto Rico ha optado por la modificación de los tipos penales clásicos, a fin de adaptarlos para su comisión a través de las nuevas tecnologías. Por otro lado, a través de la Ley de Espionaje Cibernético Nº 1165/2008 si se han incorporado algunos delitos penales especiales para estas figuras relacionados con el espionaje. [69]

Posee una Ley Especial contra Crímenes y Delitos de Alta Tecnología. Dicha norma regula una parte general, conteniendo algunos principios y conceptos, y posteriormente tipifica los delitos informáticos según el bien jurídico afectado.

[67] Paraguay Código Penal – Ley 1.160 (1997), Ley 2.861
[68] Perú Ley 27.309 (2000), Ley 28.251 (2004)
[69] Puerto Rico Ley 146/2012 (Código Penal) + Ley de Espionaje Cibernético 1165 (2008)

Además, incluye un capítulo dedicado al aspecto procesal penal, así como en la propia normativa genera un órgano encargado de la recepción de denuncias, investigación y persecución de los delitos informáticos. [70]

Si bien no se ha encontrado legislación especial en la materia, se han encontrado diferentes normativas parcialmente aplicables a la materia. El art. 7 de la Ley 17.815, afirma que "constituye delito de comunicación la comisión, a través de un medio de comunicación, de un hecho calificado como delito por el Código Penal o por leyes especiales.", permitiendo así la aplicación de los tipos clásicos del CP. La Ley N° 17.520, penaliza el uso indebido de señales destinadas exclusivamente a ser recibidas en régimen de abonados. La Ley Nº 17.815 regula la violencia sexual, comercial o no comercial cometida contra niños, adolescentes e incapaces que contenga la imagen o cualquier otra forma de representación. [71]

Posee una ley especial sobre Delitos Informáticos. Contiene 33 artículos y están clasificados en 5 Capítulos a saber: Contra sistemas que utilizan TI; Contra la propiedad; Contra la privacidad de las personas y las comunicaciones; Contra niños y adolescentes; Contra el orden económico.[72]

En la lista de países analizados, se pueden encontrar las más variadas posturas acerca de este delito. Por ejemplo, además de los elementos básicos

[70] República Dominicana Ley Nº 53-07 (2007)
[71] Uruguay Ley 18.600 (2009), Ley 17.520 (2002), Ley 17.815 (2004), Ley 18.383 (2008), Ley 18.515 (2009)
[72] Venezuela Gaceta Oficial Nº 37.313 (2001)

(acceder sin consentimiento a un sistema o dato informático), Bolivia considera que debe existir perjuicio para un tercero. Algunos países como Argentina, exigen que el sistema o dato sea de acceso restringido. Otros como Chile, no lo mencionan. Colombia, expresa en su redacción que el sistema puede ser o no de acceso restringido. Costa Rica comienza afirmando que será delito si hay peligro para la intimidad o privacidad de un tercero. Y otra larga lista de características especiales, que como se puede identificar, requieren de un análisis técnico-jurídico riguroso sobre esta variable de estudio.

5. **MATERIALES Y MÉTODOS**

5.1. MATERIALES

Entre los materiales que se utilizaron para obtener la información están:

Guía de encuesta: Se la aplicó a una muestra seleccionada fueron aplicadas a cien personas conocedoras del tema, entre las que figuran profesionales del derecho de libre ejercicios, jueces de los juzgados de la provincia de Manabí y estudiantes de Derecho del último año de la Universidad Nacional de Loja.

Guía de entrevista: Se la diseñó y utilizó para la entrevista a jueces de lo penal, quienes aportaron con valiosas opiniones y comentarios de acuerdo a su enfoque jurídico y experiencia profesional, criterios que permitieron recopilar información sobre aspectos importantes que contribuyeron con la definición de las conclusiones, recomendaciones y la propuesta legal.

Informe técnico: Este documento permitió realizar un estudio de caso en el que se expone una demanda Contencioso Administrativa, de un fraude informático cometido en un banco de la localidad.

5.2 MÉTODOS

Método Hipotético Deductivo: De acuerdo a las características de la investigación y los datos obtenidos en la indagación y observaciones previas,

se plantea la hipótesis la misma que fue sometida a un proceso de contrastación de enfoque cualitativo.

ANALÍTICO. Se realizó un estudio de cada una de las variables con sus respectivas categorías y subcategorías, su explicación a partir de la observación de un problema, para consecuentemente realizar una hipótesis del mismo, la cual fue verificada a través de los resultados obtenidos en la investigación.

SINTÉTICO: Este complementó el estudio y análisis del problema investigado, puesto que una vez obtenidos y debatidos tanto teórica como cuantitativamente los resultados se realizaron las respectivas verificaciones, alcances y conclusiones del trabajo de investigación.

DESCRIPTIVO:

Este método se lo utilizó en todas las fases de la investigación desde el planteamiento de la problemática en la que se describen las cusas y efectos de la misma, así también en el análisis de los resultados se describen los resultados son descritos de forma expresa y cualitativa.

5.3. PROCEDIMIENTOS Y TÉCNICAS

El estudio se realizará en las fases que a continuación se detallan:

Fase de Investigación previa: En esta fase se puedo determinar la problemática en lo referente a las consecuencias jurídicas que se presentan a causa de la poca especificidad de la Ley para penalizar los delitos

informáticos, en esta fase se utilizará como técnica el diálogo, el mismo que se lo realizó con profesionales conocedores del tema y personas del colectivo púbico que hayan sido víctimas de algún tipo de delito informático en sus cuentas bancarias.

Fase de recolección de datos

En esta fase se recoge la información tanto bibliográfica, documental y de campo, en el desarrollo de esta fase se aplicó técnicas como la encuesta a profesionales y conocedores del tema; la entrevista que fue realizada a especialistas en derecho penal y el estudio de caso, cuya revisión y análisis permitió contrastar la hipótesis, realizar las respectivas conclusiones y reconvenciones así como elaborar la propuesta de Reforma Jurídica al Código Integral Penal.

Fase de elaboración de la Propuesta Legal

En esta fase se revisaron y seleccionaron los fundamentos legales para elaborar la propuesta, la misma que se realizó considerando los resultados de la investigación y las bases legales existentes en el Código Integral Penal y leyes conexas.

6. RESULTADOS

6.1 Resultados de la encuesta aplicada a profesionales de libre ejercicio, especialistas en derecho penal y a estudiantes de los últimos niveles de la carrera de derecho.

Pregunta No. 1

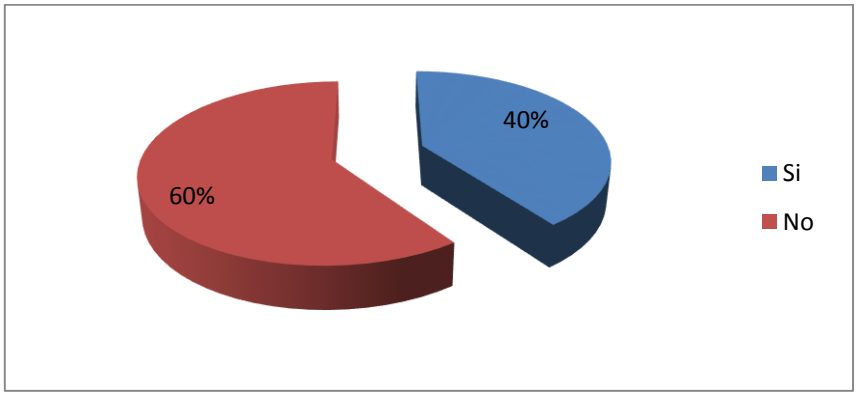
Considera Usted que los delitos informáticos que se pueden cometer en el Sistema Financiero Ecuatoriano, son un tema de conocimiento público?

Tabla No 1

Alternativas	F	%
Si	12	40,00
No	18	60,00
Total	**30**	**100,00**

Fuente: Profesionales y estudiante de derecho
Elaborado por: Autora de la investigación

Gráfico No 1



Interpretación

A esta interrogante 12 de los encuestados que representan el 40,00% de los encuestados respondieron que sí, mientras que 18 de ellos que corresponden al 60,00% indicó que no, que los delitos informáticos que se pueden cometer en sistema financiero no son de conocimiento público.

Análisis

De acuerdo a los resultados se puede deducir, que tanto los profesionales como los entendidos en el tema que fueron encuestados, opinan que el tema sobre delitos informáticos en el sistema financiero, aún no es de conocimiento público, pues consideran que si bien cierto tanto la banca estatal como la privada hacen ciertos anuncios sobre las precauciones que los usuarios deben tener al momento de hacer uso de su cuenta, tarjetas o cualquier medio que pueda ser utilizado por las personas que se dedican a realizar este tipo de delito, existe mucho desconocimiento de los usuarios del sistema sobre los diferentes tipos de delitos informáticos de los que pueden ser víctimas.

Quienes consideran que el tema sobre delitos informáticos en el sistema financiero, es un tema de conocimiento público, fundamentan su respuestas en que las instituciones financieras en especial los bancos, si dan a conocer sobre estos delitos y las precauciones que se debe tener al momento de hacer una transacción o uso de los documentos que el banco le entrega al momento de hacerse socio.

Pregunta No. 2

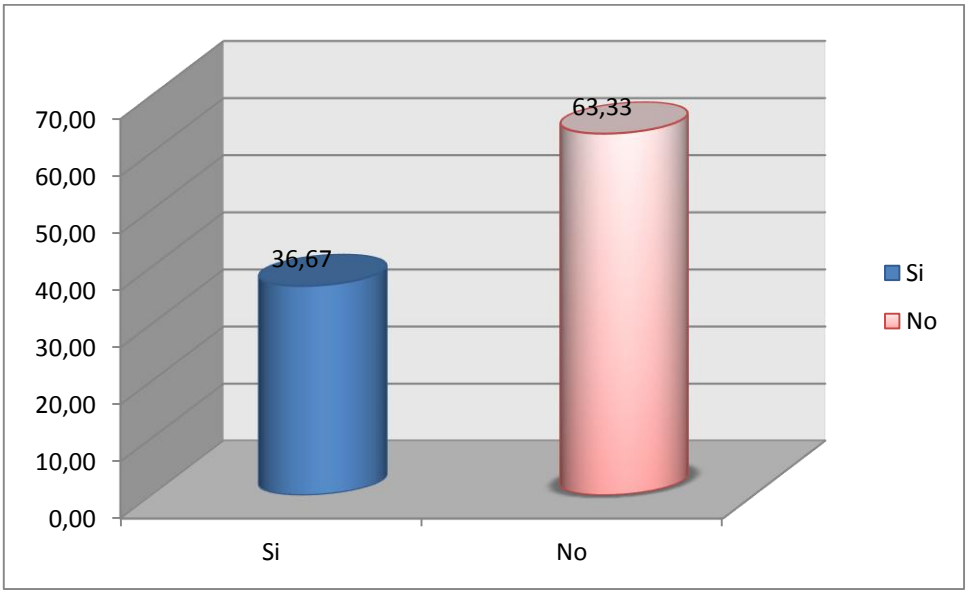
Considera Usted que el sistema jurídico ecuatoriano ampara y respalda eficazmente al sistema financiero a través de las leyes y normas establecidas actualmente.

Tabla No 2

Alternativas	F	%
Si	11	36,67
No	19	63,33
Total	30	100,00

Fuente: Profesionales y estudiante de derecho
Elaborado por: Autora de la investigación

Gráfico No 2



Interpretación

Sobre este aspecto 19 de los encuestados que representan el 63,33%, señalaron que NO consideran que el sistema jurídico ecuatoriano ampara y respalda eficazmente al sistema financiero a través de las leyes y normas

establecidas actualmente. Sin embargo 11 de los profesionales y conocedores del tema que representan el 36,67% a quienes se aplicó la encuesta, indicaron que bajo su punto de vista, el sistema jurídico ecuatoriano logra a través de las leyes que actualmente rigen, amparar eficazmente a los usuarios pues aún los delitos informáticos son un tema que cada día crece en el país.

Interpretación

Las respuestas encontradas muestran que la mayoría de quienes conocen del tema, consideran el sistema jurídico ecuatoriano no ampara y respalda eficazmente al sistema financiero a través de las leyes y normas establecidas actualmente, que estas si se aplican, pero que requieren ser revisadas para mejorarlas e incorporar cambios significativos sobre todo en lo que se refiere a las sanciones pues consideran que las actualmente establecidas son muy generales y flexibles a la hora de juzgar a quienes cometen este tipo de fechorías,

En cuanto a quienes consideran que sistema jurídico ampara y respalda eficazmente al sistema financiero, expresaron que el Código Integral Penal y otras leyes conexas, han tipificado este tipo de delito, por lo tanto, solo es cuestión de aplicar y materializar lo estipulado en cuanto a proceso y penalización de estos delitos.

Pregunta No. 3

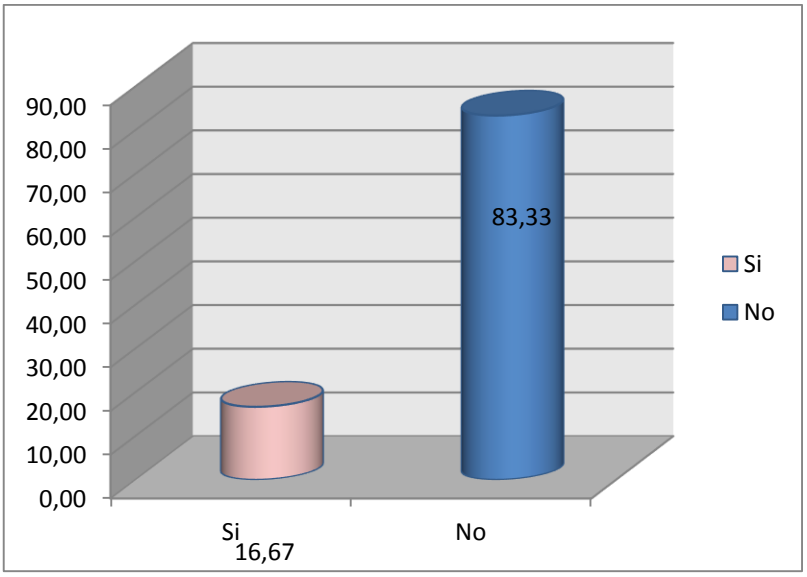
Comparando las diferencias y similitudes que existen entre las bases legales ecuatorianas y los otros países, respecto a los delitos financieros, considera Usted que la Legislación Ecuatoriana sanciona adecuadamente éstos delitos?

Tabla No. 3

Alternativas	F	%
Si	05	16,67
No	25	83,33
Total	30	100

Fuente: Profesionales y estudiante de derecho
Elaborado por: Autora de la investigación

Gráfico No 3



Interpretación

En cuanto a materia de derecho comparado relacionada con delitos informáticos, al cuestionar los profesionales encuestados sobre las similitudes que existen entre las bases legales ecuatorianas y los otros países, respecto a los delitos financieros, 5 de ellos que representan el 16,67% indicaron que

comparada con las leyes de otros países la Legislación Ecuatoriana si sanciona adecuadamente éstos delitos. En relación a la misma interrogante 25 conocedores del tema, que representan el 83,33% de los encuestados de acuerdo a su criterio indicaron que si se compara la Legislación ecuatoriana con la de otros países, las leyes actuales no sancionan adecuadamente este tipo de delito.

Análisis

De acuerdo a los resultados obtenidos se puede determinar que los profesionales y quienes conocen en materia de derecho sobre la penalización de los delitos informáticos en su mayoría consideran que la Legislación Ecuatoriana no penaliza adecuadamente este tipo de delito mucho menos si se compara con el derecho de Costa Rica, Colombia y Chile cuya Legislaciones son mucho más específicas en cuanto a la tipificación y penalización de estos delitos.

En cuanto a quienes consideran que los delitos financieros en la Legislación Ecuatoriana si se sancionan adecuadamente, su criterio se sustenta en la Incorporación y tipificación de los delitos informáticos en Código Integral Penal y no en el Código Civil, se alega que el mismo hecho de que se hayan incorporado como delitos sea procesado y penalizados como tal., de acuerdo a lo que estipula el cuerpo legislativo

Pregunta No. 4

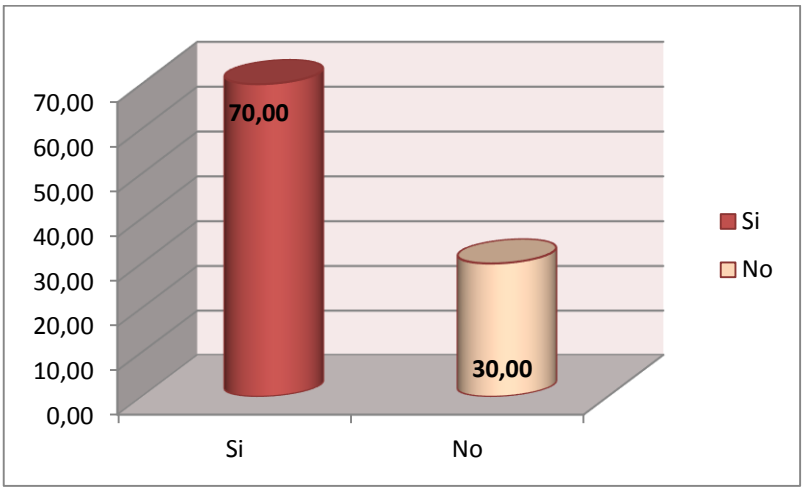
De acuerdo a su criterio jurídico, ¿Cree usted que la tipificación y tratamiento de los delitos informáticos en el sistema financiero nacional, posee falencias que deben ser corregidas por el sistema jurídico ecuatoriano?

Tabla No 4

Alternativas	F	%
Si	21	70,00
No	9	30,00
Total	**30**	**100**

Fuente: Profesionales y estudiante de derecho
Elaborado por: Autora de la investigación

Gráfico No 4



Análisis

A esta interrogante el 70,00% de los encuestados respondieron que si consideran que existen falencias en el Sistema Jurídico Ecuatoriano en cuanto al tratamiento de los delitos informáticos que se cometen en el sistema

financiero; mientras que un 30,00% indicaron que de acuerdo a su criterio no existe falencia en sistema el sistema jurídico ecuatoriano para abordar esto delitos.

Interpretación

Analizando las respuestas positivas podemos analizar varios criterios que nos parecen importantes retomar: *"No existe un cuerpo colegiado preparado al momento de emitir leyes"* sin duda coincidimos que quienes son responsables de crear las leyes, deben ser personas con amplios conocimientos en la materia en que estén legislando; *"El crimen organizado esta siempre delante de las leyes"*, un criterio que es valedero, puesto que en la actualidad los delitos que vemos a diario son perpetradas por personas que invierten grandes sumas de dinero en prepararse; "… quienes cometen delitos informáticos, tienen accesos a información privilegiada…", concordamos con este criterio, puesto que toda protección que el sistema financiero nacional procura para sus clientes, se supone es reservado, sin embargo los cyber-delincuentes conocen la manera de vulnerarlos.

Es importante indicar que las respuestas negativas, en su totalidad indicaron que si bien creen que en la actualidad tenemos una legislación que se adapta a las nuevas circunstancias de un mundo globalizado, creen que es importante que al tratarse de nuevos delitos y nuevas formas de quebrantar la ley, la legislación debe avanzar de manera simultánea, pero que consideran que no existe falencia en las leyes, que el crear más y más leyes, lo único que conlleva un sistema de administración de justicia más lento y con mayores demandas. *"El sistema de justicia debe ser simple y preciso en su administración y no*

buscar cambiar o incrementar leyes a diestra y siniestra", por lo tanto lo más coherente es realizar los ajustes legislativos pertinentes a la ley ya existente

Pregunta No. 5

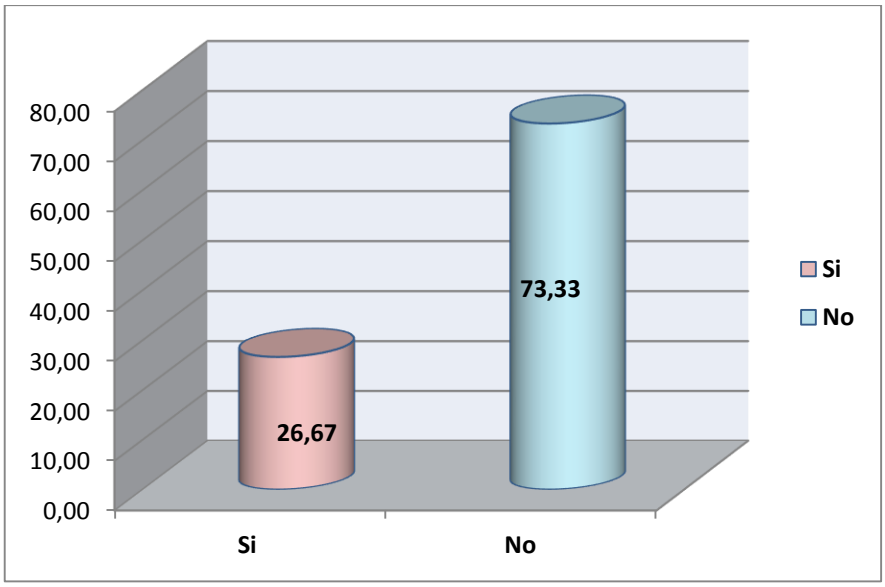
De acuerdo su criterio jurídico, las penas que establece el Código Orgánico Integral, para sancionar los delitos informáticos en el sistema financiero nacional, se encuentran en concordancia con el tipo de delito cometido?

Tabla No 5

Alternativas	F	%
Si	8	26,67
No	22	73,33
Total	30	100,00

Fuente: Profesionales y estudiante de derecho
Elaborado por: Autora de la investigación

Gráfico No 5



Interpretación

A esta interrogante, el 26,67% de los profesiones y conocedores en materia penal que fueron encuestados, respondieron que las penas que establece el Código Orgánico Integral, para sancionar los delitos informáticos en el sistema financiero nacional, se encuentran en concordancia con el tipo de delito cometido; mientras que el 73,33 % señalaron que no se encuentran en concordancia con lo que establece el Código Orgánico Integral.

Análisis

Los encuestados en su mayoría consideran que existe falta de proporcionalidad y concordancia con la sanción prevista en el COIP con respecto a los delitos informáticos en el sistema financiero nacional; no obstante es preciso reiterar que la pena privativa de 1 a 5 años que establece el citado Cuerpo Legal, no equivale la afectación que pudiera sufrir una persona por la apropiación fraudulenta por medios electrónicos, dada la connotación y efectos colaterales que inciden en esta clase de delito; que si bien, hay que resaltar la incorporación en el ordenamiento jurídico de esta innovadora figura legal, también lo es que la sanción no es concordante con el daño ocasionado, salvo mejor e ilustrado criterio.

Pregunta No. 6

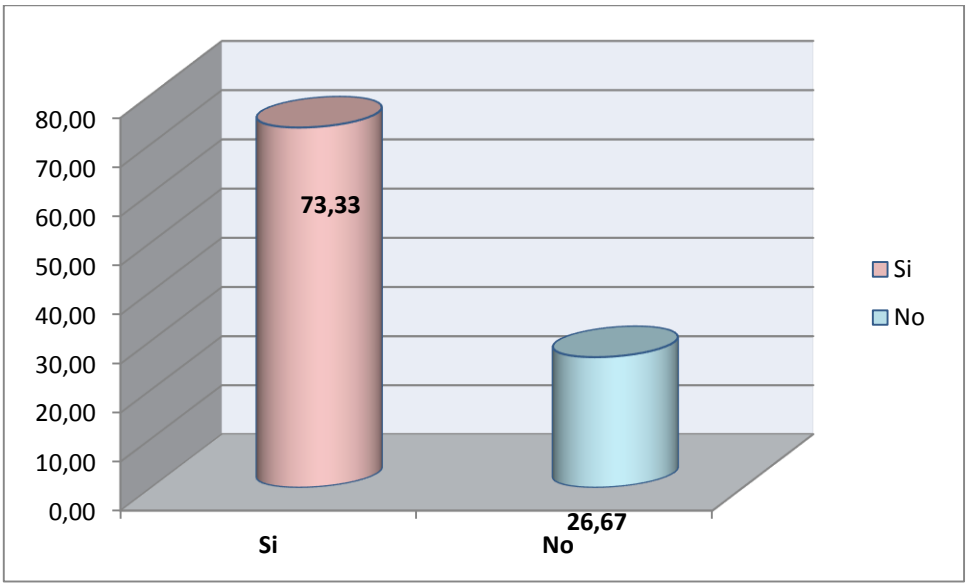
¿Considera Usted, que el Código Integral Penal debe incorporar la tipificación de penas específicas para cada tipo de delito de acuerdo a su gravedad y consecuencias para la victima?

Tabla No 6

Alternativas	F	%
Si	22	73,33
No	8	26,67
Total	30	100,00

Fuente: Profesionales y estudiante de derecho
Elaborado por: Autora de la investigación

Gráfico No 6



Interpretación

A esta interrogante, el 73,33% de los profesiones y conocedores en materia penal que fueron encuestados, respondieron que el Código Integral Penal debe incorporar la tipificación de penas específicas para cada tipo de delito informático de acuerdo a su gravedad y consecuencias para la víctima ;

mientras que 8 de ellos que representan 26,67 % señalaron que no consideran necesaria la tipificación e incorporación de penas específicas para cada tipo de delito, pues actualmente el Código Integrar Penal ya tipifica la pena los delitos informáticos, que a su criterio son jurídicamente adecuados

Análisis

De acuerdo a las respuestas emitidas por la mayoría de los profesionales y conocedores del derecho, se debe incorporar penas específicas de acuerdo a la gravedad del delito y al daño tanto moral como económico que el delito cauce a la víctima.

Los profesionales que no consideran necesario esta tipificación y mucho menos la incorporación de penas de acuerdo a cada tipo de delito, mantienen su criterio alegando que en el Código Integral Penal ya cuenta la tipificación y penalización de estos delitos, por lo tanto, consideran innecesarias cualquier propuesta jurídica en cuanto a cambios o implementación de penas para juzgar estos delitos.

Pregunta No. 7

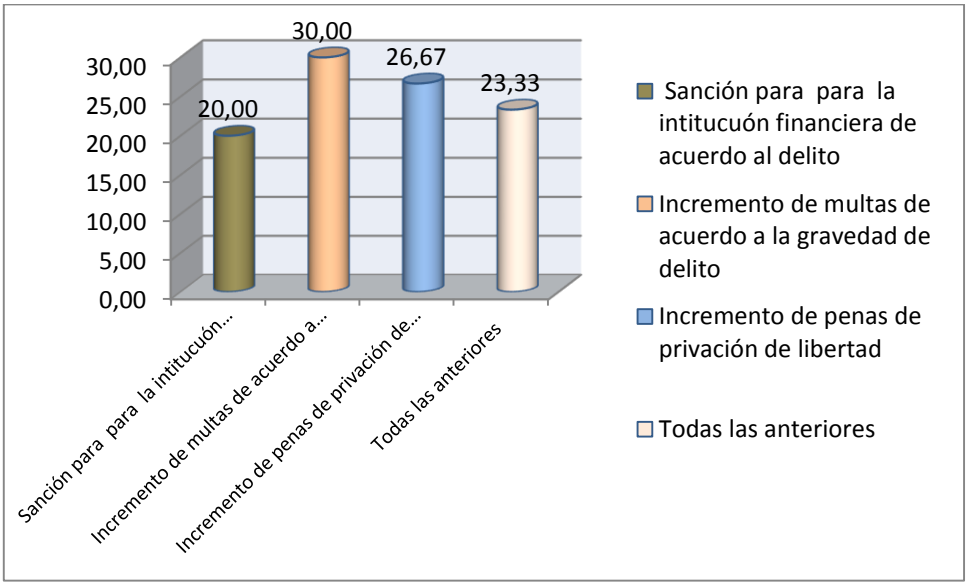
¿Qué aspectos de la penalización de los delitos informáticos, considera deben ser revisados, cambiados y tipificado en el Código Integral Penal COIP?

Tabla No. 7

Alternativas	F	%
Sanción para para la institución financiera de acuerdo al delito	6	20
Incremento de multas de acuerdo a la gravedad de delito	9	30
Incremento de penas de privación de libertad	8	26,67
Todas las anteriores	7	23,33
Total	30	**100**

Fuente: Profesionales y estudiante de derecho
Elaborado por: Autora de la investigación

Gráfico No. 7



Interpretación

A esta interrogante 6 de los profesionales encuestados que representan el 20,00%, indicaron que debe haber una Sanción para para la institución financiera de acuerdo al delito si comprobase negligencia en la operaciones bancarias o los sistemas informáticos implementados para dichas acciones; 9 de los encuestados que son el 30,00% indicaron que se deben implementar las multas de acuerdo al delito; 8 de ellos que corresponden al 26,67% de los profesionales encuestados indicaron que se deben incrementar las penas de privación de libertad, mientras que 7 que corresponden al 23,33% de los profesionales y conocedores del derecho señalaron que todas las alternativas consideradas deben considerarse para introducir cambios en Código Integral Penal.

Análisis

Los criterios expuesto en esta pregunta y la significativa homogeneidad de las respuestas con la que han seleccionado los profesionales encuestados, parecen que estos están plenamente justificados: *"La legislación penal en este aspecto, está en pañales respecto de los delitos financieros, ya que no existe aún capacitación en la fiscalía para investigación de estos delitos"* entendemos que la superintendencia de bancos, tiene un sistema de capacitación a sus funcionarios, más se puede entender que quienes se dedican a realizar delitos financieros, son personas con alta capacitación, y que han metido sus tentáculos incluso en los sistemas informáticos de la fiscalía y la policía nacional; *"Este tipo de delitos, siempre conlleva que exista información previa, que permita a los delincuentes acceder a información que se puede clasificar como reservada, y cada uno de los usuarios del sistema financiero no se*

encuentra preparados para generar seguridades personales, las mismas que son fácilmente vulneradas"; es verdad que los usuarios del sistema financiero, son quienes nos responsabilizamos por nuestras claves, tarjetas y demás dispositivos electrónicos, y que almacenamos mucha información sin las seguridades, que somos vulnerables al estar en desigualdad de conocimientos., por lo tanto los bancos e instituciones financieras son llamadas a tener un mayor control y seguridad sobre los sistema informáticos que ponen a servicio de los usuarios

Los cyber-delicuentes, poseen softwares que les permiten con información básica de todos nosotros generar las claves de podamos tener, por ejemplo, es muy común que nuestras tarjetas de débito mantengan claves como fechas de nacimientos, aniversarios, fechas de nacimiento de hijos, padres, etc., en la actualidad los sistemas de genera claves son software que pueden simular esta información, en la actualidad las redes sociales permiten acceder a información básica de cada uno de los usuarios, y de alguna manera, los cyber-delincuentes pueden Hackear nuestra información, procesarla, pulirla y finalmente obtener lo que necesitan.

Actualmente el sistema financiero, está dotando de mejores protecciones a sus usuarios, existen campañas constantes en los bancos para informar a sus usuarios a través de correos y demás medios de transmitir información, pero es común que a pesar de todo aquello, exista el cometimiento de estos delitos.

6.2. RESULTADOS DE LA APLICACIÓN DE ENTREVISTA A JUECES ESPECIALISTAS EN DERECHO PENAL

1. Considera Usted que los delitos informáticos que los delitos informáticos que se cometen contra en el sistema Financiero Nacional son un tema de conocimiento público.

Respuesta del especialista No 1

> *"El origen de los delitos en general, obligo a que las sociedades creen las normas y leyes para evitarlos, con cada avance de la humanidad un nuevo tipo delito se ha creado; con la informática, el mundo del internet, las redes sociales, el facilitar transacciones bancarias, y brindar atención a los clientes por parte de la banca, origina que existan delitos informáticos en el sistema financiero; por lo que cada día estaremos pendientes de nuevas formas de delitos en lo que tiene que ver con el sistema financiero nacional, y nos toca a los profesionales del derecho prepararnos en conocer los avances tecnológicos, el conocer estos nos permitirá entender su origen y fin, y de allí poder realizar estudios que permitan proponer, reformar, o ajustar las leyes a las nuevas realidades.*

Análisis e Interpretación

Para este especialista el tema de delitos informáticos, es un tema del que todas personas no conocen, no están conscientes pese a que el sistema financiero ecuatoriano ha puesto en alerta a los ciudadanos, el avance de la tecnología y de métodos cada vez más insospechables de delitos informáticos tornan el

entorno delictivo propicio para personas que logran tener acceso a las cuentas bancarias y cometer cualquier tipo de fraude.

Actualmente las modalidades conocidas para el cometimiento de delitos informáticos que afectan a los clientes de la banca han sido tipificadas en el COIP, pero no se especifica ni aplica de manera individual la penalización, sobre todo considerando el daño que estas ocasione a la víctima.

Respuesta del especialista No 2

> *"Es común escuchar que en Derecho, se dice que creada la Ley creada la trampa, yo diría creada la nueva tecnología, creado una nueva forma de delito, y se aplica a todas las actividades comerciales, bancarias, mercantiles, incluso educacionales. Por lo que yo solo me atrevería a decir que el hombre crea y el hombre destruye, es nuestra naturaleza."*

Análisis e interpretación

A través de la respuesta emitida por este especialista se puede inferir que de alguna manera las personas y la sociedad en general como agente activo del sistema financiero, debe estar alerta siempre, es decir, estar conscientes de que todo avance tecnológico o innovación que se haga utilizando medios tecnológicos para atender las necesidades que como usuarios se tiene , los cyber-delincuentes, crearán y utilizarán softwares que les permiten acceder al sistema del banco para obtener información que les ayuda a cumplir con sus fechorías informáticas, logrando así las transacciones que quiera hacer con la cuenta, tarjeta**.**

Respuesta del especialista No 3

> *"El Sistema Financiero, cuenta con herramientas informáticas para evitar el cometimiento de los delitos informáticos, la Superintendencia de Bancos, se encuentra capacitando preparando normas, y obligando al sistema financiero a brindar protección a sus usuarios, por lo que es importante conocer que si bien no se puede parar los delitos, existe dentro del sistema financiero nacional, mecanismos para prevenirlos."*

De acuerdo a este especialista el sistema financiero nacional, cuenta con los suficientes mecanismos de prevención para prevenir este tipo de delito, en concordancia con lo que expone este especialista, A pesar de los mecanismos de seguridad que debe suministrar el banco y guardar el cliente, éstos son violentados por terceras personas que buscan apropiarse de los depósitos del último, lo que indudablemente coloca en una situación de indefensión a las partes, ya que conforme a lo que se ha podido analizar en esta investigación, entre los mecanismos más usuales está la creación de páginas web falsas y que aparentan ser las de los bancos con la finalidad de obtener información del cliente relacionada con sus cuentas y seguridades para luego utilizarlas y hacer transferencias electrónicas.

Por lo tanto, es importante establecer que los actuales mecanismos de seguridad que utilizan los bancos no son suficiente, y mucho menos eficientes para salvaguardar a sus clientes.

2. Según su criterio jurídico, las penas que establece el Código Orgánico Integral, para sancionar los delitos informáticos en el sistema financiero nacional, está en concordancia con el delito cometido.

Respuesta del especialista No 1

> *"Es una pregunta, que no creo ser capaz de resolver, no podría determinar si un castigo es justo o no, son temas que conciernen a nuestros legisladores, que son quienes establecen las leyes que rigen nuestro país; si es o no concordante un castigo con un delito cometido, no podría definirlo, ya que me ha tocado estar en ambos lados del ejercicio profesional, es decir, procurar disminuir la pena de mis defendidos y, como fiscal procurar el mayor castigo para quién comete un delito; que es concordante o no guarda el equilibrio, es difícil definir"*

De acuerdo a la respuesta emitida por este especialista se puede interpretar que la protección de los sistemas informáticos puede abordarse tanto desde una perspectiva penal como de una perspectiva civil o comercial, e incluso de derecho administrativo. Estas distintas medidas de protección no tienen por qué ser excluyentes unas de otras, sino que, por el contrario, éstas deben estar estrechamente vinculadas. Por eso, dadas las características de esta problemática, sólo a través de una protección global, desde los distintos sectores del ordenamiento jurídico, es posible alcanzar una cierta eficacia en la defensa de los ataques a los sistemas informáticos.

Respuesta del especialista No 2

> *"Como manifesté anteriormente, se debe analizar cada caso en particular, por ello las leyes establecen la pena mínima y la pena máxima, en este tipo de delitos, podría enumerar agravantes, como es la premeditación y, la ventaja; y saber el perjuicio causado a la víctima, ya que no es lo mismo robarle cien a quien tiene fortuna que robarle los mismos cien a la persona que tiene como salario el mínimo que establece la ley; sin embargo es bastante complicado este tipo de delitos."*

Los delitos que se cometen contra los clientes de la banca por medios informáticos, deben considerar que si el agente activo de la infracción tiene el ánimo de lucro será un delito contra la propiedad y si no lo tuvo será un delito contra los sistemas de información como los llama actualmente el COIP, por lo tanto se hace necesario que cada uno de estos delitos sean abordados procesados y juzgados de acuerdo a la gravedad de cada uno de estos y de acuerdo a la consecuencias y perjuicios que traiga consigo para la víctima . Actualmente de acuerdo al *"Art. 186.- "...La pena máxima se aplicará a la persona que: Defraude mediante el uso de tarjeta de crédito, débito, pago o similares, cuando ella sea alterada, clonada, duplicada, hurtada u obtenida sin legítimo consentimiento de su propietario".*

3. ¿Considera Usted que la sanción tipificada en Código Integral Penal para los delitos informáticos, debe ser cambiada tipificando penas específicas para cada tipo de delito de acuerdo a su gravedad y consecuencias para la victima?

Respuesta especialista N.1

"De acuerdo a mi criterio considero que las penas y sanciones establecidas actualmente en l legislación ecuatoriana, específicamente en el COIP, si deben ser revisadas puesto que actualmente sin bien es cierto se establecen penas para los delitos informático, estas penas son de carácter bastante general, por ejemplo tienen la misma sanción aquel que haciendo uso de la información financiera que conoce sobre su víctima sustrae un monto de dinero de $3.000,00, que aquel que le ocasiona a su víctima una pérdida económica mucho mayor agravando este delito el hecho de que el monto sustraído es para cancelar los servicios de salud de un médico tratante de la enfermedad de uno de sus hijos, es decir, que este delito cometido trae consigo otras situaciones que deben ser consideradas al momento de la sentencia.

Análisis e interpretación

De acuerdo a lo expuesto por este especialista la legislación sobre protección de los sistemas informáticos ha de perseguir acercarse lo más posible a los distintos medios de protección ya existentes, creando una nueva regulación sólo en aquellos aspectos en los que, en base a las peculiaridades del objeto de protección, sea imprescindible como en el ejemplo expuesto.

Respuesta especialista N. 2

De acuerdo a mi punto de vista considero que las actuales penas establecidas en el Código Integral Penal si deben ser revisadas e incrementadas de acuerdo al tipo de delito, sobre todo considerando el

daño tanto económico como moral que ocasione a la víctima, considerando además que generalmente si bien es cierto la víctima es la afectada directa, pero existen caso en los que otras personas que indirectamente también sufren las consecuencias de un delito de esta naturaleza.

Análisis e interpretación

Los nuevos tipos penales son fruto de una demanda expresada por la sociedad, los cuales se recogen en el libro primero, que se relaciona con lo sustantivo penal y en donde se establecen cuáles son las conductas delictivas y las sanciones; el segundo libro es de procedimiento penal y el tercero es el de ejecución de penas, es precisamente en este parte donde aún existen algunos aspectos que deben ser revisado, considerando que actualmente existen nievas formas de delitos informáticos y sobre todo que cada uno de estos traen consigo un impacto en mayor o menor grado para la víctima.

Respuesta especialista N.3

De acuerdo a mi opinión, considero que si se debería revisar la sanción tipificada en Código Integral Penal para los delitos informáticos, debe ser cambiada tipificando penas específicas para cada tipo de delito de acuerdo a su gravedad y consecuencias para la víctima.

Análisis e interpretación

Si bien es cierto en el COIP se han tipificado delitos informáticos no solo buscando la protección de derechos constitucionales y bienes jurídicos conocidos tradicionalmente, como es por ejemplo el derecho a la propiedad,

sino también el derecho de información, que se lo cataloga como un “derecho del buen vivir”. En esta línea, los delitos que afectan a los clientes de la banca, considerando no solo delitos contra la propiedad sino también delitos contra la información, ya que como se advertirá actualmente la interceptación de datos así no tenga el ánimo de lucro constituye delito, sin embargo de acuerdo al sentir de la víctimas y conocedores del tema, existen alguno aspectos que deben ser revisados en el COIP, de tal manera que se incorpore también diferente tipos de penas, las mismas que deben estar en concordancia con el delito cometido, es decir, a mayor gravedad mayor debe ser la pena. De esta forma al menos si bien la víctima no recupera su tiempo, o sus pérdidas económicas, al menos quien cometa el e delito será sancionado de acuerdo a la gravedad de lo que ha hecho.

4. Que opina respecto del incremento de las sanciones en el cometimiento de los delitos financieros, como mecanismo para evitar se cometan los mismos.

Respuesta especialista No 1

“Mi criterio personal, y profesional, es que amenazar a las personas con mayores penas de las ya establecidas en el COIP, no soluciona ni detiene el cometimiento de los delitos, comparando con los actuales sistemas de radares y multas en el tránsito de las ciudades, las mismas no han reducido las infracciones de tránsito, solo ha incrementado el valor de recaudaciones de multas; igual cosa sucedería al aumentar penas, por un delito que además, es difícil de investigar y comprobar la culpabilidad del presunto autor, ya que las evidencias en este caso son totalmente

inexistentes, ya que quién puede acceder a un sistema informático para cometer delitos, estoy seguro debe conocer la forma su incriminación."

Análisis e interpretación

De acuerdo al criterio de este especialista el incrementar las penas no ayuda a disminuir el cometimiento de delitos informáticos, además considera que es difícil de investigar y comprobar la culpabilidad del presunto autor, ya que las evidencias en este caso son totalmente inexistentes.

Corroborando de alguna forma lo expuesto por este especialista, una publicación del Diario El Comercio sobre los delitos informáticos que afectan a los clientes de la Banca, expone que después de la tipificación de los delitos informáticos en el COIP, estos han aumentado, así por ejemplo del delito de apropiación ilícita de datos personales que en el año 2010 existieron 903 denuncias aumentaron al año 2013 a 1380 denuncias y en el año 2014 se registraron 1452 denuncias

Si bien es cierto los denuncias sobre delitos informáticos en el sistema financiero han aumentado, es evidente que tampoco se ha tratado de optimizar los procesos jurídicos para su tratamiento, por lo tanto, al no haber cambios en el sistema jurídico especialmente en el COIP, respecto a estos delitos, es posible que su cifra siga en aumento pues quienes cometen este tipo de delitos generalmente obtienen cuantiosas ganancias ilícitas que comparadas con las penas y sanciones impuestas en el COIP, seguramente no dudan en poner en práctica sus habilidades informáticas para cometer sus fechorías.

Respuesta especialista No 2

“El Derecho, y específicamente el Derecho Penal, establece un castigo para quien atenta contra las leyes o vive al margen de las mismas; aumentar o disminuir las ya existentes no soluciona ni erradica el cometimiento de este u otro tipo de delitos; una vez establecidas las penas para un delito, el derecho penal establece condiciones de agravantes y atenuantes para la aplicación del castigo por parte del administrador de justicia, por tanto, se debe legislar en tener bien definidos los atenuantes o agravantes y fijar los techos mínimos y máximos de un castigo, y que sea el administrador de justicia, quién de acuerdo a las pruebas procesales presentadas, defina el castigo.”

Análisis e interpretación

De acuerdo a lo expuesto por éste especialista, en el momento de dictar una sentencia, es importante “tener bien definidos los atenuantes o agravantes”. lo expuesto por este especialista se puede concebir como uno de los criterios jurídicos que se deben considerar para incorporar cambios en cuanto a la tipificación de las penas para quienes cometen delitos informáticos, es decir, se debe establecer de forma explicitas que tipos de atenuantes agravan los delitos cometidos en el sistema financiero, de esta forma al menos quienes se dedican a cometer este tipo de delitos serán sancionados de una forma mucho más justa y objetiva considerando la gravedad y consecuencias que ha sufrido la victima por causa de este delito.

Respuesta especialista No 3

"Las actuales penas establecen de tres a cinco años, como penas para quienes cometen delitos informáticos; mi criterio profesional, es que estas penas no se compadecen con el tipo de delito, puesto que quien comete este delito no es una persona que lo hace por necesidad, falta de trabajo o circunstancia especial; es gente que dedica tiempo, esfuerzo, ingentes recursos económicos, para planificar, y perpetrar el delito; por tanto no estamos ante un delincuente de la calle, sino ante un ser que posee cualidades y habilidades para generar producción, y ser útil a la sociedad."

Análisis e interpretación

De acuerdo a lo que expone este especialista, se puede deducir que para su criterio jurídico las penas tipificadas en el COIP para la penalizar los delitos informáticos, no se encuentran en concordancia con la gravedad del delito y mucho menos si analiza que para cometer un acto de éste tipo, quien lo comete generalmente tiene que planificar, es decir, está consciente de lo que hace y de las consecuencia y perjuicios no solo económicos sino también emocionales que en caso extremos hasta podrían costarle la vida.

4. **¿Qué aspectos de la penalización de los delitos informáticos, considera deben ser revisados, cambiados y tipificado en el Código Integral Penal COIP?**

Respuesta Especialista No 1

"Si se tiene en cuenta que los sistemas informáticos pueden proporcionar datos e informaciones sobre miles de personas, físicas y morales, en aspectos tan fundamentales para el normal desarrollo y funcionamiento de diversas actividades como bancarias, financieras, tributarias, previsionales y de identificación de las personas, y si a ello se agrega que existen bancos de datos, empresas o entidades dedicadas a proporcionar, si se desea, cualquier información, sea de carácter personal o sobre materias de las más diversas disciplinas a un Estado o particulares, se comprenderá que están en juego o podrían llegar a estarlo de modo dramático, algunos valores colectivos y los consiguientes bienes jurídicos que el ordenamiento jurídico-institucional debe proteger, por lo tanto, si considero que aspectos como el monto del perjuicio económico que le genere a la víctima; el daño indirecto que a causa de este delito le afecte a los familiares directos de la víctima, en síntesis las penas deben estar en proporción directa al perjuicio que este delito le ocasiones a la víctima"

Respuesta Especialista N. 2

La estructuración actual de los delitos de riesgo informático y de la información, sobre la base de su caracterización y conceptualización en torno a los nuevos bienes jurídicos requeridos de protección jurídico penal, la información en sí misma, los datos informáticos, y la seguridad y fiabilidad en los sistemas informáticos, es al término actual del delito informático a la que debemos aplicar el calificativo de económico, y no al

revés, y que comprenden aquellos comportamientos ilícitos informáticos en el ámbito económico/patrimonial, y referirnos consecuentemente a los mismos como delitos informáticos económicos patrimoniales, considero que este sería un aspecto fundamental que se requiere hacer en el Código Integral Penal "

Análisis e interpretación

Se infiere que cuando los delitos informáticos son cometidos con el ánimo de lucro se enmarcan dentro de los ilícitos económicos y cuando afectan al derecho de información podemos hablar de "otros delitos informáticos" siguiendo lo arriba manifestado por Rovira del Canto Rovira del Canto. Siguiendo la línea de pensamiento citada, en cuanto a los delitos que se cometen contra los clientes de la banca por medios informáticos pienso que si el agente activo de la infracción tiene el ánimo de lucro será un delito contra la propiedad y si no lo tuvo será un delito contra los sistemas de información como los llama actualmente el COIP.

Especialista No 3

"El Derecho Penal por ser un derecho sancionador sólo puede actuar cuando se pone en peligro o se lesiona un bien jurídico. ¿Pero que es un bien jurídico?. El bien jurídico según lo entiende la doctrina es siempre un interés vital, que no puede ser creado por el derecho sino por la sociedad de acuerdo a los valores vigentes en un tiempo dado, por lo tanto, se hace necesario, que se revisen e incorporen aspectos que como los montos y tiempos de sanción actualmente establecidos como pena máxima en el

Código Integral Penal, los mismos de acuerdo a mi criterio deben ser incorporados y de forma específica.

Análisis e interpretación

De acuerdo a esta noción expuesta por este especialista se puede afirmar que la información ha sido elevada a la categoría de un bien jurídico porque ha pasado a ser un interés jurídicamente protegido, que interesa a toda sociedad. Esa es la noción de bien jurídico que sostenemos. Un bien jurídico novedoso, complejo que puede tener implicancias en lo económico, en la privacidad, en la seguridad y en otros órdenes, pero que no deja de ser la información como objeto del delito, por lo tanto las penas y sanciones deben ser establecidas de acuerdo a las pérdidas económicas que éste delito ocasione en la víctima.

6.3 Estudio del caso sobre un delito informático cometido en el Sistema Financiero al usuario Mery Leisbel De Valle Pico del Banco Pichincha C.A.

El presente estudio de caso describe un informe técnico realizado por la Intendencia Regional de Portoviejo referente a la demanda Contencioso Administrativa No. 17811-2015-01021, interpuesta por el doctor Jaime Manuel Flor Rubianes, representante jurídico del Banco Pichincha C.A., por el reclamo administrativo presentado de la señora Mery Leisbel Del Valle Pico. **(Apéndice A)**

El Informe total se anexa como apéndice del presente estudio, para efectos del análisis de la problemática que se presenta, y la resolución emitida por la Intendencia Regional de Portoviejo

Luego del análisis expuesto, de los descargos y la información remitida por la entidad financiera, esta Intendencia Regional concluyó lo siguiente:

La responsabilidad de gestionar los riesgos inherentes al canal de banca electrónica es de competencia exclusiva de la entidad financiera, quien es la que ha puesto éste servicio a disposición del usuario, por lo cual debió contar con los resguardos necesarios que permitan minimizar los efectos de accesos no autorizados a las cuentas de sus clientes, quienes no pueden asumir las omisiones y/o falta de implementación de controles oportunos en los servicios ofertados.

Que el Banco Pichincha C.A., no cumplió completamente con el envío de la información solicitada por la Superintendencia de Bancos y Seguros, conforme lo establece la Ley General de Instituciones del Sistema Financiero, así como de incumplimientos a normas de la Codificación de Resoluciones de la Superintendencia de Bancos y Seguros y de la Junta Bancaria como se detalla en el presente documento.

Considerando las políticas conozca a su cliente y de debida diligencia, en el presente caso, no se ha aplicó un monitoreo a las operaciones de la cuenta de corriente N° 3339118904 y cuenta de ahorro N° 6227036600 correspondientes a la señora Del Valle y señora Cabrera respectivamente, el cual hubiera permitido al banco definir los parámetros inusuales de comportamiento de su cliente en las transacciones a través del proceso de transferencias por Internet.

Banco Pichincha C.A., no ha probado que el cliente actuó negligente e irresponsablemente en la custodia de la tarjeta E-Key N° 1170032 asignada, ni que efectuó la transferencia desde Perú, más aún cuando no se ha comprobado que la usuaria financiera haya abandonado el país en aquellas fechas.

Existió incumplimientos de la respuesta del Banco Pichincha C.A., a la reclamante en el plazo establecido en la Codificación de la Superintendencia de Bancos y Seguros y de la Junta Bancaria, del Ecuador ausencia de una efectiva gestión por parte del banco para confirmar la veracidad de los datos suministrados por los clientes.

Con estas consideraciones la Intendencia Regional de Portoviejo, resolvió en base a lo dispuesto en los literales b y o, del artículo 180 de la Ley General de Instituciones del Sistema Financiero y en ejercicio de la delegación de atribuciones conferidas a través de la resolución N° ADM-2013-11454 del 2 de abril de 2013, en concordancia con el Artículo 5, Sección I, Capítulo IV, Título XX, Libro I de la Codificación de Resoluciones de la Superintendencia de Bancos y Seguros y de la Junta Bancaria, que Banco Pichincha C.A. dentro del plazo de setenta y dos horas proceda al reintegro de USD3.500,00 reclamado por la señora Mery Leisbel Del Valle Pico.

ARGUMENTOS DE HECHO Y DE DERECHO DEL DEMANDANTE

En el oficio de impugnación presentado por el Banco Pichincha C.A., se realizaron las siguientes aseveraciones como fundamentos del recurso interpuesto y que se citan textualmente:

Entre los principales argumentos que el Banco manifiesta son los siguientes:

"La propia Intendencia de Portoviejo ratifica el hecho de que "efectivamente", la claves privadas, usuarios y coordenadas de la tarjeta E-key, "se encuentran bajo custodia y resguardo del cliente titular o propietario de la cuenta"; consecuentemente, se confirma el criterio de que la Institución no tiene responsabilidad respecto de la transacción objeto del reclamo, esto es, una transferencia realizada desde la cuenta de la cliente el mes de febrero del 2012, por el valor total de US$ 3.500,00 (tres mil quinientos dólares de los Estados Unidos de América)"

"(...) Temas como los de notificaciones de alerta para transferencias electrónicas, constituyen más bien esquemas adicionales…"

"La afectación al cliente se produce, no por falta de seguridad en los sistemas del Banco, en ningún caso. La afectación es producto del uso incorrecto del canal electrónico. Y este hecho solo puede ser imputable al usuario."

De los argumentos planteados por la entidad financiera, se evidencia claramente la pretensión del Banco Pichincha C.A., de deslindarse de toda responsabilidad respecto de la transferencia electrónica realizada el 24 de febrero de 2012 a las 11:56:24 por el valor de USD. 3,500, de la cuenta corriente No. 3339118904 perteneciente a Mery Leisbel Del Valle Pico, ejecutada desde el IP 200.108.108.173 cuya ubicación es en Lima-Perú, manifestando que las claves, usuarios y coordenadas de la tarjeta e-key sólo se encuentran bajo la custodia y resguardo del cliente titular de la cuenta y que la afectación es producto del uso incorrecto del canal electrónico y que por lo tanto este hecho solo puede ser imputable al usuario financiero.

Al respecto no se observa en el expediente que el Banco haya remitido a este Organismo de Control la documentación suficiente y competente respecto si los procedimientos internos responden a una validación y verificación adecuada del sistema operativo informático implementado por el Banco para la realización de transferencias entre cuentas.

Además como se puede observar en el "log de transacciones" que con fecha 24 de febrero de 2012 a las 11:50:09, mediante el IP 200.108.108.173 como ya se dijo anteriormente queda ubicado en Lima-Perú se acceso al sistema biométrico registrando el siguiente mensaje "Denied because the user-s biometric registry indicates a posible fraud", que traducido significa "Negado por el usuario-s el registro biometric indica un posible fraude" luego a las 11:51:51 vuelven a accesar al sistema y esta vez logra entrar desde el mismo IP, haciendo la validación de cuentas para transferencia y aumento del cupo diario de transferencia entre cuentas en USD. 4,000.00 y a las 11:56:24 con el mismo IP realiza la transferencia de USD. 3,500.00 a la cuenta de propiedad de Mercy Cabrera Pilligua, también cliente del Banco Pichincha C.A.,

De lo expuesto, se advierte que el Banco Pichincha C.A., si tuvo un indicador

alerta, y además por tratarse de un IP que no era utilizado habitualmente en las transacciones de la cliente, el banco se encontraba en la responsabilidad de rechazar de manera oportuna la ejecución de dicha transacción, situación que no sucedió y por lo tanto no cumplió con lo previsto en el segundo inciso del artículo 5, capitulo IV.- Procedimiento para atención de los reclamos contra las instituciones del sistema financiero, título XX.- De la Superintendencia de Bancos y Seguros, libro de la Codificación de Resoluciones de la Superintendencia de Bancos y Seguros y de la Junta Bancaria.

"Art. 5. (...) Si la situación que motivó el reclamo referido en el inciso anterior, se originó en un procedimiento incorrecto de la institución controlada, que hubiese ocasionado un perjuicio al reclamante, la Superintendencia de Bancos y Seguros podrá ordenar la devolución de los valores reclamados, en ejercicio de las funciones y atribuciones contempladas en las letras b) y o) del artículo 180 de la Ley General de Instituciones del Sistema Financiero, otorgando al representante legal de la entidad un plazo que no podrá exceder de quince (15) días a partir de la notificación para que remita, bajo las prevenciones de Ley, la constancia del cumplimiento de la orden impartida."

En la letra d) de la comunicación del 30 de agosto emitida por el Banco Pichincha C.A., argumenta lo siguiente:

"(...) Si ha existido un acto delictivo le corresponde a la cliente, como afectada, impulsar la denuncia correspondiente."

"La inseguridad permanente que vivimos, no puede constituirse en un argumento para que las consecuencias de los actos cometidos por la delincuencia común, se le endosen al Banco, cuando es el Estado el que debe garantizar la seguridad humana a través de políticas y acciones integradas, para prevenir las formas de violencia y la comisión de infracciones y delitos, conforme lo dispone el Art. 393 de la Constitución de la República."

Ante el argumento esgrimido por el Banco se deduce entonces que el Organismo de Control debería abstenerse de tramitar, conocer, y resolver casos en el ámbito administrativo sobre transferencias por internet, basado en el simple argumento y presupuesto de que el cliente es poseedor de claves y coordenadas para acceder al producto financiero sin entrar a valorar otros elementos o aspectos necesarios dentro del procedimiento interno, ni sus niveles de cumplimiento.

Ante la demanda presentada, se debe recordar al Banco Pichincha C.A. que la Superintendencia de Bancos del Ecuador, tiene la función y atribución de velar por la estabilidad, solidez y correcto funcionamiento de las instituciones sujetas a su control; y, vigilar que las mismas cumplan las normas que las rigen; y, exigir que dichas instituciones presenten y adopten las correspondientes medidas del correctivas cuando sea necesario.

Además, le compete emitir las disposiciones necesarias para resolver las reclamaciones que presenten los clientes del sistema financiero, siempre atenta a la protección de los intereses del público.

Adicionalmente, el Banco del Pichincha, nunca remitió a este Organismo de

Control la documentación requerida de la señora Cabrera Pilligua Mercy Madele, cuenta ahorrista 6222036600, beneficiaria de la transferencia por el valor de USD. 3,500, así como no se conoce sobre las investigaciones llevadas a cabo por la entidad, más aún si la señora Cabrera Pilligua Mercy Madele, es una clienta del propio Banco Pichincha C.A., situación que no permite evidenciar si el funcionario de la entidad financiera efectúo las gestiones de confirmar la veracidad de los datos suministrados por el titular de la cuenta beneficiaria de la transferencia, a través del Formulario de solicitud de inicio de relación comercial "Conozca a su cliente", actividad que para la adecuada aplicación de la política "Conozca a su Cliente", las instituciones del sistema financiero están obligadas a cumplir, lo cual permite conocer la información relativa del beneficiario; teniendo en cuenta la obligación del banco de monitorear las transacciones realizadas por sus clientes, a fin de que el dinero confiado a su custodia sea protegido adecuadamente, incumpliendo con lo establecido en el artículo 77 de la Ley General de Instituciones del Sistema Financiero, que señala:

"ARTÍCULO 77.- Las instituciones del sistema financiero estarán obligadas a dar todas las facilidades para que la Superintendencia cumpla sus funciones y deberán dar acceso a su contabilidad, libros, correspondencia, archivos o documentos justificativos de sus operaciones al Superintendente o a sus delegados."

Esta entidad financiera, únicamente se limitó a responsabilizar a la cliente sobre la transferencia electrónica, sin evidenciar ni valorar de manera oportuna si efectivamente los procedimientos internos revela una validación y verificación adecuada del sistema operativo informático implementado por el Banco; en contrario, se imputa la carga de la prueba exclusivamente a la reclamante, por lo que no se entiende cuando se aborda el tema de afectación al cliente se determina que es producto del uso incorrecto del canal electrónico, de lo cual el Banco no ha podido comprobar tal afirmación, considerando que las seguridades para el bloqueo de la transacciones cuando se evidencie comportamientos inusuales NO se ejecutaron, por lo que queda evidenciado la omisión de procedimientos, procesos y políticas establecidos para proteger los derechos del usuario financiero.

Respecto de la no competencia de la Superintendencia de Bancos en ordenar la devolución de valores al demandante, el recurrente no considera lo dispuesto en el artículo 5, sección I, capitulo IV, Título XX, Libro I de la Codificación de Resoluciones de la SBS y de la JB que establece:

ARTÍCULO 5.- Si el resultado del análisis que realice la Superintendencia determinare la necesidad de que la institución controlada introduzca correctivos que regularicen la situación que motivó el reclamo, el Superintendente de Bancos y Seguros o el funcionario que cuente con la delegación de dicha autoridad, impartirá la disposición correspondiente.

Si la situación que motivó el reclamo referido en el inciso anterior, se originó en un procedimiento incorrecto de la institución controlada, que hubiere ocasionado un perjuicio al reclamante, la Superintendencia de Bancos y Seguros podrá ordenar la devolución de los valores reclamados, en ejercicio de las funciones y atribuciones contempladas en las letras b) y o) del artículo 180 de la Ley General de Instituciones del Sistema Financiero, otorgando al representante legal de la entidad un plazo que no podrá exceder de quince (15) días a partir de la notificación para que remita, bajo las prevenciones de ley, la constancia del cumplimiento de la orden impartida.

Artículo 180, de la Ley General de Instituciones del Sistema Financiero, literales:

b) Velar por la estabilidad, solidez y correcto funcionamiento de las instituciones sujetas a su control y, en general, que cumplan las normas que rigen su funcionamiento;

c) Autorizar la cesión total de activos, pasivos y contratos de las instituciones del sistema financiero, cuando ello implique la cesación de las operaciones de una oficina…

En virtud de la expuesto en las normas legales invocadas, la Superintendencia de Bancos del Ecuador, es competente para conocer los reclamos administrativos que presente el usuario externo a nivel nacional, y; en ejercicio de esta competencia la Intendencia Regional de Portoviejo conoció y resolvió el reclamo objeto de este proceso judicial. En consecuencia el argumento del recurrente esgrimido en la demanda ante el Organismo de Control, carece de sustento legal.

En cuanto al argumento, manifestando que la Junta Bancaria incurrió en silencio administrativo positivo a favor del demandante, es necesario mencionar que el artículo 182 ibidem establece:

Artículo 182.- Cuando el Superintendente de Bancos no se pronunciase o no resolviese un asunto sometido a su aprobación, dentro de los términos fijados por esta ley o por otras leyes cuya aplicación corresponda resolver a la Superintendencia, sin haber dispuesto las ampliaciones de dichos plazos antes de su expiración, la petición sometida a su aprobación se entenderá favorablemente resuelta bajo su responsabilidad.

La misma norma se aplicará respecto de los asuntos sometidos a resolución de la Junta Bancaria, excepto las solicitudes de constitución o establecimiento de nuevas instituciones.

Si la demora es imputable a cualquier otro funcionario de la Superintendencia, éste podrá ser sancionado inclusive con la remoción o destitución, dependiendo de la gravedad del hecho a criterio del Superintendente, quien podrá revisar el efecto resultante de la falta de pronunciamiento, en el término de ocho días de producido.

El secretario de la Junta Bancaria como lo reconoce el demandante, comunicó al Banco del Pichincha C.A. la ampliación de los plazos de manera oportuna en estricto apego a la norma legal que antecede, por lo expuesto la pretensión de alegar silencio administrativo carece de sustento legal.

De las consideraciones legales expuestas, el Recurso Subjetivo o de Plena Jurisdicción en contra de la Resolución No, JB-2015-3234, de 14 de enero de 2015, es improcedente por no contar con la fundamentación jurídica para el efecto.

ANÁLISIS E INTERETACIÓN:

De acuerdo a la resolución emitida por la Intendencia Regional de Portoviejo, se puede concluir que la actual normativa jurídica sobre el tratamiento y penalización de los delitos informáticos tipificada en los diferentes instrumentos jurídicos, aún requieren de revisión y ajustes legales, los cuáles deben considerar cada uno de los aspectos y el nivel de responsabilidad que tienen las entidades que conforman el sistema financiero nacional.

Si bien es cierto "*La responsabilidad civil de los bancos nace del principio de tutela reparatoria o resarcitoria frente al perjuicio sufrido como producto de la culpa de la entidad bancaria frente a un detrimento patrimonial de sus clientes y usuarios de ésta: "..la tutela del cliente bancario relativa, en líneas generales, a la protección de derechos crediticios, merece ser abordada desde la perspectiva de la tutela resarcitoria, pero en subsidio de la tutela preventiva y coercitiva, de modo que aquella protección más débil sea compensada adecuadamente, no ya en ocasión de la reparación sino para evitar llegar a ella" (Babier, 2015)*

Para ello es necesario recordar la clásica división de las obligaciones en DAR; HACER; y, NO HACER. La clasificación mencionada es de extrema importancia al momento que en la praxis se la debe tomar en cuenta para entablar una acción, pues cada una de estas categorías delimita lo que podemos plantear en relación a los perjuicios; así si la obligación es de dar aplicaremos el Art. 1564 del Código Civil si la obligación es de hacer se aplica

el Art. 1569, del mismo cuerpo legal y, si la obligación es de no hacer tendrá que aplicarse el Art. 1571 del citado Código.

Las obligaciones de hacer, son consideradas obligaciones positivas, se encuentran constituidas por una prestación, acción, comportamiento, conducta, que justamente consisten es un hacer, producir, realizar y, o ejecutar algo. Según la autora Virginia Pardo Iranzo, las obligaciones de hacer "*son aquellas cuya prestación consiste en la realización de una actividad diferente de la de entregar una cosa También es considerado un hacer… Las obligaciones de hacer tienen siempre un objeto indeterminado (incertum); aunque el resultado de la operación (p.ej. la casa ya construida) esté previsto como concreto, el hacer mismo es previamente indeterminado."*

Por otra parte la autora citada manifiesta que *"las obligaciones de hacer pueden ser de medio y resultado, clasificación que es importante a efectos de determinar lo que el acreedor puede exigir como contenido de su derecho de crédito. En las obligaciones de medio (también llamadas de mera actividad o de diligencia) el deudor se compromete a mantener una determinada actitud (una actividad diligente), mientras que las obligaciones de resultado la prestación consiste en alcanzar una determinada meta; el objeto de la obligación no es, simplemente, mantener una determinada actitud, sino conseguir un determinado resultado*

Se definen por tanto de manera negativa ya que entregar una cosa también es un hacer…Las obligaciones de hacer tienen siempre un objeto indeterminado

(incertum); aunque el resultado de la operación (p.ej. la casa ya construida) esté previsto como concreto, el hacer mismo es previamente indeterminado."

La obligación del banco frente al cliente en el tema objeto de estudio es de hacer una obligación de resultados, afirmación que se origina, en la tecnificación con la que debe contar una entidad bancaria para brindar un servicio seguro y óptimo dado su alto grado de profesionalización de ésta actividad que supone llevar a cabo todo un proceso no solo de custodia de los dineros de los depositantes sino de preservación de los mismos, tanto más cuanto que, al momento de hacerle firmar al cliente un contrato de banca en línea o bien si el cliente solicita éste, el Banco se obliga a brindar e implementar medios tecnológicos.

La obligación que el Banco contrae en el momento de la firma del contrato de los servicios bancarios incluidos los servicios en línea, presupone que éste ya cuenta con este servicio es decir con la plataforma electrónica previamente implementada que es puesta a disposición del cliente, y por ello no se podría manifestar que a su vez a parte de una obligación de hacer, la contraída por el Banco es una obligación a plazo, entendido éste según el caso objeto de análisis, el Código Civil en su Art. 1510 como "*la época que se fija para el cumplimiento de la obligación",* ya que la prestación es cumplida por el Banco de manera inmediata a la suscripción del contrato en el momento en el que el cliente accede al servicio de banca en línea.

La obligación del banco se torna así en una obligación de tracto sucesivo, es decir una obligación que no es realizada en un solo acto, sino que debe ser reiterada durante un tiempo determinado, debiendo garantizar la entidad bancaria no solo el comienzo de la realización de la actividad, sino también su realización continuada

El Art. 54 de la Constitución de la República establece: "*Las personas o entidades que presten servicios públicos o que produzcan o comercialicen bienes de consumo, serán responsables civil y penalmente, por la deficiente prestación der servicio, por la calidad defectuosa del producto, o cuando sus condiciones no estén de acuerdo con la publicidad efectuada o con la descripción que incorpore…".* Esta disposición fue invocada para la determinación de la responsabilidad objetiva que se imputó a las entidades bancarias, pero pese a esto aún ciertas instituciones bancarias como la del caso expuesto no asumen con verdadera responsabilidad con sus clientes las normativas jurídicas establecidas, por lo que se hace necesario que se considere la posibilidad de especificar de forma explícita en el COIP responsabilidad penal de acuerdo al delito informático y de acuerdo a los daños económicos, emocionales que afecten directamente al usuario o víctima.

7. DISCUSIÓN

7.1 Verificación de objetivos

A continuación se especifican los objetivos planteados para el presente estudio, con la respectiva argumentación de su alcance.

Objetivo General.-

Realizar un estudio jurídico, crítico y doctrinario del CÓDIGO ORGANICO INTEGRAL PENAL en relación al delito informático.

El alcance de este objetivo se logra demostrar a lo largo del desarrollo de la investigación, específicamente en el apartado de la revisión de la literatura donde se aborda el marco teórico, doctrinario y la legislación comparada, existente en el marco jurídico ecuatoriano y a nivel internacional sobre el objeto variables de estudio.

En el marco doctrinario se describen las bases teóricas jurídicas que sustentan el estudio sobre los delitos informáticos el sistema financiero, se hace además un análisis teórico sobre el marco jurídico del Código Integral Penal relacionado a los delitos informáticos en el sistema financiero. El alcance de este objetivo también se logra demostrar mediante el análisis de las encuestas y entrevistas que se realizaron a profesionales y especialistas del derecho penal, cuyos criterios y argumentos jurídicos complementan el estudio y análisis del objeto de estudio.

Objetivos específicos

- **Identificar las falencias en el Sistema Jurídico Ecuatoriano en lo referente los delitos financieros**.

El alcance de este objetivo se logró mediante la revisión y análisis del marco jurídico existente en la legislación ecuatoriana, sobre los delitos informáticos, y el reglamento para el control del sistema financiero que posee el Ecuador dictado por el órgano que controla el Sistema Financiero Nacional, esta revisión permitió identificar que en ninguno de los instrumento jurídicos existentes señalan sanciones específicas de acuerdo al tipo de delito y mucho menos sanciones que en las que se consideren la gravedad del delito para estipular la pena. Otra de las falencias que se logró identificar a través del estudio de caso fue que el sistema jurídico vigente presenta vacíos en cuanto a la responsabilidad que deben tener las instituciones financieras como lo banco en cuanto al control de los delitos informáticos, temas que debe ser analizado en futuras investigaciones.

- **Determinar las diferencias y similitudes que existen entre las bases legales ecuatorianas y los otros países, mediante un análisis comparativo.**

El alcance de este objetivo demuestra mediante el análisis de la doctrina comparada, para el efecto ha revisado la literatura respecto de los delitos informáticos, y se conoce el reglamento para el control del sistema financiero

que posee nuestro país, dictado por el órgano que controla el sistema financiero nacional.

Se realizó también la revisión de la legislación de países vecinos, respecto de los delitos informáticos, lo que permitió tener una visión más amplia sobre las bases teóricas y jurídicas para proponer una reforma para los castigos de los delitos informáticos en el sistema financiero nacional.

- **Proponer que nuestra legislación, reforme al CÓDIGO ORGÁNICO INTEGRAL PENAL, aumentando las sanciones con penas y multas más fuertes para las personas que cometan este tipo de delitos, en consideración a la gravedad, perjuicio moral y económico que cause a la víctima.**

El alcance de este objetivo se lo puede evidenciar en el desarrollo de la propuesta de reforma al Código Orgánico Integral Penal, la misma que se sustenta jurídicamente en los argumentos teóricos y razones jurídicas por las que se hace necesaria esta reforma propuesta al COIP.

7.2. Contrastación de la Hipótesis

¿Las penas que establece el Código Orgánico Integral, para sancionar los delitos informáticos en el sistema financiero nacional, están en concordancia con el tipo de delito cometido?

Del análisis objetivo de las bases conceptuales, teóricas, el marco jurídico y la legislación comparada estudiada, así como de las encuestas y entrevistas realizadas; se ha podido determinar que las penas que establece el Código Orgánico Integral Penal ecuatoriano, no guarda concordancia con el tipo de delito informático cometido en el sistema financiero nacional.

7.3. Fundamentación Jurídica para la Propuesta de Reforma Legal

“El Derecho Penal por ser un derecho sancionador sólo puede actuar cuando se pone en peligro o se lesiona un bien jurídico. El bien jurídico según lo entiende la doctrina es siempre un interés vital, que no puede ser creado por el derecho sino por la sociedad de acuerdo a los valores vigentes en un tiempo dado. De acuerdo a esta noción hoy podemos afirmar que la información ha sido elevada a la categoría de un bien jurídico porque ha pasado a ser un interés jurídicamente protegido, que interesa a toda sociedad.

En este contexto la información que manejan los bancos e instituciones que son parte del sistema financiero, están expuestas día a día a que se cometan delitos informático ya sea de forma deliberada con fines de lucro o indeliberadamente por descuido o fallas de los sistemas.

Por lo expuesto se hace necesario que el Sistema Jurídico sea el organismo competente que determine el marco legislativo que regule y controle de forma clara, específica y objetiva las funciones que estos cumplen como parte del estado. N este contexto el Código Integral Penal es precisamente una de las

herramientas jurídicas en la que se debe establecer la normativa y penalización de los delitos informáticos que se puedan cometer en el sistema financiero.

Ante este antecedente se considera estrictamente necesario que el Código Orgánico integral pena**l,** debe tipificar este delito de tipo informático con más rigor, ya que se viola lo privativo de un ser humano como son los bienes intangibles amparados por el Derecho de Propiedad, ya que se manipularía los datos personales y privados, cometimiento fraude en títulos de dominio, intimidad personal, sabotajes informáticos, infracciones a los derechos de la propiedad intelectual y afines,

Ante esta falencia jurídica identificada y analizada a través del presente estudio y considerando la magnitud y daño que causan los delitos informáticos de acuerdo a su gravedad, se propone que aumente la pena privativa actual que es de 3 a 5 años; por una pena de 10 a 12 años.

8. CONCLUSIONES

1. El Código Orgánico Integral Penal (COIP) y la Ley de Comercio Electrónico Firmas y Mensajes de Datos, poseen falencias y vacíos en cuanto al tipificar los delitos informáticos dentro del sistema financiero nacional; esto es, incorporar aspectos y hechos relevantes que la legislación actual no ha normado o plasmado literalmente para evitar vacíos de orden y ejecución penal, ámbito de la materia investigada.

2. Las actuales penas que se estipulan para el cometimiento de delitos informáticos, no son concordantes con el delito cometido, ya que de lo investigado, se ha podido identificar que se trata de delitos que son bien preparados (PREMEDITACIÓN, VENTAJA, ALEVOSÍA); sin embargo la imposición de las penas consignadas son ostensiblemente bajas para el daño y perjuicio que se ocasiona.

3. Analizadas las legislaciones de países vecinos, se puede colegir que es necesario la creación de un organismo regional de control, toda vez que al tratarse de un delito que afecta a todos por igual, la ley y las penas deberían tener parámetros de aplicación similares. Circunstancia que dentro del Derecho Comparado, significa la aplicación de principios de uniformidad y armonía legislativa.

4. En el Ecuador no existe responsabilidad penal de los bancos e instituciones financieras por los delitos informáticos de apropiación ilícita de fondos de los que sus clientes son víctimas.

9. RECOMENDACIONES

1. Reformar las leyes actuales, para que las mismas se encuentren actualizadas con respecto a los nuevos delitos informáticos, que afectan principalmente al sistema financiero nacional. Proyecto reformatorio que deberá ser considerado por la Asamblea Nacional para protección de todos los ecuatorianos.

2. Agravar la imposición de penas por los delitos informáticos en el sistema financiero nacional, por su connotación y perjuicio. Recomendación concordante con la anteriormente consignada, puesto que la Asamblea Legislativa es la llamada a las reformas propuestas en el presente trabajo investigativo.

3. Crear un organismo regional de control, tipo Superintendencia de Instituciones Financieras que guarde armonía legislativa para la aplicación de la normativa sobre el tema.

4. Elaborar propuesta jurídica que sustente la tipificación en el Código Orgánico Integral Penal, de la responsabilidad de los bancos e instituciones financieras por los delitos informáticos de apropiación ilícita de fondos de los que sus clientes son víctimas

Cabe manifestar, en atención a las CONCLUSIONES Y RECOMENDACIONES consignadas en el presente trabajo investigativo, que me encuentro consciente de las debilidades que éste pudiera adolecer, precisamente por ser una nueva

figura tipificable en el ordenamiento jurídico del país; no obstante quiero relevar el aporte que como ciudadana y futura profesional del derecho pretendo realizar con esta investigación.

9.1 PROPUESTA DE REFORMA JURÍDICA

ASAMBLEA NACIONAL DE LA REPÚBLICA DEL ECUADOR

CONSIDERANDO:

Que, es deber fundamental e ineludible del Estado, la construcción de un ordenamiento jurídico que satisfaga las expectativas sociales dentro del marco constitucional y que confiera seguridad jurídica a las partes en conflicto; garantizando la vigencia de los principios de estabilidad, intangibilidad e irrenunciabilidad dentro de los procedimientos administrativo como jurisdiccionales.

Que, es necesario reformar el Art. 234 del Código Orgánico Integral Penal, a fin de evitar que, los usuarios del sistema financiero nacional, se vean perjudicados por los delitos informáticos.

Que, a pesar que existen las leyes aplicables a los delitos informáticos, se reconoce que el avance de la tecnología, se ha convertido en una herramienta mediante el cual se ha causado y se continúa causando perjuicio a los usuarios del sistema financiero nacional.

En ejercicio de la facultad establecida en el Artículo 132 de la Constitución de la República del Ecuador:

RESUELVE

Art.1.- Refórmese el Art. 234 del Código Orgánico Integral Penal, por el siguiente texto:

“Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.- La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años; y al tratarse de delitos informáticos contra el sistema financiero nacional, la pena privativa de la libertad será de diez a quince años.”

Art. 2.- La presente reforma entrará en vigencia a partir de la correspondiente promulgación y publicación en el Registro Oficial.

Dado y Firmado, en la ciudad de San Francisco de Quito, Distrito Metropolitano, en la sala de sesiones de la Asamblea Nacional del Ecuador, a los cuatro días del mes de septiembre de 2016.

f.…… **f.……...**
PRESIDENTA DE LA ASAMBLEA NACIONAL **SECRETARIA DE LA ASAMBLEA NACIONAL**

10. BIBLIOGRAFÍA

CABANELLAS G, “DICCIONARIO JURIDICO ELEMENTAL, editorial Eliasta edición actualizada 1014, pp 326

CALVO, ANTONIO; CUERVO, ÁLVARO; PAREJO, JOSÉ ALBERTO; RODRÍGUEZ, LUIS (2008). “MANUAL DEL SISTEMA FINANCIERO ESPAÑOL”, Ariel. ISBN 9788434445536. recuperado en http://www.uv.es/~fcliment/Actualidad_Financiera.pdf

CAMACHO LOSA, L: “EL DELITO INFORMÁTICO”. Graficas Cóndor, Madrid

CARRANCA Y TRUJILLO RAÚL, DERECHO PENAL MEXI- CANO (parte general), 7a. ed., México, Antigua Librería Robredo

CARREÑO, J. “USO DE MEDIOS ELECTRÓNICOS EN LA BANCA”, recuperado en http://blogtelecomunicaciones.ramonmillan.com/2008/03/tipos-transacciones-electrnicas.html

CÓDIGO DE PROCEDIMIENTO PENAL, Quito-Ecuador

CÓDIGO ORGÁNICO INTEGRAL PENAL (COIP), EN EL TITULO X. DE LOS DELITOS CONTRA LA PROPIEDAD. Cap. II. Del Robo. Cap. V De las Estafas y otras defraudaciones

CONSTITUCIÓN DE LA REPUBLICA DEL ECUADOR. TÍTULO IV, CAPITULO 4TO, EN LA SECCIÓN DÉCIMA, Asamblea Constituyente 2008

CONVENIO DE CYBER-DELINCUENCIA DEL CONSEJO DE EUROPA ESTADOS MIEMBROS DEL CONSEJO DE EUROPA Y OTROS ESTADOS-BUDAPEST 2001 http://www.coe.int/

CORREA, C. - BATTO, H. - CZAR DE ZALDUENDO, S. & NAZAR ESPECHE, F. (1987). Cap. El derecho ante el desafío de la informática. En "Derecho informático"(p. 295). Buenos Aires: Depalma. ISBN 950 14 0400 5

CUELLO CALÓN”, “GUÍA PRACTICA DE DERECHO” recuperado en http://derecho911.blogspot.com/2013/06/que-es-la-antijuricidad.html

CUERVO, JOSÉ. “DELITOS INFORMÁTICOS: PROTECCIÓN PENAL DE LA INTIMIDAD”. Publicado en http://www.INFORMÁTICA-jurídica.com/trabajos/delitos.asp (2008)

DE LA LUZ LIMA MARIA, “DELITOS ELECTRÓNICOS”, Ediciones Porrúa-México,. Pág100, 1984

DELGADO GRANADOS MARÍA LOURDES, “DELITOS INFORMÁTICOS DELITOS ELECTRÓNICOS”, recuperado en www.ordenjuridico.gob.mx/Congreso/pdf/120.pdf

DEPARTAMENTO DE JUSTICIA NORTEAMERICANO, “DELITOS INFORMÁTICOS”, recuperado en http://www.eumed.net/rev/cccss/14/ecra.html

EDWIN SUTHERLAND”, EL DELITO DE CUELLO BLANCO, Madrid: La Piqueta, 1999I. Título II. Serie Pág.- 339

ERNST BELING “INTRODUCCIÓN A LA TEORÍA DEL DELITO", artículo jurídico publicado en diposit.ub.edu/dspace/bitstream/2445/41555/1/TOL77.pdf

JULIO TELLEZ VALDEÉS, “DERECHO INFORMÁTICO”, 2da edición Mc Graw Hill-México 1996

JULIO TELLEZ VALDEÉS, “DERECHO INFORMÁTICO”, 2da edición Mc Graw Hill-México 1996

JULIO TELLEZ VALDEÉS, “DERECHO INFORMÁTICO”, 2da edición Mc Graw Hill-México 1996

LÍBANO MANSSUR, CLAUDIO. “LOS DELITOS DE HACKING EN SUS DIVERSAS MANIFESTACIONES”. Revista Electrónica de Derechos informáticos, bajados de Internet.

LIBRO I.- NORMAS GENERALES PARA LAS INSTITUCIONES DEL SISTEMA FINANCIERO ITULO X.- DE LA GESTIÓN Y ADMINISTRACIÓN DE RIESGOS CAPÍTULO V.- DE LA GESTIÓN DEL RIESGO OPERATIVO (incluido con resolución No JB-2005-834 de 20 de octubre del 2005

LIBRO I.- NORMAS GENERALES PARA LAS INSTITUCIONES DEL SISTEMA FINANCIERO: SECCIÓN VII.- DE LAS MEDIDAS DE SEGURIDAD (incluida con resolución No. JB-2011- 1851 de 11 de enero del 2011)

MANUEL BAJO FERNÁNDEZ, LOS DELITOS INFORMÁTICOS, Editorial Juristas, Enero 2012.

MEDINA, R “DISEÑO DE POLÍTICAS PÚBLICAS PARA ENFRENTAR EL DELITO EN DEMOCRACIA”, Instituto de Ciencia Política de la Universidad de Chile (2001).

NORTON, INFORME SOBRE DELITOS INFORMÁTICOS 2011, URL: http://norton.com/cybercrimereport. - Las víctimas de los delitos informáticos aumentaron de un 10% a un 13% este año entre 2011 a 2012.

NÚÑEZ PONCE, J: “DERECHO INFORMÁTICO. UNA NUEVA DISCIPLINA JURÍDICA PARA UNA SOCIEDAD MODERNA”. Perú, Editores S.A, 1996.

ORGANIZACIÓN DE LAS NACIONES UNIDAS, MANUAL PARA LA PREVENCIÓN Y CONTROL DE DELITOS INFORMÁTICOS

ORGANIZACIÓN DE LAS NACIONES UNIDAS, MANUAL PARA LA PREVENCIÓN Y CONTROL DE DELITOS INFORMÁTICOS

ORGANIZACIÓN PARA LA COOPERACIÓN ECONÓMICA Y EL DESARROLLO,

Organización para la Cooperación y Desarrollo Económico (OCDE).", recuperado en http://www.eumed.net/rev/cccss/14/ecra.html

PALAZZI, PABLO ANDRÉS, DELITOS INFORMÁTICOS, AD-HOC, Buenos Aires, 2000.

PECOY, MARTÍN. CONCEPTO DE DELITO INFORMÁTICO. EN "DELITOS INFORMÁTICOS". Universidad de Montevideo. (2012). pp.29-32

PÉREZ EDWIN, DELITOS INFORMÁTICOS EN ECUDOR, Diario el Universo, 2015

PÉREZ MARÍA DE LOS A, DELITOS FINANCIEROS http://resources.lawinfo.com/es/Preguntas-Frecuentes/delitos-financieros/Federal/qu-son-delitos-financieros.html

Periféricos de computadores - Memorias Flash USB». Periféricos - "Introducción a la Informática", A. Prieto (c) McGraw-Hill Interamericana. Archivado desde el original el 25 de noviembre de 2015.

POLAINO NAVARRETE, "DERECHO PENAL, PARTE GENERAL", editorial Bosch Colección: 1ª Edición,

RAYMOND, ERIC (2003). "THE ART OF UNIX PROGRAMMING". pp. 87-91. Consultado el 9 de febrero de 2015.

REAL ACADEMIA DE LA LENGUA ESPAÑOLA, La 23.ª edición (2014) · El Diccionario en el BRAE

SARNAZA, C." CRIMINALITÁ E TECNOLOGÍA", COMPUTER CRIMES, RASEGNA PENITENZIARIA E CRIMINOLOGIA", Nos 1-2, Anno 1, Gennaio €" Giugno, 1979, Roma, Italia. Página 59.

SEGU.INFO "LEGISLACIÓN Y DELITOS INFORMÁTICOS - EL DELINCUENTE Y LA VÍCTIMA", recuperado en http://www.segu-info.com.ar/delitos/delincuenteyvictima.htm

SOLANO BÁRCENAS "MANUAL DE INFORMÁTICA JURÍDICA". Ediciones Jurídicas Gustavo Ibáñez.

SOLANO BARCENAS, ORLANDO: “Manual de Informática Jurídica”. Ediciones Jurídicas Gustavo Ibáñez.

SOLANO BARCENAS, ORLANDO: “Manual de Informática Jurídica”. Ediciones Jurídicas Gustavo Ibáñez.

SUPER INTENDENCIA DE INTENDENCIA, recuperado en Portal del Usuario http://portaldelusuario.sbs.gob.ec/contenido.php?id_contenido=23

SUPER INTENDENCIAS DE BANCOS DEL ECUADOR, Portal del Usuario http://portaldelusuario.sbs.gob.ec/contenido.php?id_contenido=23

SUPERINTENDENCIA DE BANCOS DEL ECUADOR, LIBRO I.- NORMAS GENERALES PARA LAS INSTITUCIONES DEL SISTEMA FINANCIERO: SECCIÓN VII.- DE LAS MEDIDAS DE SEGURIDAD (incluida con resolución No. JB-2011- 1851 de 11 de enero del 2011)

SUPERINTENDENCIA DE BANCOS DEL ECUADOR. “SISTEMA FINANCIERO”,

TÉLLEZ VALDÉS, J, DERECHO INFORMÁTICO, Universidad Autónoma de. México ...

VALLEJO CRISTINA, FALSIFICACIÓN INFORMÁTICA, recuperado en http://www.derechoecuador.com/articulos/detalle/archive/doctrinas/derechoinformatico/2005/11/24/falsificacioacuten-informaacutetica

11. ANEXOS

UNIVERSIDAD NACIONAL DE LOJA

UNIDAD DE EDUCACIÓN A DISTANCIA

CARRERA DE DERECHO

TEMA

"LOS DELITOS INFORMATICOS EN EL SISTEMA FINANCIERO NACIONAL"

PROYECTO DE TESIS PREVIO A LA OBTENCIÓN DEL TITULO DE ABOGADA

AUTORA:

- Tamy Ghislaine Izaguirre García

Loja - Ecuador

2016

1. TEMA

“LOS DELITOS INFORMATICOS EN EL SISTEMA FINANCIERO NACIONAL”

2. PROBLEMÁTICA

Con el avance de la tecnología, esta última década el ser humano, se ha visto obligado a usar los sistemas informáticos para la mayor parte de sus actividades económicas, sociales, educativas y culturales; la verdad es que en nuestro país se podría decir que con todo el retraso tecnológico que llevamos respecto de países industrializados y económicamente poderosos, no hay una persona que siendo económicamente activa no haya usado el sistema informático para alguna actividad, por ejemplo, la mayor parte de las empresas ya no cancelan a sus obreros con cheques, o dinero en efectivo, ahora se recibe la transferencia electrónica de sus remuneración en una cuenta que se asigna en una entidad financiera del sistema financiero nacional.

Actualmente, estamos ya incursionando en la facturación electrónica, dinero electrónico, podemos pagar servicios básicos y de educación a través de una simple transferencia, que hace que un usuario mantenga una cuenta de correo electrónico, acceso a internet y cuenta en el sistema financiero nacional, para a través de un computador, tablet y ahora hasta por celular se pueda realizar transacciones financieras para cualquier actividad económica.

La tecnología nos ahorra tiempo y dinero, ya que no tenemos que ir a un banco o a una ventanilla para realizar pagos por cualquier concepto, ahora lo podemos hacer cuando nos encontramos en nuestro trabajo, en una sala de espera del aeropuerto, en la casa, en un cyber o en cualquier oficina, etc.

Como toda actividad del hombre, siempre generó desde sus inicios personas que se apropien de lo ajeno, la tecnología también ha creado un nuevo orden de delincuentes, que ya no necesitan estar en las calles “atracando” con armas de fuego o realizando daños físicos a sus víctimas; así como nos facilita nuestras actividades económicas también nos está ocasionando ser víctimas de un tipo de delincuentes que ya se preparan y que intelectualmente conocen de estos sistemas más que cualquiera de los usuarios que los usamos.

Por ello, los legisladores, han tenido que crear leyes que protejan a las víctimas de estos delitos, y en nuestro estudio analizaremos los delitos informáticos dentro del sistema financiero nacional, para ello realizamos un análisis de lo que establece el COIP respecto de estos delitos y tenemos:

“Art. 190.- Apropiación fraudulenta por medios electrónicos.- La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona

alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años.

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

El art. 230.- de COIP respecto de la interceptación ilegal de datos, se sancionará con pena privativa de libertad de tres a cinco años, en su numeral 2.

"La persona que diseñe, desarrolle, venda, ejecute, programe o envíe mensajes, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente a la que quiere acceder."

3. JUSTIFICACIÓN

Actualmente los delitos informáticos han aumentado considerablemente al punto de ser necesario legislarlos para que tengan una justa penalización que pueda controlar su difusión y crecimiento. Se debe conocer el panorama de la legislación nacional e internacional en contra de los delitos informáticos, para dimensionar la problemática que está afectando a Ecuador y a países que se pueden encontrar en las mismas condiciones.

Esta normativa legal, debe estar bajo un marco internacional para que se creen alternativas que puedan favorecer su mejor aplicabilidad y sean óptimas en el control de los delitos. Se debe propender porque estas abarquen la mayor parte de manifestación de un hecho delictivo, y máxime si se tienen lineamientos establecidos por países más desarrollados en la lucha por frenar este delito.

La presente investigación, se desarrollará con el objetivo de establecer las falencias existentes en la legislación Ecuatoriana en cuanto a la pena de los delitos informáticos con respecto a la seguridad Informática, la defensa y preservación integral de los sistemas informáticos en contra de los ciber-delincuentes. En este orden de ideas, se hace necesario someter la normativa vigente a revisión para que se puedan determinar falencias que

motiven la formulación de nuevos proyectos de ley que permitan fortalecer la legislación que garantice la protección a las personas y a los datos.

Como individuos y desde cualquier campo de la ciencia, cada ecuatoriano está llamado a realizar aportes que contribuyan al fortalecimiento del sistema jurídico, y desde la ingeniería de sistemas, aún más, desde el punto de vista de los Especialistas en Seguridad Informática debe existir una preocupación más profunda para formular alternativas de cambios y mejoras a la normatividad actual.

4. OBJETIVOS

4.1.- OBJETIVO GENERAL

Realizar un estudio jurídico, crítico y doctrinario del CÓDIGO ORGANICO INTEGRAL PENAL en relación al delito informático.

4.2.- OBJETIVOS ESPECÍFICOS:

4.2.1.- Identificar las falencias en el sistema jurídico ecuatoriano en lo referente los delitos financieros.

4.2.2.- Proponer que nuestra legislación, reforme al CÓDIGO ORGANICO INTEGRAL PENAL aumentando las sanciones con penas y multas más fuertes para las personas que cometan este tipo de delitos.

4.2.3.- Determinar las diferencias y similitudes que existen entre las bases legales ecuatorianas y los otros países, mediante un análisis comparativo.

5.- MARCO TEÓRICO

5.1.1.- Delitos Financieros

El delito financiero se comete en un entorno profesional o comercial con el objetivo de ganar dinero. Estos delitos no son violentos, pero ocasionan pérdidas a compañías, empresas, inversores y empleados. Estos delitos incluyen fraude, hurto y algunas otras violaciones de la ley.

5.1.2 Delito Informático.

En primer lugar se define el Delito como tal, definición de un ilustre en el tema de las ciencias jurídicas:

Ferri: “Son delitos las acciones determinadas por motivos individuales (egoístas) y antisociales, que turban las condiciones de vida y lesionan la moralidad media de un pueblo dado, en un momento dado”.

Hace ya algún tiempo se viene operando en el ambiente tecnológico el concepto de Delito Informático, varios organismos han emitido sus conceptos desde diferentes puntos de vista. Muchos consideran que no es necesario hacer la diferencia con los delitos tradicionales, un ejemplo claro de este concepto se demuestra en el Código Penal de España, en el cual no se compendian los Delitos Informáticos en un grupo específico, los artículos

que se emplean a la hora de castigar un Delito Informático se encuentran inmersos en distintos lugares de la normatividad española.

Un punto de referencia que puede dar un concepto universal de Delito Informático en un ambiente internacional es el Convenio de Ciberdelincuencia del Consejo de Europa, del cual se puede decir:

- Delitos Informáticos: Los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos.

Este tipo de Delitos tiene las siguientes características:

- Son delitos difíciles de demostrar ya que, en muchos casos, es complicado encontrar las pruebas.

- Son actos que pueden llevarse a cabo de forma rápida y sencilla. En ocasiones estos delitos pueden cometerse en cuestión de segundos, utilizando sólo un equipo informático y sin estar presente físicamente en el lugar de los hechos.

Los delitos informáticos tienden a proliferar y evolucionar, lo que complica aún más la identificación y persecución de los mismos.

En definitiva, el Delito Informático es todo acto que haga uso de medios informáticos, que sea contrario a una legislación establecida en un país lo cual acarrea una sanción judicial.

5.1.2.- Convenio de Ciberdelincuencia de 2001.

El Delito Informático fue tema de discusión, cuando en Budapest se reunieron los Países miembros, hasta ese entonces, de la ONU (Organización de Naciones Unidas) para definir los diferentes delitos informáticos como precedente a lo que sería en adelante la fuente principal para legislar acerca de este tipo de problemática que cobra fuerza en todo el ámbito informático, flagelo que se ha ido extendiendo y desarrollando a la par de los diferentes avances tecnológicos.

Existen fuentes muy importantes que ofrecen la tipología de los Delitos Informáticos; para el estudio propuesto también me basaré en el Convenio de Ciberdelincuencial 18 firmado en Budapest, el 23 de noviembre de 2001, el cual entró en vigencia el 01 de julio de 2004.

Adoptado en la actualidad por 43 países según estadísticas que presenta el Concilio de Europa.

Siendo uno de los últimos países no miembros Panamá, quien ratificó su posición frente al convenio el 5 de marzo de 2014 y entró en vigencia a partir del primero de julio de 2014. Y de los países miembros el último a la fecha en ratificar su adhesión al Convenio es Turquía el 29 de septiembre de 2014 para entrar en vigencia a partir del Primero de enero de 2015.

El Convenio de Ciberdelincuencia define los Delitos Informáticos distribuidos en cuatro (4) grupos, así:

1. Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos. Art. 2: Acceso ilícito Art. 3: Interceptación ilícita Art. 4: Interferencia en los datos (Ataques a la integridad de los datos) Art. 5: Interferencia en el sistema (Ataques a la integridad del sistema) Art. 6: Abuso de los dispositivos

2. Delitos informáticos. Art. 7: Falsificación informática Art. 8: Fraude informático

3. Delitos relacionados con el contenido. Art. 9: Delitos informáticos relacionados con la pornografía infantil

4. Delitos relacionados con infracciones de la propiedad intelectual y derechos afines. Art. 10: Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines.

Para el presente estudio se han seleccionado 8 de los 10 Artículos del Convenio Ciberdelincuencia, el Artículo 1 no se menciona porque en este

hace referencia a un glosario de términos, y el Artículo 10 no se incluye en el estudio porque abarcaría un análisis más extenso que incluiría la mención de otras leyes que protegen a los ciudadanos de delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines; los siguientes artículos se tienen en cuenta en el análisis comparativo:

Artículo 2: Acceso ilícito: “Acceso deliberado e ilegítimo a la totalidad o a una parte de un sistema informático. Cualquier Parte podrá exigir que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos o con otra intención delictiva, o en relación con un sistema informático que esté conectado a otro sistema informático”.

Artículo 3: Interceptación ilícita: “la interceptación deliberada e ilegítima, por medios técnicos, de datos informáticos comunicados en transmisiones no públicas efectuadas a un sistema informático, desde un sistema informático o dentro del mismo, incluidas las emisiones electromagnéticas procedentes de un sistema informático que contenga dichos datos informáticos. Cualquier Parte podrá exigir que el delito se haya cometido con intención delictiva o en relación con un sistema informático conectado a otro sistema informático”.

Artículo 4: Interferencia en los datos: “la comisión deliberada e ilegítima de actos que dañen, borren, deterioren, alteren o supriman datos informáticos.

Artículo 5: Interferencia en el sistema: “la obstaculización grave, deliberada ilegitima del funcionamiento de un sistema informático mediante la introducción, transmisión, provocación de daños, borrado, deterioro, alteración o supresión de datos informáticos.”

Artículo 6: Abuso de los dispositivos: “La comisión deliberada e ilegítima de la producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de: un dispositivo, incluido un programa informático, diseñado o adaptado principalmente para la comisión de cualquiera de los delitos previstos de conformidad con los anteriores artículos 2 a 5; una contraseña, un código de acceso o datos informáticos similares que permitan tener acceso a la totalidad o a una parte de un sistema informático. La posesión de alguno de los elementos contemplados, con el fin de cometer cualquiera de los delitos previstos en los artículos del 2 al 5”.

Artículo 7: Falsificación Informática: “cuando se cometa de forma deliberada e ilegítima, la introducción, alteración, borrado o supresión de datos informáticos que dé lugar a datos no auténticos, con la intención de que sean tenidos en cuenta o utilizados a efectos legales como si se tratara de datos auténticos, con independencia de que los datos sean o no directamente legibles e inteligibles. Cualquier Parte podrá exigir que exista una intención fraudulenta o una intención delictiva similar para que se considere que existe responsabilidad penal”.

Artículo 8: Fraude Informático: “los actos deliberados e ilegítimos que causen un perjuicio patrimonial a otra persona mediante: a) Cualquier introducción, alteración, borrado o supresión de datos informáticos; b) Cualquier interferencia en el funcionamiento de un sistema informático, con la intención fraudulenta o delictiva de obtener ilegítimamente un beneficio económico para uno mismo o para otra persona”.

Artículo 9: Delitos relacionados con la Pornografía Infantil: Todo lo relacionado a la Producción de Pornografía Infantil, oferta, difusión o transmisión, adquisición, posesión, utilizando sistemas informáticos.

Según referencia del Doctor Santiago Acurio del Pino (Profesor de Derecho Informático) a través de su libro Delitos Informáticos: Generalidades, en la página 49, manifiesta que La INTERPOL en su 6ª Conferencia Internacional sobre Ciberdelincuencia realizada en el Cairo (Egipto), del 13 al 15 de abril de 2005, recomienda a todos los países miembros de la INTERPOL (que actualmente opera en 190 países), que se utilice el Convenio de Ciberdelincuencia del Consejo de Europa como fuente para legislar en materia de Delitos Informáticos.

De lo manifestado, referente a la existencia o no de leyes que atiendan esta clase de delito, lo cual está contemplado en Ecuador en la LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS (Ley No. 67 del 27 de Febrero de 2002)

Ley que se debe robustecer, también en la explotación pornografía, sexual con niños, niñas y adolescentes, se debe considerar la cooperación Internacional en lo referente al ciber-crimen porque es un fenómeno que traspasa fronteras y a todos atañe.

EN EL PRESENTE TRABAJO DE INVESTIGACIÓN, UTILIZARÉ LOS SIGUIENTES CONCEPTOS:

MOBBING: Situación en la que una persona ejerce una violencia psicológica extrema, de forma sistemática y recurrente y durante un tiempo prolongado sobre otra persona o personas en el lugar de trabajo con la finalidad de destruir las redes de comunicación de la víctima o víctimas, destruir su reputación, perturbar el ejercicio de sus labores y lograr que finalmente esa persona o personas acaben abandonando el lugar de trabajo3.

PHISHING: Consiste en el envío de correos electrónicos que, aparentando provenir de fuentes fiables (por ejemplo, entidades bancarias), intentan obtener datos confidenciales del usuario, que posteriormente son utilizados para la realización de algún tipo de fraude. Para ello, suelen incluir un enlace que, al ser pulsado, lleva a páginas web falsificadas. De esta manera, el usuario, creyendo estar en un sitio de toda confianza, introduce la información solicitada que, en realidad, va a parar a manos del estafador.

SPAM: Son aquellos mensajes que no han sido solicitados, es decir, son de destinatarios desconocidos a los cuales nosotros no hemos contactado. Si bien la principal vía de llegada de estos mensajes es a través del correo electrónico, también puede difundirse por otras vías, por ejemplo, a través de

los teléfonos celulares. También denominado correo basura o mensaje basura.

INTERPOL: Abreviatura de Organización Internacional de Policía Criminal.

Organización fundada en Viena en 1923 y reestructurada en 1946, con sede en París. Persigue los delitos cuando un criminal, burlando la policía de su país, pasa a país extranjero.

6. METODOLOGÍA

6.1. Métodos

La Investigación es de tipo bibliográfico, cualitativa de tipo evaluativa por cuanto se estudia la normativa en cuanto a delitos informáticos para definir las falencias que existen en la legislación ecuatoriana.

En el proceso de investigación socio-jurídico se aplicará el método científico, entendido como camino a seguir para encontrar la verdad acerca de una problemática determinada. Es válida la concreción del método científico hipotético-deductivo para señalar el camino a seguir en la investigación socio-jurídica propuesta; pues, partiendo de las hipótesis y con la ayuda de ciertas condiciones procedimentales, se procederá al análisis de las manifestaciones objetivas de la realidad de la problemática de la investigación, para luego verificar si se cumplen las conjeturas que subyacen en el contexto de la hipótesis, mediante la argumentación, la reflexión y la demostración.

En la ejecución del presente trabajo también emplearemos los métodos que nos permitirán seguir la secuencia pertinente para la obtención respectiva de la información, análisis e interpretación jurídica de los hechos establecidos.

Para el efecto los otros métodos que aplicaremos son: el inductivo, deductivo, analítico-sintético, comparativo y dialéctico, los mismos que nos servirán para desarrollar el proyecto investigativo y concretamente llegar a la

verificación de los objetivos y la contrastacion de la hipótesis a fin de obtener nuevos conocimientos.

El método inductivo y deductivo será aplicado en el desarrollo de la revisión de la literatura tomando referentes de doctrinas y nuevas tendencias relacionadas a la problemática a investigar de aspectos generales a particularidades de temáticas objeto de estudio o viceversa.

El método comparativo será empleado en el estudio de la normativa extrajera relacionada con la prescripción de la acción proveniente de actos y contratos.

El método exegético que será utilizado al momento de desarrollar y analizar las normas jurídicas nacionales e internacionales.

Para el desarrollo de la investigación de campo, específicamente en la tabulación de los cuadros y gráficos de las encuestas emplearemos el método estadístico. En el análisis de los resultados será aplicado el método analítico.

La presente investigación será de tipo generativa, para la recopilación de información recurriremos a las técnicas de investigación bibliográfica, documental, descriptiva, participativa y de campo que será desarrollada en el transcurso de cinco meses.

6.2. Procedimientos y Técnicas.-

Serán los procedimientos de observación, análisis y síntesis los que requiere la investigación jurídica propuesta, auxiliados de técnicas de acopio teórico como el de fichaje bibliográfico o documental; y, de técnicas de acopio

empírico, como la encuesta y entrevista. El estudio de casos judiciales reforzará la búsqueda de la verdad objetiva sobre la problemática. La investigación de campo se concretará a consultas de opinión a personas conocedoras de la problemática, previo muestreo poblacional de por lo menos treinta personas para las encuestas y cinco personas para las entrevistas; en ambas técnicas se plantearán cuestionarios derivados de la problemática, objetivos y de la hipótesis. Los resultados de la investigación empírica se presentarán en tablas, barras o gráficos y en forma discursiva con deducciones derivadas del análisis de los criterios y datos concretos, que servirán para la verificación de objetivos e hipótesis y para arribar a conclusiones y recomendaciones

Las entrevistas pretendemos dirigirlas a personas jurídicas y naturales que laboran en instituciones financieras, ingenieros de sistemas, medios de Comunicación Social, todos ellos entendidos en el tema objeto de nuestra investigación.

7. CRONOGRAMA

ACTIVIDADES	AÑO 2016																															
	ABRIL				MAYO				JUNIO				JULIO				AGOSTO				SEPT.				OCTUBRE				NOV.				DIC.	
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Selección y definición del problema.	X																																			
Elaboración del Proyecto de Investigación.		X																																		
Presentación del Proyecto de Investigación.			X																																	
Aprobación del Proyecto de Investigación.				X																																
Recopilación de información bibliográfica.					X	X	X	X	X	X	X	X																								
Aplicación de encuestas y trabajo de campo.													X	X	X	X	X																			
Fundamentación Jurídica sobre el tema																		X	X																	
Presentación del borrador del avance del Trabajo de Investigación.																				X																
Trámites procesos al grado.																					X	X	X	X	X	X	X	X								
Informe Final, defensa y sustentación del Trabajo de Investigación.																													X	X	X	X	X	X	X	X

8. PRESUPUESTO

8.1 RECURSO HUMANO.-

- Investigadora:

  Tamy Ghislaine Izaguirre García

- Director:

  Por Designar

- Población a Encuestarse:

  30 profesionales del Derecho.

8.2 RECURSOS MATERIALES.-

Los recursos materiales requeridos en la elaboración de esta tesis se encuentran consignados de acuerdo con el siguiente presupuesto.

No.	Material	Costo (USD)
01	Servicios de Internet.	$ 200.00
2	Material de oficina	$ 500.00
03	Reproducción de encuestas.	$ 50.00
04	Reproducción y anillado del trabajo final	$ 200.00
05	Gastos imprevistos	$ 200.00
	Total:	$1.150.00

8.3 FINANCIAMIENTO.-

Los recursos financieros para el desarrollo del Trabajo de la presente tesis, serán solventados por la autora.

9. BIBLIOGRAGIA.-

1. CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR, R. O- 449- 20-10-2008.

2. CÓDIGO ORGANICO INTEGRAL PENAL, Ediciones Legales, Quito - Ecuador, 2014.

3. LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS (Ley No. 67 del 27 de Febrero de 2002.)

4. CODIFICACIÓN DE RESOLUCIONES DE LA SUPERINTENDENCIA DE BANCOS Y SEGUROS Y DE LA JUNTA BANCARIA.

5. CONVENIO DE CIBERDELINCUENCIAL 18 firmado en Budapest, el 23 de noviembre de 2001, en vigencia desde el 01 de Julio de 2004.

6. CABANELLAS DE TORRES, Guillermo. Diccionario Jurídico Elemental, 16va Edición, Editorial Heliasta, Buenos Aires, 2003.

7. CABANELLAS DE LA TORRE Guillermo, Diccionario Enciclopédico de Derecho Usual, Editorial Helianista SRL. Buenos Aires Argentina, 25 abril. Edición, tomo. I. II. III.

ANEXO 2

UNIVERSIDAD NACIONAL DE LOJA

MODALIDAD DE ESTUDIOS A DISTANCIA
CARRERA DE DERECHO

Guía de encuesta aplicada los profesionales de derecho y estudiantes de los últimos años de la carrea de derecho de la Universidad Nacional de Loja

Objetivo. Analizar los delitos informáticos en el Sistema financiero Nacional

1. Considera Usted que los delitos informáticos que se pueden cometer en el sistema financiero ecuatoriano, son un tema de conocimiento público?

Si ( )

No ( )

2. Considera Usted que el sistema jurídico ecuatoriano ampara y respalda eficazmente al sistema financiero a través de las leyes y normas establecidas actualmente.

Si ( )

No ( )

3. Comparando las diferencias y similitudes que existen entre las bases legales ecuatorianas y los otros países, respecto a los delitos financieros, considera Usted que la Legislación Ecuatoriana sanciona adecuadamente éstos delitos.

Si ( )

No ( )

4. De acuerdo a su criterio jurídico ¿Cree Usted que la tipificación tratamientos de los delitos informáticos en el sistema financiero nacional, posee falencias que deben ser corregidas por el sistema jurídico ecuatoriano?

Si ( )
No ( )

5. De acuerdo su criterio jurídico, las penas que establece el Código Orgánico Integral, para sancionar los delitos informáticos en el sistema financiero nacional, se encuentran en concordancia con el tipo de delito cometido?

Si ( )
No ( )

6. Considera Usted, que el Código Integral Penal debe incorporar la tipificación de penas específicas para cada tipo de delito de acuerdo a su gravedad y consecuencias para la víctima?

Si ( )
No ( )

7. ¿Qué aspectos de la penalización de los delitos informáticos, considera deben ser revisados, cambiados y tipificado en el Código Integral Penal COIP?

Sanción para para la institución financiera de acuerdo al delito ( )

Incremento de multas de acuerdo a la gravedad de delito ( )

Incremento de penas de privación de libertad ( )

Todas las anteriores ( )

ANEXO 3

UNIVERSIDAD NACIONAL DE LOJA

MODALIDAD DE ESTUDIOS A DISTANCIA
CARRERA DE DERECHO

Guía de entrevista aplicada a jueces especialistas en derecho penal

Objetivo. Analizar los delitos informáticos en el Sistema financiero Nacional

1. Considera Usted que los delitos informáticos que los delitos informáticos que se cometen contra en el sistema Financiero Nacional son un tema de conocimiento público.

2. Según su criterio jurídico, las penas que establece el Código Orgánico Integral, para sancionar los delitos informáticos en el sistema financiero nacional, está en concordancia con el delito cometido.

3. ¿Considera Usted que la sanción tipificada en Código Integral Penal para los delitos informáticos, debe ser cambiada tipificando penas específicas para cada tipo de delito de acuerdo a su gravedad y consecuencias para la víctima?

4. Que opina respecto del incremento de las sanciones en el cometimiento de los delitos financieros, como mecanismo para evitar se cometan los mismos.

5. ¿Qué aspectos de la penalización de los delitos informáticos, considera deben ser revisados, cambiados y tipificado en el Código Integral Penal COIP?

ANEXO 4

MEMORANDO No. IRP-DL-2015-043 Portoviejo, 30 de octubre 2015

PARA : Abogada Teresa Roca Espinel
INTENDENTE REGIONAL DE PORTOVIEJO

ASUNTO: Informe referente al Juicio Contencioso Administrativo No. 17811-2015-01021

En atención al Memorando No. PJ-2015-778 de 26 de octubre de 2015, recibido en esta Intendencia Regional de Portoviejo el 29 de octubre de 2015, mediante el cual solicita un informe técnico referente a la demanda Contencioso Administrativa No. 17811-2015-01021, interpuesta por el doctor Jaime Manuel Flor Rubianes, representante jurídico del Banco Pichincha C.A., por el reclamo administrativo presentado de la señora Mery Leisbel Del Valle Pico.

Al respecto y para los fines consiguientes, sírvase encontrar el informe solicitado:

ANTECEDENTES

Mediante comunicación ingresada a esta Intendencia Regional de Portoviejo con fecha 16 de agosto de 2012, la contadora pública señora Mery Leisbel Del Valle Pico, portadora de la cédula de ciudadanía No.1306292523, formula reclamo administrativo en contra de la referida entidad financiera, entre los aspectos más relevantes, manifiesta lo siguiente:

"Resulta señor Superintendente que mantengo una cuenta corriente en el Banco Pichincha de esta la Manta desde el año 2006, la cual la he venido manejando sin ningún inconveniente, hasta que el 22 de Febrero del año 2012, día que me fue hecha una transferencia por parte de la Empresa MAREROCE EXPORT IMPORT CIA LTDA, a mi cuenta por la cantidad de USD$15.000,00 Dólares Americanos, tal como lo justifico con la copia del comprobante de la transacción que, adjunto valor del cual se giraron algunos cheques quedando un restante de caso USD$4.000,00 Dólares, por tal motivo siempre tengo que estar pendiente de las transacciones que se realizan desde mi cuenta, en tal circunstancia el día 24 de febrero del presente año 2012, aproximadamente a las 11:58, cuando me encontraba en la Empresa MAREROCE IMPORT CIA LTDA, para la cual venido prestando mis servicios lícitos y personales bajo relación de dependencia de su Gerente y representante legal Ing. Iván Arturo Rodríguez Vera, desempeñándome en calidad de secretaria de gerencia, además encargada del departamento de comercio exterior, de bancos..."

(...) en tal sentido señor superintendente pude observar que a mi correo electrónico bryanmeryvahotmail.com, había llegado un mensaje de la banca electrónica del Banco Pichincha cuya dirección de correo es bancopichincha.com, (servicio que brinda el banco)

ASPECTOS LEGALES

Para el análisis y la resolución del reclamo en mención, se tomaron en consideración varios aspectos de orden legal, mismos que a continuación se detallan:

Constitución de la República del Ecuador:

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

"La Ley establecerá los mecanismos de control de calidad en los procedimientos de defensa de las consumidoras y los consumidores; y las sanciones por vulneración de estos derechos, la reparación e indemnización por deficiencias, daños o mala calidad de bienes y servicios (...)"

Artículo 54.- "Las personas o entidades que prestan servicios públicos o que produzcan o comercialicen bienes de consumo, serán responsables civil y penalmente por la deficiente prestación del servicio...".

Artículo 66.- "Se reconoce y garantizará a las personas:

Numeral 25, "El derecho a acceder a bienes y servicios públicos y privados de calidad, con eficiencia, eficacia y buen trato, así como a recibir información adecuada y veraz sobre su contenido y características"

Ley Orgánica de Defensa del Consumidor, establece lo siguiente:

Artículo 4.- "Derechos del consumidor.- Son derechos fundamentales del consumidor, a más de los establecidos en la Constitución Política de la República, tratados o convenios internacionales, legislación interna, principios generales del derecho y costumbre mercantil, los siguientes:

Numeral 8, "Derecho a la reparación e indemnización por daños y perjuicios, por deficiencias y mala calidad de bienes y servicios;"

Numeral 10, "Derecho a acceder a mecanismos efectivos para la tutela del Ecuador administrativa y judicial de sus derechos e intereses legítimos, que conduzcan a la adecuada prevención sanción y oportuna reparación de su lesión;"

Numeral 11, "Derecho a seguir las acciones administrativas y/o judiciales que correspondan; y,"

Ley General de Instituciones del Sistema Financiero, establece lo siguiente:

Artículo 1.- "Esta Ley regula la creación, organización, actividades, funcionamiento y extinción de las instituciones del sistema financiero privado, así como la organización y funciones de la Superintendencia de Bancos, entidad encargada de la supervisión y control del sistema financiero, en todo lo cual se tiene presente la protección de los intereses del público" (...)

Codificación de Resoluciones de la Superintendencia de Bancos y Seguros y de la Junta Bancaria.

Artículo 6, sección I, capítulo IV, título XIV.- De La Trasparencia de la Información.- que estipula:

"Las instituciones del sistema financiero deberán adoptar las medidas necesarias, de modo que se garantice independencia en las decisiones referentes al ámbito de su actividad y, asimismo, que se eviten conflictos de interés.

Sin perjuicio de lo establecido en el inciso anterior, las instituciones del sistema financiero adoptarán las medidas oportunas para garantizar que los procedimientos previstos para la transmisión de la información requerida por el servicio de atención al cliente y al resto de servicios de la organización respondan a los principios de rapidez, seguridad, eficacia y coordinación."

Artículo 7 de la misma sección, establece:

"Las instituciones del sistema financiero pondrán a disposición de sus clientes, en todas y cada una de las oficinas abiertas al público, la información siguiente:

Inciso cuarto del numeral 7.4, manifiesta:

"Las decisiones que se adopten al término de la tramitación de quejas y reclamaciones mencionarán expresamente el derecho que asiste al reclamante para, en caso de disconformidad con el del Ecuador resultado del pronunciamiento, acudir a La Superintendencia de Bancos y Seguros."

Primer inciso del artículo 3, sección II, capítulo I, título X, libro I de la misma Codificación de Resoluciones de la Superintendencia de Bancos y Seguros y de la Junta Bancaria, que señala:

"Las instituciones del sistema financiero tienen la responsabilidad de administrar sus riesgos, a cuyo efecto deben contar con procesos formales de administración integral de riesgos que permitan identificar, medir, controlar / mitigar y monitorear las exposiciones de riesgo que están asumiendo"

Artículo 4, Tecnología de Información.-, subnumeral 4.3.4.3, del numeral 4.3, sección II.- Factores del Riesgo Operativo, capítulo V.- De la Gestión del Riesgo Operativo, título X.- De la Gestión y Administración de los Riesgos, indica lo siguiente:

"Los controles necesarios para asegurar la integridad, disponibilidad y confidencialidad de la información administrada;"

Artículo 4, Tecnología de Información.-, subnumeral 4.3.4.12, del numeral 4.3, sección II.- Factores del Riesgo Operativo, capítulo V.- De la Gestión del Riesgo Operativo.-, título X.- De la Gestión y Administración de los Riesgos,

indica:

"Las instituciones controladas que ofrezcan los servicios de transferencias y transacciones electrónicas deberán contar con políticas y procedimientos de seguridad de la información que garanticen que las operaciones sólo pueden ser realizadas por personas debidamente autorizadas; que el canal de comunicaciones utilizado sea seguro, mediante técnicas de encriptación de información; que existan mecanismos alternos que garanticen la continuidad del servicio ofrecido; y, que aseguren la existencia de pistas de auditoría."

Artículo 4, Tecnología de información.-, subnumeral 4.3.8.2 del numeral 4.3, sección II.- Factores del Riesgo Operativo.-, capítulo V.- De la Gestión del Riesgo Operativo.-, título X.- De la Gestión y Administración de los Riesgos.-, que señala lo siguiente:
"Establecer procedimientos y mecanismos para monitorear de manera periódica la efectividad de los niveles de seguridad implementados en hardware, software, redes y comunicaciones, así como en cualquier otro elemento electrónico o tecnológico utilizado en los canales electrónicos, de tal manera que se garantice permanentemente la seguridad y calidad de la información.

Artículo 4, Tecnología de información.-, subnumeral 4.3.8.4 del numeral 4.3, sección II.- Factores del Riesgo Operativo.-, capítulo V.- De la Gestión del Riesgo Operativo.-, título X.- De la Gestión y Administración de los Riesgos.-, que señala lo siguiente:

"La información que se transmita entre el canal electrónico y el sitio principal de procesamiento de la entidad, deberá estar en todo momento protegida mediante el uso de técnicas de encriptación y deberá evaluarse con regularidad la efectividad y vigencia del mecanismo de encriptación utilizado"

Artículo 4, Tecnología de información.-, subnumeral 4.3.8.5 del numeral 4.3, sección II.- Factores del Riesgo Operativo.-, capítulo V.-De la Gestión del Riesgo Operativo.-, título X.- De la Gestión y Administración de los Riesgos, que señala lo siguiente:

"Las instituciones del sistema financiero deberán contar en todos sus canales electrónicos con software antimalware que esté permanentemente actualizado, el cual permita proteger el software instalado, detectar oportunamente cualquier intento o alteración en su código, configuración y/o funcionalidad, y emitir las alarmas correspondientes para el bloqueo del canal electrónico, su inactivación y revisión oportuna por parte de personal técnico autorizado de la institución"

Artículo 4, Tecnología de información.-, subnumeral 4.3.8.6 del numeral 4.3, sección II.- Factores del Riesgo Operativo.-, capítulo V.-De la Gestión del Riesgo Operativo.-, título X.- De la Gestión y Administración de los Riesgos.-, que señala lo siguiente:

"Las instituciones del sistema financiero deberán utilizar hardware de propósito específico para la generación y validación de claves para ejecutar transacciones en los diferentes canales electrónicos y dicha información no deberá ser almacenada en ningún momento;"

Artículo 4, Tecnología de información.-, subnumeral 4.3.8.7 del numeral 4.3,

sección II.- Factores del Riesgo Operativo.-, capítulo V.-De la Gestión del Riesgo Operativo.-, título X.- De la Gestión y Administración de los Riesgos.-, que indica:

"Establecer procedimientos para monitorear, controlar y emitir alarmas en línea que informen oportunamente sobre el estado de los canales electrónicos, con el fin de identificar eventos inusuales, fraudulentos o corregir las fallas;"

Artículo 4, Tecnología de información.-, subnumeral 4.3.8.8 del numeral 4.3, sección II.- Factores del Riesgo Operativo.-, capítulo V.-De la Gestión del Riesgo Operativo.-, Título X.- De la Gestión y Administración de los Riesgos, que señala lo siguiente

"Ofrecer a los clientes los mecanismos necesarios para que personalicen las condiciones bajo las cuales desean realizar sus transacciones a través de los diferentes canales electrónicos y tarjetas, dentro de las condiciones o límites máximos que deberá establecer cada entidad."

Artículo 4, Tecnología de información.-, subnumeral 4.3.8.10 del numeral 4.3, sección II.- Factores del Riesgo Operativo.-, capítulo V.-De la Gestión del Riesgo Operativo.-, Título X.- De la Gestión y Administración de los Riesgos.-, que señala lo siguiente:

"Las instituciones deberán establecer procedimientos de control y mecanismos que permitan registrar el perfil de cada cliente sobre sus costumbres transaccionales en el uso de canales electrónicos y tarjetas y definir procedimientos para monitorear en línea y permitir o rechazar de manera oportuna la ejecución de transacciones que no correspondan a sus hábitos, lo cual deberá ser inmediatamente notificado al cliente mediante mensajería móvil, correo electrónico, u otro mecanismo;"

Artículo 4, Tecnología de información.-, subnumeral 4.3.8.11 del numeral 4.3, sección II.- Factores del Riesgo Operativo.-, capítulo V.-De la Gestión del Riesgo Operativo.-, título X.- De la Gestión y Administración de los Riesgos.-, que establece lo siguiente:

"Incorporar en los procedimientos de administración de la seguridad de la información, el bloqueo de los canales electrónicos o de las tarjetas cuando se presenten eventos inusuales que adviertan situaciones fraudulentas o después de un número máximo de tres (3) intentos de acceso fallido. Además, se deberán establecer procedimientos que permitan la notificación en línea al cliente a través de mensajería móvil, correo electrónico u otro mecanismo, así como su reactivación de manera segura;"

Artículo 4, Tecnología de información.-, subnumeral 4.3.8.16 del numeral 4.3, sección II.- Factores del Riesgo Operativo.-, capítulo V.- De la Gestión del Riesgo Operativo.-, título X.- De la Gestión y Administración de los Riesgos.-, que establece lo siguiente:

"(...) Además, la entidad deberá mantener y monitorear un log de auditoría sobre las consultas realizadas por los funcionarios a la información confidencial de los clientes, la cual debe contener como mínimo: identificación del funcionario, sistema utilizado, identificación del equipo (IP), fecha, hora, e información consultada. Esta

información deberá conservarse por lo menos por doce (12) meses;"

Artículo 4, Tecnología de información.-, subnumeral 4.3.8.20 del numeral 4.3, sección II.- Factores del Riesgo Operativo.-, Capítulo V, De la Gestión del Riesgo Operativo.-, título X.- De la Gestión y del Ecuador Administración de los Riesgos.-, que indica lo siguiente:

"Las instituciones del sistema financiero deberán ofrecer a los clientes el envío en línea a través de mensajería móvil, correo electrónico u otro mecanismo, la confirmación del acceso a la banca electrónica, así como de las transacciones realizadas mediante cualquiera de los canales electrónicos disponibles, o por medio de tarjetas;"

Subnumeral 4.3.11.4, del numeral 4.3, artículo 4, Tecnología de Información, sección II.- Factores del Riesgo Operativo.-, capítulo V.- De la Gestión del Riesgo Operativo.-, título X.- De la Gestión y Administración de los Riesgos.-, que establece lo siguiente:

"Implementar mecanismos de control, autenticación mutua y monitoreo, que reduzcan la posibilidad de que los clientes accedan a páginas web falsas similares a las propias de las instituciones del sistema financiero"

Artículo 4, Tecnología de Información.-, subnumeral 4.3.11.7 del numeral 4.3, sección II.- Factores del Riesgo Operativo.-, capítulo V.-De la Gestión del Riesgo Operativo.-, título X.- De la Gestión y Administración de los Riesgos.-, que establece lo siguiente:

"Se deberá informar al cliente al inicio de cada sesión, la fecha y hora del último ingreso al canal de banca electrónica"

Artículo 4, Tecnología de Información, subnumeral 4.3.11.8, del numeral 4.3, sección II.- Factores del Riesgo Operativo.-, capítulo V.-De la Gestión del Riesgo Operativo.-, título X.- De la Gestión y Administración de los Riesgos.-, que establece lo siguiente:

"La institución del sistema financiero deberá implementar mecanismos para impedir la copia de los diferentes componentes de su sitio web, verificar constantemente que no sean modificados sus enlaces (links), suplantados sus certificados digitales, ni modificada indebidamente la resolución de su sistema de nombres de dominio (DNS)"

Artículo 5, capítulo IV.- Procedimientos para la atención de los reclamos contra las instituciones del sistema financiero, Título XX.- De la Superintendencia de Bancos y Seguros, libro I.- "Normas generales para la aplicación de la Ley General de Instituciones del Sistema Financiero" de la Codificación de Resoluciones de la Superintendencia de Bancos y Seguros y de la Junta Bancaria, dice:

"Si el resultado del análisis que realice la Superintendencia determinare la necesidad de que la institución controlada introduzca

correctivos que regularicen la situación que motivó el reclamo.

FUNDAMENTOS DE LA RESOLUCIÓN DE LA INTENDENCIA REGIONAL DE PORTOVIEJO.

Luego de la revisión y el análisis efectuado a la información remitida por la entidad financiera mediante los oficios detallados en los antecedentes, se desprende lo siguiente:

1) OFICIO BP-ACEC-2012-0923 DEL 13 DE NOVIEMBRE DE 2012.

A través del oficio BP-ACEC-2012-0923 del 13 de noviembre de 2012, la entidad financiera, indica:

"(...) Banco Pichincha C.A., de ningún modo, puede responsabilizarse por las transacciones realizadas con las claves personales o coordenadas del cliente."

Es importante indicar que el Artículo 38 de la Constitución de la República del Ecuador, señala que:

"Las actividades financieras son un servicio de orden público (...); tendrán la finalidad fundamental de preservar los depósitos y atender los requerimientos de financiamiento para la consecución de los objetivos de desarrollo del país. Las actividades financieras intermediarán de forma eficiente los recursos captados para fortalecer la inversión productiva nacional, y el consumo social y ambientalmente responsable."

Artículo 52 de la Constitución de la República del Ecuador:

La ley establecerá los mecanismos de control de calidad y los procedimientos de defensa de las consumidoras y consumidores; y las sanciones por vulneración de estos derechos, la reparación e indemnización por deficiencias, daños o mala calidad de bienes y servicios (...)"

Artículo 54 de la Constitución de la República del Ecuador:

"Las personas o entidades que presten servicios públicos o que produzcan o comercialicen bienes de consumo, serán responsables civil y penalmente por la deficiente prestación del servicio, por la calidad defectuosa del producto, o cuando sus condiciones no estén de acuerdo con la publicidad efectuada o con la del Ecuador descripción que incorpore."

Por su parte en los numerales 8, 10 y 11 del artículo 4 de la Ley Orgánica del Consumidor, estipula:

Numeral 8: "Derecho a la reparación e indemnización por daños y perjuicios, por deficiencias y mala calidad de bienes y servicios;"

Numeral 10: "Derecho a acceder a mecanismos efectivos para la tutela administrativa y judicial de sus derechos e intereses legítimos, que conduzcan a la adecuada prevención sanción y oportuna reparación de su lesión;

Numeral 11: Derecho a seguir las acciones administrativas y/o judiciales que correspondan; y,"

En el Artículo 75 ibídem.- Servicios Defectuosos, establece:

"Cuando los servicios prestados sean manifiestamente defectuosos, ineficaces, causen daño o no se ajusten a lo expresamente acordado, los consumidores tendrán derecho, además de la correspondiente indemnización por daño y perjuicios, a que le sea restituido el valor cancelado (...)"

2) CUENTAS DE AHORROS Y CORRIENTES DE LA SEÑORA MERY LEISBEL DEL VALLE PICO.

Conforme lo indica el Oficio BP-ACEC-2012-0923 del 13 de noviembre de 2012 remitido por la institución financiera, la señora Mery Leisbel Del Valle Pico mantuvo las siguientes cuentas en el Banco Pichincha CA

Tipo	Moneda	Cuenta	Estado	Relación
CA	USO	4564120800	ACTIV	PROPIETARIO
CC	USO	3339118904	ACTIV	PROPIETARIO

Apreciándose dos cuentas, una de ahorros y una de cuenta corriente con relación de propietaria o dueña.

3) INFORME DOCUMENTADO POR LOS RESPONSABLES DE LAS ÁREAS: SEGURIDAD DE LA INFORMACIÓN Y DE ATENCIÓN AL CLIENTE.

Si bien en el Oficio BP-ACEC-2012-0923 del 13 de noviembre de 2012, suscrito por la Ingeniera Mary Ferrín Villavicencio, Gerente Sucursal Portoviejo, en el literal e. del punto 1, indica que

"La resolución adoptada en el presente caso, así como nuestra fundamentación, la hacemos conocer en el presente Oficio."

Es de puntualizar que esta Intendencia Regional de Bancos a través del Oficio IDP-SAC-2012-291 del 29 de agosto de 2012, requirió informes documentados y sustentados de las áreas involucradas, especialmente de Seguridad de la Información y de Atención al Cliente, sin que a la fecha se haya recibido los mencionados documentos.

El Artículo 80 de la Ley General de Instituciones del Sistema Financiero, determina:

"La información que las instituciones financieras remitan a la Superintendencia deberá ser suministrada de acuerdo con las instrucciones que ésta imparta."

4) RESPUESTA AL RECLAMO EFECTUADO POR LA SEÑORA MERY LEISBEL DEL VALLE PICO.

La entidad financiera a través del oficio BP-ACEC-2012-0923 del 13 de noviembre de 2012, anexó copia del escrito que la reclamante puso en conocimiento al Banco Pichincha C.A., sobre las transacciones que

están siendo reclamadas. En el documento se identifica que el número de reclamo es el 1781362, cuya fecha de su generación fue el 24 de febrero de 2012, el mismo día de la última transacción que forma parte del petitorio.

Banco Pichincha C.A., dio respuesta a la reclamante a través del oficio BP-UAC-2012-7675 del 22 de marzo de 2012, es decir 27 días después de conocer esta entidad financiera el caso, contraviniendo lo dispuesto en el numeral 12.2, artículo 12, Sección IV.- Objetos y Funciones del Servicio de Atención de Reclamos, Capítulo V.- De la Protección al Usuario Financiero de los Servicios de Información y Atención de Reclamos, Título XIV.- Código de Transparencia y de Derechos del Usuario, Libro I.- Normas Generales para la Aplicación de la Ley General de Instituciones del Sistema Financiero de la Codificación de Resoluciones de la Superintendencia de Bancos y Seguros y de la Junta Bancaria, que dispone:

"La obligación por parte de la entidad de atender y resolver las quejas y reclamaciones presentadas por los usuarios financieros en el plazo de hasta quince (15) días tratándose de reclamos originados en el país; (...) desde su presentación en el servicio de atención al usuario financiero, de acuerdo con las normas que para el efecto expida el directorio de la entidad o el organismo que haga sus veces y que serán sometidas a aprobación de Superintendencia de Bancos y Seguros;"

Adicionalmente en el Artículo 16, Parágrafo I.- Derecho a Reclamo, Sección III.- De la Defensa de los Derechos del Usuario del Sistema Financiero, Capítulo III.- Código de Derechos del usuario del Sistema Financiero, Título XIV.- Código de Transparencia y de Derecho del Usuario, Libro I.- de la Codificación de Resoluciones de la Superintendencia de Bancos y Seguros y de la Junta Bancaria, establece:

"El usuario tiene derecho a que su reclamo o queja sea recibido en la institución financiera, a que sea atendido en forma diligente; a que las respuestas que reciba sean escritas, motivadas, oportunas y que tengan firma de responsabilidad."

De la respuesta del Banco Pichincha C.A., a la reclamante a través del oficio BP-UAC-2012-7675 del 22 de marzo de 2012, se establece que estos documentos no se encuentran motivados ya que no indica ningún artículo o cláusula que se infrinja de alguna ley, norma o contrato.

5) FORMULARIO DE SOLICITUD DE INICIO DE RELACIÓN COMERCIAL "CONOZCA A SU CLIENTE".

La entidad financiera no ha presentado a este Ente de Control el "Formulario de Actualización Anual de Información Básica Personas Naturales" en donde se indica la información básica, actividad económica, declaración de bienes, vehículo, entre otros aspectos del cliente reclamante, no obstante la Intendencia Regional de Portoviejo a través del Oficio IDP-SAC-291 del 29 de agosto de 2012, solicitó también, copia certificada del Formulario de solicitud de inicio de relación comercial "Conozca a su Cliente", correspondiente a los beneficiarios de la transferencia así como el documento

donde se evidencie y conste la firma del funcionario de la entidad, que efectuó las gestiones para confirmar la veracidad de los datos suministrados por la reclamante y beneficiarios de la transferencias, ante tales requerimientos la entidad no ha presentado lo solicitado por el Ente de Control.

Ante la situación descrita en el párrafo anterior, es de recalcar lo que estipula el artículo 14, Sección V.- De la Debida Diligencia y sus Procedimientos, Capítulo IV.- Normas de Prevención de Lavado de Activos y Financiamiento de Delitos para las Instituciones del Sistema Financiero, Libro I de la Codificación de Resoluciones de la Superintendencia de Bancos y Seguros y de la Junta Bancaria, del Ecuador establece:

"Las instituciones del sistema financiero deben diseñar y adoptar el formulario de solicitud de inicio de relación comercial en el que se incorporará como mínimo la información y documentación que se detalla a continuación:

Los procedimientos implementados para la identificación del cliente, deben permitir la realización de las diligencias necesarias, a través de mecanismos que dispone la institución, para confirmar la veracidad de los datos suministrados por éste en el formulario de solicitud de inicio de relación comercial con la institución del sistema financiero."

6) DOCUMENTOS DE REFERENCIA DE LA USUARIA RECLAMANTE Y DE LA USUARIA BENEFICIARIA DE LA TRANSACCION EN DISPUTA.

Con el fin de establecer el destino del dinero objeto de la transacción materia de este reclamo, mediante oficio IDP-SAC-2012-291 del 29 de agosto de 2012 remitido por la Intendencia Regional de Portoviejo se solicitó la copia certificada de la cédula de identidad, papeleta de votación, recibo de servicios básicos y referencias que Banco Pichincha C.A., solicitó al titular para aperturar la cuenta correspondiente a la beneficiaria de la transferencia en disputa; la entidad financiera no ha remitido a esta Intendencia Regional de Portoviejo los documentos concernientes ni de la reclamante ni de la beneficiaria de la transferencia, situación que inobserva lo dispuesto en el literal 14.1.15 del artículo 14, Sección V.- De la Debida Diligencia y sus Procedimientos, Capítulo IV.- Normas de Prevención de Lavado de Activos y Financiamiento de Delitos para las Instituciones del

Sistema Financiero, Libro I de la Codificación de Resoluciones de la Superintendencia de Bancos y Seguro y de la Junta Bancaria, que establece:

"Las instituciones del sistema financiero deben diseñar y adoptar el formulario de solicitud de inicio de relación comercial en el que se incorporará como mínimo la información y documentación que se detalla a continuación:

(…) "Referencias personales, y/o bancarias y/o comerciales;"

7) PERFIL FINANCIERO DE LA RECLAMANTE Y DE LA BENEFICIARIA DE LA TRANSFERENCIA ELECTRÓNICA.

La entidad anexó a través del oficio BP-ACEC-2012-0923 del 13 de noviembre de 2012, dos pantallas de la herramienta utilizada por el Banco de Pichincha C.A., en la que se indica en forma general la propuesta del perfil y proceso de cálculo de riesgo del usuario reclamante, sin embargo es de indicar que la Intendencia Regional de Portoviejo a través del oficio IDP-SAC-2012-291 del 29 de agosto de 2012, solicitó también el detalle del perfil financiero de los beneficiarios de las transferencias, de los cuales no se recibió evidencia de lo requerido.

Situación que incumple lo dispuesto en el artículo 89 de la Ley General de Instituciones del Sistema Financiero que indica:

"Las instituciones del sistema financiero están obligadas a mantener sistemas de control interno que permitan una adecuada identificación de las personas que efectúan transacciones con la institución".

Tarjeta de coordenadas E-KEY N° 1170032

De acuerdo a lo que indica el oficio BP-ACEC-2012-0923 del 13 de noviembre de 2012, la señora Mery Leisbel Del Valle Pico, consta como propietaria de la tarjeta E-Key N° 1170032, no obstante la entidad no remitió evidencia documentada sobre la solicitud, entrega y cancelación de dicha tarjeta, pese a ser solicitado por el Organismo de Control mediante oficio No. IDP-SAC-2012-291 del 29 de agosto de 2012

8) EVIDENCIA DE LA CLAVE INICIALMENTE ASIGNADA A LA CLIENTE Y DE LOS DIFERENTES CAMBIOS DE CLAVES EFECTUADOS.

La Intendencia Regional de Portoviejo a través del oficio IDP-SAC-2012-291 del 29 de agosto de 2012, requirió evidencias (log especificando fecha, hora y dirección ip) de la clave electrónica asignada al cliente y diferentes cambios de claves efectuados u otros tipos de controles establecidos por la entidad como mecanismos de seguridad, sin embargo Banco Pichincha C.A., en el oficio BP-ACEC-2012-0923 del 13 de noviembre de 2012 señala que:

"La clave electrónica es personal y generada por el propio cliente por lo que nos vemos impedidos de atender su requerimiento."

Dicha contestación no se ajusta a lo solicitado por el Organismo de Control.

9) GRABACIONES REALIZADAS POR EL BANCO SOBRE LAS COMUNICACIONES TELEFÓNICAS MANTENIDAS CON LA RECLAMANTE.

La Intendencia Regional de Portoviejo a través del oficio IDP-SAC-2012-291 del 29 de agosto de 2012, requirió del Banco Pichincha C.A., formato mp3 de las grabaciones realizadas por el banco sobre las comunicaciones mantenidas con la reclamante, para lo cual la entidad

financiera adjuntó un cd con la llamada efectuada por la reclamante al servicio de Cali Center el día 24 de febrero de 2012, dicha grabación tiene una duración de 6 minutos 3 segundos, entre los aspectos más importantes se destacan los siguientes:

- La señora Del Valle indica que se percató de las transacciones en su cuenta de mail.
- De acuerdo a lo mencionado por la señora Del Valle nunca le enviaron mensajes al celular en donde se le informe el débito de los valores de las transferencias electrónicas que están siendo objeto del reclamo.
- El Asesor de Cali Center recibe la llamada a las 12h42 y le indica a la señora Del Valle que efectivamente le ha sido transferido la cantidad de USD$3.500,00 desde su cuenta corriente y que se quedan bloqueadas las tarjetas Ekey y de Débito siendo las 12h44, además de indicarle a cliente que registre por escrito su reclamo por fraude electrónico.

Al respecto, el Call Center debería tener en estos casos más agilidad y la opción de ver a que cuenta fue realizada la transferencia para bloquear el dinero en la cuenta beneficiara hasta comprobar si es lícita la misma.

Hubo el tiempo de 2 minutos para bloquear el dinero en la cuenta beneficiaria ya que uno de los retiros (el de mayor valor $3.500) fue hecho a las 12h44.

9) LISTADO DE MOVIMIENTOS DE LA CUENTA CORRIENTE DE LA RECLAMANTE.

A través del oficio IDP-SAC-2012-291 del 29 de agosto de 2012, esta Intendencia Regional de Bancos, solicitó el listado de movimientos de la cuenta de corriente N°3339118904 de la reclamante desde el mes de diciembre de 2011 hasta agosto de 2012

De la revisión a la cuenta de corriente N° 3339118904 perteneciente a la señora Mery Leisbel Del Valle Pico, se identificó las siguientes transacciones en los días del 22 al 24 de febrero de 2012

Fecha Contable	Receptora	Tipo	Transacción	Documento	N° Operació	Valor	Saldo
22/02/2012	0098- CALLE 13	D	COMISIÓN SOLICITUD DE CHEQUE	1301	651247824	9,00	14.530,35
22/02/2012	0098- CALLE	D	PAGO CHQ.	13016	652716183	2.000,	12.530,
22/02/2012	0006-MANTA	D	INTERES DE		54	0,45	12.529,
23/02/2012	8763-CENTRO	D	PAGO CHQ CÁMARA	12740	3762	286,88	12.243,
23/02/2012	0098-CALLE 13	H	DEPOSITO		65393711	350,0	12.593,
23/02/2012	0006-MANTA	D	PAGO CHEQUE	13031	65554033	357,4	12.235,
23/02/2012	0098-CALLE 13	D	PAGO CHEQUE	13020	65660923	9.000,	3.235,5
24/02/2012	23/02/2012	D	ENTREGA ESTADO DE		2605	1,66	3.233,8
24/02/2012	8763-CENTRO	D	PAGO CHEQ. CAMARA	12795	2361	153,6	3.080,2
24/02/2012	0006-MANTA	D	TRASNFERENCIA INTERNET		659373871	3.500,00	-419,74
27/02/2012	0197-	D	TELEFONIA CELULAR	79205	668291362	44,80	-464,54
28/02/2012	0151- SAMBORON	H	DEPOSITO CHEQUE EFECTIVIZADO	2925	669640682	560,00	95,46
28/02/2012	0098- CALLE	D	DEPOSITO		67294028	180,0	275,46
28/02/2012	0197- SERVICIOS	H	TELEFONIA CELULAR	792224783	673342370	47,81	227,65
28/02/2012	0006-MANTA	D	INTERESES		46	0,76	226,89

El Banco Pichincha C.A., en el Oficio BP-ACEC-2012-0923 del 13 de noviembre de 2012, señala:

"De la cuenta 3339118904 de la Señora Mery Del Valle Pico se realizó la transferencia desde la dirección IP. 200.108.108.73, como se detalla a continuación:

Fecha	Valor	Cta Origen	Cta Destino	Beneficiario	IP
2012-02-24 11:56	3.500,000	3339118904	3502901800	POTOSITABI, LAURA-ROSA	200.108.108.73

Existiendo, una inconsistencia ya que en este oficio da otra cuenta (3502901800) y otra beneficiaria (POTOSI-TABI, LAURA-ROSA) que se contrasta con el oficio de auditoria interna AUD-C-R-026-2013, en el que indica:

"Al validar los archivos proporcionados por el área de tecnología, se observa que el 24 de febrero de 2012, se realizó la transferencia a través del canal electrónico internet, desde la cuenta corriente No. 3339118904 de propiedad del reclamante por el valor de USD 3,500, con destino a la cuenta de ahorros No. 6227036600 del Banco Pichincha y que de acuerdo con la información del sistema, pertenece a la señora Mercy Madelena Cabrera Pilligua"

Ante ello, es importante mencionar, lo establecido en el Artículo 80 de la Ley General de Instituciones Financieras que manifiesta:

"(...) Las copias de la información que remitan las instituciones del sistema financiero a la Superintendencia, certificadas en la forma que ésta determine, servirán como medio de prueba conforme al Código de Procedimiento Civil, y su falsificación o alteración acarreará responsabilidad penal."

11) DETALLE O LOG DE LAS DISTINTAS TRANSACCIONES EFECTUADAS A TRAVÉS DE LA TARJETA E-KEY.

La Intendencia Regional de Portoviejo a través del Oficio IDP-SAC-2012-291 del 29 de agosto de 2012, solicitó un detalle o log de las distintas transacciones efectuadas (exitosas y fallidas) en el período de diciembre de 2011 hasta agosto de 2012, en donde se señala: consultas, pagos, actualización de información, transferencias, incluyendo la fecha, hora y dirección IP desde donde se efectuaron las mismas.

Banco Pichincha remitió un documento denominado "Log Internexo" en cuya revisión se observa que el día 24 de febrero de 2012 a las 11:50:09, se efectuó la "validación de la firma en el sistema Ingreso Biométrico" desde la dirección ip 200.108.108.173 denegando el acceso y queda registrado el siguiente mensaje "Denied because the user-s biometric registry indicates a posible fraud", que una vez traducido al español significa "Negado porque el usuario-s el registro del biometric indica un posible fraude", esto evidencia que el Banco Pichincha C.A., si tuvo un indicador de fraude, luego a las 11:51:51 vuelven a accesar y esta vez logra entrar desde el mismo ip haciendo la activación de cuentas para transferencia y aumentando el cupo diario de transferencia entre cuentas en USD$4.000,00 y a las 11:56:24 con el mismo ip realiza la transferencia de USD$3.500,00 a la cuenta del mismo banco No. 6227036600 de propiedad de Mercy Cabrera Pilligua. Además se verifica que al momento de la transferencia el saldo contable era inferior al valor de la referida transferencia, sobregirando el Banco a la reclamante la cantidad de USD$419,74.

Evidenciándose, que algunas transacciones que constan en el corte de movimientos de la cuenta corriente 3339118904 desde diciembre de 2011 hasta marzo de 2012, no se registran en el Log Internexo proporcionado por el Banco Pichincha C.A.

Ante lo expuesto, es de indicar que el literal b) del artículo 180, de la Ley General de Instituciones del Sistema Financiero manifiesta:

"El Superintendente de Bancos tiene las siguientes funciones y atribuciones:

(...) evaluar la calidad y control de la gestión de riesgo y verificar la veracidad de la información que genera"

12) DETALLE DE USUARIOS INTERNOS QUE TUVIERON ACCESO A LA CUENTA CORRIENTE N° 3339118904.

Mediante Oficio IDP-SAC-2012-291 del 29 de agosto de 2012, la Intendencia Regional de Portoviejo solicitó el detalle de los usuarios internos-empleados que tuvieron acceso a la cuenta corriente N° 3339118904 entre diciembre de 2011 hasta agosto de 2012. Banco Pichincha C.A., remitió el documento denominado "Log de Asesores y Balcones", de cuya revisión se observa que el día 23 de febrero de 2012, un día antes de la fecha en que se produjo las transacción objeto del presente reclamo, existieron ingresos al aplicativo denominado "Asesores" por parte del usuario EPZAMBRA a la cuenta corriente N° 3339118904 perteneciente al usuario reclamante.

Aplicación	Cod-Oficina	Cod Usuario	Fecha Inicio	Cod_ Recurso	Tipo Acción	Identificación Cliente	Cuenta Origen
Asesores	98	EPZAMBRA	2012-02-23 15:33:59.703	TAEACUEN 1100	Ingreso	1306292523	3339118904
Asesores	98	EPZAMBRA	2012-02-23 15:34:29.703	TAEACLIEO 100	Ingreso	1306292523	
Asesores	8464	DPADILLA	2012-02-24 12:43:10.240	TAEACUEN 1100	Ingreso	1311120701	4564120800
Asesores	8464	DPADILLA	2012-02-24 12:43:15.257	TAEACUEN 0400	Ingreso	1311120701	4564120800
Asesores	8464	DPADILLA	2012-02-24 12:43:19.553	TAEACUEN 1100	Ingreso	1311120701	3339118904
Asesores	8464	DPADILLA	2012-02-24 12:43:24.257	TAEACUEN 0400	Ingreso	1311120701	3339118904
Asesores	8464	DPADILLA	2012-02-24 12:43:50.790	TAEACUEN 0400	Ingreso	1311120701	3339118904
Asesores	8464	DPADILLA	2012-02-24 12:54:41.993	TAEACUEN 1100	Ingreso	1311120701	3339118904
Asesores	8464	DPADILLA	2012-02-24 12:54:50.997	TAEACUEN 0400	Ingreso	1311120701	3339118904
Asesores	6	EALCIVAR	2012-02-24 13:28:07.323	TAEACLIEO 100	Ingreso	1311120701	
Asesores	6	EALCIVAR	2012-02-24 13:28:18.607	TAEACLIEO 100	Ingreso	1311120701	3339118904
Asesores	6	EALCIVAR	2012-02-24 13:28:20.557	TAEACUEN 1100	Ingreso	1311120701	3339118904
Asesores	6	EALCIVAR	2012-02-24 13:28:25.997	TAEACUEN 0400	Ingreso	1311120701	3339118904
Asesores	6	EALCIVAR	2012-02-24 13:28:40.153	TAEACUEN 0400	Ingreso	1311120701	3339118904
Asesores	6	EALCIVAR	2012-02-24 14:14:20.500	TAEACUEN 0400	Ingreso	1311120701	3339118904

No obstante, Banco Pichincha C.A., no remitió a esta Intendencia los sustentos o justificativos de los motivos que los usuarios EPZAMBRA, DPADILLA Y EALCIVAR ingresaron a las cuentas anteriormente descritas como se solicitó mediante IDP-SAC-2012-291 del 29 de agosto de 2012.

Por lo anterior, es de indicar que el artículo 80 de la Ley General de Instituciones del Sistema Financiero, estipula:

"La información que las instituciones financieras remitan a la Superintendencia deberá ser suministrada de acuerdo con las instrucciones que ésta imparta."

13) MONITOREO DE LAS TRANSACCIONES REALIZADAS DE LA RECLAMANTE Y DEL TITULAR DE LA CUENTA BENEFICIARIA DE LAS TRANSFERENCIAS DESDE EL 1 DE MARZO HASTA AGOSTO DE 2012.

A través del oficio IDP-SAC-2012-291 del 29 de agosto de 2012 enviado por la Intendencia Regional de Portoviejo al Banco Pichincha C.A., solicitó el análisis del monitoreo de las transacciones realizadas de la reclamante y de la titular de la cuenta beneficiaria desde diciembre de 2011 a agosto de 2012 en función del perfil transaccional, así como de las señales de alerta generadas y de las autorizaciones según nivel de aprobación establecido.

Banco Pichincha C.A., a través del Oficio BP-ACEC-2012-0923 del 13 de noviembre de 2012, manifiesta:

"Respecto del monitoreo de las transferencias vía intemet las mismas son realizadas por el titular de la cuenta, no obstante de ello, en el momento que el cliente solicita el usuario y clave biométrica el sistema requiere el ingreso de un correo electrónico y número celular, estos campos son obligatorios debido a que la información proporcionada, permite notificar automáticamente a través de un SMS al número celular y dirección de e-mail las transferencias realizadas vía intemet"

La respuesta emitida por Banco Pichincha C.A., no se ajusta a lo requerido por el Ente de Control y más bien da entrever que la entidad financiera no posee una herramienta informática de control y monitoreo de transacciones así como de políticas y procedimientos de la debida diligencia, situación que inobserva lo dispuesto en el literal 12.4, artículo 12, sección V.- De la debida diligencia y sus del Ecuador procedimientos, capítulo IV.- Normas de Prevención de Lavado de Activos y Financiamiento de Delitos para las Instituciones del Sistema Financiero, Libro I de la Codificación de Resoluciones de la Superintendencia de Bancos y Seguros y de la Junta Bancaria, que estipula:

"Las instituciones del sistema financiero están obligadas a aplicar procedimientos de debida diligencia, que implican:
(- -.)

Efectuar de forma permanente los procesos de monitoreo a todas las transacciones, de manera tal que se determine si la transaccionalidad del cliente se ajusta a los perfiles transaccional y de comportamiento establecidos;

Para la ejecución de los procedimientos contemplados en el presente artículo, la entidad dispondrá de recursos humanos suficientes, herramientas informáticas confiables y seguras, infraestructura adecuada independiente y segura y controles internos, que garanticen la calidad de la información de sus clientes, el establecimiento de perfiles transaccionales y de comportamiento reales, que detecten permanentemente las transacciones inusuales y viabilicen en forma oportuna los reportes de todas las transacciones inusuales e injustificadas."

De igual manera el artículo 15, sección V.- De la debida diligencia y sus procedimientos, capítulo IV.- Normas de Prevención de Lavado de Activos y Financiamiento de Delitos para las Instituciones del Sistema Financiero, Libro I de la Codificación de Resoluciones de la Superintendencia de Bancos y Seguros y de la Junta Bancaria, que estipula:

"(...)

Es responsabilidad de la institución del sistema financiero monitorear todas las transacciones de las cuentas que se mantengan en la institución."

14) MANUAL DE PREVENCIÓN DE LAVADOS DE ACTIVOS, MANUAL DE MONITOREO DE FRAUDES Y MANUAL DE TRANSFERENCIAS ELECTRÓNICAS.

No se evidenció que Banco Pichincha C.A., haya remitido los siguientes manuales:

- Manual de Control Interno Para la Prevención de Lavados de Activos.
- Manual de Monitoreo de Fraudes.
- Manual de Políticas, Procesos y Procedimientos de transferencias electrónicas y para la emisión, entrega y activación de las tarjetas para realizar transferencias electrónicas y la solicitud suscrita por la reclamante.

Pese a que dicho requerimiento fue solicitado por la Intendencia de Portoviejo, mediante Oficio IDP-SAC-2012-291 del 29 de agosto de 2012.

15) MECANISMOS DE CONTROL Y NIVELES DE SEGURIDAD IMPLEMENTADAS EN EL CANAL DE BANCA VIRTUAL

Banco Pichincha C.A., no remitió evidencia certificada sobre los mecanismos de control y niveles de seguridad que estuvieron implementadas en el canal de banca electrónica, aplicativos informáticos, dispositivos, redes y demás recursos informáticos que operaron en la entrega del servicio de transferencias vía internet e impedir que el sitio web sea suplantados, indicando las fechas en que fueron implementadas en cada uno de ellos.

16) MEDIDAS PREVENTIVAS EJECUTADAS POR EL BANCO PICHINCHA C.A. PARA MINIMIZAR EL RIESGO DEL SERVICIO ELECTRÓNICO.

En oficio BP-ACEC-2012-0923 del 13 de noviembre de 2012 como medida complementaria de seguridad, Banco Pichincha C.A., manifiesta lo siguiente:

"... el Banco implementó la tarjeta de carácter personal e intransferible denominada "E-key", en la cual se registra la coordenada solicitada por el

sistema para aceptar la transacción, siendo igualmente de responsabilidad exclusiva del cliente mantener en secreto las coordenadas constantes en su tarjeta "E-key", y la más estricta custodia de la misma..."

No obstante, la Intendencia Regional de Portoviejo a través del oficio IDP-SAC-2012-291 del 29 de agosto de 2012, solicitó a la entidad financiera las medidas preventivas para minimizar este tipo de riesgos así como de evidencias de las mismas puntualizando a partir de qué fecha se iniciaron; de los cuales Banco Pichincha C.A., no remitió dicha información.

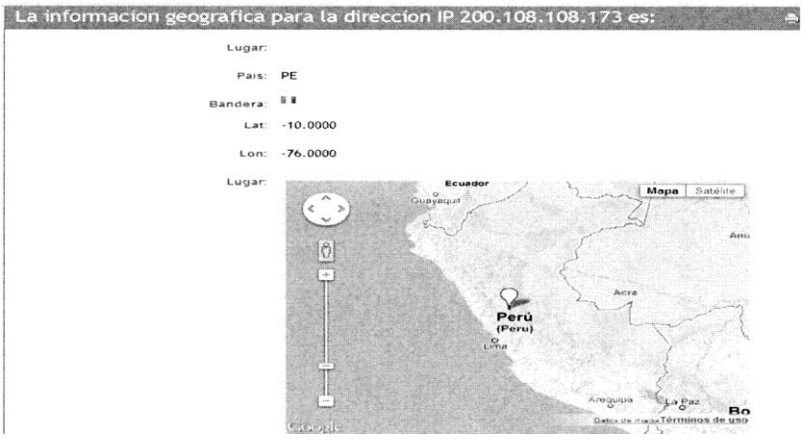
Así mismo, la Intendencia Regional de Portoviejo solicitó mediante oficio IRP-SAC-2013-180 del 14 de mayo de 2013, las políticas y procedimientos que Banco Pichincha C.A., aplica cuando las cuentas de ahorros y cuentas corrientes pasa al estado "desautorizada", tal como se menciona en el informe de Auditoría Interna AUD-C-R-026-2013 del 30 de enero de 2013; y se les volvió a insistir que envíen el sustento debidamente certificado de las papeletas de los retiros en anverso y reverso de la cuenta de ahorros No. 6227036600 perteneciente a la señora Mercy Madelane Cabrera Pilligua del 24 de febrero de 2012, ante tal instrucción la entidad financiera envía en oficio BP-ACEC-2013-0530 de 16 de mayo de 2013, lo solicitado, evidenciado que los retiros fueron hechos el mismo día, uno de USD504,00 a las 12h36 y el segundo por el valor de USD3.000,00 a las 12h44.

Ante lo expuesto se puede observar que la llamada al Call Center del Banco del Pichincha C.A., fue realizada a las 12h42 existiendo la posibilidad de bloquear los fondos de la cuenta beneficiara y no se lo hizo.

17) DIRECCIONES IP'S UTILIZADA EN LA TRANSFERENCIA ELECTRÓNICA.

Del análisis efectuado a la dirección ip: 200.108.108.173 de la cual se efectuó la transacción que está siendo objeto del presente reclamo, se evidenció que ésta pertenece al Proveedor de Internet Telefónica de Perú, localizado en Lima, como se muestra en la siguiente pantalla

Dirección IP: 200.108.108.173



De la revisión efectuada al documento denominado "Log Internexo" proporcionado por la entidad financiera, no se identificó que la dirección ip: 200.108.108.173 haya sido utilizada anteriormente para efectuar transferencias electrónicas en el comportamiento de la señora Del Valle, es de resaltar que llama la atención que esta misma dirección ip se encuentre registrada en aquellos intentos por accesar y cambio de montos en el cupo de transferencia y que el banco mismo califica como dudosas en su logs enviados.

La Intendencia Regional de Portoviejo a través del oficio IRP-SAC-2012-291 de 29 de agosto de 2012, solicitó análisis del monitoreo de las transacciones realizadas de la reclamante y del titular de la cuenta beneficiaria de la transferencia desde diciembre a de 2011 a agosto de 2012 con los respectivos sustentos emitidos por la Unidad de Prevención de Lavado de Activos, referente a los movimientos transaccionales de las cuentas involucradas, de las cuales esta Intendencia Regional no recibió informe alguno.

De acuerdo al análisis de la información, su representado ha incumplido con lo estipulado en el artículo 77 de la Ley General de Instituciones del Sistema Financiero en los ítems 3, 6,15 y 17 del presente oficio, que estipula:

"Las instituciones del sistema financiero estarán obligadas a dar todas las facilidades para que la Superintendencia cumpla sus funciones y deberán dar acceso a su contabilidad, libros, correspondencia, archivos o documentos justificativos de sus operaciones al Superintendente o a sus delegados."

Igualmente incumplió en el artículo 134 de la Ley General de Instituciones del Sistema Financiero, en lo ítems 5, 6, 7 del presente oficio, que estipula:

"Cuando en una institución del sistema financiero sus directores, administradores, funcionarios o empleados infringiesen leyes o reglamentos que rijan su funcionamiento y dichas leyes o reglamentos no establezcan una sanción especial, o en los casos en que contravinieren instrucciones impartidas por la Superintendencia, ésta impondrá la sanción de acuerdo con la gravedad de la infracción, la misma que no será menor de 50 UVCs y no excederá de 3.000 UVCs."

Adicionalmente incumplió lo que establece el artículo 128 y su literal d) de la Ley General del Sistema Financiero, en los ítems 8, 9 y 16 del presente oficio que determina:

"Cualquier director, administrador, funcionario o empleado de una institución del sistema financiero o la persona que actúe en nombre y representación de aquellos, será personalmente responsable, cuando hubiere cometido una de las siguientes infracciones:

d) Ocultamiento, alteración fraudulenta o supresión en cualquier informe de operación, de datos o de hechos respecto de los cuales la Superintendencia y el público tengan derecho a estar informados; y,

Así como también incumple con lo dispuesto en el literal n) del artículo del Ecuador 180 de la Ley General de Instituciones del Sistema Financiero, que indica:

"El Superintendente de Bancos tiene las siguientes funciones y atribuciones:

Exigir que se le presenten, para su examen, todos los valores, libros, comprobantes de contabilidad, correspondencia y cualquier otro documento relacionado con el negocio o con las actividades inspeccionadas, sin que se pueda aducir reserva de ninguna naturaleza;"

Luego del análisis expuesto, de los descargos y la información remitida por la entidad financiera, esta Intendencia Regional concluyó lo siguiente:

La responsabilidad de gestionar los riesgos inherentes al canal de banca electrónica es de competencia exclusiva de la entidad financiera, quien es la que ha puesto éste servicio a disposición del usuario, por lo cual debió contar con los resguardos necesarios que permitan minimizar los efectos de accesos no autorizados a las cuentas de sus clientes, quienes no pueden asumir las omisiones y/o falta de implementación de controles oportunos en los servicios ofertados.

Que el Banco Pichincha C.A., no cumplió completamente con el envío de la información solicitada por la Superintendencia de Bancos y Seguros, conforme lo establece la Ley General de Instituciones del Sistema Financiero, así como de incumplimientos a normas de la Codificación de Resoluciones de la Superintendencia de Bancos y Seguros y de la Junta Bancaria como se detalla en el presente documento.

Considerando las políticas conozca a su cliente y de debida diligencia, en el presente caso, no se ha aplicó un monitoreo a las operaciones de la cuenta de corriente N° 3339118904 y cuenta de ahorro N° 6227036600 correspondientes a la señora Del Valle y señora Cabrera respectivamente, el cual hubiera permitido al banco definir los parámetros inusuales de comportamiento de su cliente en las transacciones a través del proceso de transferencias por Internet.

Banco Pichincha C.A., no ha probado que el cliente actuó negligente e irresponsablemente en la custodia de la tarjeta E-Key N° 1170032 asignada, ni que efectuó la transferencia desde Perú, más aún cuando no se ha comprobado que la usuaria financiera haya abandonado el país en aquellas fechas.

Existió incumplimientos de la respuesta del Banco Pichincha C.A., a la reclamante en el plazo establecido en la Codificación de la Superintendencia de Bancos y Seguros y de la Junta Bancaria, del Ecuador ausencia de una efectiva gestión por parte del banco para confirmar la veracidad de los datos suministrados por los clientes.

Con estas consideraciones la Intendencia Regional de Portoviejo, resolvió en base a lo dispuesto en los literales b y o, del artículo 180 de la Ley General de

Instituciones del Sistema Financiero y en ejercicio de la delegación de atribuciones conferidas a través de la resolución N° ADM-2013-11454 del 2 de abril de 2013, en concordancia con el Artículo 5, Sección I, Capítulo IV, Título XX, Libro I de la Codificación de Resoluciones de la Superintendencia de Bancos y Seguros y de la Junta Bancaria, que Banco Pichincha C.A. dentro del plazo de setenta y dos horas proceda al reintegro de USD3.500,00 reclamado por la señora Mery Leisbel Del Valle Pico.

ARGUMENTOS DE HECHO Y DE DERECHO DEL DEMANDANTE

En el oficio de impugnación presentado por el Banco Pichincha C.A., se realizaron las siguientes aseveraciones como fundamentos del recurso interpuesto y que se citan textualmente:

Entre los principales argumentos que el Banco manifiesta son los siguientes:

"La propia Intendencia de Portoviejo ratifica el hecho de que "efectivamente", la claves privadas, usuarios y coordenadas de la tarjeta E-key, "se encuentran bajo custodia y resguardo del cliente titular o propietario de la cuenta"; consecuentemente, se confirma el criterio de que la Institución no tiene responsabilidad respecto de la transacción objeto del reclamo, esto es, una transferencia realizada desde la cuenta de la cliente el mes de febrero del 2012, por el valor total de US$ 3.500,00 (tres mil quinientos dólares de los Estados Unidos de América)"

"(...) Temas como los de notificaciones de alerta para transferencias electrónicas, constituyen más bien esquemas adicionales…"

"La afectación al cliente se produce, no por falta de seguridad en los sistemas del Banco, en ningún caso. La afectación es producto del uso incorrecto del canal electrónico. Y este hecho solo puede ser imputable al usuario."

De los argumentos planteados por la entidad financiera, se evidencia claramente la pretensión del Banco Pichincha C.A., de deslindarse de toda responsabilidad respecto de la transferencia electrónica realizada el 24 de febrero de 2012 a las 11:56:24 por el valor de USD. 3,500, de la cuenta corriente No. 3339118904 perteneciente a Mery Leisbel Del Valle Pico, ejecutada desde el IP 200.108.108.173 cuya ubicación es en Lima-Perú, manifestando que las claves, usuarios y coordenadas de la tarjeta e-key sólo se encuentran bajo la custodia y resguardo del cliente titular de la cuenta y que la afectación es producto del uso incorrecto del canal electrónico y que por lo tanto este hecho solo puede ser imputable al usuario financiero.

Al respecto no se observa en el expediente que el Banco haya remitido a este Organismo de Control la documentación suficiente y competente respecto si los procedimientos internos responden a una validación y verificación adecuada del sistema operativo informático implementado por el Banco para la realización de transferencias entre cuentas.

Además como se puede observar en el "log de transacciones" que con fecha 24 de febrero de 2012 a las 11:50:09, mediante el IP 200.108.108.173 como ya se

dijo anteriormente queda ubicado en Lima-Perú se acceso al sistema biométrico registrando el siguiente mensaje "Denied because the user-s biometric registry indicates a posible fraud", que traducido significa "Negado por el usuario-s el registro biometric indica un posible fraude" luego a las 11:51:51 vuelven a accesar al sistema y esta vez logra entrar desde el mismo IP, haciendo la validación de cuentas para transferencia y aumento del cupo diario de transferencia entre cuentas en USD. 4,000.00 y a las 11:56:24 con el mismo IP realiza la transferencia de USD. 3,500.00 a la cuenta de propiedad de Mercy Cabrera Pilligua, también cliente del Banco Pichincha C.A.,

De lo expuesto, se advierte que el Banco Pichincha C.A., si tuvo un indicador alerta, y además por tratarse de un IP que no era utilizado habitualmente en las transacciones de la cliente, el banco se encontraba en la responsabilidad de rechazar de manera oportuna la ejecución de dicha transacción, situación que no sucedió y por lo tanto no cumplió con lo previsto en el segundo inciso del artículo 5, capitulo IV.- Procedimiento para atención de los reclamos contra las instituciones del sistema financiero, título XX.- De la Superintendencia de Bancos y Seguros, libro de la Codificación de Resoluciones de la Superintendencia de Bancos y Seguros y de la Junta Bancaria.

"Art. 5. (...) Si la situación que motivó el reclamo referido en el inciso anterior, se originó en un procedimiento incorrecto de la institución controlada, que hubiese ocasionado un perjuicio al reclamante, la Superintendencia de Bancos y Seguros podrá ordenar la devolución de los valores reclamados, en ejercicio de las funciones y atribuciones contempladas en las letras b) y o) del artículo 180 de la Ley General de Instituciones del Sistema Financiero, otorgando al representante legal de la entidad un plazo que no podrá exceder de quince (15) días a partir de la notificación para que remita, bajo las prevenciones de Ley, la constancia del cumplimiento de la orden impartida."

En la letra d) de la comunicación del 30 de agosto emitida por el Banco Pichincha C.A., argumenta lo siguiente:

"(...) Si ha existido un acto delictivo le corresponde a la cliente, como afectada, impulsar la denuncia correspondiente."

"La inseguridad permanente que vivimos, no puede constituirse en un argumento para que las consecuencias de los actos cometidos por la delincuencia común, se le endosen al Banco, cuando es el Estado el que debe garantizar la seguridad humana a través de políticas y acciones integradas, para prevenir las formas de violencia y la comisión de infracciones y delitos, conforme lo dispone el Art. 393 de la Constitución de la República."

Ante el argumento esgrimido por el Banco se deduce entonces que el Organismo de Control debería abstenerse de tramitar, conocer, y resolver casos en el ámbito administrativo sobre transferencias por internet, basado en el simple argumento y presupuesto de que el cliente es poseedor de claves y coordenadas para acceder al producto financiero sin entrar a valorar otros elementos o aspectos necesarios dentro del procedimiento interno, ni sus niveles de cumplimiento.

Ante la demanda presentada, se debe recordar al Banco Pichincha C.A. que la Superintendencia de Bancos del Ecuador, tiene la función y atribución de velar por la estabilidad, solidez y correcto funcionamiento de las instituciones sujetas a

su control; y, vigilar que las mismas cumplan las normas que las rigen; y, exigir que dichas instituciones presenten y adopten las correspondientes medidas del correctivas cuando sea necesario.

Además, le compete emitir las disposiciones necesarias para resolver las reclamaciones que presenten los clientes del sistema financiero, siempre atenta a la protección de los intereses del público.

Adicionalmente, el Banco del Pichincha, nunca remitió a este Organismo de Control la documentación requerida de la señora Cabrera Pilligua Mercy Madele, cuenta ahorrista 6222036600, beneficiaria de la transferencia por el valor de USD. 3,500, así como no se conoce sobre las investigaciones llevadas a cabo por la entidad, más aún si la señora Cabrera Pilligua Mercy Madele, es una clienta del propio Banco Pichincha C.A., situación que no permite evidenciar si el funcionario de la entidad financiera efectúo las gestiones de confirmar la veracidad de los datos suministrados por el titular de la cuenta beneficiaria de la transferencia, a través del Formulario de solicitud de inicio de relación comercial "Conozca a su cliente", actividad que para la adecuada aplicación de la política "Conozca a su Cliente", las instituciones del sistema financiero están obligadas a cumplir, lo cual permite conocer la información relativa del beneficiario; teniendo en cuenta la obligación del banco de monitorear las transacciones realizadas por sus clientes, a fin de que el dinero confiado a su custodia sea protegido adecuadamente, incumpliendo con lo establecido en el artículo 77 de la Ley General de Instituciones del Sistema Financiero, que señala:

"ARTÍCULO 77.- Las instituciones del sistema financiero estarán obligadas a dar todas las facilidades para que la Superintendencia cumpla sus funciones y deberán dar acceso a su contabilidad, libros, correspondencia, archivos o documentos justificativos de sus operaciones al Superintendente o a sus delegados."

Esta entidad financiera, únicamente se limitó a responsabilizar a la cliente sobre la transferencia electrónica, sin evidenciar ni valorar de manera oportuna si efectivamente los procedimientos internos revela una validación y verificación adecuada del sistema operativo informático implementado por el Banco; en contrario, se imputa la carga de la prueba exclusivamente a la reclamante, por lo que no se entiende cuando se aborda el tema de afectación al cliente se determina que es producto del uso incorrecto del canal electrónico, de lo cual el Banco no ha podido comprobar tal afirmación, considerando que las seguridades para el bloqueo de la transacciones cuando se evidencie comportamientos inusuales NO se ejecutaron, por lo que queda evidenciado la omisión de procedimientos, procesos y políticas establecidos para proteger los derechos del usuario financiero.

Respecto de la no competencia de la Superintendencia de Bancos en ordenar la devolución de valores al demandante, el recurrente no considera lo dispuesto en el artículo 5, sección I, capitulo IV, Título XX, Libro I de la Codificación de Resoluciones de la SBS y de la JB que establece:

ARTÍCULO 5.- Si el resultado del análisis que realice la Superintendencia determinare la necesidad de que la institución controlada introduzca correctivos que regularicen la situación que motivó el reclamo, el Superintendente de Bancos y Seguros o el funcionario que cuente con la delegación de dicha autoridad, impartirá la disposición correspondiente.

Si la situación que motivó el reclamo referido en el inciso anterior, se originó en un procedimiento incorrecto de la institución controlada, que hubiere ocasionado un perjuicio al reclamante, la Superintendencia de Bancos y Seguros podrá ordenar la devolución de los valores reclamados, en ejercicio de las funciones y atribuciones contempladas en las letras b) y o) del artículo 180 de la Ley General de Instituciones del Sistema Financiero, otorgando al representante legal de la entidad un plazo que no podrá exceder de quince (15) días a partir de la notificación para que remita, bajo las prevenciones de ley, la constancia del cumplimiento de la orden impartida.

Artículo 180, de la Ley General de Instituciones del Sistema Financiero, literales:

b) Velar por la estabilidad, solidez y correcto funcionamiento de las instituciones sujetas a su control y, en general, que cumplan las normas que rigen su funcionamiento;

c) Autorizar la cesión total de activos, pasivos y contratos de las instituciones del sistema financiero, cuando ello implique la cesación de las operaciones de una oficina…

En virtud de la expuesto en las normas legales invocadas, la Superintendencia de Bancos del Ecuador, es competente para conocer los reclamos administrativos que presente el usuario externo a nivel nacional, y; en ejercicio de esta competencia la Intendencia Regional de Portoviejo conoció y resolvió el reclamo objeto de este proceso judicial. En consecuencia el argumento del recurrente esgrimido en la demanda ante el Organismo de Control, carece de sustento legal.

En cuanto al argumento, manifestando que la Junta Bancaria incurrió en silencio administrativo positivo a favor del demandante, es necesario mencionar que el artículo 182 ibidem establece:

Artículo 182.- *Cuando el Superintendente de Bancos no se pronunciase o no resolviese un asunto sometido a su aprobación, dentro de los términos fijados por esta ley o por otras leyes cuya aplicación corresponda resolver a la Superintendencia, sin haber dispuesto las ampliaciones de dichos plazos antes de su expiración, la petición sometida a su aprobación se entenderá favorablemente resuelta bajo su responsabilidad.*

La misma norma se aplicará respecto de los asuntos sometidos a resolución de la Junta Bancaria, excepto las solicitudes de constitución o establecimiento de nuevas instituciones.

Si la demora es imputable a cualquier otro funcionario de la Superintendencia, éste podrá ser sancionado inclusive con la remoción o destitución, dependiendo de la gravedad del hecho a criterio del Superintendente, quien podrá revisar el efecto resultante de la falta de pronunciamiento, en el término de ocho días de producido.

El secretario de la Junta Bancaria como lo reconoce el demandante, comunicó al Banco del Pichincha C.A. la ampliación de los plazos de manera oportuna en estricto apego a la norma legal que antecede, por lo expuesto la pretensión de alegar silencio administrativo carece de sustento legal.

De las consideraciones legales expuestas, el Recurso Subjetivo o de Plena Jurisdicción en contra de la Resolución No, JB-2015-3234, de 14 de enero de 2015, es improcedente por no contar con la fundamentación jurídica para el efecto.

ANEXO 5

UNIVERSIDAD NACIONAL DE LOJA
MODALIDAD DE ESTUDIOS A DISTANCIA

Presentado el 06 de Mayo del 2016, a las 11H20.- Lo certifica.- El Secretario.

Dr. Yonny Eduardo Tobar Lozano
SECRETARIO ABOGADO DE LA MED-UNL

Loja, 06 de Mayo del 2016, a las 11H30.- De conformidad a lo determinado en el Art. 136 del Reglamento de Régimen Académico, y una vez que se ha emitido informe favorable sobre la estructura y coherencia del Proyecto de Tesis titulado **"LOS DELITOS INFORMÁTICOS EN EL SISTEMA FINANCIERO NACIONAL",** previo a la obtención del grado de ABOGADO del (la) aspirante: **TAMY GHISLAINE IZAGUIRRE GARCIA,** emitido por el Dr. Mg. Augusto Patricio Astudillo Ontaneda, Docente de la Carrera de Derecho, con fecha 06 de Mayo de 2016; consecuentemente se autoriza la ejecución de dicho proyecto; y, se designa como Director de Tesis al /o la/ **Dr. Mg. Augusto Patricio Astudillo Ontaneda**.-NOTIFÍQUESE.-

Dr. Marcelo Armando Costa Cevallos
COORDINADOR DE LAS CARRERAS DE DERECHO Y TRABAJO SOCIAL DE LA MED DE LA UNL (e)

Loja, 06 de Mayo del 2016, a las 11H40.- Notifiqué con el decreto que antecede al /o la/ Dr. Mg. Augusto Patricio Astudillo Ontaneda, personalmente y firma.

Dr. Mg. Augusto Patricio Astudillo Ontaneda
DIRECTOR (A) DE TESIS

Dr. Yonny Eduardo Tobar Lozano
SECRETARIO-ABOGADO

Confiere: Dr. Marcelo Costa Cevallos.

INDICE