UNIVERSIDAD LAICA VICENTE ROCAFUERTE DE GUAYAQUIL

FACULTAD DE CIENCIA SOCIALES Y DERECHO

CARRERA DE DERECHO

PROYECTO DE INVESTIGACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE:
ABOGADO DE LOS JUZGADOS Y TRIBUNALES DE LA REPÚBLICA

TEMA:

ANALISIS DE LOS DELITOS INFORMATICOS EN BASE A LA ALTERACION Y MODIFICACION MEDIANTE TRANSFERENCIA ELECTRONICA EN MODALIDAD TARJETA DE CREDITO

AUTOR:

RODRIGUEZ BRAVO OLGA MARIA

TUTOR:

AB. RICHARD PROAÑO MOSQUERA M.SC.

GUAYAQUIL-2020

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA	
FICHA DE REGISTRO DE TESIS	
TÍTULO Y SUBTÍTULO: ANALISIS DE LOS DELITOS INFORMATICOS EN BASE A LA ALTERACION Y MODIFICACION MEDIANTE TRANSFERENCIA ELECTRONICA EN MODALIDAD TARJETA DE CREDITO	
AUTOR/ES: RODRIGUEZ BRAVO OLGA MARIA	**REVISORES O TUTORES:** Ab. Richard Proaño Mosquera MSc.
INSTITUCIÓN: UNIVERSIDAD LAICA VICENTE ROCAFUERTE DE GUAYAQUIL	**Grado obtenido:** ABOGADO DE LOS JUZGADOS Y TRIBUNALES DE LA REPÚBLICA
FACULTAD: FACULTAD DE CIENCIAS SOCIALES Y DERECHO	**CARRERA:** CARRERA DE DERECHO
FECHA DE PUBLICACIÓN: 2020	**N. DE PAGS:** 99.
ÁREAS TEMÁTICAS: Derecho	
PALABRAS CLAVE: Delito Informático- Derecho Penal- Comercio Electrónico - Protección de datos	
RESUMEN: En el presente estudio se realiza un análisis de los delitos informáticos desde el punto de vista doctrinal y en las normas vigentes en el ordenamiento jurídico ecuatoriano, con el objetivo de sistematizar sus características principales, el bien jurídico protegido y las leyes de carácter preventivo y sancionador cuando se trata de delitos cometidos utilizando	

<table>
<tr><td colspan="3">tarjetas de crédito. Para alcanzar ese objetivo se realizó un análisis de algunos de los delitos previstos en el COIP donde el autor se vale de medios electrónicos o tarjetas de crédito para alcanzar sus fines delictivos, y que pueden afectar derechos, valores o bienes dela víctima.</td></tr>
<tr><td>N. DE REGISTRO (en base de datos):</td><td colspan="2">N. DE CLASIFICACIÓN:</td></tr>
<tr><td colspan="3">DIRECCIÓN URL (tesis en la web):</td></tr>
<tr><td>ADJUNTO PDF:</td><td>SI [X]</td><td>NO [ ]</td></tr>
<tr><td>CONTACTO CON AUTOR/ES:
RODRIGUEZ BRAVO OLGA MARIA</td><td>Teléfono:
0990044188</td><td>E-mail:
Oguita.rodri@gmail.com</td></tr>
<tr><td>CONTACTO EN LA INSTITUCIÓN:

UNIVERSIDAD LAICA VICENTE ROCAFUERTE</td><td colspan="2">M.sc. Patricia Jurado Ávila, Decano de la Facultad de Ciencias Sociales y Derecho
Teléfono: 2596500 Ext. 250
E-mail: pjuradoa@ulvr.edu.ec

M.sc. Carlos Pérez Leiva Director de la Carrera de Derecho
Teléfono: 2595500 Ext. 233
E-mail: cperezl@ulvr.edu.ec</td></tr>
</table>

CERTIFICADO DE ANTIPLAGIO ACADÉMICO

Turnitin Informe de Originalidad

Procesado el: 28-oct.-2020 14:21 -05
Identificador: 1429387536
Número de palabras: 18971
Entregado: 1

Tesis Por Olga Maria Rodriguez Bravo

Índice de similitud	Similitud según fuente	
3%	Internet Sources:	3%
	Publicaciones:	0%
	Trabajos del estudiante:	8%

3% match (Internet desde 10-jul.-2020)
https://www.uchile.cl/documentos/boletin-n-12192-25-proyecto-de-ley-que-establece-normas-sobre-delitos-informaticos-implementa-convencion-cibercrimen-deroga-la-ley-n-19223-y-modifica-otros-cuerpos-doc-97kb_149004_1_5031.doc

CAPÍTULO I DISEÑO DE LA INVESTIGACIÓN 1.1. Tema Analisis de los delitos informaticos en base a la alteracion y modificacion mediante transferencia electronica en modalidad tarjeta de credito. 1.2. Planteamiento del problema Siendo que la presente investigación, trata de ahondar en los delitos informáticos para determinar las causas que conllevan a realizar este tipo de delitos y establecer las repercusiones que tienen actualmente en la sociedad con este estudio se pretenderá establecer mecanismos de prevención de las transferencia electrónica por medio de las tarjetas de créditos, partiendo de las falencias que puedan existir actualmente dentro de los delitos informáticos para así posteriormente poder proponer una implementación respecto a la creación de la policía informática particularmente respecto en las transferencias electrónicas. Siendo que a partir del crecimiento de la tecnología a nivel internacional tanto como nacional es visible el incremento y el agravio de los delitos informáticos tanto como en clonación de tarjetas de créditos, transferencia electrónica como ataques a la privacidad, fraudes, entre otros tipos de delitos, así quedando cada vez más vulnerables tanto personas naturales y personas jurídicas por el mal empleo de la tecnología y a la vez del desconocimiento de información, desde que empezó a darse este tipo crecimiento en el campo tecnológico ŷ surgieron nuevos tipos de delitos se dio la necesidad de tipificarlos y establecer una sanción penal acorde con cada tipo de delito. A la actualidad en el Ecuador desde la vigencia del Código Orgánico Integral Penal (en adelante COIP) a partir del 10 de agosto de 2014, dentro de su Libro I, Título IV de las Infracciones en Particular, Capítulo Segundo Delitos contra los Derechos de Libertad, Sección IX Delitos contra los Derechos de la Propiedad en su artículo 190 contempla el delito de transferencia electrónica y sus respectivas sanciones. Así equiparándolo como delito informático a las trasferencias electrónica de tarjetas de créditos dando a conocer el ánimo de lucro de la persona atrás del delito por medio de 1 la manipulación o modificación de sistemas manifestando de una manera clara esta modalidad de delito con el fin de apropiarse de un bien o valor de una persona. 1.3. Formulación del problema ¿Cómo se podría establecer un mecanismo para evitar los delitos informáticos mediante transferencia electrónica con la modalidad de tarjetas de crédito? 1.4. Sistematización del problema ¿Cuál es la frecuencia con la que se realizan fraudes por medio de tarjetas de créditos? ¿Cuáles son las diferentes facetas o modalidades delitos informáticos que afectan a la sociedad ecuatoriana? ¿De qué manera se

CERTIFICACIÓN DE ACEPTACIÓN DEL TUTOR

CERTIFICACIÓN DE ACEPTACIÓN DEL TUTOR

En mi calidad de Tutor del Proyecto de Investigación ANALISIS DE LOS DELITOS INFORMATICOS EN BASE A LA ALTERACION Y MODIFICACION MEDIANTE TRANSFERENCIA ELECTRONICA EN MODALIDAD TARJETA DE CREDITO designado por el Consejo Directivo de la Facultad de Ciencias Sociales y Derecho de la Universidad Laica VICENTE ROCAFUERTE de Guayaquil.

CERTIFICO:

Haber dirigido, revisado y aprobado en todas sus partes el Proyecto de Investigación titulado: ANALISIS DE LOS DELITOS INFORMATICOS EN BASE A LA ALTERACION Y MODIFICACION MEDIANTE TRANSFERENCIA ELECTRONICA EN MODALIDAD TARJETA DE CREDITO, presentado por la estudiante OLGA MARIA RODRIGUEZ BRAVO como requisito previo, para optar al Título de ABOGADO DE LOS JUZGADOS Y TRIBUNALES DE LA REPÚBLICA, encontrándose apto para su sustentación.

Firma:

NOMBRES Y APELLIDOS DEL TUTOR

MSC. AB. RICHARD PROAÑO MOSQUERA

C.C.

DECLARACIÓN DE AUTORÍA Y CESIÓN DE DERECHOS PATRIMONIALES

DECLARACIÓN DE AUTORÍA Y CESIÓN DE DERECHOS PATRIMONIALES

La estudiante egresada OLGA MARIA RODRIGUEZ BRAVO, declara bajo juramento, que la autoría del presente proyecto de investigación, ANALISIS DE LOS DELITOS INFORMATICOS EN BASE A LA ALTERACION Y MODIFICACION MEDIANTE TRANSFERENCIA ELECTRONICA EN MODALIDAD TARJETA DE CREDITO, corresponde totalmente a la suscrita y me responsabilizo con los criterios y opiniones científicas que en el mismo se declaran, como producto de la investigación realizada.

De la misma forma, cedo los derechos patrimoniales y de titularidad a la Universidad Laica VICENTE ROCAFUERTE de Guayaquil, según lo establece la normativa vigente.

Autora
OLGA MARIA RODRIGUEZ BRAVO
Firma: Olga Rodríguez .
C.I.0952992949

AGRADECIMIENTOS

Mi agradecimiento principalmente es para mí mama Carmen Bravo, por el apoyo y sacrificio brindado durante todos estos años que han transcurrido, siendo gracias a ella que logre culminar este escalón en la vida.

A mi padre porque de alguna manera también contribuyó desde la distancia a este logro que hoy es posible y el cual me llena de felicidad.

A mis tutores M.sc. Ab Nicolás Pulecio y M.sc. Ab. Richard Proaño, quienes desde el primer momento me brindaron su amistad, bondad, compresión y apoyo en toda la trayectoria de mi tesis.

A mis tíos, por todo su amor y apoyo incondicional en todas las formas posibles de mi vida y más aún en esta trayectoria universitaria, gracias a ellos también es posible este logro.

A mi padrino Ab. Marcelo Caicedo por todo su apoyo brindado a mí y mi familia en todas las formas posible en la vida, en especial en mi trayectoria universitaria.

DEDICATORIA

Este trabajo investigativo lo dedico principalmente a Dios, por ser el que me ha dado fuerza para continuar y cumplir mis deseos más anhelados.

A mi madre, por su fuerza, dedicación, sacrificio y trabajo en todos los años que lo necesite para hoy poder estar realizando este sueño. El logro es de las dos y para mí es un privilegio ser hija de una mujer tan luchadora que me sacó adelante.

A mi demás familia que me apoyaron de diversas formas en todo lo posible para que esto fuera posible para ellos también es este logro.

ÍNDICE GENERAL

CERTIFICACIÓN DE ACEPTACIÓN DEL TUTOR 5
DECLARACIÓN DE AUTORÍA Y CESIÓN DE DERECHOS PATRIMONIALES 6
AGRADECIMIENTOS 7
DEDICATORIA 8
CAPÍTULO I 1
DISEÑO DE LA INVESTIGACIÓN 1
1.1. Tema 1
1.2. Planteamiento del problema 1
1.3. Formulación del problema 2
1.4. Sistematización del problema 2
1.5. Objetivos de la investigación 2
1.5.1. Objetivo general 2
1.5.2. Objetivos específicos 3
1.6. Justificación de la investigación 3
1.7. Delimitación o alcance de la investigación 4
1.8. Hipótesis de la investigación o idea a defender 5
1.9. Variables 5
1.9.1. Variable independiente 5
1.9.2. Variable dependiente 5
1.10 Línea de investigación institucional/facultad 5
CAPITULO II 6
MARCO TEÓRICO 6
2.1. Definición de delito informático 6
2.1.1. Definiciones 7
2.2. El bien jurídico protegido 8
2.3. Sujetos del delito informático 10
2.4 Vulnerabilidad Informática. 10
2.5. Relación entre la informática jurídica y el Derecho informático 12
2.6. Características de delitos informáticos 12
2.7. Delito informático en legislación ecuatoriana 13
2.8. Derecho informático y derecho penal 14

2.8.1. Medio y fin en el delito informático 15
2.8.2. Naturaleza Jurídica del Delito Informático 15
2.8.3. Comercio Electrónico 16
2.8.4. Modelos del comercio electrónico 17
2.9. Definición de tarjeta de crédito 17
2.9.1. Tarjeta de crédito 18
2.9.2. Elementos presentes en una tarjeta de crédito 18
2.10. Definición de fraude 19
2.10.1. Tipos o Formas de fraude 20
2.10.2. Causa y Efecto del Fraude 22
2.10.2.1. Causas Internas 23
2.10.2.2. Causas Externas 23
2.10.3. Modalidades de fraude informático 23
2.11. Fraude informático en Ecuador 25
2.12. Perito Informático En Ecuador 27
2.13. La Banca 28
2.14. Legislación comparada 30
2.14.1. Delito informático en Chile 30
2.13.2. Delitos informáticos en Argentina 31
2.14. Marco legal 32
2.15 Jurisprudencia 38
Resolución Interinstitucional 001–FGE–SBS–2011 38
Resolución JB-2012-2090, Junta Bancaria del Ecuador, 2012 43
Resolución JB-2012-2148 Junta Bancaria del Ecuador, 2013 45
2.16. Tratados internacionales 57
2.16.1. Convenio de Budapest 57
CAPÍTULO III 59
METODOLOGÍA DE LA INVESTIGACIÓN 59
3.1. Metodología 59
3.2. Tipo de investigación 59
3.3. Enfoque 60
3.4. Técnica e instrumentos 61
3.5. Población 61
3.6. Muestra 62
CAPÍTULO IV 63

INFORME FINAL 63
ANÁLISIS DE RESULTADOS 63
4.1. Análisis de los resultados de la encuesta 63
Pregunta No. 1. 63
TABLA 1. 63
GRÁFICO 1 63
Interpretación y análisis de datos No.1: 64
Pregunta No. 2 64
TABLA 2. 64
GRÁFICO 2 64
Interpretación y análisis de datos No.02: 64
Pregunta No. 3 65
TABLA 3. 65
GRÁFICO 3 65
Interpretación y análisis de datos No3.: 66
Pregunta No. 4. 66
TABLA 4. 66
GRÁFICO 4 66
Interpretación y análisis de datos No.4: 67
Pregunta No. 5. 67
TABLA 5. 67
GRÁFICO 5 67
Interpretación y análisis de datos No.5: 68
Pregunta No. 6. 68
TABLA 6. 68
GRÁFICO 6 68
Interpretación y análisis de datos No.6: 69
Pregunta No. 7. 69
TABLA 7. 69
GRÁFICO 7 69
Interpretación y análisis de datos No.7: 70
Pregunta No. 8. 70
TABLA 8. 70
GRÁFICO 8 70
Interpretación y análisis de datos No.8: 71

Pregunta No. 9. 71
TABLA 9. 71
GRÁFICO 9 71
Interpretación y análisis de datos No.9: 72
Pregunta No. 10. 72
TABLA 10. 72
GRÁFICO 10 72
Interpretación y análisis de datos No.10: 73
Pregunta No. 11. 73
TABLA 11. 73
GRÁFICO 11 74
Interpretación y análisis de datos No.11 74
Pregunta No. 12. 74
TABLA 12. 74
GRÁFICO 12 75
Interpretación y análisis de datos No.12: 75
Pregunta No. 13. 75
TABLA 13. 75
GRÁFICO 13 76
Interpretación y análisis de datos No.13: 76
CONCLUSIONES 77
RECOMENDACIONES 79
PROPUESTA 81
REFERENCIAS BIBLIOGRÁFICAS 82
Bibliografía 82
Anexos 85

CAPÍTULO I

DISEÑO DE LA INVESTIGACIÓN

1.1. Tema

Analisis de los delitos informaticos en base a la alteracion y modificacion mediante transferencia electronica en modalidad tarjeta de credito.

1.2. Planteamiento del problema

Siendo que la presente investigación, trata de ahondar en los delitos informáticos para determinar las causas que conllevan a realizar este tipo de delitos y establecer las repercusiones que tienen actualmente en la sociedad con este estudio se pretenderá establecer mecanismos de prevención de las transferencia electrónica por medio de las tarjetas de créditos, partiendo de las falencias que puedan existir actualmente dentro de los delitos informáticos para así posteriormente poder proponer una implementación respecto a una reforma en el inciso 3ero del Articulo 230 del Código Orgánico Integral Penal.

Siendo que a partir del crecimiento de la tecnología a nivel internacional tanto como nacional es visible el incremento y el agravio de los delitos informáticos tanto como en clonación de tarjetas de créditos, transferencia electrónica como ataques a la privacidad, fraudes, entre otros tipos de delitos, así quedando cada vez más vulnerables tanto personas naturales y personas jurídicas por el mal empleo de la tecnología y a la vez del desconocimiento de información, desde que empezó a darse este tipo crecimiento en el campo tecnológico y surgieron nuevos tipos de delitos se dio la necesidad de tipificarlos y establecer una sanción penal acorde con cada tipo de delito.

A la actualidad en el Ecuador desde la vigencia del Código Orgánico Integral Penal (en adelante COIP) a partir del 10 de agosto de 2014, dentro de su Libro I, Título IV de las Infracciones en Particular, Capítulo Segundo Delitos contra los Derechos de Libertad, Sección IX Delitos contra los Derechos de la Propiedad en su artículo 190 contempla el delito de transferencia electrónica y sus respectivas sanciones; y en el Capítulo Tercero Delitos Contra los Derechos del Buen Vivir, Sección III Delitos contra

la seguridad de los activos de los sistemas de información y comunicación en su Artículo 230 contempla la Interceptación Ilegal de datos.

Así equiparándolo como delito informático a las trasferencias electrónica de tarjetas de créditos dando a conocer el ánimo de lucro de la persona atrás del delito por medio de la manipulación o modificación de sistemas manifestando de una manera clara esta modalidad de delito con el fin de apropiarse de un bien o valor de una persona.

1.3. Formulación del problema

¿Cómo se podría establecer un mecanismo para evitar los delitos informáticos mediante transferencia electrónica con la modalidad de tarjetas de crédito?

1.4. Sistematización del problema

¿Cuál es la frecuencia con la que se realizan fraudes por medio de tarjetas de créditos?

¿Cuáles son las diferentes facetas o modalidades delitos informáticos que afectan a la sociedad ecuatoriana?

¿De qué manera se relaciona el uso del internet con los delitos informáticos mediante tarjeta de crédito?

¿Qué tanto de la población ecuatoriana está informada actualmente de estos delitos?

¿Qué tipo de modalidades utilizan para el fraude por medio de transferencia de crédito?

¿Qué tipo de tarjetas de créditos existen?

1.5. Objetivos de la investigación

1.5.1. Objetivo general

Analizar la relación entre los tipos penales de apropiación fraudulenta por medios electroncito e interceptación ilegal de datos, contenidos en los Art. 190 y 230 del COIP.

1.5.2. Objetivos específicos

- Analizar el concepto de delitos informáticos, transferencia electrónica, clonación y tarjeta de crédito
- Analizar la definición de los delitos informáticos.
- Estudiar las normas jurídicas que hacen referencia a delitos informáticos y transferencia electrónica, mediante derecho comparado con la legislación ecuatoriana e internacional.
- Comparar de las diferentes aplicaciones electrónicas bancarias de acuerdo al nivel de seguridad que brinda cada una.
- Reconocer qué tipo de falencias existen en la investigación de delitos informáticos en el Ecuador, en especial en la trasferencia electrónica con modalidad de las tarjetas de créditos.
- Identificar qué perjuicios tiene la víctima ante la comisión del delito de trasferencia electrónica mediante las tarjetas de créditos.
- Diagnosticar si la ciudadanía en realidad denuncia este tipo de delitos en el Ecuador, particularmente en el caso de transferencia electrónica de tarjetas de créditos.

1.6. Justificación de la investigación

Referente a los delitos de fraude electrónico estos ostentan diferentes tipos o modalidades es por ello que se considera importante revisar su clasificación. Este trabajo se justificará en medida a la importancia que actualmente se vive en cuanto a los fraudes por medio de las tarjeta de crédito o débito, por medio de las transferencia de los medios electrónicos siendo que actualmente los ataques informáticos se han vuelto muy comunes y cuya proporción ha ido en aumento, más con la mayor parte de la sociedad teniendo posesión de una tarjeta de crédito y así estando expuesto a delitos como el fraude.

Cada día que las personas lleguen a realizar una compra con cualquier de sus tarjetas, de alguna manera su privacidad e identidad quedan vulnerables a todo tipo de delito estafa, fraude, robo de información etc., a pesar de los avances que se realizan para proteger de este tipo de delito tanto de los usuarios como a las instituciones financieras por el uso de las tarjetas.

En relación a los fraudes electrónicos desde una perspectiva se profundizara en el delito de transferencia electrónica mediante tarjeta de crédito por ser un delito con una gran problemática cometiéndose a diario y de distinta modalidades, pero a su vez una problemática a la que todavía no se le da fin por descuido muchas veces del usuario mismo debiendo ser un poco más responsable en cuanto a la forma como utiliza las tarjetas de crédito.

Los delitos informáticos requieren especial atención y una mejor avance tecnológico en los diferentes sistemas implementados a nivel privado y a nivel público de las instituciones financieras, ya que lamentablemente nuestro país presenta muchas vulnerabilidades en este ámbito por lo que los mencionados delitos tipificados en el Código Integral Penal ecuatoriano, y la realización de un análisis de estos delitos para establecer mecanismos de concientizar a una mejor realización de compras, ventas teniendo un poco más de responsabilidad y llegar a evitar fraudes por medios de las tarjetas de créditos como las de débitos.

Por esa razón se analizara la relación entre los Art 190 y 230 del Código Orgánico Integral Penal establecido si existe algún vacío entre estos dos Artículos, estableciendo si se sanciona de la misma forma a los Autores como a los Cómplice, se analizara así mismo la posibilidad de incorporar un párrafo al numeral 3 del Articulo 230 estableciendo que se sancione por igual a la persona que haga utilización de las tarjetas clonadas, manipuladas o alteradas aunque no sea el autor principal del delito de apropiación fraudulenta.

Estos delitos informáticos alrededor del mundo al menos en Latinoamérica vemos que los países que han avanzado en cuanto a esta problemática, son Perú, Colombia, Argentina, y quien más avanzado esta en cuanto a este tipo de delitos es Argentina siendo que han desplegado el mejor equipo de investigación para resolver el tema del cyber crimen.

1.7. Delimitación o alcance de la investigación

LUGAR: Este tema se desarrollara dentro del alcance de Ecuador.

TIEMPO: Para la elaboración de la presente investigación se tomará en cuenta 3 meses y medio desde la fecha de julio del 2020 a noviembre del 2020.

1.8. Hipótesis de la investigación o idea a defender

Con un anteproyecto de ley reformatoria al Código Orgánico Integral Penal incorporando un nuevo parrafo del Art 230 numeral 3ero del COIP tipificando y sancionado el delito de la utilización de los datos electrónicos para apropiación fraudulenta

1.9. Variables

1.9.1. Variable independiente

Anteproyecto de ley reformatoria al Código Orgánico Integral Penal

1.9.2. Variable dependiente

Tipificar y sancionar el delito de la utilización de los datos electrónicos para apropiación fraudulenta.

1.10 Línea de investigación institucional/facultad

Línea 2. Derechos Humanos, Sociedad civil y Gestión de la comunicación

CAPITULO II

MARCO TEÓRICO

2.1. Definición de delito informático

El delito informático como tal se volvió una de las formas de delitos más nuevas y complejas de la historia en sus formas de delinquir Téllez afirma “actitudes ilícitas que tienen a las computadoras como instrumento o fin" (concepto atípico) o las "conductas típicas, antijurídicas y culpables que tienen a las computadoras como instrumento o fin" (concepto típico)” (Téllez, 2008, pág. 188) .

“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 y, 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.” (Lima, 2014, pág. 44)

Nidia Callegari define al “delito Informático" como "aquel que se da con la ayuda de la informática o de técnicas anexas” (CALLEGARI, 2013, pág. 44)

Definición de Camacho Losa “toda acción dolosa que provoca un perjuicio a personas o entidades, sin que necesariamente conlleve un beneficio material para su autor aun cuando no perjudique de forma directa o inmediata a la víctima y en cuya comisión intervienen necesariamente de forma activa dispositivos habitualmente utilizados en las actividades informáticas” Citado por (Hermández Diaz, pág. 227)

Así mismo otro autor da su definición “podemos definir el delito informático como: acción delictiva que realiza una persona, con la utilización de un medio informático o lesionando los derechos del titular de un elemento informático, se trate de máquinas- hardware- o de los programas software” (Dávara Rodríguez, 1993, citado en (Chinchilla Sandí, 2004))

Por su parte, el tratadista penal italiano Carlos Sarzana, nos da una definición más sencilla pero no menos importante, que los delitos informáticos son "cualquier comportamiento criminal en que la computadora está involucrada como material, objeto o mero símbolo." (Sarzana, 2014, pág. 44)

Siendo así por cualquier medio que se cometa el delito a la medida que los sistemas informáticos se generalizan cada vez más, y las personas confían cada vez más en los computadores y, a menudo, almacenan su información confidencial sobre ellas.

2.1.1. Definiciones

- Delito. "El delito es el hecho humano previsto de modo típico por una norma jurídica sancionada con pena en sentido estricto, lesivo o peligroso para los bienes o intereses considerados merecedores de la más; enérgica tutela y expresión reprobable de la personalidad del agente, tal cual es el momento de su comisión"
- Patrimonio: en el derecho se refiere a el conjunto de relaciones jurídicas pertenecientes a una persona, que tienen una utilidad económica y por ello son susceptibles de estimación pecuniaria, y cuya relaciones jurídicas están constituidas por deberes y derechos vinculados a una persona, ya sea física o moral.
- Activo: Corresponde a todos los bienes y derechos que posee una empresa, susceptibles de ser valorados en dinero, tales como bienes raíces, automóviles, derechos de marcas, patentes, cuentas por cobrar, entre otros.
- Tarjeta de crédito. Las tarjetas de crédito son tarjetas de plástico compuestas por una banda magnética o un microchip y que constituyen una forma de financiación que permite a los titulares de las tarjetas pagar por productos o servicios sin necesidad de disponer de dinero en efecto o cheques
- Fraude con tarjeta de crédito. Implica el uso no autorizado de la información de la tarjeta de crédito de una persona con el propósito de cargar compras en la cuenta de la víctima o extraer fondos de su cuenta. El fraude con tarjeta de crédito está considerado como una forma de robo de identidad
- Pishing. Método que los ciberdelincuentes utilizan para engañarle y conseguir que revele información personal, como contraseñas o datos de tarjetas de crédito y de la seguridad social y números de cuentas bancarias. Lo hacen mediante el envío de correos electrónicos fraudulentos o dirigiéndole a un sitio web falso
- Base de datos: serie de datos organizados y relacionados entre sí, los cuales son recolectados y explotados por los sistemas de información de una empresa o negocio en particular
- Skimming. Robo de información de tarjetas de crédito utilizado en el momento de la transacción, con la finalidad de reproducir o clonar la tarjeta de crédito o

débito para su posterior uso fraudulento. Consiste en el copiado de la banda magnética de una tarjeta (crédito, débito, etc)

- Alteración: Agitación, cambio o variación de una cosa respecto a su estado norm al o a un orden establecido
- Modificación es la acción y efecto de modificar. Este verbo, cuyo origen etimológico nos remite al latín modificāre, hace mención a cambiar o transformar algo, dar un nuevo modo de existencia a una sustancia material o a limitar algo a cierto estado de manera en que se distinga de otras cosas.
- Fraude: acto cumplido intencionalmente, con la finalidad de herir los derechos o intereses ajenos. Der civil. Derecho penal: el fraude es un elemento constitutivo del robo
- Ftp o file transfer protocol (protocolo de transferencia de fichero) (sigla en inglés de file transfer protocol - protocolo de transferencia de archivos) en informática, es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red tcp (transmission control protocol), basado en la arquitectura cliente-servidor. Desde un equipo cliente se puede conectar a un servidor para descargar archivos desde él o para enviarle archivos, independientemente del sistema operativo utilizado en cada equipo
- Internet: internet es una red de redes que permite la interconexión descentralizada de computadoras a través de un conjunto de protocolos denominado tcp/ip.
- Sistema informático: conjunto organizado de programas y bases de datos que se utilizan para, generar, almacenar, tratar de forma automatizada datos o información cualquiera que esta sea.
- Acceso ilícito: cuando se accede a un sistema informático infringiendo las medidas de seguridad con la finalidad de obtener datos u otra intención delictiva

2.2. El bien jurídico protegido

Dentro de los derechos constitucionales que se protege y de la división de los tipos penales que protegen a cada uno de los derechos dentro del delito informático, el bien jurídico protegido en cada delito informático sería distinto, hablando de un delito informático de apropiación ilícita, el bien jurídico protegido vendría siendo la propiedad, como otros bienes jurídicos que pueden llegar hacer afectados como la

intimidad personal, el patrimonio, seguridad nacional, integridad sexual, etc., todo dentro de los distintos tipos penales que enmarcan los delitos informáticos. Así mismo sabiendo que más allá de cualquier elemento o medio para la comisión del delito informático tenemos la vulneración del bien jurídico y como prioridad de estas teniendo a los datos e información.

Existen varios criterios en que se coincide en establecer como el bien jurídico protegido de los delitos informáticos es la **información** mientras que otros casos se habla de que este bien jurídico seria la **libertad informática.**

La autora Patricia Herrmann Fernández con referencia a la información como bien jurídico protegido dentro delitos informáticos indica: "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 .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. 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." (Herrmann Fernández, 2006, pág. 191)

Santiago Acurio del Pino y Juan José Páez Rivadeneira, con referencia a la libertad informática sostienen: "En conclusión podemos decir que el bien jurídico protegido de acuerdo con nuestra Constitución es la llamada libertad de informática la misma que consiste, como expresión de la libertad del individuo, en el derecho de utilizar lícita y libremente, con los límites constitucionales y legales la tecnología informática. Esto está dado en el reconocimiento de nuestra Constitución del acceso universal a las TICs por tanto a su uso libre." (Acurio del Pino & Paéz Rivadeneira Juan, Derecho y Nuevas Tecnologías, 2010, pág. 210)

Dentro de toda esta línea que se está manejando sobre los bienes jurídicos protegidos se puede establecer: patrimonio en el caso de fraudes informáticos; reserva y

confidencialidad en el caso de delitos que afecten alrededor de la intimidad; la fe pública en el simple caso de las falsificaciones.

Sin embargo autores como Luis Bramont Arias Torres manifiesta que no existe un bien jurídico protegido dentro del delito informático porque este no es más que solo una forma o método de ejecución de las conductas delictivas que afectan a los bienes jurídicos que ya gozan de protección específica en lo referente al Derecho Penal. (Arias Torres Luis, pág. 58)

2.3. Sujetos del delito informático

Dentro de los delitos informáticos también tenemos al igual que en otros delitos el sujeto del delito y este es preciso para conocer posibles formas de comisión delictiva y profundizar en las posibles formas de prevención y detención de estas conductas. Clasificándose estos en:

- Sujeto activo
- Sujeto pasivo

SUJETO ACTIVO

Este tipo de delitos, sujeto activo sabemos que tenemos en frente a una acción u omisión, que generalmente tiene conocimientos técnicos de la informática, de en cierto modo, una persona con nivel de instrucción avanzado en tecnología, para poder manipular información o sistemas de computación para lograr su cometido, lesionar un bien jurídico protegido.

SUJETO PASIVO

Dentro de estos casos de delito informático se reitera la conducta de acción u omisión que la ejecuta el sujeto activo se puede decir que los perjudicados son individuos, instituciones que otorgan crédito, gobiernos, entidades que usan sistemas de información, portales de venta se servicios y vienen son los afectados por el sujeto activo que es quien tiene conocimiento para logar el delito.

2.4 Vulnerabilidad Informática.

Dentro de la vulnerabilidad decimos que es una debilidad del sistema informático que puede llegar a ser utilizada para causar un daño. Estas debilidades pueden aparecer

en cualquier elemento de una computadora, tanto como el hardware, sistema operativo, cómo el software.

Una cosa es cierta, que exista una de estas vulnerabilidades no significa que se llegue a producir un daño en los equipo de forma automática. Es decir, la computadora tiene un punto flaco, pero no necesariamente por eso va a fallar, lo único que puede ocurrir es que alguien ataque el equipo aprovechando ese punto débil.

Es muy común descubrir estas vulnerabilidades constantemente en variados de los programas de un computador y su rápida propagación por internet, inclusive a veces mucho antes de que se descubra una solución o se publique la misma. Podemos mencionarlas como vulnerabilidades más comunes:

- Buffer overflow o desbordamiento de pila: Trata de un fallo del software debido a la mala programación que se verá reflejado durante la ejecución de algún programa, el cual no se logra controlar de una forma adecuada la cantidad de datos que se deberían copiar en el área de memoria reservada para el buffer, permitiendo así que ese espacio se supere, sobrescribiendo espacios de memorias continuas a éste incluyéndole el contenido de la misma.
- Inyección SQL: Es el método que se aprovecha de algún fallo de programación, específicamente en lo que es la validación de entrada de datos en una consulta SQL. Este método se aprovecha de la vulnerabilidad en la validación de entrada durante la construcción de una Sentencia SQL que se va ejecutando frente una Base de Datos, permitiéndose alterar la consulta de una forma que el atacante puede obtener datos importantes de los registros almacenados en las diferentes tablas existentes en la base de datos atacada, como de la estructura e inclusive de usuarios administradores de la misma, permitiendo escalar privilegios dentro del sistema.
- Secuestro de sesiones: En primer lugar definamos cookies, siendo un archivo generado al iniciar sesión en algún sitio web y que identifica de forma unívoca a la dualidad que se da entre una cuenta de usuario y el servicio web enlazados. Entonces decimos que un secuestro de sesión es el método de ataque informático del cual se captura la cookie activa de algún usuario en la red, lo cual permite al atacante acceder al servicio web enlazado con esa cookie sin pasar por las medidas de autenticación que se requiere. De esta forma el atacante puede actuar de la misma forma que un usuario titular frente al servicio web con su cookie secuestrada.

- Ejecución de código remoto: Es un método que consiste en aprovechar una vulnerabilidad que le permitirá tomar los privilegios sobre una máquina y ejecutar código en ella, de lo cual sería darle la potestad al atacante de alterar, borrar o consultar de alguna información no autorizada e inclusive poder escalar privilegios dentro de la maquina atacada.
- XSS (Cross-Site Scripting): Seria en español, las Secuencias de Comandos en Sitios Cruzados. Una vulnerabilidad muy común dentro de las aplicaciones Web, brindando la oportunidad al atacante a inyectar en una página web códigos escritos en lenguajes tipo script como lo son JavaScript o VBScript, de lo cual le permitiría esquivar controles ya establecidos dentro de las políticas de seguridad de un sistema de información atacado.

2.5. Relación entre la informática jurídica y el Derecho informático.

Dentro de lo que abarca la Informática Jurídica, son ciencias de computación utilizadas en el campo jurídico para facilitar el desempeño de toda forma posible la Administración de Justicia variando la aplicación de este conociendo en diversos campos aplicando la tecnología derivada de esta ciencia como tal, así tenemos la automatización del funcionamiento de los Juzgados y Tribunales, sistemas de documentación legislativa y jurisprudencial, sistema de archivos, entre otras.

Y dentro de lo que abarca el Derecho Informático, sería el conjunto de normas jurídicas utilizado para una regulación apropiada sobre los recursos de la Ciencia Informática.

Entonces podemos decir el Derecho Informático es el que regula con las normas la utilización de la ciencia informáticas en todo los diversos campos tanto como la informática jurídica que es la utilizada también por los administradores de justicas de muchas formas, esas es una de las razones de los avances que va teniendo día a día el ordenamiento jurídico con la creación de leyes para protección de la tecnología de la informática que va creciendo de una manera increíble como la reforma que tuvo el COIP Código Orgánico Integral Penal tipificando delitos informáticos.

2.6. Características de delitos informáticos

El autor Julio Téllez Valdez establece las principales características de las acciones que configuran el delito informático: a) Conductas Criminógenas de cuello

blanco: se refiere a que únicamente personas con conocimientos técnicos en el área de la informática pueden cometerlos.

b) Son acciones ocupacionales: cuando el sujeto se encuentra trabajando.

c) Son acciones de oportunidad: el sujeto lo realiza aprovechando una ocasión creada en el mundo de funciones y organizaciones del sistema tecnológico y económico.

d) Provocan serias pérdidas económicas: quienes realizan será principalmente con una intención de beneficiarse económicamente, produciendo un decremento patrimonial al sujeto pasivo

e) Ofrecen facilidades de tiempo y espacio: susceptibles a ser realizados en tan solo segundos y sin necesidad que el sujeto se encuentre físicamente puede consumarse el hecho.

f) Son muchos los casos y pocas las denuncias: muchas de las veces por vacíos jurídicos, o por la dificultad probatoria.

g) Son muy sofisticados y relativamente frecuentes en el ámbito militar; en este ámbito suele suceder por cuanto el personal está altamente capacitado para trabajar con equipos de última tecnología que le facilita el cometimiento del ilícito.

h) Presentan grandes dificultades para su comprobación: el sujeto no suele dejar evidencias.

i) Son imprudenciales: se los cometen por descuido, con respecto a esto se debe discrepar porque el sujeto no actúa imprudentemente, sino al contrario con voluntad y conocimiento del hecho.

j) Ofrecen facilidades para su comisión a los menores de edad: se ven en la red tutoriales de cómo pueden hackear cuentas de un app store por ejemplo, y está al alcance de todos inclusive los niños y adolescentes.

k) Tienden a proliferar cada vez más: la tecnología avanza y nuevas formas de atacar a esta tecnología y hacer mal uso de la misma aparecen, por lo que se hace necesario una regulación.

l) Por el momento siguen siendo ilícitos manifiestamente impunes ante la ley. (Téllez Valdez, 2014, pág. 270)

2.7. Delito informático en legislación ecuatoriana

De los delitos informáticos en nuestra legislación tiene momentos significativos:

- La Ley de Comercio Electrónico, Firmas y Mensajes de Datos que se publicó el 17 de Abril del año 2002 marcó un hito histórico ya que fue por primera vez se

reguló estos delitos. Uno de los aspectos innovadores fue la incorporación de las infracciones informáticas en el Código Penal

- El Código Orgánico Integral Penal (COIP), publicándose el 10 de febrero del año 2014, que aun conservó varios de los tipos del Código Penal del año 2002 e introdujo nuevos tipos penales en lo que respecta a los delitos contra la propiedad que es el que analizaremos en el presente trabajo.

En el año 2002, al incorporar mediante la Ley de Comercio Electrónico, Firmas y Mensajes de Datos los Delitos Informáticos en el Código Penal, estos no fueron ubicados ni dentro de un capítulo ni dentro de un título exclusivos al contrario desde un principio fueron agregados a los capítulos y títulos referentes a los distintos delitos que ya existían dentro de la legislación. Para entender lo manifestado he ubicado en la extinta norma penal los capítulos y títulos que fueron modificados mediante la incorporación en mención

En diferencia al Código Penal el COIP sí ha realizado un intento por agrupar en una sola sección estos tipos de delitos.

La apropiación ilícita por medios electrónicos, dentro del COIP se encuentra contemplada en el primer inciso del Art. 190, dentro de la sección Novena relativa a los Delitos contra el Derecho de Propiedad: "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".

2.8. Derecho informático y derecho penal

"Existe una estrecha relación entre el Derecho Informático y el Derecho Penal, porque el Derecho Penal regula las sanciones para determinados hechos que constituyen violación de normas del Derecho y en este caso del Derecho Informático, en materia del delito cibernético o informático, entonces se podría comenzar a hablar del Derecho Penal Informático" (EcuaRed, 2020).

Referente al Derecho Informático, se puede decir que la informática ha sido la que dio lugar a la implementación de los de nuevos delitos estando inmersos con el uso

de una computadora y teniendo conocimiento de informática, poniendo como un punto de partida la relación entre derecho y la informática dentro del campo penal.

Actualmente estando tipificada en el Código Orgánico Penal las sanciones para los actos cometidos mediante delito informático como en el Art. 190.-Apropiación fraudulenta por medios electrónicos y Art230 Interceptación Ilegal de Datos.

2.8.1. Medio y fin en el delito informático

Para los llamados delitos informáticos existe una importante clasificación mediante los criterios medio o instrumento, o fin u objeto.

El profesor Julio Téllez Valdés cita que como medio o instrumento "se tienen a las conductas criminógenas que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito"; y como fin u objeto "se enmarca las conductas criminógenas que van dirigidas en contra de la computadoras, accesorios o programas como entidad física" Téllez Valdez, Julio. Citado por (Levene & Chiaravalloti, 2020) ".

"Si bien es cierto los delitos informáticos pueden ser enfocados como medios o fin, ya que lo que vale la pena ser rescatado es que la computadora, en sí, puede ser vista desde ambos criterios, esto debido a que puede ser como medio para la consumación del delito, y como fin en relación al objeto material de la infracción, así se podría decir que trabaja el hardware, no sin antes necesitar imperioso e invaluablemente un software." (Fernández, 2016, pág. 76)

Entonces decimos que en el delito informático puede ser visto dentro de un medio y fin, siendo vista desde los dos puntos la importación que se le da a la computadora, como medio dentro de la consumación del delito y como fin en relación al objeto material de la infracción.

2.8.2. Naturaleza Jurídica del Delito Informático

"Centrar la naturaleza jurídica del delito informático debe partir de un hecho jurídico, en donde los varios comportamientos irregulares que se dan con el avance tecnológico, determinan algunas conductas que permiten la comisión del delito, debido a esto se vuelve necesario encontrar una forma o método para hacer de estas conductas un hecho punible y no dejaras en la impunidad como se acostumbra". (Acurio del Pino, Delitos Informáticos: Generalidades, 2020, pág. 39)

"Los Delitos Informáticos en su mayoría son delitos tradicionales que con la ayuda de los Tics suponen nuevas vías de delinquir, que conllevan y en ciertos casos la creación de nuevos tipos penales, y de una nueva tendencia criminal que se conceptualiza y deriva a una nueva manera de aplicar y verificar la validez del principio de territorialidad por la manera en que se cometen estos delitos en cualquier parte del mundo". (Acurio del Pino, Derecho Penal Informatico, 2015, pág. 49)

2.8.3. Comercio Electrónico

Dentro de la actualidad experimentamos lo que es una transformación con respecto al uso de las redes y de las telecomunicaciones, todos los desarrollos tecnológicos son parte de esta revolución donde el comercio electrónico o en inglés llamado e-commerce juega un papel trascendental al incrementar inmensurablemente el número de negocios en el mundo.

"El comercio electrónico puede definirse como aquella forma de transacción comercial en la que un suministrador provee de bienes y servicios a un cliente a cambio de un pago, y donde ambas partes interactúan electrónicamente en lugar de hacerlo por intercambio o contacto físico directo. El comercio electrónico implica la realización de negocios online o, lo que es lo mismo, vender y comprar productos y prestar servicios a través de sites, ubicados en la red, independientemente del canal por el que luego circule el producto o servicio (electrónico o tradicional)". (Borrego, 2014, pág. 53)

"El Comercio electrónico se puede considerar como un aspecto imprescindible para la internacionalización de las pymes debido a que el gran alcance que tiene la web en la actualidad permite que las empresas puedan ofertar sus productos y servicios con mejores resultados, se ha podido comprobar que a pesar de que muchas pymes tienen una alta calidad en sus productos y servicios no han logrado promocionar lo que ofrecen hacia los mercados internacionales. (Ministerios de Comercio Exterior, 2016)

2.8.4. Modelos del comercio electrónico

Dentro de la revista Merca2.0, infiere que existen unos seis modelos de que se refiere al comercio electrónico, los cuales veremos a continuación:

- B2B o business to business: Donde la transacción se realiza entre empresas que operan en internet.
- B2C o business to costumer: El comercio entre la empresa que produce, la que vende o prestadora de servicios y el consumidor final.
- B2E o business to employee: Donde se realizan los negocios entre la empresa y sus colaboradores a través de tiendas online con beneficios exclusivos.
- C2C o costumer to costumer: Una transacción en la que el cliente adquiere un producto o servicio y realiza la acción de reventa.
- G2C o government to customer: Es la relación entre el gobierno con el consumidor por ejemplo pagos de impuestos o multas vehiculares.
- G2B o governmente to business: Corresponde al negocio con el gobierno y las empresas como lo son los portales de compras y licitaciones. (Merca2.0, 2020)

Dentro de esto es muy importante poder diferenciar del comercio electrónico tanto de los negocios electrónicos ya que en términos son parecidos, aunque distintos a la vez, lo que es el comercio electrónico nos facilita realizar transacciones de compra y venta repetitivamente, por otro lado los negocios electrónicos habilitan los procesos y funciones dentro de una empresa como lo es la producción, administración de inventarios, desarrollo de productos, finanzas entre otros.

2.9. Definición de tarjeta de crédito

Al referirnos a las dichas tarjetas de crédito sabemos que actualmente toda una población cuenta con una de ellas, siendo estas de fácil manejo diariamente la población la utiliza como un medio de pago utilizándose a través de cajeros automáticos como en Terminal Punto de Venta , estas están estructuradas básicamente por chip o banda magnética que guardan cantidades de datos e información, un número en relieve, tienen una dimensión establecida son de plásticos, tienen medidas de seguridad y varían según la institución que la otorga. Por su capacidad de realizar pagos se las sabe llamar dinero plástico.

2.9.1. Tarjeta de crédito

Alfredo Contreras Villavicencio, nos dice: "…La Tarjeta de Crédito propiamente dicha está representada por un número de afiliación que da acceso a una línea de crédito que concede el emisor de dicha tarjeta al cliente o tarjetahabiente. Este número de afiliación se lo consigna en una tarjeta plástica sensibilizada que registra la compra de un bien o servicio y lo carga a la cuenta del tarjetahabiente. Registra así mismo a favor de la persona natural o jurídica afiliada el valor de la venta que hace…" (Alfredo Contreras Villavicencio, pág. 76).

El autor Eduardo Guillermo Cogorno, refiere que es "un contrato complejo de características propias que establece una relación triangular entre comprador, un vendedor y una entidad financiera, posibilitando al primero la adquisición de bienes y servicios que ofrece el segundo, mediante promesa previa formulada a la entidad emisora de abonar el precio de sus compras en un plazo dado por esta última, la que se hará cargo de la deuda abonado inmediatamente el importe al vendedor previa deducción de las comisiones que hayan estipulado entre ambos por acercamiento de la demanda" (Cogorno, 1979, pág. 205).

Dentro de sus características encontramos que es "una tarjeta de plástico numerada, que presenta una banda magnética o un microchip, y que permite realizar compras que se pagan a futuro. El usuario debe tramitar las tarjetas ante una institución financiera o entidad bancaria, que le solicitará distintas documentaciones para asegurarse de que está en condiciones de pagar sus compras" (Juárez Angel, Accesible 2020).

Estas tarjetas brindan seguridad al usuario al momento de realizar comprar no el hecho de no tener que cargar fuertes sumas de dinero consigo para cualquier compra y con Un gran beneficio de que si no dispones de dinero para realizar el pago en ese momento se puede diferir cualquier compra a 3, 6, 9 y 12 meses en algunos casos existiendo posibilidades que se realice esta compra sin interés

2.9.2. Elementos presentes en una tarjeta de crédito

- El nombre de la entidad emisora en la parte superior (una entidad financiera).
- Los logos de marca y aceptación en la parte derecha
- El chip

- El Personal Account Number (PAN), o número de tarjeta.
- La fecha de caducidad de la tarjeta.
- El nombre del titular.

En el reverso de la tarjeta figurará:

- La banda magnética: contiene grabados los datos del titular y caracteres alfanuméricos que hacen que los cajeros y terminales actúen de una forma determinada.
- El panel de firmas.
- Carácter especial CVV (número de seguridad)
- Firma. (Edufinext, 2020)

2.10. Definición de fraude

Este vocablo de Fraude hace referencia a: el engaño que se realiza, dentro del término fraude se refiere al acto intencional por parte de uno o más, dando como resultado una representación errónea de los estados financieros.

Según ACFE Association of Certified Fraud: "Actividades/acciones con el propósito de enriquecimiento personal a través del uso inapropiado o la sustracción de recursos/activos de una organización por parte de una persona" (Association of Certified Fraud Examiners, 2020)

Ramírez Granda, en su diccionario jurídico define el fraude como "una sustracción hecha maliciosamente a las normas de la ley o del contrato en perjuicio de alguien. Una de las causas de la existencia de la nulidad de los actos jurídicos" (Ramírez Granda, pág. 160)

Dentro del fraude se puede implicar:

- Falsificación, manipulación o alteración de documentos.
- Malversación de fondos.
- Omisión de los efectos de transacciones en los registros o documentos
- Registro de las transacciones sin constancia
- Mal uso de las políticas contables.

El fraude puede ocurrir en todo tipo de ente: público y privado, de beneficencia y con fines de lucro, industrial, comercio, de servicio y financiero.

2.10.1. Tipos o Formas de fraude

Se dice que existen 7 tipos de fraudes los cuales los expresa Shoshanah Posner:

- El fraude clásico:

  Tipo de fraude que suele ser cometido un ladrón para nada sofisticado. Este se compra una credencial de crédito en la ***dark web***, y los bienes se envían a su vez a otro mensajero para intentar quedarse con la mercancía robada. Saben por lo general usar *proxies* para así poder cubrir su IP internacional de donde se originan la mayoría de estos fraudes.

- Fraude por triangulación

  La forma de fraude está involucrada en tres partes: estafador, comprador legítimo que sabe nada, comercio digital.

  Los estafadores crean una tienda virtual que sería falsa, por lo general de eBay o Amazon, vienen y realizan una gran oferta para bienes a precios bajos. Esta tienda cobra por el bien vendido, allí los estafador usan otra tarjeta de crédito robada y el nombre que recibió de las órdenes que se realizaron en su tienda virtual falsa para así comprar de un sitios web que sea legítimos y enviarle al cliente que compro en su tienda en línea.

  Este fraude puede ser identificado por los productos que se dirige, así como un poco de trabajo de investigación, ubicar al comprador confiado que puede identificar la tienda donde se compró los productos robados.

- Fraude de intercepción

  Serán pedidos en los que las direcciones de envío y las direcciones de facturación deberán coincidir con la dirección que están asociada a la tarjeta de crédito. Dentro de esta forma es objetivo esta interceptar el paquete en alguna de estas formas:

  - Pidiéndole a un representante de servicio al cliente que cambie la dirección antes de que el producto sea enviado.
  - Contactando al servicio de mensajería para cambiar la dirección del paquete a una en la que puedan quedarse con los bienes robados.
  - Y en casos en los que el estafador viva cerca de la dirección en la que vive el dueño de la tarjeta, esperar directamente a que el paquete llegue y firmarlo como si fuera el dueño del mismo o alguien de la familia

- Fraude con pruebas a la tarjeta

  Esto lo realizan con la práctica de probar los números de las tarjetas de crédito y su validez, lo suelen hacen hacer en sitios que muestran respuesta distinta a las tarjetas declinadas, en muchos de los casos por la fecha de expiración que este incorrecta en ese caso el estafador solo tendrá que probar con distintas fechas lo cual suelen hacerlos con bots siendo rápido.
- Fraude de adquisición de cuenta

  Esta se da cuando el estafador tiene de una forma legítima los datos de acceso del cliente y así aprovechar de las tarjetas de crédito para comprar cualquier bien. Lo que realizan es cambio en la dirección para el envío y hacerse con bienes robados por las tarjetas.
- Fraude por robo de identidad

  Un estafador asume la identidad de otra persona cualquiera, así sacando una tarjeta de crédito por medio de dicho nombre y realizan las compras. Esta forma de fraude se aumenta regularmente por la fuga de información que aún existe. Siendo una forma difícil de identificar porque los que lo suelen realizar son personas más sofisticadas.
- Fraude amistoso, también llamado fraude de contracargos

  Una persona en línea hace una compra y luego mete un contracargo con el cual alega que la tarjeta fue robada. Dicho contracargo se suele presentar después de que los bienes ya fueran entregados. Esta forma de fraude suele hacerse por un consumidor que sabe lo que está realizando, y suele ser difícil de comprobarse porque los bancos saben favorecer a sus clientes en este tipo de tema. (Shoshanah Posner, 2019)

  También se puede agregar como formas de fraude las:
- Pérdida o robo de la tarjeta

  Es cuando una tarjeta se roba físicamente, o se ha perdido y alguien la ha encontrado, y después es utilizada por otra persona que finge ser usted.
- Duplicado de tarjeta o skimming

  El duplicado de la tarjeta se realiza y se codifica sin el permiso de la compañía de la tarjeta. La mayoría de los casos implican la copia de la información de la banda magnética de una tarjeta genuina sin el conocimiento del titular. De este

fraude será inconsciente hasta que los costes inexplicados aparecen en sus facturas.

- Robo de datos

  Esto ocurre cuando le roban la información de la tarjeta durante una transacción o por medio de un recibo y lo utiliza para hacer compras a distancia, por ejemplo por teléfono o a través del Internet.

- Robo de la tarjeta antes de que nos llegue por correo: Éste fraude se produce cuando su tarjeta es robada antes de llegar a su domicilio. Generalmente cuando la entidad financiera de la tarjeta se la envía por correo.

- Cambio de la identidad en tarjetas

  Éste fraude es cuando un timador utiliza su información personal para abrir una cuenta en nombre. Hay dos tipos:

  - Fraude del uso: Éste fraude se produce cuando un criminal roba documentos, tales como extractos de cuenta, y los utiliza para abrir una cuenta nueva en su nombre.
  - Toma de posesión de la cuenta: Con este fraude un estafador utilizará su información personal para presentarse como usted y para convencer al banco que dirija pagos a otra parte.

- Fraude en cajero

  Este tipo de fraude lo realizan colocando entradas de tarjetas falsos que leen la banda magnética y la almacena para más tarde ser copiadas, este método normalmente se combina con un teclado que también almacena nuestro código secreto o una cámara en la parte superior para poder grabar el número. De esta manera pueden hacer una copia de la tarjeta y sacar dinero de los cajeros sin ningún problema gracias a la obtención del PIN. (La tarjetas de Credito)

2.10.2. Causa y Efecto del Fraude

Indudablemente dentro de los fraudes se llegan a cometer por diversas causas que dentro de la mayoría de los casos, la persona lo justifica con el simple hecho para sentirse bien de haber cometido dicho delito. Se diría que una de las principales causas por las que se llega a cometer un fraude se originaria por la necesidad del dinero y que no causaría ningún daño al tomarla. Como una segunda causa por la que se comete este delito de fraude, se debe a un sentimiento de ser mal remunerado o se siente en

condiciones de desventaja en relación con otros funcionarios o empleados en el orden económico. Una tercera causa es controles y procedimientos deficientes en el manejo de las actividades y operaciones de las empresas, otra causa es simplemente el querer hacer daño a las demás personas.

2.10.2.1. Causas Internas

Por controles de seguridad deficientes. Custodia de plásticos vírgenes: ¿Quién o quienes tienen acceso a la bóveda de plásticos? Custodia de plásticos troquelados: ¿Qué empleado es el responsable de la custodia de las tarjetas emitidas, que aún no han sido entregadas? ¿Qué procedimiento se tiene para la custodia de los mismos? Aprobación de créditos: Antes de aprobar la solicitud, se debe hacer la verificación de datos. (Número de teléfono, confirmar la dirección, referencias bancarias, confirmar ingresos, etc.). Emisión y envió de tarjetas: Es uno de los momentos más peligrosos en el ciclo de fraudes, ya que el plástico puede caer en manos de delincuentes.

2.10.2.2. Causas Externas

Por la Situación económica del país: Cada día hay más personas pobres, lo que hace se involucren en actividades delictivas. Robo de tarjeta o clonación de plásticos: Los asaltos y la tecnología hacen que para los delincuentes el negocio de la tarjeta de crédito represente una fuente magnífica para obtener beneficio económico. Aumento de bandas de delincuentes: La decadencia de principios morales, desintegración familiar, etc. hace que haya aumento en el crimen organizado.

2.10.3. Modalidades de fraude informático

Dentro de los fraudes informáticos para obtener beneficio propio existen los más comunes y utilizados que como define Solano pueden ser:

- Introducción de datos falsos, es una manipulación de datos de entrada al ordenador con el fin de producir o lograr movimientos falsos en transacciones de una empresa ora otorgarle solvencia moral y económica a una persona que no la tiene. También puede ocurrir de publicar datos sensibles, como los referentes a las convicciones religiosas, políticas o a la vida íntima de las personas.
- Caballo de Troya, consiste en introducir rutinas en un programa para que actúen en forma distinta a como estaba previsto.

- Técnica de salami, consiste en introducir al programa unas instrucciones para que remita a una determinada cuenta los céntimos de dinero de muchas cuentas corrientes. Aprovecha las repeticiones automáticas de los procesos de cómputo. Es una técnica especializada, consistente en que las cantidades de dinero muy pequeñas, se van sacando repetidamente de una cuenta y se transfiere a otra. Esta modalidad de fraude informático se realiza sin grandes dificultades y es muy difícil de detectar. Uno de los casos más ingeniosos es el redondeo hacia abajo, que consiste en una instrucción que se da al sistema informático para que transfiera a una determinada cuenta, los centavos que se descuenten por el redondeo.
- Llave no autorizada que abre cualquier archivo del ordenador por muy protegido que esté, con el fin de alterar, borrar, copiar, insertar o utilizar, en cualquier forma no permitida, datos almacenados en el ordenador.
- Puertas falsas, consiste en la práctica de introducir interrupciones en la lógica de los programas con objeto de chequear en medio de procesos complejos, si los resultados intermedios son correctos, producir salidas de control con el mismo fin o guardar resultados intermedios en ciertas áreas para comprobarlos más adelante.
- Bombas lógicas o cronológicas, son programas diseñados para producir sus efectos dañinos a futuro, en una fecha determinada por su creador, "es una especie de bomba de tiempo que debe producir daños posteriormente." Las bombas lógicas, son difíciles de detectar antes de que exploten; son las que pueden resultar más dañinas y prever que exploten cuando el delincuente ya se encuentra lejos. La bomba lógica puede utilizarse también como instrumento de extorsión y se puede pedir un rescate a cambio de dar a conocer el lugar en donde se halla.
- Ataques sincrónicos, basados en la forma de funcionar los sistemas operativos y sus conexiones con los programas de aplicación a los que sirven y soportan en su ejecución. Es un fraude de alto conocimiento técnico, muy difícil de detectar.
- Recogida de información residual, es el aprovechamiento de información abandonada sin ninguna protección como residuo de un trabajo previamente autorizado. To scavenge, traduce, recoger basura. Puede efectuarse físicamente

cogiendo papel de desecho de papeleras o electrónicamente, tomando información residual que ha quedado en memoria o en soportes magnéticos.

- Divulgación no autorizada de datos reservados, es una variedad del espionaje industrial que sustrae información confidencial de una empresa.
- Toma no autorizada de información, consiste en acceder a áreas restringidas para pillar información de una empresa, aprovechando que el empleado encargado del equipo no está presente.
- Pinchado de líneas telefónicas de transmisión de datos para recuperar la información que circula por ellas, por medio de un radio, un modem y una impresora.
- Planificación y simulación de un delito informático antes de realizarlo, para ver qué repercusión va a tener en los asientos contables de una empresa.
- Manipulación de información de los hackers o jóvenes fanáticos de la informática, que son capaces con un modem de acceder a redes de transmisión de datos, saltándose las medidas de seguridad y leer información confidencial, sustraerla, alterarla, destruirla o cometer fraude sobre ella. (Solano Orlando, 2020)

2.11. Fraude informático en Ecuador

De los fraudes informáticos que van creciendo inmensurablemente en la actualidad según las cifras son que un 85% causados por errores de los mismos consumidores siendo un 33% por Descuido, 31% Redes Sociales, 13% Correos Electrónicos, 23% Información en la nube.

En el lapso de 9 meses en el año 2013 se registraron 624 denuncias, registró 626 denuncias desde el 10 de agosto del 2014 -cuando entró en vigencia el COIP hasta el 31 de mayo del 2015, en el 2016 de enero a junio se registró 530 denuncias, en el 2017 se registró un total de 340 denuncias siendo las mayores denuncias la apropiación fraudulenta por medio electrónico.

Dentro del Código Orgánico Integral Penal se sancionan delitos informáticos, para cuyos actos se comenten por medio del 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.

Por trasferencia electrónica, se encuentra contemplada en el Artículo 190 “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”, se lo puede contemplar dentro del Pishing por caracterizarse por acceder, interceptar, retener, reproducir en cualquier forma un dato informático, clonar, duplicar, copiar, robar la información contenida en las bandas magnéticas, chips u otro dispositivo electrónico de las tarjetas de crédito o débito.

Siendo que se realizan por medio de un sistema informático que ejecuta, programa, certificados de seguridad o páginas electrónicas, ventanas emergentes o que modifique el sistema de un servicio financiero de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente a la que quiere acceder.

Para tipificarse y penalizar delito informático como delito autónomo; en la Constitución se refiere al derecho a la propiedad en la siguiente norma: “Art. 66.- Se reconoce y garantizará a las personas:

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

20. El derecho a la intimidad personal y familiar.

21. El derecho a la inviolabilidad y al secreto de la correspondencia física y virtual; ésta no podrá ser retenida, abierta ni examinada, excepto en los casos previstos en la ley, previa intervención judicial y con la obligación de guardar el secreto de los asuntos ajenos al hecho que motive su examen. Este derecho protege cualquier otro tipo o forma de comunicación. (Constitucion de la República del Ecuador, 2008)

26. El derecho a la propiedad en todas sus formas, con función y responsabilidad social y ambiental. El derecho al acceso a la propiedad se hará efectivo con la adopción de políticas públicas, entre otras medidas” (Constitucion de la República del Ecuador, 2008)

Se reconoce a todo ciudadano su derecho a la protección de datos, es decir, nadie puede invadir privacidad de los individuos.

2.12. Perito Informático En Ecuador

Dentro de la palabra perito informático sabemos que es una persona que se especializa en la materia en este caso la informática y en las nuevas tecnologías, siendo una figura definida por la ley como un experto

Hablando de peritaje informático sabemos que es algo relativamente nuevo dentro de muestro medio, es algo que ha surgido con el tiempo debió a la utilización de la tecnología dentro de nuestras vidas en el día a día, actualmente tanto personas naturales como jurídicas que se ven afectadas por algún delito informático se ven en la necesidad de la utilización de un peritaje informático para que todo lo que se evidencie quede en un informe pericial siendo eso lo que sirva como pruebas en lo caso de un proceso legal.

Sabemos que el Peritaje Informático se refiere a los estudios e investigaciones orientados a la obtención de una prueba o evidencia electrónica de aplicación en un asunto judicial o extrajudicial para que sirva para decidir sobre la culpabilidad o inocencia de una de las partes.

Dentro de las responsabilidades de los peritos este es el de realizar un Informe Pericial que servirá como prueba en todos los asuntos relacionados a:

- Uso irregular del correo electrónico
  Abuso de los sistemas informáticos
- Violación de la seguridad
- Piratería
- Borrado intencionado de archivos
- Comercio electrónico
- Manipulación inadecuada de equipos, sabotajes
- Cualquier otro tipo de delitos informático

Dentro dela elaboración de un peritaje informático tenemos algunos puntos relevantes como los son:

- Análisis de situación inicial
- Desarrollo de la investigación
- Elaboración del informe pericial
- Testificación en el juicio

Así mismo existe lo que es el contra-peritaje siendo un informe pericial de un informe pericial ya emitido, en ocasiones este contra-peritaje viene siendo la clave para la obtención de información que un primer perito no incluyo, dentro de este contra-peritaje existen puntos que se deben de tener en cuenta como:

- El objetivo de la pericia no es relevante dentro del caso
- Obtener n el analizado aspectos que no demuestran el problema
- Demostrar parcialidad dentro del informe a realizar
- Deberá probar cada evidencia
- Verificara si se realizó pruebas modificatorias a las evidencias
- Levantamiento de evidencia informática no incluida en el informe.

2.13. La Banca

Los principales obstáculos para la determinación de la responsabilidad penal de la persona jurídica antes de la expedición del COIP, tenían que ver con tres imposibilidades: a) la imposibilidad de imputar a ésta una acción u omisión, ya que se ponía en entredicho que la persona jurídica pueda actuar independientemente de la voluntad de sus socios; b) la imposibilidad de culpabilizar a una persona jurídica de un acto; y, c) la de imposibilidad de que cumpla una pena.

Se debe partir del pensamiento de que frente al delito informático, la banca y los clientes de esta entidad son víctimas de delito, siendo que por lo general los que vulneran las seguridades provocando daño son personas extrañas al sistema financiero.

En los años 2010 y 2011 se presentaron múltiples denuncias ante la Fiscalía General del Ecuador por los casos de delitos informáticos, todos los denunciantes eran clientes de la banca.

Ante todo eso la Fiscalía General del Estado en colaboración junto a la Superintendencia de Bancos conformaron una comisión para investigar el aumento de

los fraudes que afectaban a todos los clientes de la banca, temiendo en cunetas diversos puntos como lo fueron:

1) Si los Bancos daban cumplimiento a lo dispuesto en los Arts. 4 y 8 de la Ley de Defensa del Consumidor, en concordancia con lo establecido en los Arts. 20 y 21 del Reglamento de la Ley de Comercio Electrónico.
2) Si las instituciones que debían ser analizadas podían comprobar que tenían alertas de control interno para prevenir fraudes.
3) Si las instituciones bancarias ante reclamos por fraudes informáticos contaban con procesos internos y si éstos cumplían las disposiciones emanadas de la Superintendencia de Bancos.
4) Si demostraban en los procesos de investigación de reclamos del cliente una adecuada información del avance de ésta.
5) Si las entidades bancarias mantenían provisión de riesgos en caso de fraudes informáticos.
6) Cuáles eran las soluciones a corto, mediano y largo plazo implementadas por las instituciones bancarias para minimizar el fraude informático

Luego del análisis de la investigación lo que sucedió es que la Fiscalía y la Superintendencia de Bancos representadas por sus máximos personeros suscribieron la resolución interinstitucional 001–FGE–SBS–2011 el 21 de Marzo del año 2011.

Ante el creciente número de denuncias de delitos se relacionaban con la clonación de tarjetas de créditos o débito y el robo de contraseñas de cuentas bancarias, posteriormente en el año 2012, lo que es la Superintendencia de Bancos y Seguros del Ecuador en una resolución JB-2012-2090 (Junta Bancaria del Ecuador, Superintendecia de Bancos y Seguros del Ecuador, 2020), pidió a las instituciones financieras que contrataran a un seguro privado para así poder evitar fraudes a través de la tecnologías de información. (Philco & Rosero, 2014)

Además, en una resolución JB-2012-2148 (Junta Bancaria del Ecuador, Superintendecia de Bancos y Seguros del Ecuador) , la Superintendencia de Bancos y Seguros pidió a las instrucciones bancarias la implementación de medidas de seguridad en los cajeros automáticos, así como también, en los canales electrónicos. Entre las medidas de seguridad que se implementaron están: Protección contra clonación de tarjetas,

Protección al software e información del cajero automático, accesos físicos al interior de los cajeros automáticos, entre otras medidas (Ecuador Inmediato, 2013)

2.14. Legislación comparada

2.14.1. Delito informático en Chile

En Chile en el 2017 se presentó por medio de un Boletín 12.192-25 siendo este un proyecto de ley que modifico la legislación sobre delitos informáticos y derogo a la ley 19223 que fue de 1993. Este proyecto busco poder cumplir con los compromisos que tenían adquiridos por el Convenio de Budapest. Introduce modificaciones en la materia procesal penal para así facilitar una persecución adecuada a los delitos informáticos.

Artículo 1°.- Perturbación informática. El que maliciosamente obstaculice o perturbe el funcionamiento de un sistema informático, a través de la introducción, transmisión, daño, deterioro, alteración o supresión de datos informáticos, será castigado con la pena de presidio menor en su grado medio a máximo. Si además se hiciere imposible la recuperación del sistema informático en todo o en parte, se aplicará la pena de presidio menor en su grado máximo. (Proyecto de Ley Boletín N° 12.192-25, s.f.)

Artículo 2°.- Acceso ilícito. El que indebidamente acceda a un sistema informático será castigado con presidio menor en su grado mínimo o multa de once a veinte unidades tributarias mensuales. El que indebidamente acceda con el ánimo de apoderarse, usar o conocer la información contenida en un sistema informático, será castigado con presidio menor en su grado mínimo a medio. Si en la comisión de las conductas descritas en este artículo se vulnerasen, evadiesen o transgrediesen medidas de seguridad destinadas para impedir dicho acceso, se aplicará la pena de presidio menor en su grado medio. (Proyecto de Ley Boletín N° 12.192-25, s.f.)

Artículo 3°.- Interceptación ilícita. El que indebida y maliciosamente intercepte o interfiera la transmisión no pública de información entre los sistemas informáticos, será castigado con presidio menor en su grado mínimo a medio. El que capte ilícitamente datos contenidos en sistemas informáticos a través de las emisiones electromagnéticas

de los dispositivos, será castigado con presidio menor en su grado medio. (Proyecto de Ley Boletín N° 12.192-25, s.f.)

Artículo 4°.- Daño informático. El que maliciosamente altere, borre o destruya datos informáticos, será castigado con presidio menor en su grado medio, siempre que con ello se cause un daño serio al titular de los mismos. (Proyecto de Ley Boletín N° 12.192-25, s.f.)

Artículo 5º.- Falsificación informática. El que maliciosamente introduzca, altere, borre, deteriore, dañe, destruya o suprima datos informáticos con la intención de que sean tomados o utilizados a efectos legales como auténticos, será sancionado con la penas previstas en el artículo 197 del Código Penal, salvo que sean o formen parte de un instrumento, documento o sistema informático de carácter público, caso en que se sancionará con las penas previstas en el artículo 193 de dicho cuerpo legal. (Proyecto de Ley Boletín N° 12.192-25, s.f.)

Artículo 6°.- Fraude informático. El que, causando perjuicio a otro y con la finalidad de obtener un beneficio económico ilícito para sí o para un tercero, utilice la información contenida en un sistema informático o se aproveche de la alteración, daño o supresión de documentos electrónicos o de datos transmitidos o contenidos en un sistema informático, será penado:

1) Con presidio menor en sus grados medio a máximo y multa de once a quince unidades tributarias mensuales, si el valor del perjuicio excediera de cuarenta unidades tributarias mensuales.

2) Con presidio menor en su grado medio y multa de seis a diez unidades tributarias mensuales, si el valor del perjuicio excediere de cuatro unidades tributarias mensuales y no pasare de cuarenta unidades tributarias mensuales.

3) Con presidio menor en su grado mínimo y multa de cinco a diez unidades tributarias mensuales, si el valor del perjuicio no excediere de cuatro unidades tributarias mensuales. Si el valor del perjuicio excediere de cuatrocientas unidades tributarias mensuales, se aplicará la pena de presidio menor en su grado máximo y multa de veintiuna a treinta unidades tributarias mensuales. (Proyecto de Ley Boletín N° 12.192-25, s.f.)

2.13.2. Delitos informáticos en Argentina

En Argentina la cámara de Senadores del Congreso Nacional en el 2008 aprobó la ley 26.388 donde se penaliza delitos electrónicos, el Código Penal Argentino, tipifica y sanciona lo relacionado al fraude informático en su capítulo IV Estafa y otras defraudaciones en los siguientes artículos:

Artículo 172. - Será reprimido con prisión de un mes a seis años, el que defraudare a otro con nombre supuesto, calidad simulada, falsos títulos, influencia mentida, abuso de confianza o aparentando bienes, crédito, comisión, empresa o

negociación o valiéndose de cualquier otro ardid o engaño. (CODIGO PENAL DE LA NACION ARGENTINA, s.f.)

Artículo 173.- Sin perjuicio de la disposición general del artículo precedente, se considerarán casos especiales de defraudación y sufrirán la pena que él establece:

15. El que defraudare mediante el uso de una tarjeta de compra, crédito o débito, cuando la misma hubiere sido falsificada, adulterada, hurtada, robada, perdida u obtenida del legítimo emisor mediante ardid o engaño, o mediante el uso no autorizado de sus datos, aunque lo hiciere por medio de una operación automática. (Codigo Penal de la Nacion Argentina, 2004)

16. El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos. (Código Penal de la Nacion Argentina, 2008)

Una Resolución del Ministerio de Defensa N° 343, el 14 de mayo del año 2014, dispuso la creación de un Comando Conjunto de Ciberdefensa dependiente orgánica, funcional y operacionalmente del Estado Mayor Conjunto de las Fuerzas Armadas (Artículo primero de la Resolución MD N° 343/2014 del 14 de mayo de 2014). Su competencia específica es ejercer la conducción de las operaciones de ciberdefensa en forma permanente a los efectos de garantizar las operaciones militares del Instrumento Militar de la Defensa Nacional.

2.14. Marco legal

En esta sección nos referimos a las normas que se aplican para regular todo lo relacionado con los delitos informáticos en el Ecuador, siendo estos los principios por los cuales se deben regir en primer lugar los previstos en la Constitución de la República del Ecuador siguiendo con las demás leyes, especialmente las que regulan el sector financiero y bancario y el Código Orgánico Integral Penal.

Entre las leyes que protegen los derechos de los usuarios del sistema bancario y particularmente de las tarjetas de crédito se encuentra la Ley Orgánica de Defensa del Consumidor, en cuyo artículo 55 se describen las prácticas abusivas de mercado absolutamente prohibidas al proveedor, entre otras, el redondeo de tiempos para efectivizar el cobro de intereses, multas u otras sanciones económicas en tarjetas de crédito, préstamos bancarios y otros similares.

Otro cuerpo legal relevante es el Código Orgánico Monetario Financiero, en cuyo artículo 157 se establece que **l**os usuarios financieros podrán interponer quejas o

reclamos ante la propia entidad, organismo de control o al Defensor del Cliente o plantear cualquier acción administrativa, judicial o constitucional reconocida en la ley para exigir la restitución de sus derechos vulnerados y la debida compensación por los daños y perjuicios ocasionados.

Respecto al narco legal debe añadirse además las actuaciones realizadas en su momento por el Fiscal General del Estado, Dr. Washington Pesántez, quien siguió una política activa en la protección de los derechos de las personas víctimas de delitos financieros, al obligar a las entidades del sector a devolver a los clientes los valores perdidos por esa causa, y a crear un seguro contra delitos informáticos para proteger a los usuarios del sistema financiero.

Entre algunas de las medidas que se adoptaron desde entonces, para la protección del sistema financiero y de los propios usuarios, puede mencionarse el uso de mensajes y correos electrónicos alertando de cualquier movimiento no realizado por el titular de la tarjeta de crédito, así como la implementación de mayores medidas de seguridad para el manejo de las tarjetas de crédito y el acceso a los datos para efectuar pagos, trasferencias y operaciones de cualquier naturaleza.

Constitución de la República del Ecuador

Luego de explicado los aspectos generales pasamos a las disposiciones particulares. En la Constitución del Ecuador no se menciona de una manera específica los delitos informativos en base a la alteración y modificación mediante transferencia electrónica en modalidad tarjeta de crédito, pero si existe cierto bien jurídico protegido que se puede denominar como parte de este tipo de conducta siendo el acceso universal a las tecnologías de información y comunicación y el derecho a la intimidad personal y familiar establecidos en artículo 66.

Art. 16.- Todas las personas, en forma individual o colectiva, tienen derecha a:

1. Una comunicación libre, intercultural, incluyente, diversa y participativa, en todos los ámbitos de la interacción social, por cualquier medio y forma, en su propia lengua y con sus propios símbolos.
2. El acceso universal a las tecnologías de información y comunicación.
3. La creación de medios de comunicación social , y al acceso en igualdad de condición al uso de las frecuencias del espectro radioeléctrico para la gestión de estaciones de radio y televisión públicas, privadas y comunitarias, y a bandas libres para la explotación de redes inalámbricas.

4. El acceso y uso de todas las formas de comunicación visual, auditiva sensorial y a otras que permiten la inclusión de personas con discapacidad.
5. Integrar los espacios de participación previstos en la Constitución en el campo de la comunicación. (Constitucion de la República del Ecuador, 2008)

Art. 17.- EI Estado fomentará la pluralidad y la diversidad en la comunicación, y al efecto:

2. Facilitará la creación y el fortalecimiento de medios de comunicación públicos, privados y comunitarios, así como el acceso universal a las tecnologías de información y comunicación en especial para las personas y colectividades que carezcan de dicho acceso o lo tengan de forma limitada. (Constitucion de la República del Ecuador, 2008)

Art. 18.- Todas las personas, en forma individual o colectiva, tienen derecho a:

1. Buscar, recibir, intercambiar, producir y difundir información veraz, Verificada, oportuna, contextualizada, plural, sin censura previa acerca de los hechos, acontecimientos y procesos de interés general, y con responsabilidad ulterior. (Constitucion de la República del Ecuador, 2008)

Art. 66.- El derecho de toda persona agraviada por informaciones sin pruebas o inexactas, emitidas por medios de comunicación social, a la correspondiente rectificación, réplica o respuesta, en forma inmediata, obligatoria y gratuita, en el mismo espacio u horario. (Constitución de la República del Ecuador, 2008)

Art. 384.- El sistema de comunicación social asegurará el ejercicio de los derechos de la comunicación, la información y la libertad de expresión, y fortalecerá la participación ciudadana. (Constitucion de la República del Ecuador, 2008)

Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos

En 2002 que fue promulgada la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos fue con el fin de regular el tráfico de información que se da. Al respecto varios de sus artículos expresan que:

Art. 5.- Confidencialidad y reserva.- Se establecen los principios de confidencialidad y reserva para los mensajes de datos, cualquiera sea su forma, medio o intención. Toda violación a estos principios, principalmente aquellas referidas a la intrusión electrónica, transferencia ilegal de mensajes de datos o violación del secreto profesional, será sancionada conforme a lo dispuesto en esta Ley y demás normas que rigen la materia. (Ley de Comercio electrónico Firmas electrónicas y mensajes de datos, 2002)

Art. 9.- Protección de datos.- Para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá el consentimiento expreso del titular de éstos, quien podrá seleccionar la información a compartirse con terceros.

La recopilación y uso de datos personales responderá a los derechos de privacidad, intimidad y confidencialidad garantizados por la Constitución Política de la República y esta ley, los cuales podrán ser utilizados o transferidos únicamente con autorización del titular u orden de autoridad competente.

No será preciso el consentimiento para recopilar datos personales de fuentes accesibles al público, cuando se recojan para el ejercicio de las funciones propias de la administración pública, en el ámbito de su competencia, y cuando se refieran a personas vinculadas por una relación de negocios, laboral, administrativa o contractual y sean necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato.

El consentimiento a que se refiere este artículo podrá ser revocado a criterio del titular de los datos; la revocatoria no tendrá en ningún caso efecto retroactivo. (Ley de Comercio electrónico Firmas electrónicas y mensajes de datos, 2002)

Código Orgánico Monetario Financiero

Art. 157.- Vulneración de derechos. Los usuarios financieros podrán interponer quejas o reclamos ante la propia entidad, organismo de control o al Defensor del Cliente o plantear cualquier acción administrativa, judicial o constitucional reconocida en la ley para exigir la restitución de sus derechos vulnerados y la debida compensación por los daños y perjuicios ocasionados. (Código Orgánico Monetario Financiero, 2014)

Código Orgánico Integral Penal COIP

Dentro de la reforma del COIP del año 2014 no se encuentra tipificados los nuevos delitos informáticos como el ciberbulling, ciberataques, subastas y ventas ilegales en internet, uso de redes robot o zombi, entre otros.

Art. 186.2.- Estafa. La persona que, para obtener un beneficio patrimonial para sí misma o para una tercera persona, mediante la simulación de hechos falsos o la deformación u ocultamiento de hechos verdaderos, induzca a error a otra, con el fin de que realice un acto que perjudique su patrimonio o el de una tercera, será sancionada

con pena privativa de libertad de cinco a siete años. La pena máxima se aplicará a la persona que:

1. Defraude mediante el uso de tarjeta de crédito, débito, pago o similares, cuando ella sea alterada, clonada, duplicada, hurtada, robada u obtenida sin legítimo consentimiento de su propietario.

2. Defraude mediante el uso de dispositivos electrónicos que alteren, modifiquen, clonen o dupliquen los dispositivos originales de un cajero automático para capturar, almacenar, copias o reproducir información de tarjetas de crédito, débito, pago o similares.

3. Entregue certificación falsa sobre las operaciones o inversiones que realice la persona jurídica.

4. Induzca a la compra o venta pública de valores por medio de cualquier acto, práctica, mecanismo o artificio engañoso o fraudulento.

5. Efectúe cotizaciones o transacciones ficticias respecto de cualquier valor.

La persona que perjudique a más de dos personas o el monto de su perjuicio sea igual o mayor a cincuenta salarios básicos unificados del trabajador en general será sancionada con pena privativa de libertad de siete a diez años.

La estafa cometida a través de una institución del Sistema Financiero Nacional, de la economía popular y solidaria que realicen intermediación financiera mediante el empleo de fondos privados públicos o de la Seguridad Social, será sancionada con pena privativa de libertad de siete a diez años.

La persona que emita boletos o entradas para eventos en escenarios públicos o de concentración masiva por sobre el número del aforo autorizado por la autoridad pública competente, será sancionada con pena privativa de libertad de treinta a noventa días. (Código Orgánico Integral Penal Ecuatoriano, 2020)

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. (Código Orgánico Integral Penal Ecuatoriano, 2020)

Art. 229.- Revelación ilegal de base de datos.- La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años. Si esta conducta se comete por una o un servidor público, empleadas o empleados bancarios internos o de instituciones de la economía popular y solidaria que realicen intermediación financiera o contratistas, será sancionada con pena privativa de libertad de tres a cinco años (Código Orgánico Integral Penal Ecuatoriano, 2020)

Art. 230.3.4.- Interceptación ilegal de datos.- Será sancionada con pena privativa de libertad de tres a cinco años:

1. La persona que sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible.

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. La persona que a través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que esté soportada en las tarjetas de crédito, débito, pago o similares.

4. La persona que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior. (Código Orgánico Integral Penal Ecuatoriano, 2020)

Art. 231.- Transferencia electrónica de activo patrimonial.- La persona que, con ánimo de lucro, altere, manipule o modifique el funcionamiento de programa o sistema informático o telemático o mensaje de datos, para procurarse la transferencia o

apropiación no consentida de un activo patrimonial de otra persona en perjuicio de esta o de un tercero, será sancionada con pena privativa de libertad de tres a cinco años. Con igual pena, será sancionada la persona que facilite o proporcione datos de su cuenta bancaria con la intención de obtener, recibir o captar de forma ilegítima un activo patrimonial a través de una transferencia electrónica producto de este delito para sí mismo o para otra persona. (Código Orgánico Integral Penal Ecuatoriano, 2020)

2.15 Jurisprudencia

Resolución Interinstitucional 001–FGE–SBS–2011

FISCALÍA GENERAL DEL ESTADO

RESOLUCIÓN INTERINSTITUCIONAL
No. 001-FGE-SBS-2011

Ab. Pedro Solines Chacón
SUPERINTENDENTE DE BANCOS Y SEGUROS

Dr. Washington Pesántez Muñoz
FISCAL GENERAL DEL ESTADO

CONSIDERANDO:

QUE, el artículo 194 de la Constitución de la República establece que la Fiscalía General del Estado tiene autonomía administrativa, económica y financiera, funciona de manera desconcentrada, y su máxima autoridad y representante legal es el Fiscal General;

QUE, la Superintendencia de Bancos y Seguros es un organismo técnico de vigilancia, auditoria, intervención y control de actividades financieras de la Banca Pública y Privada;

QUE, la norma constitucional determina que el titular de la acción penal y de la investigación pre procesal y procesal penal, de hechos que sean presumiblemente considerados delitos de acción pública, dentro del nuevo Sistema Procesal Penal Acusatorio, es el Fiscal;

QUE, la Superintendencia de Bancos y Seguros, debe velar porque las entidades sujetas a su control, actúen bajo el ordenamiento jurídico vigente y atiendan al interés general.

Este Organismo de Control ejercerá la supervisión, vigilancia y control del sistema financiero, con especial atención a **LA PROTECCIÓN DE LOS INTERESES DEL PÚBLICO;**

QUE, de acuerdo a lo dispuesto en el Art. 226 de la Constitución, las Instituciones del Estado, sus organismos, dependencias, tendrán el deber de coordinar acciones para el cumplimiento de sus fines y hacer efectivo **EL GOCE Y EJERCICIO DE LOS DERECHOS RECONOCIDOS EN LA CONSTITUCIÓN**. Por este mandato de la Carta Fundamental, la Fiscalía General del Estado y la Superintendencia de Bancos y Seguros, ante el aumento de los Fraudes en el Sistema Informático a nivel nacional, han decidido en el ámbito de sus funciones coordinar acciones y conformar una Comisión para investigar estos hechos que revisten el carácter de delito, a fin de buscar una solución viable al perjuicio patrimonial que han sufrido varios usuarios del Sistema Financiero, por el cometimiento de este hecho ilícito, además de evitar que las transferencias fraudulentas de estos fondos sirvan para el cometimiento de delitos relacionados al lavado de activos en el país;

DESPACHO FISCAL GENERAL
Av. Eloy Alfaro N 32-250 y República - Teléfonos: (593-2) 255-8561 /562 /563
Quito - Ecuador

QUE, el Art. 426 de la Constitución menciona que todas las personas, autoridades e instituciones están sujetas a la Constitución. Por tanto la Fiscalía General del Estado y la Superintendencia de Bancos deben actuar en consecuencia y ceñidos a la norma constitucional, y velar por la aplicación directa de los derechos humanos reconocidos en ella sin que se pueda alegar falta de ley o desconocimiento de las normas para justificar la vulneración de derechos y garantías establecidos en la Constitución;

QUE, las actividades financieras son un servicio de **ORDEN PÚBLICO**, y 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;

QUE, los perjudicados por los fraudes del sistema informático han acudido tanto a la Fiscalía General del Estado como a la Superintendencia de Bancos a fin de hacer valer sus derechos;

QUE, los servicios públicos que prestan las entidades financieras privadas, están sujetos al control de la Superintendencia de Bancos y su accionar está sometido al régimen legal de derecho público consagrado en la Ley de Instituciones del Sistema Financiero, que regula entre otros los contratos Bancarios, los mismos que establecen la relación jurídica entre el cliente y la entidad financiera la cual se crea normalmente a través de un contrato de cuenta corriente o cuenta de ahorros, que no es otra cosa que una acción mediante la cual el depositante transfiere el dinero al depositario, debiendo éste restituirlo cuando se le reclame. **LA OBLIGACIÓN LEGAL DE CUSTODIA** del depositario implica guardar y conservar el dinero objeto de depósito;

QUE, el Art. 52 de la Constitución señala que: *Las personas tienen derecho a disponer de **BIENES Y SERVICIOS DE ÓPTIMA CALIDAD**, así como a una información precisa, no engañosa,* una **INFORMACIÓN ADECUADA, VERAZ, CLARA, OPORTUNA Y COMPLETA** sobre los bienes y servicios ofrecidos en el mercado, así como sus precios, características, calidad, condiciones de contratación y demás aspectos relevantes de los mismos, incluyendo **LOS RIESGOS QUE PUDIEREN PRESTAR**; en igual sentido la Carta Magna dispone que *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 descripción que incorpore, por tanto y dado que las actividades financieras son tanto **SERVICIO PÚBLICO** como un servicio de **ORDEN PÚBLICO**, se considera como **NO NEGOCIABLES. LA RUPTURA DEL ORDEN PÚBLICO o PUESTA EN PELIGRO** del servicio público da lugar a la imposición de una sanción dependiendo de la gravedad desde la administrativa, a la civil e inclusive la penal;

QUE, la Responsabilidad es aquella situación jurídica en la que el patrimonio de una persona natural o jurídica debe responder para resarcir por una lesión producida a un tercero, atribuible a ésta, por un acto doloso, negligente o simplemente por la omisión de su deber y el riesgo creado. Como resultado del daño causado se genera una obligación de resarcimiento o reparación integral material e inmaterial;

QUE, un elemento determinante para el surgimiento de la responsabilidad civil, es la omisión de proteger los depósitos de los clientes del sistema financiero, desatención que produce **UN DAÑO EN EL PATRIMONIO** de cuenta corrientitas y cuenta ahorristas, quienes han sido perjudicados por el fraude informático. Es así que **EL NEXO CAUSAL** se verifica entre estos dos hechos cuando el banco al **OMITIR SU DEBER DE PROTECCIÓN**, no le informa al cliente de los riesgos que existe al usar el servicio de banca en línea, si bien el cliente es responsable de las claves de acceso al sistema, el banco es responsable de la seguridad del sitio web y de informar al usuario el uso correcto del sitio, brindando para ello la información adecuada, veraz, clara, oportuna y completa procurando entonces la educación del usuario con la finalidad ulterior de que éste haga un uso responsable del servicio de banca en línea. Por tanto el banco no puede alegar la entera responsabilidad del usuario perjudicado por este delito, cuando **el banco es también responsable por la omisión de su obligación de preservar los depósitos de sus clientes como manda la Carta Fundamental**.

El desarrollo de servicios asumidos por las Instituciones Financieras, lleva implícito el deber de garantizar la seguridad de estos. **La falla en el funcionamiento del servicio que ofrece el intermediario financiero, radica en la falta de seguridad en los mecanismos de identificación del cliente para acceder a la plataforma interna.** Desde esta perspectiva, producto de los riesgos inherentes a la transmisión de datos mediante Internet, se deben **brindar las herramientas necesarias para reducir la posibilidad de que ocurra una suplantación de identidad**. Se trata de una característica intrínseca del servicio que ofrece el banco. En este sentido, la responsabilidad se imputa como

consecuencia del riesgo creado y la inseguridad que presenta el sistema; y,

En mérito de las consideraciones señaladas y en ejercicio de las facultades conferidas en la Constitución y en la Ley.

RESUELVEN:

Art. 1.- Las Instituciones del Sistema Financiero emprenderán acciones correctivas necesarias para impedir el cometimiento del denominado "fraude informático" y de los delitos relacionados con el lavado de activos.

Art. 2.- Las Instituciones del Sistema Financiero, realizarán campañas de información personalizada a sus clientes a fin de evitar que sean perjudicados por las transacciones a través del sistema informático.

Art. 3.- La Comisión conformada por funcionarios de la Fiscalía General del Estado y de la Superintendencia de Bancos y Seguros, han investigado las denuncias presentadas por usuarios, clientes de la banca privada, que han sido víctimas de la fragilidad del sistema informático por ella utilizado y que les ha ocasionado pérdidas en sus depósitos en cuentas aperturadas en las diferentes instituciones financieras del país, determinándose la responsabilidad directa o indirecta de éstas, por lo que la Comisión como resultado de las indagaciones y procesos de control practicados, recomienda y considera que los depositantes y usuarios que han resultado perjudicados deben recibir el resarcimiento de su patrimonio por parte de las instituciones bancarias, custodias de esos depósitos.

Art. 4.- Por lo señalado, las Instituciones del Sistema Financiero del país reconocerán valores a sus clientes, que han sufrido pérdidas patrimoniales a consecuencia de la fragilidad y vulnerabilidad del Sistema Informático empleado (fraude informático), en el periodo comprendido entre el 1ro de Enero del 2010 hasta la presente fecha, según este cuadro:

MONTO RECLAMADO	% RESTITUIDO
De 1 USD a 2000 USD	100%
De 2001 USD a 10.000 USD	80%
Más de 10.000 USD	60%

La devolución de los dineros a los usuarios perjudicados, se hará de forma inmediata, por medio de transferencia bancaria a la cuenta corriente o de ahorros que los usuarios perjudicados posean en las correspondientes Instituciones Financieras del país.

Art. 5.- Si los usuarios perjudicados no aceptaren los montos señalados en esta Resolución, podrán seguir las acciones legales correspondientes a fin de reclamar el cien por ciento de su pérdida patrimonial.

Art. 6.- Las Instituciones Financieras Privadas, serán notificadas por parte de la Superintendencia de Bancos y Seguros con la presente Resolución y con el listado elaborado por la Comisión en el que se señalan los datos de las personas que aparecen como perjudicadas. La inobservancia de esta Resolución dará lugar a las sanciones previstas en la Ley de Instituciones del Sistema Financiero, sin perjuicio de las de orden civil y penal a que hubiere lugar.

Art 7.- La Superintendencia de Bancos y Seguros, elevará a consideración de la Junta Bancaria, se requiera a las Instituciones Financieras Privadas, la contratación de una "Póliza de Fidelidad Bancaria" que incluya la cobertura denominada "Delito Informático y Cibercrimen", que brinde amparo contra fraudes informáticos bajo condiciones pactadas entre los clientes y el Banco y que aseguren la cobertura necesaria sobre estos hechos y las exclusiones que se aplicarán, o la expedición de una normativa que persiga similar finalidad.

Art. 8.- La presente Resolución entrará a regir a partir de la presente fecha, y de su efectiva ejecución y cumplimiento encárguese la Superintendencia de Bancos y Seguros, en su calidad de Organismo de Control de las Instituciones Financieras.

Dado y firmado en Quito, Distrito Metropolitano, a los veinte y un días del mes de marzo del dos mil once.

Ab. Pedro Solines Chacón
SUPERINTENDENCIA DE BANCOS Y SEGUROS

Dr. Washington Pesántez Muñoz
FISCAL GENERAL DEL ESTADO

CER...

...TIFICAMOS que la Resolución que antecede la suscribieron el señor abogado Pedro Solines Chacón Superintendente de Bancos y Seguros y el señor doctor Washigton Pesántez Muñoz Fiscal General del Estado, en esta ciudad de Quito a los 21 días del mes de marzo del 2011.-

Abg. Luis Alberto Cabezas- Klaere
SECRETARIO GENERAL
SUPERINTENDENTE DE BANCOS Y SEGUROS

Dr. Jorge Cevallos Dillon
SECRETARIO GENERAL
FISCALÍA GENERAL DEL ESTADO

Resolución JB-2012-2090, Junta Bancaria del Ecuador, 2012

Junta Bancaria del Ecuador

SBS
Superintendencia de Bancos y Seguros del Ecuador

RESOLUCIÓN JB-2012-2090

LA JUNTA BANCARIA

CONSIDERANDO:

Que frente al auge de los nuevos tipos de fraudes informáticos y las pérdidas económicas que generan a las entidades controladas y sus usuarios, la Superintendencia de Bancos y Seguros y la Fiscalía General del Estado expidieron las resoluciones No. 001-FGE-SBS-2011 y No. 002-FGE-SBS-2011 de 21 de marzo y 25 abril del 2011, respectivamente;

Que el artículo 7 de la citada resolución interinstitucional No. 001-FGE-SBS-2011, establece que la Superintendencia de Bancos y Seguros elevará a consideración de la Junta Bancaria, para que se requiera a las instituciones financieras privadas la contratación de una "Póliza de fidelidad bancaria" que incluya la cobertura denominada "Delito informático y cibercrimen", que brinde amparo contra fraudes informáticos bajo condiciones pactadas entre los clientes y la institución y que aseguren la cobertura necesaria sobre estos hechos y las exclusiones que se aplicarán;

Que el artículo 1, del capítulo I "De la gestión integral y control de riesgos", del título X "De la gestión y administración de riesgos", del 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, dispone que las instituciones del sistema financiero, deberán establecer esquemas eficientes y efectivos de administración y control de todos los riesgos a los que se encuentran expuestas en el desarrollo del negocio, conforme su objeto social, sin perjuicio del cumplimiento de las obligaciones que sobre la materia establezcan otras normas especiales y/o particulares; y, que la administración integral de riesgos es parte de la estrategia institucional y del proceso de toma de decisiones;

Que el artículo 18 del citado capítulo I "De la gestión integral y control de riesgos", dispone que el Superintendente de Bancos y Seguros deberá disponer la adopción de medidas adicionales a las previstas en el referido capítulo o en otras normas con el propósito de atenuar la exposición a los riesgos que enfrentan las instituciones del sistema financiero; y, que dichas medidas podrán ser de carácter general para el sistema financiero en su conjunto; o, particular, para una institución determinada;

Que es un compromiso de la Superintendencia de Bancos y Seguros, en su calidad de organismo técnico de vigilancia, auditoría, intervención y control, determinar un mecanismo efectivo que permita precautelar la seguridad financiera de los usuarios del sistema financiero;

Que en el capítulo I "Apertura y cierre de oficinas en el país y en el exterior, de las instituciones financieras privadas y públicas sometidas al control de la Superintendencia de Bancos y Seguros", del título II "De la organización de las instituciones del sistema financiero", del referido libro I "Normas generales para la aplicación de la Ley General de Instituciones del Sistema Financiero", se establecen las medidas de seguridad que deben implementar las instituciones financieras públicas y privadas;

Que es necesario reformar dicha norma, con la finalidad de que las instituciones del sistema financiero nacional, contraten coberturas relacionadas con fraudes informáticos dentro de los servicios financieros ofertados mediante canales electrónicos; y,

En ejercicio de la atribución legal que le otorga la letra b) del artículo 175 de la Ley General de Instituciones del Sistema Financiero,

RESUELVE:

En el 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, efectuar el siguiente cambio:

ARTÍCULO ÚNICO.- En el capítulo I "Apertura y cierre de oficinas en el país y en el exterior, de las instituciones financieras privadas y públicas sometidas al control de la Superintendencia de Bancos y Seguros", del título II "De la organización de las instituciones del sistema financiero privado", efectuar las siguientes reformas:

1. Incluir como artículo 41, el siguiente y renumerar los restantes:

   "**ARTÍCULO 41.-** Las instituciones financieras contratarán anualmente con las compañías de seguro privado, coberturas que aseguren a la entidad contra fraudes generados a través de su tecnología de la información, sistemas telemáticos, electrónicos o similares, como mínimo ante los siguientes riesgos:

   41.1 Alteraciones de bases de datos;

   41.2 Accesos a los sistemas informáticos y de información de forma ilícita;

   41.3 Falsedad informática;

   41.4 Estafa informática;

   41.5 Daño informático; y,

   41.6 Destrucción a la infraestructura a las instalaciones físicas necesarias para la transmisión, recepción o procesamiento de información."

2. Insertar como disposición transitoria primera la siguiente, y numerar como segunda la disposición transitoria existente:

   "**PRIMERA.-** Hasta el 30 de junio del 2012, las instituciones financieras contratarán las coberturas previstas en el artículo 41 del presente capítulo."

COMUNÍQUESE Y PUBLÍQUESE EN EL REGISTRO OFICIAL.- Dada en la Superintendencia de Bancos y Seguros, en Quito, Distrito Metropolitano, el diecisiete de enero del dos mil doce.

Ab. Pedro Solines Chacón
PRESIDENTE DE LA JUNTA BANCARIA

LO CERTIFICO.- Quito, Distrito Metropolitano, el diecisiete de enero del dos mil doce.

Lcdo. Pablo Cobo Luna
SECRETARIO DE LA JUNTA BANCARIA, (E)

Resolución JB-2012-2148 Junta Bancaria del Ecuador, 2013

Junta Bancaria del Ecuador

RESOLUCIÓN JB-2012-2148

LA JUNTA BANCARIA

CONSIDERANDO:

Que en el título II "De la organización de las instituciones del sistema financiero privado", del 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, consta el capítulo I "Apertura y cierre de oficinas en el país y en el exterior de las instituciones financieras privadas y públicas sometidas al control de la Superintendencia de Bancos y Seguros";

Que en el título X "De la gestión integral y control de riesgos", del citado libro I, consta el capítulo V "De la gestión del riesgo operativo";

Que la Superintendencia de Bancos y Seguros debe propender a que las instituciones del sistema financiero cuenten con fuertes medidas de seguridad en la tecnología de información y comunicaciones a fin de que los elementos tecnológicos utilizados para entregar sus productos y/o servicios sean seguros y confiables;

Que las instituciones del sistema financiero deben contar con los controles necesarios para proteger los intereses del público, de acuerdo con lo señalado en el artículo 1 de la Ley General de Instituciones del Sistema Financiero;

Que entre los eventos de riesgo operativo que enfrentan las instituciones supervisadas en el desarrollo de sus actividades, se encuentran el "fraude interno" y el "fraude externo", los cuales podrían ocasionarse a través del uso inseguro de la tecnología de información y comunicaciones;

Que es de vital importancia que las instituciones del sistema financiero implementen suficientes medidas de seguridad para mitigar el riesgo de fraude por el uso de la tecnología de información y comunicaciones, como elemento fundamental de una administración preventiva que reduzca la posibilidad de pérdidas e incremente su eficiencia, siendo parte de una adecuada gestión de riesgos;

Que el Comité de Supervisión Bancaria de Basilea ha definido y recomienda principios para la administración del riesgo de operación, a fin de que sean aplicados por las instituciones financieras y también consideradas por los supervisores al evaluar la gestión realizada por las entidades controladas;

Que el control por parte del supervisor no consiste únicamente en garantizar que las instituciones controladas posean el capital necesario para cubrir los riesgos de sus actividades, sino también en alentarlas a que desarrollen y utilicen mejores técnicas de gestión de sus riesgos que les permitan ser más eficientes y competitivas en un entorno de globalización;

Que por tales motivos es necesario reformar dichas normas, con el propósito de establecer medidas de seguridad en la tecnología de información y comunicaciones; y,

En ejercicio de la atribución legal que le otorga la letra b) del artículo 175 de la Ley General de Instituciones del Sistema Financiero,

RESUELVE:

En el 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, efectuar los siguientes cambios:

ARTÍCULO 1.- En el capítulo I "Apertura y cierre de oficinas en el país y en el exterior, de las instituciones financieras privadas y públicas sometidas al control de la Superintendencia de Bancos y Seguros", del título II "De la organización de las instituciones del sistema financiero privado", efectuar las siguientes reformas:

1. En el artículo 39, efectuar las siguientes reformas:

   1.1 Sustituir el numeral 39.2, por el siguiente:

   "39.2 Protección contra clonación de tarjetas.- Contar con dispositivos electrónicos y/o elementos físicos que impidan y detecten de manera efectiva la colocación de falsas lectoras de tarjetas, con el fin de evitar la clonación de tarjetas de débito o de crédito, además de los correspondientes mecanismos de monitoreo en línea de las alarmas que generen los dispositivos electrónicos en caso de suscitarse eventos inusuales;"

   1.2 Sustituir el numeral 39.6, por el siguiente:

   "39.6 Protección al software e información del cajero automático.- Disponer de un programa o sistema de protección contra intrusos (Anti-malware) que permita proteger el software instalado en el cajero automático y que detecte oportunamente cualquier alteración en su código, configuración y/o funcionalidad. Así mismo, se deberá instalar mecanismos que sean capaces de identificar conexiones no autorizadas a través de los puertos USB, comunicaciones remotas, cambio de los discos duros y otros componentes que guarden o procesen información. En una situación de riesgo deben emitir alarmas a un centro de monitoreo o dejar inactivo al cajero automático hasta que se realice la inspección por parte del personal especializado de la institución;"

   1.3 A continuación del numeral 39.6, incluir los siguientes y renumerar los restantes:

   "39.7 Procedimientos para el mantenimiento preventivo y correctivo en los cajeros automáticos.- Disponer de procedimientos auditables debidamente acordados y coordinados entre la institución y los proveedores internos o externos para la ejecución de las tareas de mantenimiento preventivo y correctivo del hardware y software, provisión de suministros y recarga de dinero en las gavetas. Las claves de acceso tipo "administrador" del sistema del cajero automático deben ser únicas y reemplazadas periódicamente;

   39.8 Accesos físicos al interior de los cajeros automáticos.- Disponer de cerraduras de alta tecnología y seguridades que garanticen el

acceso controlado al interior del cajero automático por parte del personal técnico o de mantenimiento que disponga de las respectivas llaves. Estas cerraduras deben operar con llaves únicas y no genéricas o maestras;

39.9 Reportes de nivel de seguridad de los cajeros- Comunicar oportunamente la información sobre los estándares de seguridad implementados en los cajeros automáticos, incidentes de seguridad (vandalismo y/o fraudes) identificados en sus cajeros automáticos y/o ambientes de software o hardware relacionados;"

2. Incluir como tercera disposición transitoria, la siguiente:

"TERCERA.- Las instituciones financieras informarán a la Superintendencia de Bancos y Seguros, en el plazo de treinta (30) días, a partir de la publicación en el Registro Oficial de la presente reforma, sobre el nivel de cumplimiento de las disposiciones de seguridades mencionada en el artículo 39, de este capítulo.

El Superintendente de Bancos y Seguros determinará, de ser el caso, los cronogramas de adecuación, para la implementación de las medidas de seguridad señaladas en el citado artículo, cuyo plazo no excederá de nueve (9) meses, debiendo remitir trimestralmente un informe de avance de la implementación."

ARTÍCULO 2.- En el capítulo V "De la gestión del riesgo operativo", del título X "De la gestión integral y control de riesgos", efectuar las siguientes reformas:

1. En el artículo 2, efectuar los siguientes cambios:

1.1 En el numeral 2.12, sustituir la frase "... y toma de decisiones" por "... , toma de decisiones, ejecución de una transacción o entrega de un servicio;"

1.2 En el numeral 2.34, eliminar la letra "... , y ...", incluir los siguientes numerales y renumerar el restante:

"2.35 Calidad de la información.- Es el resultado de la aplicación de los mecanismos implantados que garantizan la efectividad, eficiencia y confiabilidad de la información y los recursos relacionados con ella;

2.36 Efectividad.- Es la garantía de que la información es relevante y pertinente y que su entrega es oportuna, correcta y consistente;

2.37 Confiabilidad.- Es la garantía de que la información es la apropiada para la administración de la entidad, ejecución de transacciones y para el cumplimiento de sus obligaciones;

2.38 Banca electrónica.- Son los servicios suministrados por las instituciones del sistema financiero a los clientes a través de internet en el sitio que corresponda a uno o más dominios de la institución, indistintamente del dispositivo tecnológico a través del cual se acceda;

2.39 Banca móvil.- Son los servicios suministrados por las instituciones del sistema financiero a los clientes a través de equipos celulares mediante los protocolos propios de este tipo de dispositivos;

2.40 Tarjetas.- Para efectos del presente capítulo, se refiere a las tarjetas de débito, de cajero automático y tarjetas de crédito;

2.41 Canales electrónicos.- Se refiere a todas las vías o formas a través de las cuales los clientes o usuarios pueden efectuar transacciones con las instituciones del sistema financiero, mediante el uso de elementos o dispositivos electrónicos o tecnológicos, utilizando o no tarjetas. Principalmente son canales electrónicos: los cajeros automáticos (ATM), dispositivos de puntos de venta (POS y PIN Pad), sistemas de audio respuesta (IVR), señal telefónica, celular e internet u otro similares;

2.42 Tarjeta inteligente.- Tarjeta que posee circuitos integrados (chip) que permiten la ejecución de cierta lógica programada, contiene memoria y microprocesadores y es capaz de proveer seguridad, principalmente en cuanto a la confidencialidad de la información de la memoria; y."

2. En el numeral 4.3.7. sustituir el punto por punto y coma, e incluir los siguientes numerales:

4.3.8 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 así como los bienes de los clientes a cargo de las instituciones controladas, éstas deberán cumplir como mínimo con lo siguiente:

4.3.8.1 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;

4.3.8.2 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;

4.3.8.3 El envío de información confidencial de sus clientes y la relacionada con 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 estar sometida a técnicas de encriptación acordes con los estándares internacionales vigentes;

4.3.8.4 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;

4.3.8.5 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;

4.3.8.6 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;

4.3.8.7 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;

4.3.8.8 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.

Entre las principales condiciones de personalización por cada tipo de canal electrónico, deberán estar: registro de las cuentas a las cuales desea realizar transferencias, registro de direcciones IP de computadores autorizados, el ó los números de telefonía móvil autorizados, montos máximos por transacción diaria, semanal y mensual, entre otros.

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;

4.3.8.9 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 cajeros automáticos; dicha clave deberá ser diferente de aquella por la cual se accede a otros canales electrónicos;

4.3.8.10 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;

4.3.8.11 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;

4.3.8.12 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;

4.3.8.13 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;

4.3.8.14 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;

4.3.8.15 Mantener como mínimo durante doce (12) meses el registro histórico de todas las operaciones 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 operaciones de banca electrónica mediante dispositivos móviles: el número de teléfono con el que se hizo la conexión. En caso de presentarse reclamos, la información deberá conservarse hasta que se agoten las instancias legales. Si dicha información constituye respaldo contable se aplicará lo previsto en el tercer inciso del artículo 80 de la Ley General de Instituciones del Sistema Financiero;

4.3.8.16 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;

4.3.8.17 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;

4.3.8.18 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;

4.3.8.19 Las entidades deberán implementar los controles necesarios para que la información de claves ingresadas por los clientes mediante los centros de atención telefónica (call center), estén sometidas a técnicas de encriptación acordes con los estándares internacionales vigentes;

4.3.8.20 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;

4.3.8.21 Las tarjetas emitidas por las instituciones del sistema financiero que las ofrezcan deben ser tarjetas inteligentes, es decir, deben contar con microprocesador o chip; y, las entidades controladas deberán adoptar los estándares internacionales de seguridad y las mejores prácticas vigentes sobre su uso y manejo;

4.3.8.22 Mantener permanentemente informados y capacitar a los clientes sobre los riesgos derivados del uso de canales electrónicos y de tarjetas; y, sobre las medidas de seguridad que se deben tener en cuenta al momento de efectuar transacciones a través de éstos;

4.3.8.23 Informar y capacitar permanentemente a los clientes sobre los procedimientos para el bloqueo, inactivación, reactivación y cancelación de los productos y servicios ofrecidos por la entidad;

4.3.8.24 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;

4.3.8.25 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;

4.3.9 Cajeros automáticos.- Con el objeto de garantizar la seguridad en las transacciones realizadas a través de los cajeros automáticos, las instituciones del sistema financiero deberán cumplir como mínimo con lo siguiente:

4.3.9.1 Los dispositivos utilizados en los cajeros automáticos para la autenticación del cliente o usuario, deben encriptar la información ingresada a través de ellos; y, la información de las claves no debe ser almacenada en ningún momento;

4.3.9.2 La institución controlada debe implementar mecanismos internos de autenticación del cajero automático que permitan asegurar que es un dispositivo autorizado por la institución del sistema financiero a la que pertenece;

4.3.9.3 Los cajeros automáticos deben ser capaces de procesar la información de tarjetas inteligentes o con chip;

4.3.9.4 Los cajeros automáticos deben estar instalados de acuerdo con las especificaciones del fabricante, así como con los estándares de seguridad definidos en las políticas de la institución del sistema financiero, incluyendo el cambio de las contraseñas de sistemas y otros parámetros de seguridad provistos por los proveedores;

4.3.9.5 Disponer de un programa o sistema de protección contra intrusos (Anti-malware) que permita proteger el software instalado en el cajero automático y que detecte oportunamente cualquier alteración en su código, configuración y/o funcionalidad. Así mismo, se deberán instalar mecanismos que sean capaces de identificar conexiones no autorizadas a través de los puertos USB, comunicaciones remotas, cambio de los discos duros y otros componentes que guarden o procesen información. En una situación de riesgo deben emitir alarmas a un centro de monitoreo o dejar inactivo al cajero automático hasta que se realice la inspección por parte del personal especializado de la institución;

4.3.9.6 Establecer y ejecutar procedimientos de auditoría de seguridad en sus cajeros automáticos por lo menos una vez al año, con el fin de identificar vulnerabilidades y mitigar los riesgos que podrían afectar

a la seguridad de los servicios que se brindan a través de estos. Los procedimientos de auditoría deberán ser ejecutados por personal capacitado y con experiencia; y,

4.3.9.7 Para la ejecución de transacciones de clientes, se deberán implementar mecanismos de autenticación que contemplen por lo menos dos de tres factores: "algo que se sabe, algo que se tiene, o algo que se es";

4.3.10 Puntos de venta (POS y PIN Pad).- Con el objeto de garantizar la seguridad en las transacciones realizadas a través de los dispositivos de puntos de venta, las instituciones del sistema financiero deberán cumplir como mínimo con lo siguiente:

4.3.10.1 Establecer procedimientos que exijan que los técnicos que efectúan la instalación, mantenimiento o desinstalación de los puntos de venta (POS y PIN Pad) en los establecimientos comerciales confirmen su identidad a fin de asegurar que este personal cuenta con la debida autorización;

4.3.10.2 A fin de permitir que los establecimientos comerciales procesen en presencia del cliente o usuario las transacciones efectuadas a través de los dispositivos de puntos de venta (POS o PIN Pad), éstos deben permitir establecer sus comunicaciones de forma inalámbrica segura; y,

4.3.10.3 Los dispositivos de puntos de venta (POS o PIN Pad) deben ser capaces de procesar la información de tarjetas inteligentes o con chip;

4.3.11 Banca electrónica.- Con el objeto de garantizar la seguridad en las transacciones realizadas mediante la banca electrónica, las instituciones del sistema financiero que ofrezcan servicios por medio de este canal electrónico deberán cumplir como mínimo con lo siguiente:

4.3.11.1 Implementar los algoritmos y protocolos seguros, así como certificados digitales, que ofrezcan las máximas seguridades en vigor dentro de las páginas web de las entidades controladas, a fin de garantizar una comunicación segura, la cual debe incluir el uso de técnicas de encriptación de los datos transmitidos acordes con los estándares internacionales vigentes;

4.3.11.2 Realizar como mínimo una vez (1) al año una prueba de vulnerabilidad y penetración a los equipos, dispositivos y medios de comunicación utilizados en la ejecución de transacciones por banca electrónica; y, en caso de que se realicen cambios en la plataforma que podrían afectar a la seguridad de este canal, se deberá efectuar una prueba adicional.

Las pruebas de vulnerabilidad y penetración deberán ser efectuadas por personal independiente a la entidad, de comprobada competencia y aplicando estándares vigentes y

reconocidos a nivel internacional. Las instituciones deberán definir y ejecutar planes de acción sobre las vulnerabilidades detectadas;

4.3.11.3 Los informes de las pruebas de vulnerabilidad deberán estar a disposición de la Superintendencia de Bancos y Seguros, incluyendo un análisis comparativo del informe actual respecto del inmediatamente anterior;

4.3.11.4 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;

4.3.11.5 Implementar mecanismos de seguridad incluyendo dispositivos tales como IDS, IPS, firewalls, entre otros, que reduzcan la posibilidad de que la información de las transacciones de los clientes sea capturada por terceros no autorizados durante la sesión;

4.3.11.6 Establecer un tiempo máximo de inactividad, después del cual deberá ser cancelada la sesión y exigir un nuevo proceso de autenticación al cliente para realizar otras transacciones;

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

4.3.11.8 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);

4.3.11.9 La institución del sistema financiero debe implementar mecanismos de autenticación al inicio de sesión de los clientes, en donde el nombre de usuario debe ser distinto al número de cédula de identidad y éste así como su clave de acceso deben combinar caracteres numéricos y alfanuméricos con una longitud mínima de seis (6) caracteres;

4.3.11.10 Para la ejecución de transacciones de clientes, se deberán implementar mecanismos de autenticación que contemplen por lo menos dos de tres factores: "algo que se sabe, algo que se tiene, o algo que se es", considerando que uno de ellos debe: ser dinámico por cada vez que se efectúa una operación, ser una clave de una sola vez OTP (one time password), tener controles biométricos, entre otros;

4.3.11.11 En todo momento en donde se solicite el ingreso de una clave numérica, los sitios web de las entidades deben exigir el ingreso de éstas a través de teclados virtuales, las mismas que deberán estar enmascaradas;

4.3.12 Banca móvil.- Las instituciones del sistema financiero que presten servicios a través de banca móvil deberán sujetarse en lo que corresponda a las medidas de seguridad dispuestas en los subnumerales 4.3.8. y 4.3.11;

4.3.13 Sistemas de audio respuestas (IVR).- Las instituciones del sistema financiero que presten servicios a través de IVR deberán sujetarse en lo que corresponda a las medidas de seguridad dispuestas en los subnumerales 4.3.8. y 4.3.11; y,

4.3.14 Corresponsales no bancarios.- Las instituciones financieras controladas que presten servicios a través de corresponsales no bancarios deberán sujetarse en lo que corresponda a las medidas de seguridad dispuestas en los subnumerales 4.3.8, 4.3.10 y 4.3.11."

3. Sustituir la primera disposición transitoria, por la siguiente:

"**PRIMERA.-** Las disposiciones de esta norma deberá cumplirse en los siguientes plazos:

1. Nueve (9) meses para los numerales: 4.3.8.4, 4.3.8.5, 4.3.8.7, 4.3.8.8, 4.3.8.9, 4.3.8.11, 4.3.8.12, 4.3.8.13, 4.3.8.14, 4.3.8.15, 4.3.8.16, 4.3.8.17, 4.3.8.18, 4.3.8.19, 4.3.8.20, 4.3.8.22, 4.3.8.23, 4.3.8.24, 4.3.9.2, 4.3.9.4, 4.3.9.6, 4.3.10.1, 4.3.11.1, 4.3.11.2, 4.3.11.3, 4.3.11.4, 4.3.11.5, 4.3.11.6, 4.3.11.7, 4.3.11.8, 4.3.11.9 y 4.3.11.11;

2. Dieciocho (18) meses para los numerales: 4.3.8.1, 4.3.8.2, 4.3.8.3, 4.3.8.6, 4.3.8.10, 4.3.8.25, 4.3.9.1, 4.3.9.5 y 4.3.11.10;

3. Para los numerales 4.3.12, 4.3.13 y 4.3.14 los plazos serán los estipulados para cada subnumeral a los que se hace referencia; y,

4. Para los numerales 4.3.8.21, 4.3.9.3, 4.3.10.2, 4.3.10.3, deberán sujetarse al siguiente cronograma:

FASE	DESCRIPCIÓN	TIEMPO (meses)
0	DIAGNÓSTICO INICIAL DE LA ENTIDAD PARA IMPLEMENTAR TARJETAS INTELIGENTES	6
1	IMPLEMENTAR ADECUACIONES PARA OPERAR CON TARJETAS INTELIGENTES, EN:	12
	CAJEROS AUTOMATICOS	
	ADQUIRENCIAS	
	TARJETAS DE DÉBITO	
	TARJETAS DE CRÉDITO	
2	ENTREGA DE TARJETAS INTELIGENTES	18
	PLAZO FINAL	**36**

Las instituciones controladas deben presentar a la Superintendencia de Bancos y Seguros, en un plazo de noventa (90) días contados a partir de la fecha en la que se publiquen en el Registro Oficial, las disposiciones incorporadas en el referido artículo 4, el cronograma de las acciones a tomar por la entidad para cumplir con los subnumerales 4.3.8 hasta el 4.3.14 de acuerdo con el formato establecido que se hará conocer a través de circular; dicho cronograma deberá estar sustentado en un diagnóstico de brechas y en un portafolio de proyectos para su cumplimiento. Todos estos documentos deberán estar debidamente aprobados por el directorio u organismo que haga sus veces.

Con el objeto de que la Superintendencia de Bancos y Seguros mantenga un oportuno conocimiento sobre el avance de la implementación de las disposiciones contenidas en el artículo 4 de este capítulo, las instituciones controladas deberán remitir a la Superintendencia de Bancos y Seguros, cada 90 días, contados a partir del envío inicial del cronograma de implementación, el reporte de avance de la implementación de las presentes disposiciones normativas, cuidando de no exceder el plazo máximo establecido para su cumplimiento."

COMUNÍQUESE Y PUBLÍQUESE EN EL REGISTRO OFICIAL.- Dada en la Superintendencia de Bancos y Seguros, en Quito, Distrito Metropolitano, el veintiséis de abril del dos mil doce.

Ab. Pedro Solines Chacón
PRESIDENTE DE LA JUNTA BANCARIA

LO CERTIFICO.- Quito, Distrito Metropolitano, el veintiséis de abril del dos mil doce.

Lcdo. Pablo Cobo Luna
SECRETARIO DE LA JUNTA BANCARIA

2.16. Tratados internacionales

Dentro de estos tratados tenemos el Convenio de Budapest sobre la ciberdelincuencia, siendo un convenio para la ayuda en contra de todos delitos informáticos en vista del avance que se tiene con estos delitos, pero Ecuador es uno de los países que no se adherido al acuerdo lo que nos implica una gran limitación contra estos delitos.

2.16.1. Convenio de Budapest

Este convenio fue uno de los primeros tratados a realizarse para combatir los delitos informáticos, siendo elaborado por el consejo de Europa abrió a firma en Budapest el 8 de noviembre del 2001 y entrando en vigencia el 1 de julio del 2004 este tratado que fue creado para que varios países se unan a él con una sola finalidad siendo que a partir del 2010 el 28 de octubre 30 estados abrían firmado, ratificado y adherido al convenio; 16 solo firmaron el convenio más no se ratificaron al 2018 han sido 61 estados que se han ratificado dentro de América Latina solo cuenta con 6 países miembro (Chile, Paraguay, Panamá, República Dominicana, Argentina, Costa Rica), otros 3 lo han ratificado pero no formalizado el ingreso(México, Colombio, Perú)

Este convenio cuenta con tres ejes importantes para tratar los delitos informáticos, el primero aborda de estos delitos un objetivo de cómo establecer un catálogo de figuras dedicadas a penar las modalidades de criminalidad informática teniendo una clasificación en 4 categorías que son:

- Tecnología como fin: Que se le da a la misma, tiene múltiples como fines médicos, financieros, educativos, deportivos, etc. En este caso en concreto el fin de la tecnología es defraudar o delinquir.
- Tecnología como medio: usar la tecnología como medio para defraudar, ya sea ordenadores, teléfonos inteligentes, la red.
- Contenido: el resultado final de lo que se logró con el medio, ya sea como resultado la publicidad de pornografía, retirar fondos de cuentas de ahorro o corrientes, compras en la web mediante el uso de tarjetas de crédito del afectado.
- Infracciones a la propiedad intelectual: divulgar el contenido que está protegido por la propiedad intelectual, difundir canciones, películas, artículos, formulas patentadas, etc. (Pastorino 2017).

Ecuador no se ha suscrito desde el 2001 al Convenio de Budapest y los Ciberdelitos transnacionales se investigan a través de asistencias penales. Siendo esto de mayor preocupación al ser un país que no cuente con una ley específica paras luchar contra los Ciberdelitos por lo cual es de gran importancia que Ecuador deba ratificarse al convenio permitiendo así el cruce de información y penar así la criminalidad informática entres los países miembros del convenio.

Como un fin para la adhesión a este convenio seria la homologación de la legislación y el intercambio de información en materia de delitos informáticos para procedimientos y seguir luchando contra el Cibercrimen.

CAPÍTULO III
METODOLOGÍA DE LA INVESTIGACIÓN

3.1. Metodología

Los aspectos metodológicos de la investigación permiten validar los resultados obtenidos durante el desarrollo del estudio de acuerdo a los objetivos y las fuentes empleadas. Por esa razón es importante que en este capítulo se precisen las cuestiones principales relacionadas con el tipo de investigación realizada, el enfoque utilizado, las técnicas e instrumentos de recolección y sistematización de la información y el análisis de los principales resultados obtenidos.

3.2. Tipo de investigación

En los estudios de metodología de investigación se hace referencia dos tipos básicos de investigación; por un lado estaría la investigación experimental, y por otra la investigación no experimental. La diferencia es que en el primer tipo el investigador manipula las variables ya sea en un laboratorio o en un estudio de campo, mientras en el segundo tipo observa las variables tal como aparecen en sus circunstancias ordinarias o su estado natural.

La opción de realizar uno u otro tipo de investigación no es subjetiva por parte del investigador, sino que responde a criterios como el planteamiento del problema, los objetivos, el alcance que espera darle a su investigación y la hipótesis o idea a defender.

En el presente estudio se realiza una investigación del segundo tipo, es decir no experimental, la cual es un tipo de investigación que se realiza “sin la manipulación deliberada de variables y en los que solo se observan los fenómenos en su ambiente natural para después analizarlos...lo que se hace es observar fenómenos tal como se dan en su contexto natural, para posteriormente analizarlos (Hernández Sampieri, 2010, pág. 149).

Bajo esas consideraciones, y de acuerdo al problema, objetivos y alcance de la presente investigación, el objeto de estudio es analizado tal como se manifiesta en la práctica, pues no se interviene de ninguna manera en las formas o modalidades que se comenten los delitos informáticos, ni en las acciones o actitudes de los sujetos que lo realizan.

En el plano de la dogmática jurídica, el objeto de estudio que son los delitos informáticos en la modalidad de tarjeta de crédito, tal como están regulados en el artículo 190 COIP, son analizados tal como están tipificado en dicha norma y a partir de los elementos objetivos y subjetivos necesarios para su configuración por las acciones que han de realizar el sujeto activo para que se le pueda imputar responsabilidad penal.

3.3. Enfoque

En cuanto al enfoque de la investigación ha de significarse que en las obras de metodología de la investigación se habla de los enfoques cuantitativo y cualitativo, así como de un enfoque mixto resultante la combinación de los dos anteriores en diversas proporciones. Los dos enfoques básicos, así como la combinación de ellos, sirven de igual manera para obtener conocimiento científico confiable y verificable, así como para resolver problemas teóricos o prácticos a partir de los resultados obtenidos.

Las diferencias entre uno y otro enfoque no radican necesariamente en los objetivos de la investigación, sino en los datos que utiliza para resolver el problema y los métodos que emplea. Así, la investigación con enfoque cuantitativo recopila los datos relevantes y los utiliza en función de probar o rechazar una hipótesis a partir del análisis estadístico que permite establecer patrones de conducta de las personas o de comportamiento de objetos o procesos para elaborar teorías científicas.

Por el contrario, el enfoque cualitativo de la investigación tiene como objeto la descripción de las cualidades de un proceso o fenómeno con relación a parámetros previamente fijados para valorar su correspondencia, y de ser el caso proponer su reforma para que exista adecuación entre lo que es empíricamente hablando, y lo que debería ser en términos valorativos. Como afirma H. Sampieri “la investigación cualitativa se enfoca a comprender y profundizar los fenómenos, explorándolos desde la perspectiva de los participantes en un ambiente natural y en relación con el contexto” (2010, pág. 364).

De lo dicho se desprende que la presente es una investigación con enfoque cualitativo, donde se tiene como propósito evaluar la calidad de las normas del COIP que tipifican los delitos informático y particularmente el previsto en su artículo 190 con relación a la tarjeta de crédito, para identificar las posibles falencias que existen en la investigación de delitos informáticos en el Ecuador relacionadas con dicho medio de pago.

3.4. Técnica e instrumentos

Aunque se trata de una investigación cualitativa y no experimental, basada fundamentalmente en el estudio de fuentes documentales, los objetivos no se podrían cumplir adecuadamente sino se indaga la opinión de expertos en el tema, especialmente de abogados litigantes en materia de delitos informáticos, quienes a través de su experiencia pueden aportar elementos de juicio para fundamentar las conclusiones y verificar la viabilidad de la propuesta de la investigación.

Por esa razón como técnica de investigación se aplicará la encuesta de trabajo de campo a una muestra de abogados litigantes inscritos en el Colegio de Abogados del Guayas y en Foro de Abogados del Consejo de la Judicatura (Consejo de a Judicatura, 2020), a quienes se contactará por vía telefónica o telemática.

La investigación aplico una encuesta diseñada en función del problema de investigación, los objetivos y la información con relación a la cual se requiere el componente empírico.

Las preguntas de la encuesta apuntan básicamente a tres cuestiones distintas: experiencia profesional del experto consultado, su opinión sobre la regulación jurídica de los delitos informáticos en el COIP, particularmente los relacionados con las tarjetas de crédito, y las reformas que a su juicio debería realizarse en dicho cuerpo legal.

3.5. Población

De conformidad con lo dicho, la población considerada relevante para aplicar el instrumento de investigación estaría constituida por 17.258 profesionales del Derecho, cifra que arroja el último censo realizado por el Colegio de Abogados del Guayas para las elecciones que estaban previstas inicialmente para el 3 día de febrero del presente año, prorrogadas para el 20 de marzo y suspendidas entonces al causa de la pandemia del Covid-91.

Se trata de un universo maestral considerablemente amplio, por lo cual la encuesta solamente se aplicó a una muestra de los inscritos en el Colegio de Abogados del Guayas, la cual se seleccionó en un proceso de dos etapas: la primera a partir de la materia en que ejercen su profesión los abogados contactados inicialmente, que es el Derecho penal; y la segunda selección con base en su experiencia en delitos informáticos.

3.6. Muestra

La muestra siendo una de las características más relevantes dentro del marco metodológico, siendo la estimación la cantidad de la población objeto del estudio.

En la presente investigación se tomó como muestra a Abogados registrados en el colegio de Abogados y para obtener el tamaño de la muestra se tomó en consideración la siguiente fórmula:

$$n = \frac{N\sigma^2 Z^2}{(N-1)e^2 + \sigma^2 Z^2}$$

DESCRIPCIÓN DE VARIABLES EN LA APLICACIÓN DE LA FÓRMULA:

n = el tamaño de la muestra.

N = tamaño de la población 17.258.

$\boldsymbol{\sigma}$ **2** = Desviación estándar de la población que, generalmente cuando no se tiene su valor, suele utilizarse un valor constante de 0,5.

$\boldsymbol{Z}$ **2** = Valor obtenido mediante niveles de confianza 95% de confianza equivale a 1,96 (como más usual) o en relación al 99% de confianza equivale 2,58

$\boldsymbol{e}$ **2** = Límite aceptable de error muestral que, 5% $(0,05)^2$

$$n = \frac{N\sigma^2 Z^2}{e^2(N-1) + \sigma^2 Z^2}$$

$$n = \frac{17.258 \cdot 0,5^2 \cdot 1,96^2}{0,05^2(17.258-1) + 0,5^2 \cdot 1,96^2}$$

$$n = \frac{17.258 \cdot 0,5^2 \cdot 1,96^2}{0,05^2(17.258-1) + 0,5^2 \cdot 1,96^2} = 376$$

CAPÍTULO IV
INFORME FINAL
ANÁLISIS DE RESULTADOS

4.1. Análisis de los resultados de la encuesta

Pregunta No. 1.

¿Cuánto tiempo lleva vinculado al ejercicio de la profesión en materia de Derecho penal y delitos informáticos?

TABLA 1.

Descripción	Frecuencia	Porcentaje
Más de 8 años	113	30%
Entre 5 y 8 años	226	60%
Menos de 5 años	37	10%
Total	376	100%

Elaborado por: Rodríguez,O (2020)

GRÁFICO 1

Fuente: Abogados inscritos al Colegio de Abogados del Guayas
Elaborado por: Rodríguez,O (2020)

Interpretación y análisis de datos No.1: esta pregunta mide los años de experiencia de los encuestados en el ejercicio de la profesión relacionada con delitos informáticos en general; como puede apreciarse en los datos, el 60% de ellos tiene entre cinco y ocho años de experiencia, y el 30% más de ocho, lo que permite afirmar que la muestra cuenta con experiencia suficiente para que sus respuestas tengan un sólido fundamento práctico.

Pregunta No. 2

¿Ha participado como profesional en el juzgamiento de algún delito relacionado con el fraude de tarjeta de crédito?

TABLA 2.

Descripción	Frecuencia	Porcentaje
Sí	301	80%
No	75	20%
Total	376	100%

Elaborado por: Rodríguez,O (2020)

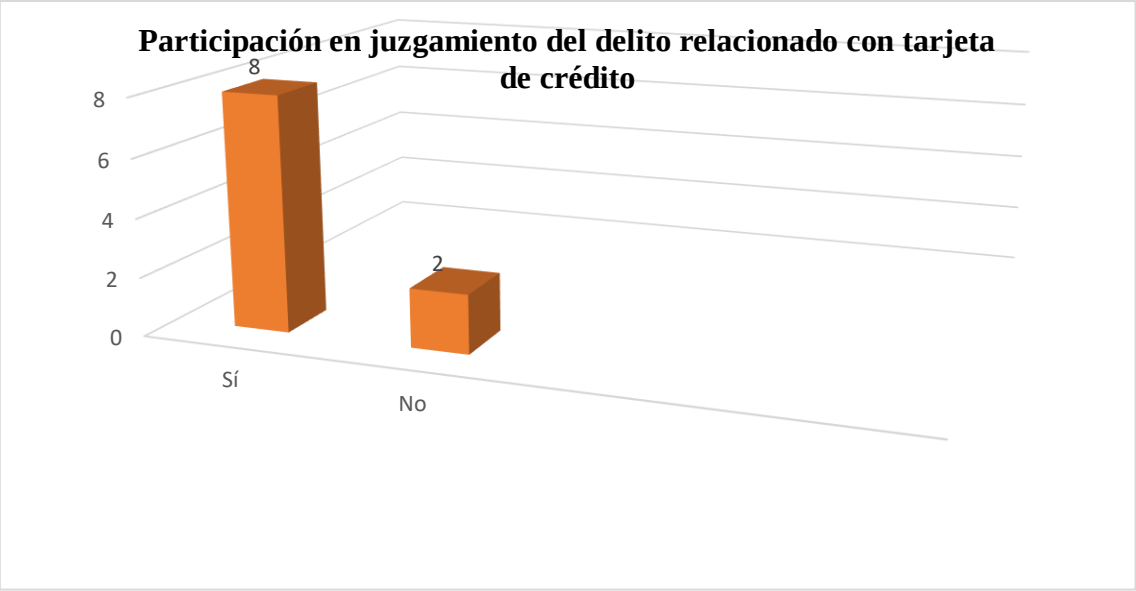

GRÁFICO 2

Fuente: Abogados inscritos al Colegio de Abogados del Guayas
Elaborado por: Rodríguez,O (2020)

Interpretación y análisis de datos No.02: los delitos informáticos se pueden cometer por acción u omisión a través de diferentes formas y bajo diversas modalidades, por eso

se consideró oportuno preguntar a los encuestados si habían participado como profesionales en el juzgamiento de delitos informáticos en la modalidad de fraude con tarjeta de crédito, a lo que el 80% respondió afirmativamente.

Además de los años de experiencia en los delitos informáticos analizada en a la pregunta anterior, el haber participado profesionalmente en el juzgamiento de delitos en la modalidad de fraude con tarjeta de crédito confiere a las respuestas de los encuestados un considerable valor para corroborar los resultados del estudio doctrinal y legal.

Pregunta No. 3

¿Considera que el estudio de los delitos informáticos a nivel internacional es importante para prevenirlo en el Ecuador?

TABLA 3.

Descripción	Frecuencia	Porcentaje
Sí	263	70%
No	113	30%
Total	376	100%

Elaborado por: Rodríguez,O (2020)

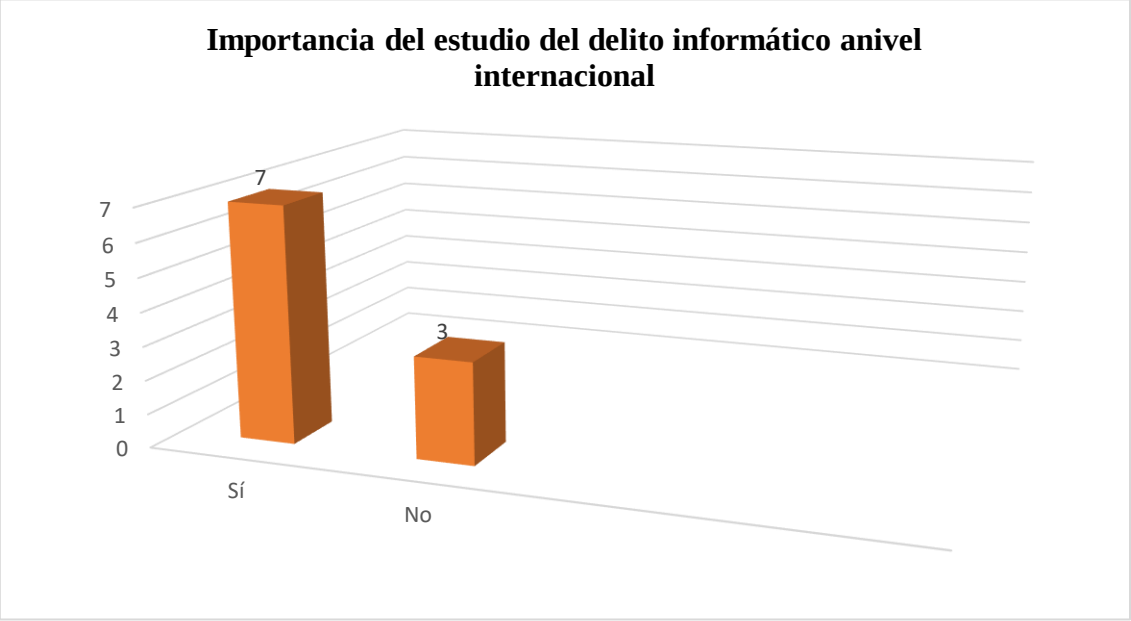

GRÁFICO 3

Fuente: Abogados inscritos al Colegio de Abogados del Guayas
Elaborado por: Rodríguez,O (2020)

Interpretación y análisis de datos No3.: conocer la experiencia acumulada en otros países es fundamental para enfrentar adecuadamente el delito informático en el Ecuador, pues éste constituye un fenómeno creciente en los últimos tiempos, vinculado de manera particular a la globalización, el tráfico de bienes y las formas de pago por vía informática.

Esa hipótesis fue corroborada por los encuestados que en un 70% consideraron que ese estudio es necesario para la adecuada formulación de políticas públicas de seguridad informática, la adecuación de los tipos delictivos al Derecho comparado y la persecución penal y sanción de los responsables.

Pregunta No. 4.

Con relación a los delitos informáticos considera que su incidencia es:

TABLA 4.

Descripción	Frecuencia	Porcentaje
Irrelevante	38	10%
Media	113	30%
Alta	75	20%
Muy alta	150	40%
Total	**376**	100%

Elaborado por: Rodríguez,O (2020)

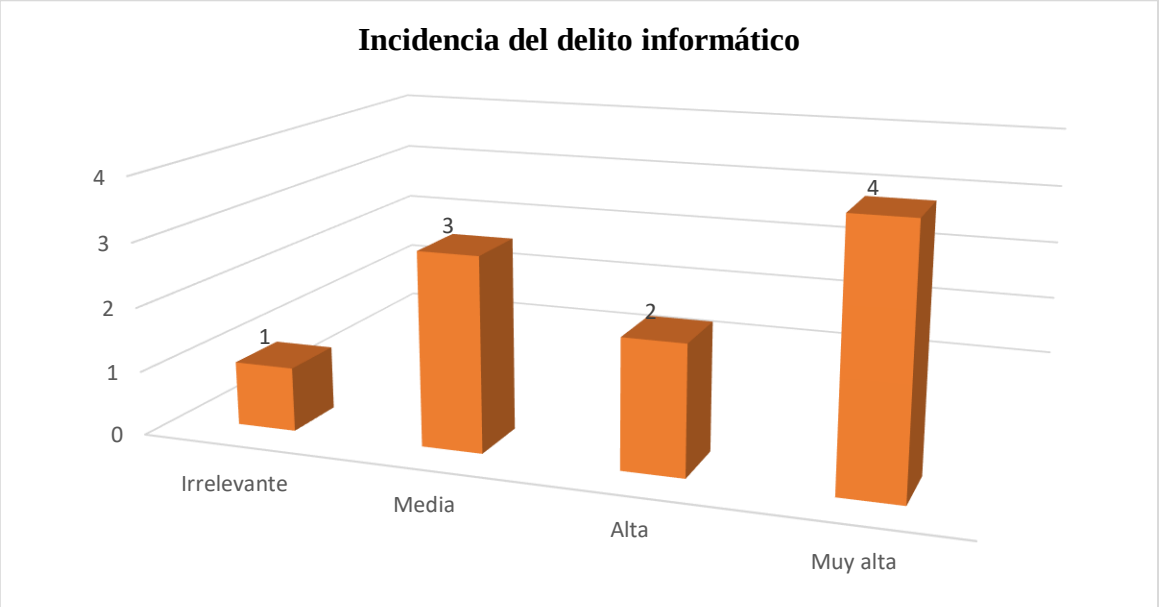

GRÁFICO 4

Fuente: Abogados inscritos al Colegio de Abogados del Guayas
Elaborado por: Rodríguez,O (2020)

Interpretación y análisis de datos No.4: aquí se les preguntó a los encuestados sobre su percepción en cuanto al delito informático en general; como puede apreciarse en los datos las respuestas fueron diversas: el 40% considera que es muy alta mientras el 10% afirmó que es irrelevante. Entre esos dos intervalos el 20% consideró que la incidencia es alta en tanto el restante 30% le otorga una relevancia media.

Debe señalarse que la pregunta se refiere a su percepción como profesional sin referencias a datos comparativos o estadísticos, por lo que el 60% repartido entre las opciones alta y muy alta es considerable como prueba de la relevancia de dichos delitos en el panorama social ecuatoriano.

Pregunta No. 5.

En su ejercicio profesional el tipo de fraude más común con tarjeta de crédito que ha presenciado es:

TABLA 5.

Descripción	Frecuencia	Porcentaje
Fraude con pruebas a la tarjeta	113	30%
Fraude de adquisición de cuenta	75	20%
Fraude por robo de identidad	150	40%
Fraude amistoso, llamado fraude de contracargos	38	10%
Total	376	100%

Elaborado por: Rodríguez,O (2020)

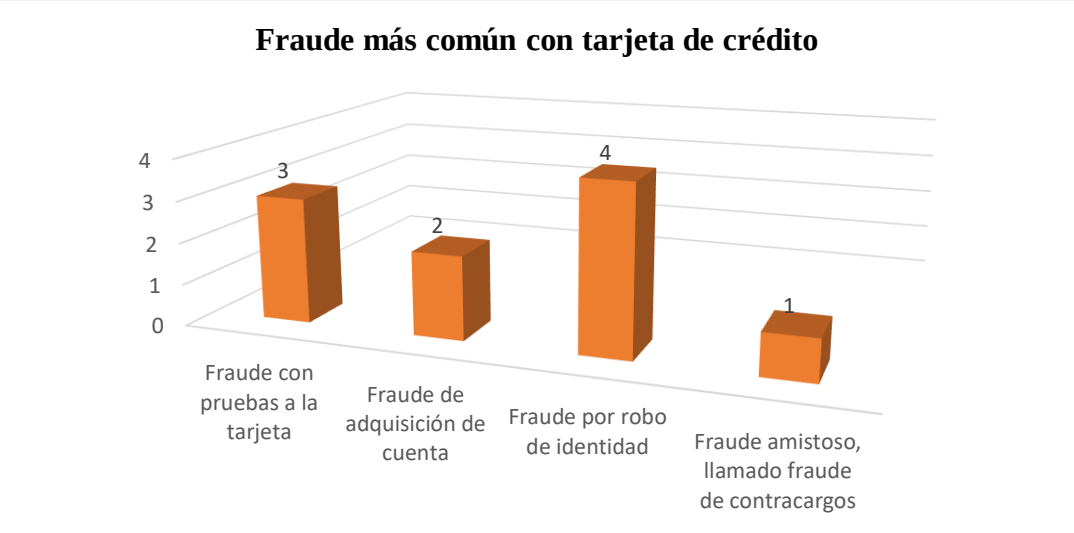

GRÁFICO 5

Fuente: Abogados inscritos al Colegio de Abogados del Guayas
Elaborado por: Rodríguez,O (2020)

Interpretación y análisis de datos No.5: esta pregunta está más enfocada en el tema específico de los delitos informáticos realizados a través de la modalidad de fraude con tarjeta de crédito. A los encuestados se les preguntó cuál es la más frecuente entre las diversas modalidades, y las respuestas fueron repartidas en cuatro categorías.

La modalidad más frecuente es la de fraude por robo de identidad que representa el 40%, seguida del fraude con pruebas a la tarjeta que fue del 30%; por debajo de esos dos intervalos el fraude amistoso que fue el 10%, mientras el fraude de adquisición de cuenta fue marcado por el 20% de los encuestados.

La diversidad de respuestas demuestra que existen varias modalidades para la comisión del delito informático a través del uso de tarjeta de crédito, y que todos los encuestados han participado en el juzgamiento de las mismas y cuentan con experiencia en ello tanto desde el punto de vista sustantivo como procesal.

Pregunta No. 6.

En su opinión: ¿Cuál es la frecuencia con la que se realizan fraudes por medio de tarjetas de crédito?

TABLA 6.

Descripción	Frecuencia	Porcentaje
Irrelevante	0	0%
Media	113	30%
Alta	113	30%
Muy alta	150	40%
Total	376	100%

Elaborado por: Rodríguez,O (2020)

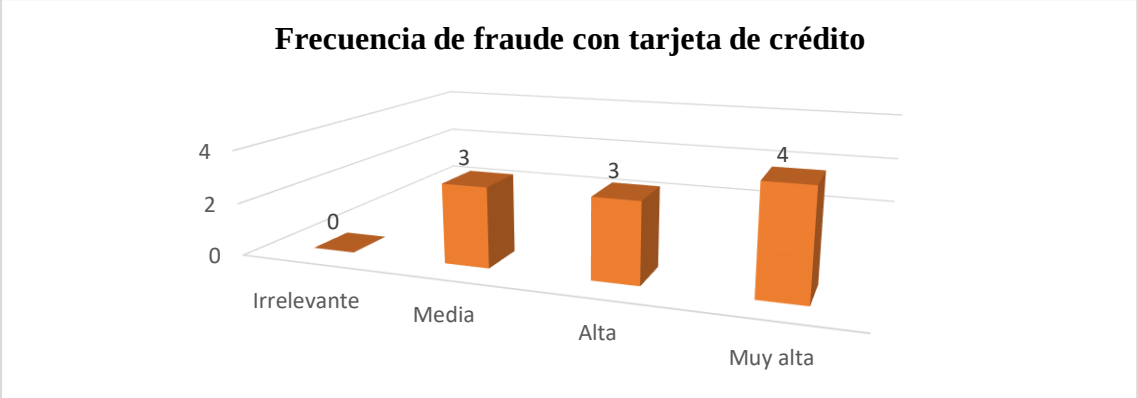

GRÁFICO 6

Fuente: Abogados inscritos al Colegio de Abogados del Guayas

Elaborado por: Rodríguez,O (2020)

Interpretación y análisis de datos No.6: a la pregunta sobre la frecuencia con que se realizan los delitos informáticos a través de las tarjetas de crédito los encuestados marcaron tres de las cuatro opciones previstas en el cuestionario.

De acuerdo a su experiencia profesional, el 40% de los expertos encuestados consideró que esa incidencia es muy alta, mientras el restante 60 % quedó repartido entre las dos opciones siguientes, alta y media; en ningún caso fue considerada la opción irrelevante.

De cualquier manera, el 100% de los encuestados consideró que el delito tiene una influencia significativa en el panorama delictivo ecuatoriano, sin contar aquellos casos en que las personas no denuncian el fraude con tarjeta de crédito en la vía penal porque acuden a otros mecanismos como el defensor del consumidor dentro de las propias instituciones bancarias o ante la Defensoría del Pueblo.

Pregunta No. 7.

De acuerdo a su experiencia profesional: ¿Qué tipo de modalidades utilizan para el fraude por medio de tarjetas de crédito?

TABLA 7.

Descripción	Frecuencia	Porcentaje
Introducción de datos falsos	38	10%
Llave no autorizada que abre cualquier archivo del ordenador por muy protegido	188	50%
Puertas falsas	38	10%
Bombas lógicas o cronológicas	112	30%
Total	376	100%

Elaborado por: Rodríguez,O (2020)

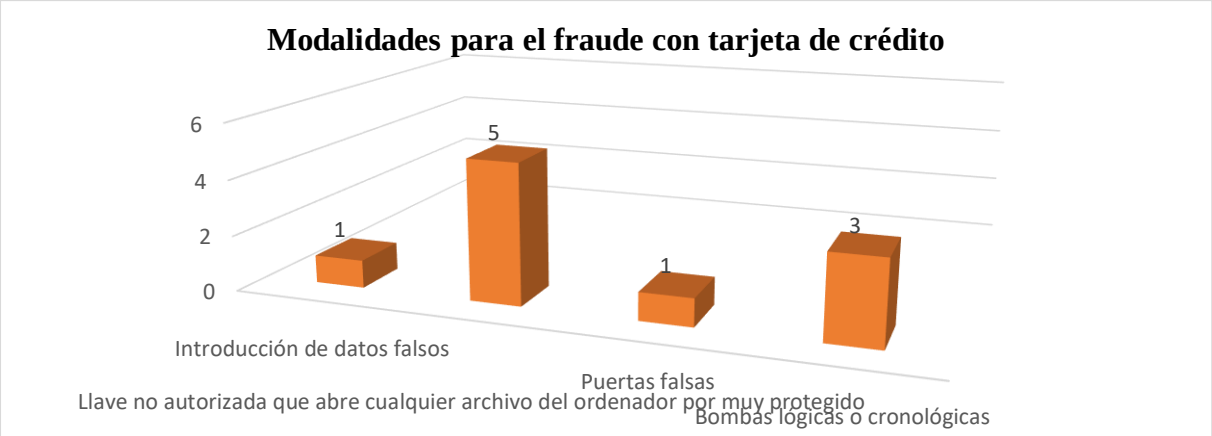

GRÁFICO 7

Fuente: Abogados inscritos al Colegio de Abogados del Guayas
Elaborado por: Rodríguez,O (2020)

Interpretación y análisis de datos No.7: a diferencia de la pregunta cinco, que se les solicitó a los profesionales encuestados información sobre los tipos de fraude más comunes con tarjeta de crédito, en esta pregunta se les pidió su opinión sobre las modalidades más frecuentes que se utilizan para cometer el delito.

En todas las opciones presentadas al menos uno de los encuestados respondió afirmativamente. Así, el valor más alto representado por un 50% fue para la modalidad del uso de llave no autorizada que abre cualquier archivo del ordenador por muy protegido de, mientras los valores mínimos del 10% fue para la modalidad de introducción de datos falsos y el uso de puertas falsas.El restante 30% marcó la opción de bombas lógicas o cronológicas como modalidad utilizada.

Como puede advertirse de los datos los delincuentes se valen de diferentes mecanismos para ejecutar los hechos delictivos utilizando las tarjetas de crédito, pero en cualquier caso el resultado final del delito es la sustracción de valores de las cuentas asociadas a dichas tarjetas, ya sea para efectuar pagos o para extraer dinero en efectivo dentro de los límites permitidos.

Pregunta No. 8.

¿Cuáles son las principales causas que propician el delito informático en el Ecuador?

TABLA 8.

Descripción	Frecuencia	Porcentaje
Errores de los propios consumidores	226	60%
Descuido en el manejo de equipos electrónicos	150	40%
Deficiencias en los sistemas informáticos	0	0%
Errores de las plataformas bancarias	0	0%
Total	376	100%

Elaborado por: Rodríguez,O (2020)

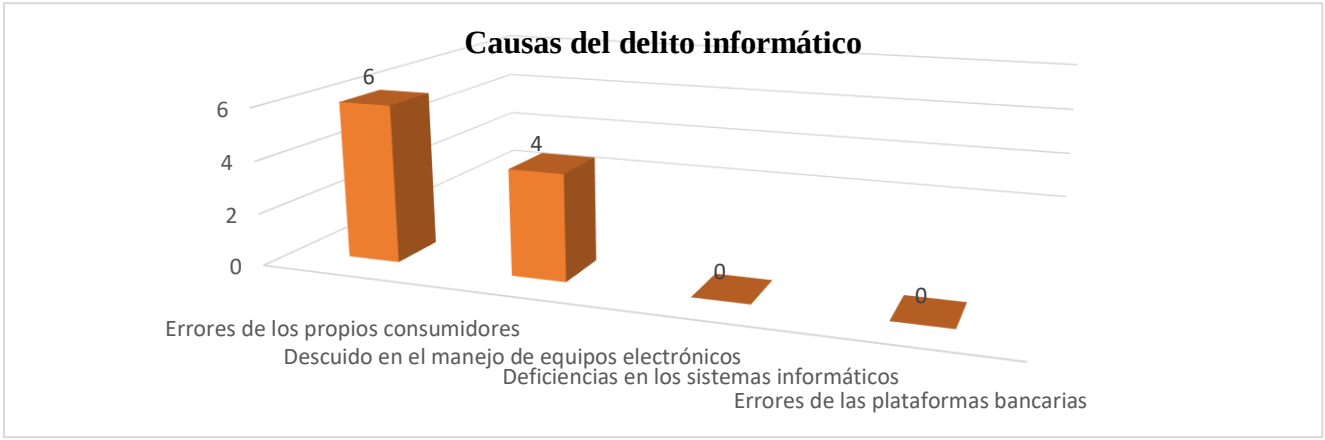

GRÁFICO 8

Fuente: Abogados inscritos al Colegio de Abogados del Guayas

Elaborado por: Rodríguez,O (2020)

Interpretación y análisis de datos No.8: en esta pregunta sobre las principales causas de los delitos informáticos los expertos encuestados estuvieron de acuerdo en que radican en errores o descuidos atribuibles al propio usuario del sistema informático.

En cuanto a los porcentajes de las diferentes opciones presentadas, el 60% indició que la perpetración del delito se debe a errores de los propios consumidores en el manejo de sus cuentas asociadas a la tarjeta de crédito, mientras el restante 40% consideró que se debe al descuido en el manejo de equipos electrónicos donde se guardan los datos y claves de acceso a los sistemas informáticos.

Las opciones que atribuyen responsabilidad a las deficiencias en los sistemas informáticos o a errores en las plataformas bancarias no fueron marcadas por ninguno de los encuestados, lo que sugiere que una adecuada protección de los datos personales de acceso a los sistemas informáticos reduciría considerablemente la incidencia del delito a través del fraude con tarjeta de crédito.

Pregunta No. 9.

¿Cuáles son los principales medios que se utilizan para el delito informático en el Ecuador?

TABLA 9.

Descripción	Frecuencia	Porcentaje
Redes sociales	113	30%
Correos Electrónicos	226	60%
Información en la nube	37	10%
Total	**376**	100%

Elaborado por: Rodríguez,O (2020)

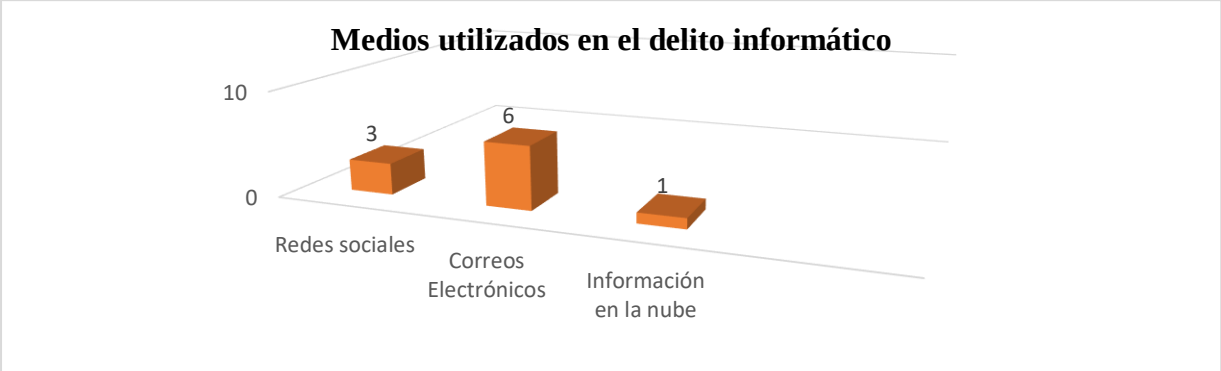

GRÁFICO 9

Fuente: Abogados inscritos al Colegio de Abogados del Guayas

Elaborado por: Rodríguez, O (2020)

Interpretación y análisis de datos No.9: sobre los medios más utilizados para ejecutar los delitos informáticos los encuestados se dividieron en tres opciones: el 60% marcó los correos electrónicos a través de las cuales personas desprevenidas o con habilidades limitadas en el manejo de esa tecnología comparten información delicada sobre sus datos o accesos a sistemas informáticos donde se alojan sus cuantas y claves de acceso.

En el otro extremo de los encuestados se sitúa el 10% que marcó la opción del acceso a la información en la nube, mientras el restante 30% refirió las redes sociales como vía para ejecutar los delitos informáticos.

En todos los casos se trata de medios que maneja directamente el usuario que al no crear las condiciones de seguridad necesarias, su información queda expuesta y es vulnerada por los cyber delincuentes siempre al acceso del descuido para ejecutar el delito.

Pregunta No. 10.

Ante la proliferación de los delitos informáticos a través de tarjetas de crédito: ¿Qué medidas considera se deberían adoptar?

TABLA 10.

Descripción	Frecuencia	Porcentaje
Creación de la policía informática especializada	113	30%
Aumentar el marco sancionador en el COIP	150	40%
Campañas de información y prevención del delito	113	30%
Total	376	100%

Elaborado por: Rodríguez,O (2020)

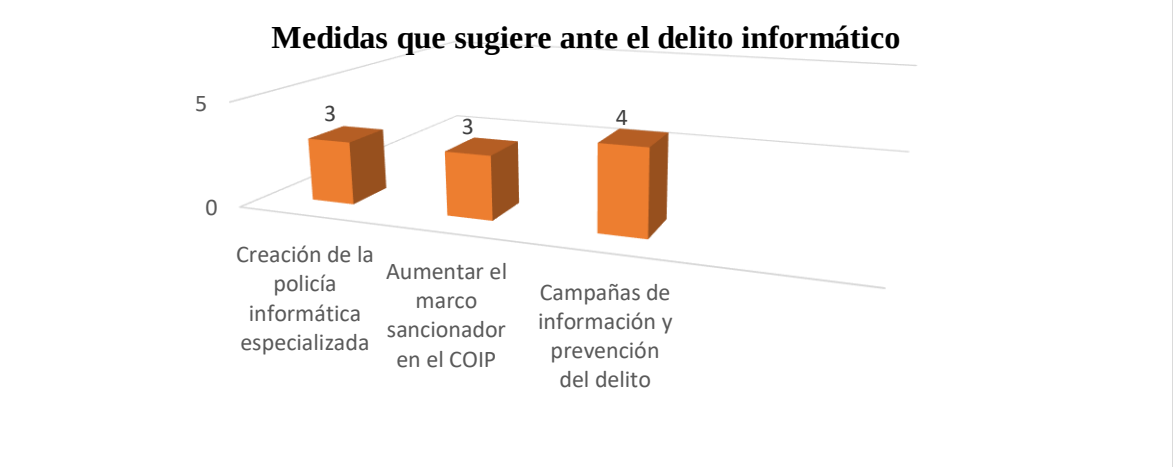

GRÁFICO 10

Fuente: Abogados inscritos al Colegio de Abogados del Guayas

Elaborado por: Rodríguez,O (2020)

Interpretación y análisis de datos No.10: Se refiere a las medidas consideran se deberían adoptar para disminuir la incidencia de los delitos informáticos, así como perseguir y sancionar a los responsables.

A los encuestados se les presentaron tres opciones: creación de la policía informática especializada, aumentar el marco sancionador en el COIP y campañas de información y prevención del delito.

La opción "campañas de información y prevención del delito" fue marcada por el 40% de los encuestados, mientras las dos restantes relativas a la creación de una policía especializada y la reforma al COIP fueron marcadas por el 30% de los encuestados en ambos casos.

Los resultados a esta pregunta, que tiene carácter propositivo, muestran una división en cuanto a las medidas que pudieran adoptarse, partiendo de la hipótesis de que una utilización más adecuada de los medios informáticos por parte de los usuarios podría contribuir a la disminución del delito de fraude con tarjeta de crédito, para lo cual se sugiere la ejecución de campañas de socialización de medidas preventivas.

Además de la perención persona que corresponde al usuario o titular de la tarjeta de crédito, los expertos encuestados sugieren que con la misma finalidad se podrían reforzar el marco institucional y legal, con la creación o potenciación de los órganos de investigación y persecución penal, por un lado, y por otro con la reforma del marco sancionador previsto en el COIP.

Pregunta No. 11.

¿Creé usted importante según su criterio en el Art. 190 dar un mejor entendimiento sobre las falsificaciones, clonaciones y modificaciones de las tarjetas de crédito y débito?

TABLA 11

Descripción	Frecuencia	Porcentaje
Sí	301	80%
No	75	20%
Total	376	100%

Elaborado por: Rodríguez, O (2020)

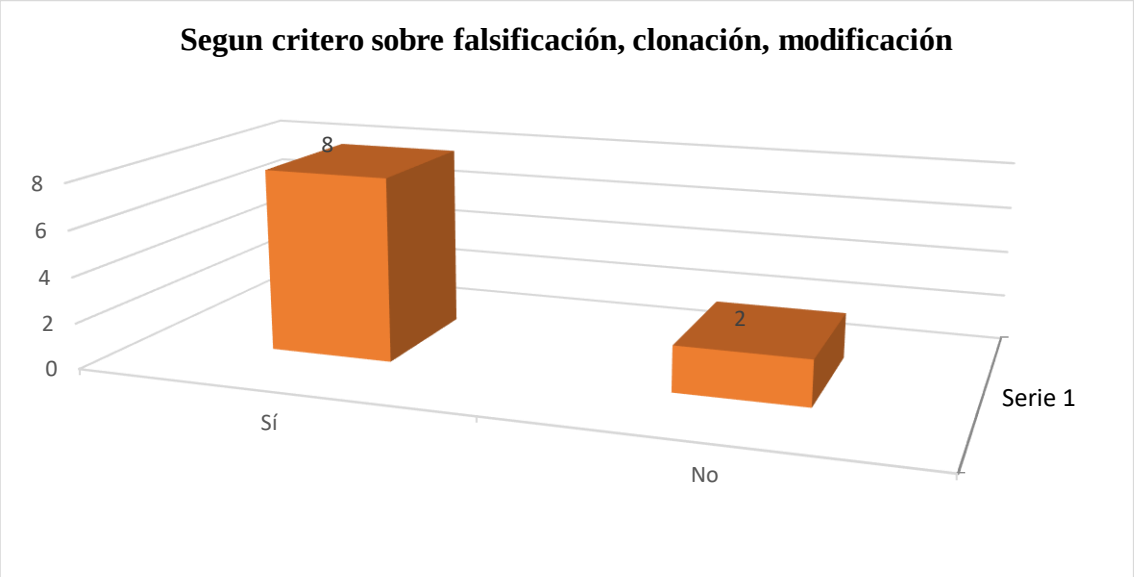

GRÁFICO 11

Fuente: Abogados inscritos al Colegio de Abogados del Guayas

Elaborado por: Rodríguez, O (2020)

Interpretación y análisis de datos No.11: Dara conocer la necesidad de un análisis más profundo para así llegar a ver la necesidad una ampliación en lo que respecta a este tipo de delito dentro del Art. Esa hipótesis fue corroborada por los encuestados que en un 80% consideraron que sí es necesario que respecto al Art. 190 se le dé una mayor ampliación para un mejor entendimiento sobre las falsificaciones, clonaciones y modificaciones referentes a las tarjetas de crédito y débito siendo necesario para una adecuada seguridad informática, el otro 20% concluye que esto no es necesario.

Pregunta No. 12.

¿Cree importante la incorporación de un inciso al Art230 para determinar la misma sanción a quien también utilice dicho datos alterados o modificados?

TABLA 12.

Descripción	Frecuencia	Porcentaje
Sí	263	70%
No	113	30%
Total	376	100%

Elaborado por: Rodríguez,O (2020)

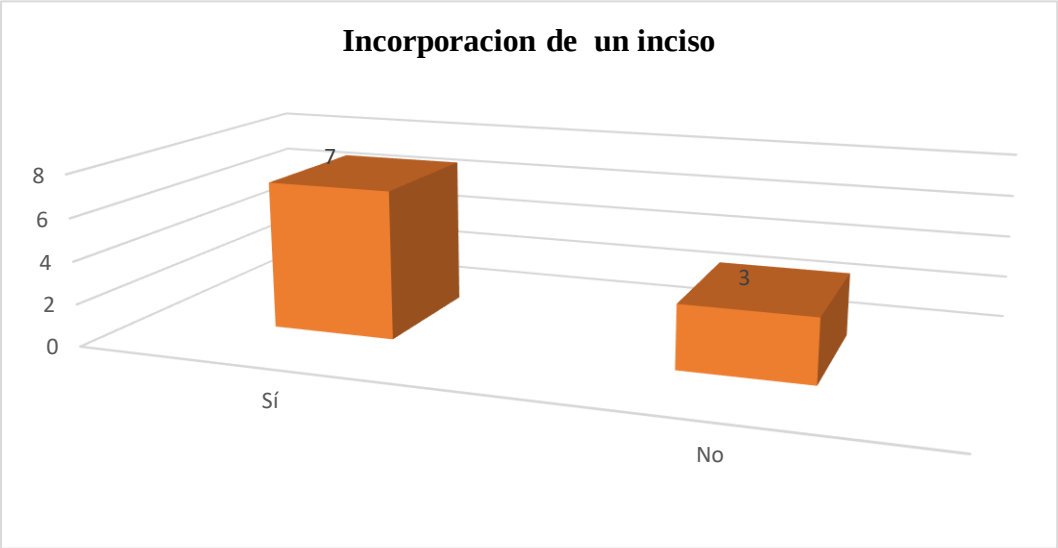

GRÁFICO 12

Fuente: Abogados inscritos al Colegio de Abogados del Guayas
Elaborado por: Rodríguez,O (2020)

Interpretación y análisis de datos No.12: esta pregunta va orientada para lograr establecer si tanto la misma sanción a la persona que falsifique, copie o altere es aplicable a la persona que sea quien utilice dichos dato, porque uno puede quien se encargue de realizar las falsificación más bien puede ser un tercero quien la utilice.
Esta fue corroborada por los encuestados que dentro de un 70% consideraron que sería mejor un estudio más amplio a este inciso para llegar a determinar si dicha interrogante esta en lo correcto y así poder aplicar una seguridad informática a los ciudadanos, el 30% No considera necesario dicho estudio de la implementación de un nuevo inciso por lo que pueda acarrear dicho estudio.

Pregunta No. 13.

¿Cree usted que reformando el artículo 230 se garantizara el derecho a los tarjetahabientes, de la alteración o manipulación de las tarjetas?

TABLA 13.

Descripción	Frecuencia	Porcentaje
Sí	263	70%
No	113	30%
Total	376	100%

Elaborado por: Rodríguez,O (2020)

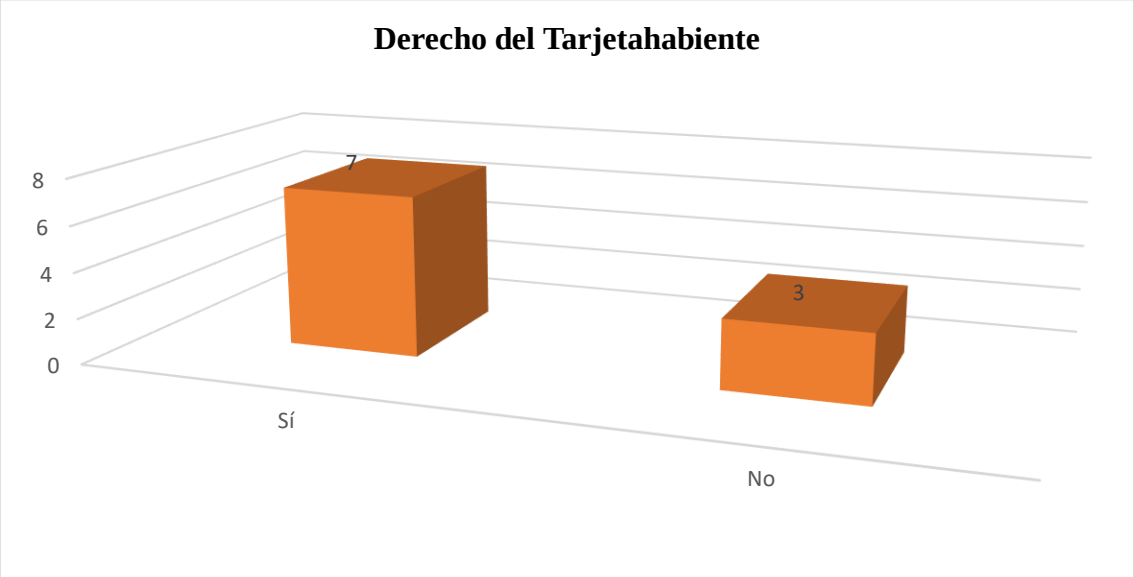

GRÁFICO 13
Fuente: Abogados inscritos al Colegio de Abogados del Guayas
Elaborado por: Rodríguez,O (2020)

Interpretación y análisis de datos No.13: esta pregunta va orientada a saber si se garantizara el derecho al tarjetahabiente respecto a la alteración y manipulación. Esto fue corroborado por los encuestados que dentro de un 70% consideraron que si se debería establecerse dicha reforma para garantizarles los derechos, el 30% No considera necesario dicha reforma para garantizar el derecho a los tarjetahabientes.

CONCLUSIONES

1. De las preguntas 1 y 2 de la encuesta aplicada se puede concluir que el 60% de los expertos en Derecho consultados tiene entre cinco y ocho años de ejercicio profesional, lo que permite afirmar que la muestra cuenta con experiencia suficiente para dar credibilidad a sus respuestas. Se puede concluir además que el 80 % ha participado profesionalmente en el juzgamiento de delitos informáticos en la modalidad de fraude con tarjeta de crédito.

2. De las preguntas 3 y 4 se puede concluir que es relevante la experiencia existente en otros países siendo esto fundamental para enfrentar adecuadamente el delito informático en el Ecuador; de los encuestados el 70% consideró que ese estudio es necesario para la adecuada seguridad informática.

3. De las preguntas 5 y 6 se concluye que dentro de los delitos informáticos realizados a través de la modalidad de fraude con tarjeta de crédito los más frecuentes son fraude por robo de identidad, fraude con pruebas a la tarjeta, fraude amistoso que, fraude de adquisición de cuenta

4. De las preguntas 7 y 8 llegamos a concluir que a diferencia de la pregunta cinco, que se les solicitó información sobre los tipos de fraude más comunes con tarjeta de crédito, en esta se les pidió su opinión sobre las modalidades más frecuentes. Un 50% fue para la modalidad del uso de llave no autorizada que abre cualquier archivo del ordenador, siguiendo introducción de datos falsos y el uso de puertas falsas, de bombas lógicas o cronológicas. También se concluye sobre las causas de los delitos informáticos en común acuerdo en que radican en errores o descuidos atribuibles al propio usuario, indicios que la perpetración del delito se debe a errores de los propios consumidores, descuido en el manejo de equipos electrónicos donde se guardan los datos y claves de acceso.

5. De las preguntas 9 y 10 concluimos que entre los medios más utilizados para ejecutar los delitos informáticos se encuentra en un 60% el correo electrónico a través de las cuales personas desprevenidas o con habilidades limitadas en el manejo

comparten información sobre sus datos, prosiguiendo el acceso a la información en la nube, las redes sociales como vía para ejecutar los delitos informáticos.

De igual manera se concluye sobre la seguridad necesaria, las "campañas de información y prevención del delito", la creación de una policía especializada y la reforma a un inciso al COIP.

6. De las preguntas 11y 12 llegamos a concluir la necesidad de una reforma en lo que respecta a este tipo de delito, siendo la mayoría que respondió que SÍ es necesario, el restante que NO es necesario este tipo de profundidad en el análisis, considerando entonces un estudio más amplio a estos incisos para llegar a determinar si dicha interrogante esta en lo correcto y así poder aplicar una seguridad informática a los ciudadanos.

7. De la pregunta 13 podemos concluir que en su mayoría considera que estableciendo la reforma se garantizara el derecho necesario al tarjetahabiente en respecto a la alteración y manipulación de sus tarjetas.

RECOMENDACIONES

1. De las conclusiones 1 y 2 establecemos como recomendación la necesidad de tener experiencia en el área para poder brindar siempre mejores criterios sobre temas relevantes que se pregunten alrededor del Derecho en sí, más aun estar actualizados con temas que cada vez son de más relevancia en el día a día respeto a la relación entre Derecho e informática. .

2. De las conclusiones 3 y 4 podemos recomendar la necesidad de siempre estar actualizados con los estudios alrededor del mundo sobre cualquier tema que se presente día a día, siendo esencial la experiencia que se adquiera y poder utilizar las doctrinas relevantes que acumulemos más aun en un tema como lo es los delitos informáticos.

3. De las conclusiones 5 y 6 se deriva como recomendación un mejor sistema de prevención en materia de delitos informáticos realizados a través de la modalidad de fraude con tarjeta de crédito, fraude por robo de identidad, fraude con pruebas a la tarjeta, fraude amistoso y fraude de adquisición de cuenta.

4. De las conclusiones 7 y 8 se recomienda que se mantenga una mejor seguridad o antivirus en lo que respecta a sus ordenadores o a las páginas que ingresan cualquiera puede ser un modo de adquirir la información necesaria para obtener datos esenciales para una falsificación, así mismo evitar dar los datos por cualquier página que le ofrecen algún servicio, tratar de que este descuido del usuario no sea una de las forma para que se llegue a lograr la falsificación o clonación.

5. De las conclusiones 9 y 10 se recomienda realizar campañas de concienciación sobre el tema de los delitos informáticos y cómo evitarlos en su mayoría, existiendo muchas personas que inconscientemente proporcionan sus datos por medios de páginas al momento de estar navegando sin saber que son víctimas de delito.

6. De las conclusión 11 y 12 se recomienda la revisión del artículo 190 del COIP para lograr una ampliación en lo que respecta a la alteración o modificación de las tarjetas de

crédito o débito, y una incorporación al artículo 230 un inciso sobre la sanción a la persona que utilice dicho material alterado o modificado, estableciendo que en el numeral 3 del artículo 230 establece sanción a la persona que realice estas alteración mas no a la que llegue a utilizarlas.

7. De la conclusión 13 se recomienda la reforma del Artículo para así poder garantizar los derechos a las víctimas de las alteraciones o modificaciones realizadas a sus tarjetas de crédito.

PROPUESTA

De las conclusiones y recomendaciones se deriva como propuesta la reforma al Código Orgánico Integral Penal mediante una Ley Orgánica Reformatoria, misma que debería realizar la Asamblea Nacional en ejercicio de las competencias legislativas atribuida en el artículo 133 de la Constitución de la República del Ecuador.

La propuesta concreta consiste en lo siguiente.

1. Que se reforme el artículo 190 del COIP ampliando las modalidades de la configuración jurídica actual de delito de alteración o modificación de las tarjetas de crédito o débito.

2. Que se incorpore un nuevo párrafo al artículo 230 numeral 3º del COIP, donde se tipifique y sancione como delito la utilización fraudulenta de los datos electrónicos para apropiación fraudulenta de fondos a través de tarjetas de crédito.

3. En esa modalidad delictiva debe ser sancionada tanto la tentativa como el delito consumado, estableciéndose una pena menor o igual para quien solo realice la alteración de los datos sin llegar a utilizar la tarjeta de crédito.

REFERENCIAS BIBLIOGRÁFICAS

Bibliografía

(s.f.). Obtenido de La tarjetas de Credito: : www.las-tarjetas-credito.com

Acurio del Pino, S. (2015). Derecho Penal Informatico. Quito: Corporacion de Estudios y Publicaciones.

Acurio del Pino, S. (2 de Octubre de 2020). *Delitos Informáticos: Generalidades*. Obtenido de Delitos Informáticos: Generalidades: elitos_informhttps://www.oas.org/juridico/spanish/cyb_ecu_d.pdf

Acurio del Pino, S., & Paéz Rivadeneira Juan, J. (2010). *Derecho y Nuevas Tecnologías.* Quito: Corporación de Estudios y Publicaciones.

Alfredo Contreras Villavicencio. (s.f.). Derecho Bancario y Monetario, Tomo I,. En Alfredo Contreras Villavicencio. Guayaquil.

Andes. (enero de 2020). *Bancos Ecuatorianos Deben Implementar Medidas Contra Clonacion* . Obtenido de http://www.andes.info.ec/es/econom%-

Arias Torres Luis, B. (s.f.). El Delito Informático en el Código Penal de Peruano. En *Vol.6* (pág. 58). Biblioteca de Derecho Comteporaneo.

Association of Certified Fraud Examiners. (2020). *ACFE.* Obtenido de Acfe, Fraude: https://acfe-spain.com/recursos-contra-fraude/que-es-el-fraude/arbol-fraude

Borrego, B. (2014). La necesaria adaptación de los tributos a las nuevas tendencias de los negocios electrónicos. *Revista de Internet,Decho y Política*, 51-59.

CALLEGARI, N. (2013). EL DELITO INFORMATICO. En C. O. DONNELL.

Chinchilla Sandí, C. (2004). *Delitos informáticos: elementos básicos para identificarlos y su aplicación.* Farben Grupo Editorial Norma.

Código Orgánico Integral Penal Ecuatoriano. (Quito de 2020). *Registro Oficial* . Obtenido de Suplemento- Registro Oficial Nº 107,: https://www.registroficial.gob.ec/index.php/registro-oficial-web/publicaciones/suplementos/item/12339-suplemento-al-registro-oficial-no-107

Código Orgánico Monetario Financiero. (Septiembre de 2014). *Registro Oficial* . Obtenido de Segundo Suplemento- Registro Oficial 332: https://www.registroficial.gob.ec/index.php/registro-oficial-web/publicaciones/suplementos/item/1716-segundo-suplemento-al-registro-oficial-no-332

CODIGO PENAL DE LA NACION ARGENTINA. (s.f.). *InfoLEG- Informacion Legislativa*. Obtenido de CODIGO PENAL DE LA NACION ARGENTINA- Ley 11.179: http://servicios.infoleg.gob.ar/infolegInternet/anexos/15000-19999/16546/texact.htm#20

Codigo Penal de la Nacion Argentina, L. 2. (Septiembre de 2004). *InfoLEG-Informacion Legislativa*. Obtenido de Codigo Penal de la Nacion Argentina, Inciso Incorporado por Ley 25.930: http://servicios.infoleg.gob.ar/infolegInternet/anexos/15000-19999/16546/texact.htm#20

Código Penal de la Nacion Argentina, L. N. (Junio de 2008). *InfoLEG Informacion Legislativa*. Obtenido de Código Penal de la Nacion Argentina, Inciso Incorporado por Ley No. 26.388: http://servicios.infoleg.gob.ar/infolegInternet/anexos/15000-19999/16546/texact.htm#20

Cogorno, E. G. (1979). TEORÍA Y TÉCNICA DE LOS NUEVOS CONTRATOS COMERCIALES. En E. G. Cogorno. Argentina: Ediciones Meuri.

Consejo de a Judicatura. (3 de junio de 2020). *https://app.funcionjudicial.gob.ec/*. Obtenido de https://app.funcionjudicial.gob.ec/ForoAbogados/Inicio/frmInicio.jsp

Constitucion de la República del Ecuador. (Octubre de 2008). *Registro Oficial*. Obtenido de Primer suplemento-registro oficial 449: https://www.registroficial.gob.ec/index.php/registro-oficial-web/publicaciones/suplementos/item/4546-suplemento-al-registro-oficial-no-449

Ecuador Inmediato. (Marzo de 2013). *Ecuador Inmediato.* . Obtenido de http://www.ecuadorinmediato.com/index.php?module=Noticias&func=news_user_view&id=193188&umt=hasta_el_19_de_marzo_

EcuaRed. (febrero de 2020). Obtenido de Ecuared, Delito Infomratico: https://www.ecured.cu/Derecho_inform%C3%A1tico#Inform.C3.A1tica_jur.C3.ADdica

Edufinext. (febrero de 2020). *Edufinext*. Obtenido de Edufinext, Medios de pago, partes de tarjetas: https://www.edufinet.com/edufinext/index.php/medios-de-pago/96-partes-de-la-tarjeta

Fernández, D. (Febrero de 2016). Delimitacion Del Delito Informatico. En F. D.

Hermández Diaz, L. (s.f.). El Delito Informatico. En *Cuaderno del Instituto Vasco de Criminología* (pág. 227). Eguzkilore.

Hernández Sampieri, R. (2010). *Metodología de la investigación.* México: McGraw-Hill.

Herrmann Fernández, P. (2006). *Comercio Electrónico.* Loja: Editorial de la Universidad Tecnica Particula de Loja.

Juárez Angel. (Accesible 2020). *Defensa del deudor, Sc*. Obtenido de Tarjeta de Credito: http://www.defensadeldeudor.org/t26881-diccionario-tarjeta-de-credito,

Junta Bancaria del Ecuador. (2020). *Superintendecia de Bancos y Seguros del Ecuador.* Obtenido de Superintendecia de Bancos y Seguros del Ecuador:

http://www.sbs.gob.ec/medios/PORTALDOCS/downloads/normativa/2012/resol_

Junta Bancaria del Ecuador. (s.f.). *Superintendecia de Bancos y Seguros del Ecuador.* Obtenido de JB-2012-2148: tenido de http://www.sbs.gob.ec/medios/PORTALDOCS/downloads/normativa/2012/resol_

Levene, R., & Chiaravalloti, A. (2020). *Delitos Y Tecnología de la Información*. Obtenido de https://delitosinformaticos.com/delitos/delitosinformaticos.shtml

Ley de Comercio electrónico Firmas electrónicas y mensajes de datos, +. (2002). *Registro Oficiaal*. Obtenido de Primer Suplemento- Registro Oficial 557: https://www.registroficial.gob.ec/index.php/registro-oficial-web/publicaciones/suplementos/item/6989-suplemento-al-registro-oficial-no-557

Lima, M. (2014). Delito Informatico como medio y fin. *Revista Ciencia Unemi*, 44.

Merca2.0. (2020). *Mesa Editorial Merca2.0*. Obtenido de Tipos de Comercio Electrónico: http://www.merca20.com/tipos-de-comercio-electronico/

Ministerios de Comercio Exterior. (Abril de 2016). *Ministerio de Comercio Exterior*. Obtenido de Ministerio de Comerio Exteiror,Más de 100 MIPYMES cuentan con herramintas de comercio electronico: http://www.comercioexterior.gob.ec

Philco, A., & Rosero, L. (2014). Los Riesgos en Transacciones Electrónicas en Línea y la. *Gaceta Sansana*, 45.

Proyecto de Ley Boletín N° 12.192-25. (s.f.). Obtenido de https://alertas.directoriolegislativo.org/wp-content/uploads/2019/08/12192-25.pdf

Ramírez Granda, J. (s.f.). Fraude. En *Diccionario Jurídico* (pág. pag.160).

Sarzana, C. (2014). Cómo Responder A un Delito Informatico. *Revista Ciencia Unemi*, 44.

Shoshanah Posner. (enero de 2019). *Entrepreneur*. Obtenido de Entrepreneur, Los 7 tipos de fraude en comercio electronico: https://www.entrepreneur.com/article/326346

Solano Orlando. (2020). *Eumed.* Obtenido de El fraude Informatico-Manual de Informática Jurídica: https://www.eumed.net/rev/cccss/14/ecra.html

Téllez Valdez, J. (2014). 3 Edicion. Mexico: Esitorial Mc. Graw Hill.

Téllez, J. (2008). Derecho informatico. En J. Téllez, *Derecho Informatico Cuarta Edición.* McGRAW-HILL/INTERAMERICANA EDITORES.

Anexos

Anexo 1. Encuestas aplicada

Información sobre el objetivo de la encuesta

Estimad(a) abogado(a), como parte de mi investigación sobre el tema **"Análisis de los delitos informaticos en base a la alteracion y modificacion mediante transferencia electronica en modalidad tarjeta de credito"**, para obtener el título de Abogado de los Juzgados y Tribunales de la República, estoy realizando una encuesta entre abogados en libre ejercicio de la profesión para conocer su opinión sobre la regulación actual de los delitos informáticos, particularmente los relacionados con la tarjeta de crédito.

Por tal motivo solicito muy comedidamente su colaboración para que responda algunas preguntas que darán soporte empírico a la investigación. La información que aporte tiene carácter anónimo y solo será utilizada para los fines señalados.

PREGUNTAS. Por favor marcar con una X la(s) opción(es) que considere según el caso.

Pregunta No. 1.

¿Cuánto tiempo lleva vinculado al ejercicio de la profesión en materia de Derecho penal y delitos informáticos?

---- 8 años o más ---- entre 8 y 5 años ---- menos de 5 años

Pregunta No. 2

¿Ha participado como profesional en el juzgamiento de algún delito relacionado con el fraude de tarjeta de crédito?

---- Sí

---- No

Pregunta No. 3

¿Considera que el estudio de los delitos informáticos a nivel internacional es importante para prevenirlo en el Ecuador?

----Sí

----No

Pregunta No. 4.

Con relación a los delitos informáticos considera que su incidencia es:

---- Irrelevante.

---- Media.

---- Alta.

---- Muy alta.

Pregunta No. 5.

En su ejercicio profesional el tipo de fraude más común que ha presenciado es:

---- Fraude con pruebas a la tarjeta

---- Fraude de adquisición de cuenta.

---- Fraude por robo de identidad.

---- Fraude amistoso, también llamado fraude de contracargos

Pregunta No. 6.

En su opinión: ¿Cuál es la frecuencia con la que se realizan fraudes por medio de tarjetas de crédito?

---- Irrelevante.

---- Media.

---- Alta.

---- Muy alta.

Pregunta No. 7.

De acuerdo a su experiencia profesional: ¿Qué tipo de modalidades utilizan para el fraude por medio de tarjetas de crédito?

---- Introducción de datos falsos.

---- Llave no autorizada que abre cualquier archivo del ordenador por muy protegido.

---- Puertas falsas.

---- Bombas lógicas o cronológicas.

Pregunta No. 8.

¿Cuáles son las principales causas que propician el delito informático en el Ecuador?

---- Errores de los propios consumidores.

----Descuido en el manejo de equipos electrónicos.

---- Deficiencias en los sistemas informáticos.

---- Errores de las plataformas bancarias.

Pregunta No. 9.

¿Cuáles son los principales medios que se utilizan para el delito informático en el Ecuador?

---- Redes sociales.

---- Correos Electrónicos.

---- Información en la nube.

Pregunta No. 10.

Ante la proliferación de los delitos informáticos a través de tarjetas de crédito: ¿Qué medidas considera se deberían adoptar?

---- Creación de la policía informática especializada.

---- Aumentar el marco sancionador en el COIP.

---- Campañas de información y prevención del delito.

Pregunta No. 11.

¿Cree usted importante según su criterio en el Art. 190 dar un mejor entendimiento sobre las falsificaciones, clonaciones y modificaciones de las tarjetas de crédito y débito?

----Sí

----No

Pregunta No. 12.

¿Cree importante la incorporación de un inciso al Art230 para determinar la sanción quien también utilice dicho datos alterados o modificados?

---- Sí

----No

Pregunta No. 13.

¿Cree usted que reformando el artículo 230 se garantizara el derecho a los tarjetahabientes, de la alteración o manipulación de las tarjetas?

---- Sí

----No