UNIVERSIDAD LAICA VICENTE ROCAFUERTE DE GUAYAQUIL

FACULTAD DE CIENCIAS SOCIALES Y DERECHO
CARRERA DE DERECHO

PROYECTO DE INVESTIGACION PREVIO A LA OBTENCION DEL TITULO DE ABOGADO DE LOS TRIBUNALES Y JUZGADOS DE LA REPUBLICA

TITULO:

“Análisis de la tendencia de los fraudes electrónicos a los usuarios del sistema financiero ecuatoriano del 2009 al 2014 en la ciudad de Guayaquil”

AUTOR:

Carla Dayana Carrera Romero

TUTORA:

AB. BLANCA LETICIA ORTEGA LOPEZ

GUAYAQUIL – ECUADOR

AÑO 2015

Guayaquil, 23 de Agosto de 2015

“Análisis de la tendencia de los fraudes electrónicos a los usuarios del sistema financiero ecuatoriano del 2009 al 2014 en la ciudad de Guayaquil”

CERTIFICACION DE ACEPTACION DEL TUTOR

En mi calidad de tutor del Proyecto de Investigación nombrado por el Consejo Directivo de la Facultad de Ciencias Sociales y Derecho

CERTIFICO

Yo, Msc Blanca Leticia Ortega, certifico que el Proyecto de Investigación con el tema “ANALISIS DE LA TENDENCIA DE LOS FRAUDES ELECTRONICOS A LOS USUARIOS DEL SISTEMA FINANCIERO ECUATORIANO DEL 2009 AL 2014 EN LA CIUDAD DE GUAYAQUIL”, ha sido elaborado por CARLA DAYANA CARRERA ROMERO bajo mi tutoría y que el mismo reúne los requisitos ante el tribunal examinador, que se designe al efecto.

_____

AB. BLANCA LETICIA ORTEGA LOPEZ

TUTORA

DECLARACION DE AUTORIA Y CESION DE DERECHOS FR AUTOR

Declaración de Autoría

Yo, Carla Dayana Carrera Romero con cedula de ciudadanía N° 0930148622 en calidad de autora, declaro bajo juramento que la autoría del presente trabajo me corresponde totalmente y me responsabilizo de los criterios y opiniones que en el mismo se declaran como producto de la investigación que he realizado.

Que soy la única autora del trabajo del Proyecto de Investigación "ANALISIS DE LA TENDENCIA DE LOS FRAUDES ELECTRONICOS A LOS USUARIOS DEL SISTEMA FINANCIERO ECUATORIANO DEL 2009 AL 2014 EN LA CIUDAD DE GUAYAQUIL".

Que el perfil del proyecto es de mi autoría, y que en su formulación se han respetado las normas legales y reglamentos pertinentes, previa obtención del título de ABOGADO DE LOS JUZGADOS Y TRIBUNALES DE LA REPUBLICA DEL ECUADOR, de la Facultad de CIENCIAS SOCIALES Y DERECHO de la Universidad Laica Vicente Rocafuerte de Guayaquil.

CESION DE DERECHOS DE AUTOR

De conformidad con lo establecido en el Capítulo I de la ley de Propiedad Intelectual del Ecuador, su reglamento y normativa institucional vigente dejo expresado mi aprobación de ceder los derechos de reproducción y circulación de esta obra, a la Universidad Laica Vicente Rocafuerte de Guayaquil. Dicha reproducción y circulación se puede realizar, en una o varias veces, en cualquier soporte, siempre y cuando sea con fines sociales, educativos y científicos.

El autor garantiza la originalidad de su aportación al proyecto como el hecho de que goza de libre disponibilidad de los derechos que cede.

_____

AUTOR

AGRADECIMIENTO

A todas las personas que han estado a mi lado apoyándome de una u otra manera a lo largo de mi carrera universitaria y en la realización de este proyecto de investigación, especialmente a mis padres, profesores y amigos.

DEDICATORIA

Dedico este trabajo principalmente a Dios por haberme dado las fuerzas y el valor para culminar con éxito esta etapa tan importante en mi vida.

A mis padres quienes con su apoyo incondicional y consejos han sabido guiarme a culminar mi meta profesional.

“ANALISIS DE LA TENDENCIA DE LOS FRAUDES ELECTRONICOS A LOS USUARIOS DEL SISTEMA FINANCIERO ECUATORIANO DEL 2009 AL 2014 EN LA CIUDAD DE GUAYAQUIL”.

RESUMEN

El presente trabajo se encuentra enfocado al análisis de los diferentes tipos de fraudes electrónicos que existen en el Ecuador específicamente en la ciudad de Guayaquil, incrementando tendencias y nuevos métodos de cometer este tipo de delitos.

También para determinar las deficiencias o carencias de controles en las entidades financieras, para así poder recomendar ajustes o proponer medidas y controles congruentes con las regulaciones establecidas por los Organismos de Control, con la finalidad de que los bancos mitiguen el riesgo de fraude, y que tanto la sociedad, la banca y el país no sufran las repercusiones económicas y de prestigio que se genera cuando se ven envueltos voluntaria o involuntariamente en delitos financieros.

El propósito de la investigación es el de determinar cuáles son las debilidades dentro de la normativa ecuatoriana y los procedimientos bancarios para proponer recomendaciones de mejoras aplicables al interior como exterior de las organizaciones financieras y efectivas para la realidad ecuatoriana.

“ANALISIS DE LA TENDENCIA DE LOS FRAUDES ELECTRONICOS A LOS USUARIOS DEL SISTEMA FINANCIERO ECUATORIANO DEL 2009 AL 2014 EN LA CIUDAD DE GUAYAQUIL”.

ABSTRACT

This work is focused on the analysis of different types of cyber fraud that exist in Ecuador specifically in the city of Guayaquil, increasing trends and new methods of committing such crimes.
Also, it is desired to determine the deficiencies or needs of controls in the financial organizations, therefore to be able to recommend adjustments or to propose congruent steps and controls with the regulations established by Organisms of Control, with the purpose of that the banks mitigate the fraud risk, exists transparency in the information between the organisms and that as much the society, the national banking and the country do not undergo the economic repercussions and of prestige that is generated when they are surrounded voluntary or involuntarily in illegal financial actions.

The purpose of the research is to determine which are the debilities within the Ecuadorian norms and the banking procedures to propose recommendations of improvements applicable as the inside as the outside of the financial organizations and effective for the Ecuadorian reality.

INDICE GENERAL

Tabla de Contenidos Página

CAPÍTULO IV

LA PROPUESTA

ÍNDICE DE GRAFICOS

Tabla de Contenidos **Página**

INDICE DE TABLAS

Tabla de Contenidos Página

INTRODUCCION

Las tecnologías de la información y las comunicaciones están cambiando a la sociedad y al mundo, al mejorar la productividad en las industrias tradicionales, revolucionar los procesos laborales y modificar la velocidad y el flujo de capitales.

Este crecimiento rápido también ha desencadenado nuevas formas de delincuencia informática. La delincuencia informática es difícil de comprender o conceptualizar plenamente.

El delito informático tuvo su origen a finales de los años noventa, a medida que el Internet se expandió por toda Norteamérica.

Con este avance masivo de la computación, la informática y el uso de Internet, en la actualidad se cometen un sin número de delitos, llamados delitos informáticos, apareciendo el Fraude Informático y sus diferentes métodos de cometerlos, como el más importante, ya que por medio de este se cometen desfalcos a entidades financieras en general, las cuales administran recursos propios y ajenos.

El estudio de estos delitos informáticos va cambiando con el pasar del tiempo, con una tendencia a incrementar y siempre buscar cada día una nueva forma de cometer fraude electrónico, gracias a las facilidades que hoy en día existen y gracias a la falta de claridad de las leyes de nuestro Ecuador sobre el tema.

CAPÍTULO I

EL PROBLEMA A INVESTIGAR

1.1. Tema

Análisis de la tendencia de los fraudes electrónicos a los usuarios del sistema financiero ecuatoriano del 2009 al 2014 en la ciudad de Guayaquil

1.2. Planteamiento del problema

El problema central de la presente investigación se basa en el análisis y la incrementación de los casos que han existido de delitos informáticos en el sistema financiero en la ciudad de Guayaquil, ya que a pesar de que se implementen normas de seguridad, estas son penetrables por bandas delictivas que se dedican y viven del fraude electrónico.

Para el análisis y estudio de fraude en esta investigación vamos a conocer los diferentes tipos de fraudes existentes como el phishing, skiming, entre otros, y que se van dando de acuerdo a la forma en como los clientes de la banca realizan las transacciones y la desinformación que existe en muchos de ellos por parte de las entidades Financieras.

Dicho inconveniente motiva al ataque de "hackers" hasta la inestabilidad económica de la institución por los montos excesivos que tienen que asumir como pérdida para luego reembolsar estos valores y mantener la relación con su cliente.

El problema legal en la investigación se basa en que las leyes o normas ecuatorianas como el nuevo Código Orgánico Integral Penal(COIP) donde si

definen algunas de las palabras que se expresan en los artículos de sus textos, sin embargo en el análisis realizado en la Ley de Comercio Electrónico no se ha encontrado definiciones de carácter importante que ayudan a regular el uso del internet, que se defina al fraude electrónico o a la forma de hacer el fraude, como un delito grave que merezca una sanción, ya que es una ley ambigua que necesita de una reforma en sus artículos entre las cuales se puede implementar la definición de las palabras como phishing, skiming, fraude informático, etc. Con la finalidad de que guarden relación con la tipificación que sobre estos delitos contempla el COIP.

Aquí se originaría "el dilema de si el internet es o no un medio seguro para realizar transacciones bancarias"

1.3. Formulación del problema

¿Cuáles son las causas que han hecho que se incrementen los casos de fraude informáticos, y los motivos que no permiten que un proceso penal llegue a su fin?

El fraude ocurre cuando el consumidor le da el número de su tarjeta de crédito a un desconocido, cuando se pierden o roban tarjetas, o cuando un correo se desvía de su destinatario, etc. A continuación vamos a reconocer e identificar algunos tipos de fraudes que involucran tarjetas de crédito y de débitos, como el copiado de banda magnética, phishing, robo de identidad y tarjetas falsificadas.

1.3.1 El robo de identidad: es el uso fraudulento de la información personal de alguien como su número de Seguro Social o fecha de nacimiento para cometer fraude financiero. Aunque las víctimas del robo de identidad no son consideradas

responsables de los delitos les cuesta mucho trabajo probar el fraude y limpiar el caos financiero causado.

1.3.2.Skiming: es el robo de información de tarjetas de crédito o debito 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 la tarjeta.

Los escenarios comunes en los que se realiza skimming en restaurantes, bares, gasolineras o en cajeros electrónicos.

En el caso de un cajero automático, el autor del fraude pone un dispositivo a través de la ranura para tarjetas del ATM, que lee la información de la banda magnética y la copia para su uso posterior. Estos dispositivos se utilizan a menudo en combinación con una micro cámara que graba el código PIN (Código de seguridad) del usuario.

1.3.3. Phishing: consiste en enviar una cantidad enorme de mensajes por correo electrónico haciéndole conocer al consumidor que los mensajes vienen de su banco tratando de conseguir que la víctima potencial revele la información personal, como los números de cuentas del banco. Este tipo de fraude ha tenido éxito ya que los mensajes de correo electrónico parecen legítimos, con logotipos bancarios tan realistas, pidiendo que contesten con números de cuentas y contraseñas y demás información personal, los bancos nunca piden información de esta manera y en cuestión de segundo los delincuentes vacían las cuentas.

Estos son algunos tipos de fraude más comunes que está ocurriendo actualmente; muchas veces cuando las entidades financieras tienen un departamento con gente

especializada, y cuentan con la ayuda de la policía nacional, logran la captura de estas bandas, pero esto no basta ya que en el proceso penal no se logra un mayor avance y el proceso se estanca, esto ocurre por falta de una denuncia puesta por los clientes o falta de información, los mismos quienes ayudarían con esta acción disminuir el fraude y evitar que les vuelva a ocurrir.

Los bancos no pueden intervenir en este tipo de proceso ya que no son las victimas afectadas directamente, pero tienen estudiado el modo de operar (modus operandi) de dichas bandas y de estas personas que viven día a día del fraude.

1.4. Delimitación del problema

El problema se lo delimita en espacio y tiempo; así, en espacio, la investigación se concentra en el Ecuador en la Ciudad de Guayaquil, al sector específico de los cuenta ahorristas y corrientitas; mientras que en tiempo, la investigación se circunscribe en el período 2009-2014.

1.5. Justificación de la investigación

La presente investigación se sustenta en un estudio práctico, teórico y metodológico.

La justificación teórica y práctica van concatenadas, puesto que si bien la teoría sostuvo que la implementación del Código Orgánico Integral Penal (COIP) ayudaría a penalizar casos de fraudes y robos electrónicos en realidad y en la práctica el (COIP) tipifica al delito como tal que es la intercepción ilegal de datos mas no hace referencia al modo de fraude como los que está ocurriendo actualmente o como los casos antes mencionados, y es precisamente porque

también tenemos una ley ambigua como lo es la ley de Comercio Electrónico, la cual necesita una reforma en sus artículos y una implementación más precisa donde se tome como referencia estos actos de fraude descritos ampliamente para que así exista una armonía de la Ley de Comercio Electrónico con el Código Orgánico Integral Penal para mejor interpretación de la ley por parte del legislador.

La investigación presenta una justificación metodológica, puesto que se realizará un análisis con observación científica y visitas de campo, donde las encuestas y las entrevistas serán de vital importancia, la tabulación de datos ayudará a formalizar resultados mediante cuadros y gráficos en matrices.

Estadísticas

Como parte fundamental de esta investigación consideramos los porcentajes de casos y reclamos presentados en el Banco Bolivariano en el periodo de tiempo del año 2009 al 2014 y denuncias receptadas en la fiscalía del Guayas por fraude electrónico que ha sufrido la población en estos seis años.

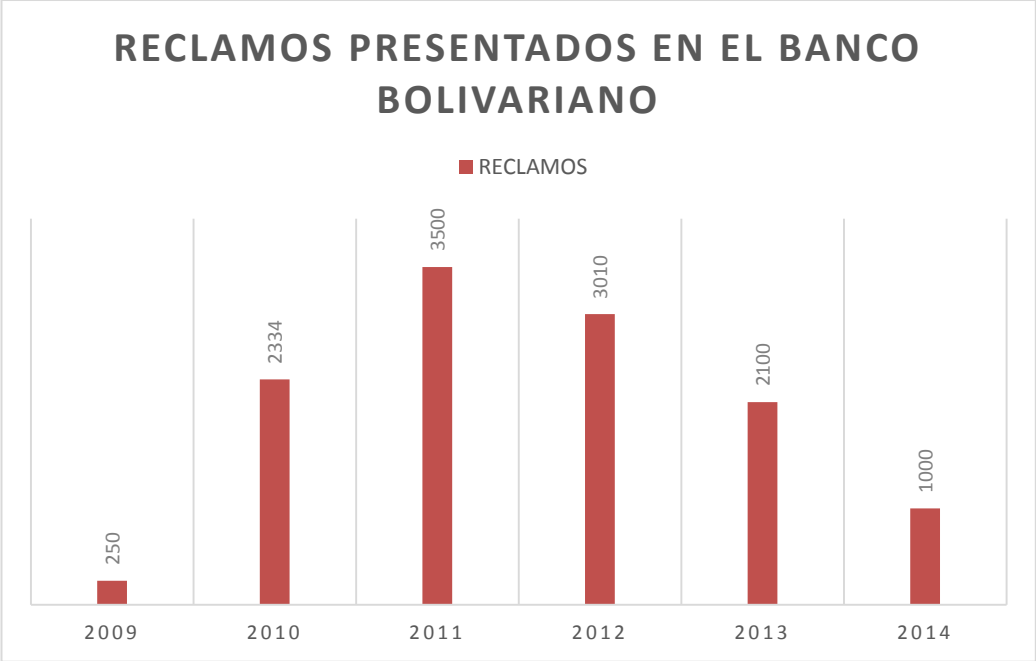
Grafico 1.- Datos emitidos por la Fiscalía del Guayas

Fuente: Fiscalía de Guayaquil

Elaborado por: Autora

Como podemos observar la gráfica en el año 2009 eran muy pocas las denuncias presentadas en la fiscalía por parte de los usuarios pero la tendencia se iba incrementando con el pasar de los años y en el 2011 el fraude electrónico aumento se disparó hasta alcanzar las 3129 denuncias de las cuales se presentaron 50 denuncias grupales por retiro de dinero con clonación de tarjetas, es decir en este año el skiming estuvo en todo su apogeo, en los años 2012 y 2013 se mantenía el fraude electrónico de diferentes tipos pero con las resoluciones y medidas tomadas por la Superintendencia de Bancos y Seguros y las alertas de prevención de todas las instrucciones financieras en el año 2014 las denuncias bajaron a 877 casos.

Grafico 2.- Estadísticas general de los reclamos presentados en el Banco Bolivariano



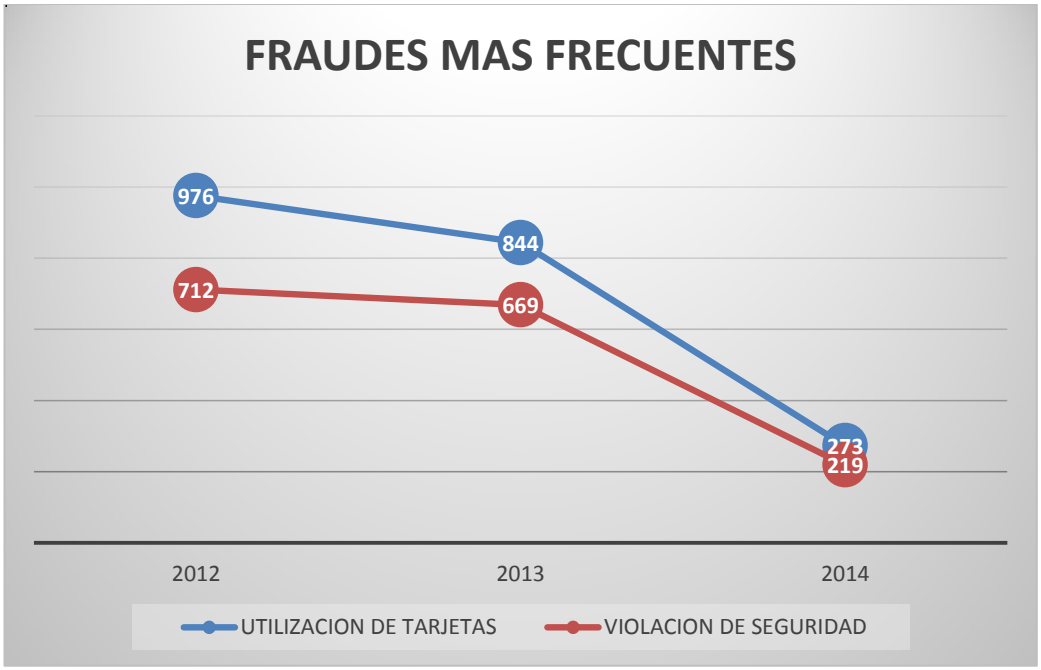
Fuente: Banco Bolivariano

Elaborado por: Autora

De acorde con los datos entregados por esta institución financiera los reclamos que ellos atendieron son en cantidades mayores a las denuncias que se presentaron en la fiscalía pero coinciden en los años de mayor incidencia del fraude electrónico.

Según Andrés Otero, de la compañía multinacional Kroll, que asesora en los procesos de investigación por este tipo de delito, en Ecuador el nivel de fraude con tarjetas llega al 0,25% del total de transacciones bancarias. Es un nivel de incidencia bajo respecto del volumen total de operaciones.

Grafico 3.- Tipos de Fraudes electrónicos más frecuentes en la ciudad de Guayaquil



Fuente: Banco Bolivariano

Elaborado por: Autora

En la gráfica tres tenemos los fraudes más comunes y frecuentes entre estos están la utilización de tarjetas y la violación de la seguridad del sistema financiero, tomamos solo como muestra los tres últimos años del 2012 al 2014, al igual que la gráfica 1 el fraude se mantiene en estos años pero en el 2014 seguimos viendo un resultado favorable que desciende y baja las cifras por completo.

Según los datos proporcionados por la Fiscalía del Guayas son pocos los casos que llegan a una sentencia definitiva, la mayoría de los usuarios desisten de sus demandas por que no ven una salida favorables para ellos, ya que la fiscalía es un

ente regulador pero su función principal es de investigar e indagar el cometimiento del delito, el mismo que es comprobable se sigue un proceso penal.

Grafico 4.- Reporte de los delitos informáticos en el año 2010

REPORTE NACIONAL DE LOS DELITOS INFORMATICOS DE ENERO A NOVIEMBRE DEL 2010										
DELITO	NOTICIA DEL DELITO	INDAGACIÓN PREVIA	INSTRUCCIONES	DICTÁMENES			SENTENCIAS			DESESTIMACIONES
				ACUSATORIOS	ABSTENTIVOS	MIXTOS	CONDENATORIAS	ABSOLUTORIAS	MIXTAS	
APROPIACIÓN ILÍCITA UTILIZANDO MEDIOS INFORMÁTICOS	903	881	31	29	3		4	2	1	146
FALSIFICACIÓN ELECTRÓNICA	60	50	4	1		1				10
DANOS INFORMÁTICOS DE SERVICIO PUBLICO	87	89	2		1					2
DANOS INFORMÁTICOS DE SERVICIO PRIVADO	82	81								4
ESTAFA UTILIZANDO MEDIOS INFORMÁTICO	1									
TOTAL NACIONAL	1133	1101	37	30	4	1	4	2	1	162

Fuente: Fiscalía de Guayaquil

Elaborado por: Autora

Según datos de la Fiscalía el total de delitos electrónicos podría llegar al millón de dólares en el primer semestre del 2011, manifestando que en el 2009 se reportaron 168 casos de este tipo de fraudes, en el 2010 los casos ascendieron a 1099 y en el primer semestre (enero a junio) se reportaron 1360 denuncias, lo que nos demuestra que esta modalidad de fraudes va en aumento. Como se puede observar todos estos datos estadísticos son motivos para la justificación de esta investigación para desarrollar un estudio de las tendencias y las falencias que existen.

1.6. Sistematización de la investigación

Los casos de suplantación de identidad de los usuarios, son mínimos en comparación de los casos de fraude en tarjetas de crédito o de débito, sin embargo, es necesario analizarlos puesto que hacen perder credibilidad no sólo a la institución financiera, sino también al Organismo de Control que las regula como la Superintendencia de Bancos y Seguros que no adopta acciones concretas de estos casos. Es por eso, que la sistematización de la investigación ayudará a obtener datos reales en espacio y tiempo, gracias a la ayuda de entrevistas a funcionarios de entidades financieras, y encuestas al público en general, con estas visitas de campo ayudarán a obtener información real al tema abordado.

1.7. Objetivos Generales de la investigación

Unos de los objetivos principales es analizar los diferentes tipos de fraude, mencionados anteriormente en el planteamiento del problema a investigar, y como se fue incrementando con el transcurso de los años en nuestro país específicamente en la ciudad de Guayaquil, analizando el comportamiento de la población con respecto al manejo del llamado dinero electrónico, la utilización de cajeros automáticos, tarjetas de débito y crédito, entre otros medios utilizados actualmente.

Definir cada uno de ellos e incorporarlos en la reforma que se propone en la ley de Comercio Electrónico con el fin de alcanzar una mejor interpretación de la ley al momento de juzgar estos tipos de delitos.

1.8 Objetivos específicos de la investigación

- Conceptualización de los tipos de fraudes más comunes y de los que han afectado más a la población financiera como tarjetas habientes, cuentas corrientitas y cuentas ahorristas.
- Comprobar las medidas de seguridad tomadas por parte de las instituciones financieras para evitar los fraudes electrónicos por parte de bandas delictivas y la capacitación que tienen los clientes para tomar conciencia del cuidado que deben tener con respecto a estos tipos de delitos que se están presentando actualmente.

1.9 Limites de la investigación

Se puede considerar como limite la falta de conocimiento y de capacitación que tiene los usuarios del sistema financiero con respecto al manejo y uso de dispositivos electrónicos como cajeros automáticos, cajeros multifuncionales, transferencias online, todas estas faltas muchas veces son causas a que hackers y líderes de bandas delictivas consigan infiltrar información por medio de correos electrónicos donde solicitaban información personal o por medio de cualquier otro método.

Otra de las limitaciones que existía, es la falta de una plataforma de seguridad informática en los sistemas de las diferentes entidades financieras, que hoy en día gracias a la autenticación de datos permite comprobar si es el usuario titular de la tarjeta o de la cuenta quien está realizando dicha transacción, situación que años atrás no existía y que con el pasar del tiempo se han ido modificando hasta alcanzar en la actualidad una plataforma de seguridad confiable para los clientes

pero al mismo tiempo compleja para aquellos usuarios que no tienen el conocimiento suficiente en el manejo de la tecnología, específicamente el sector de adultos mayores quienes son los usuarios más vulnerables al fraude electrónico.

1.10 Identificación de variables

Entre las variables que se determinan para este tipo de investigación se encuentra:

1.10.1 Variable Independiente

- Análisis del sistema financiero del Ecuador

1.10.2. Variable Dependiente

- La tendencia del fraude electrónico en los usuarios de la banca privada.
-

1.11 Hipótesis

Hipótesis General

El 60% de los usuarios de la banca privada, que realizan transacciones por medio de cajeros automáticos son víctimas de fraude electrónico por la falta de normativa clara sobre la conceptualización del delito y sus repercusiones tanto al sistema financiero como en el usuario.

1.12 Operacionalizaciòn de las variables

Tabla 1

VARIABLES	DESCRIPCION	INDICADORES
Independiente	Análisis del sistema financiero del Ecuador	• Perdidas económicas • Organismos de Control
Dependiente	Tendencia del fraude electrónico a los usuarios	• Usuarios – Banca Privada • Falta de normativa

Fuente: Resultados de la investigación

Elaborado por: Autora

CAPÍTULO II

MARCO TEORICO

2.1. Antecedentes referenciales de investigación

La Asociación de Bancos Privados del Ecuador desea conocer si en los países se ha tipificado como delito, conductas como las antes descritas o cualquier otra que pudiera afectar a los usuarios de los canales transaccionales electrónicos (Internet, Banca Celular o Móvil, ATM, etc.) de la Banca.

A continuación encontraremos una comparación con otros países de Latinoamérica sobre las leyes que se han tipificado e incorporado en su legislación sobre este tipo de delitos electrónicos y de qué forma se sanciona el fraude con sus respectivas penas para tomar como antecedente o referencia al estudio de esta investigación.

Argentina

En Argentina, el 4.6.08 se sancionó la Ley 26.388 modificatoria del Código Penal Argentino, por medio de la cual se incorporan a dicho cuerpo normativo los delitos informáticos. Es preciso mencionar que la legislación Argentina, como en el resto del mundo, es mucho más lenta que el avance tecnológico, motivo por el cual no se tipificaron expresamente las figuras delictivas expuestas en la consulta.

Sin embargo, en Argentina para dichas conductas se aplican, de forma análoga si se permite el término, la figura del fraude, estafa que se encuentran tipificadas en el Código Penal. Asimismo, en el Congreso de la Nación se encuentran bajo

estudio proyectos de Ley abordando el tema, con el objeto de que expresamente dichas figuras se incorporen en el mencionado cuerpo normativo.

Bolivia

En Bolivia aún no se han tipificado los delitos a través de medios electrónicos

Brasil

En Brasil el asunto es objeto de un Proyecto de Ley del año 1999, todavía analizado y aprobado por el Congreso de los Diputados y por el Senado Federal. Mientras tanto, los textos aprobados en cada una de las Cámaras es distinto, lo que puede significar una ampliación del tiempo de análisis y consecuente aprobación y firma del texto final.

Colombia

En Colombia, el enero 5 fue publicada la ley 1273 de 2009, "por medio de la cual se modificó el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos".

El nuevo título del Código Penal (Título VII Bis) está compuesto por dos capítulos, de la siguiente manera:

Capítulo I De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos

Capítulo II De los atentados informáticos y otras infracciones

En el capítulo I se tipifican los siguientes delitos:

Acceso abusivo a un sistema informático.

Obstaculización ilegítima de sistema informático o red de telecomunicación.

Interceptación de datos informáticos.

Daño Informático.

Uso de software malicioso

Violación de datos personales.

Suplantación de sitios web para capturar datos personales

Adicionalmente, se prevén una serie de circunstancias de agravación punitiva para los mencionados tipos penales.

Por su parte, el capítulo II tipifica una nueva modalidad de hurto (Hurto por medios informáticos y semejantes) y tipifica la "Transferencia no consentida de activos".

Finalmente, la ley 1273 de 2009, añade una nueva circunstancia de mayor punibilidad para todos los delitos, que se aplica "cuando para la realización de las conductas punibles se utilicen medios informáticos, electrónicos o telemáticos"

Costa Rica

En el caso de Costa Rica, el Código Penal, contiene dos disposiciones que regulan y sancionan los delitos informáticos. Ellos son:

Artículo 217-bis.- Fraude informático

Se impondrá pena de prisión de uno a diez años a la persona que, con la intención de procurar u obtener un beneficio patrimonial para sí o para un tercero, influya en el procesamiento o el resultado de los datos de un sistema de cómputo, mediante

programación, empleo de datos falsos o incompletos, uso indebido de datos o cualquier otra acción que incida en el proceso de los datos del sistema.

Artículo 229-bis.- Alteración de datos y sabotaje informático

Se impondrá pena de prisión de uno a cuatro años a la persona que por cualquier medio acceda, borre, suprima, modifique o inutilice sin autorización los datos registrados en una computadora.

Si como resultado de las conductas indicadas se entorpece o inutiliza el funcionamiento de un programa de cómputo, una base de datos o un sistema informático, la pena será de tres a seis años de prisión. Si el programa de cómputo, la base de datos o el sistema informático contiene datos de carácter público, se impondrá pena de prisión hasta de ocho años.

Asimismo, en la Asamblea Legislativa se han presentado varias reformas al Código Penal, para establecer una regulación más estricta en contra de este tipo de delitos.

La Sala Primera de la Corte Suprema de Justicia ha establecido que existe responsabilidad objetiva por parte de los bancos, con base en el artículo 35 de la Ley de Promoción Efectiva de la Competencia y Defensa del Consumidor. Aplicando la teoría del riesgo, la cual, postula que quien crea, ejerza, o se aproveche de una actividad lucrativa lícita que presenta elementos potencialmente peligrosos para los demás debe soportar sus inconvenientes.

El Salvador

Para el caso de El Salvador, esas conductas tampoco se han tipificado expresamente.

Guatemala

En Guatemala, no existe ninguna ley que regule tales actividades, sin embargo, existe un proyecto de ley que busca regular acciones tales como el pishing, proyecto que está actualmente en discusión en el Congreso de la República, y del cual la Asociación Bancaria de Guatemala participa de su análisis.

México

En México, el 26 de junio de 2008 se publicó una reforma a la Ley de Instituciones de Crédito, Ley General de Títulos y Operaciones de Crédito, Código Penal Federal y Código Federal de Procedimientos Penales, a fin de tipificar y sancionar diversas conductas relacionadas con el uso indebido de instrumentos de pago de bienes y servicios como son las tarjetas de crédito, de débito o cheques. Dentro de las conductas sancionadas se encuentran:

• La alteración, copia o reproducción de la banda magnética o el medio de identificación electrónica, óptica o de cualquier otra tecnología de los instrumentos de pago.

• La posesión, adquisición, utilización o comercialización de equipos o medios electrónicos, ópticos o de cualquier otra tecnología para sustraer, copiar o

reproducir información contenida en los diversos instrumentos, con el propósito de obtener recursos económicos, información confidencial o reservada.

• El acceder, sin causa legítima o sin consentimiento de quien esté facultado para ello, a los equipos o medios electrónicos, ópticos o de cualquier otra tecnología del sistema bancario mexicano, para obtener recursos económicos, información confidencial o reservada y;

• El alterar o modificar el mecanismo de funcionamiento de los equipos o medios electrónicos, ópticos o de cualquier otra tecnología para la disposición de efectivo de los usuarios del sistema bancario mexicano, para obtener recursos económicos, información confidencial o reservada.

Las sanciones a aplicarse van de los tres a los nueve años de prisión y de treinta mil a trescientos mil días multa. Tales sanciones podrán aumentarse hasta en una mitad más, si la persona que cometió el delito es consejero, funcionario, empleado o prestador de servicios de cualquier institución de crédito.

Nicaragua

En Nicaragua no se cuenta con leyes específicas al respecto.

Panamá

1. Sí, 4 artículos del Código Penal de Panamá (Ley 14 de 2007) tienen como bien jurídico protegido la seguridad informática o la seguridad jurídica de los Medios Electrónicos.

2. Los Artículos 283 y 284 del Título VIII del Código tipifican como conductas punibles el ingreso no autorizado a base de datos y el apoderamiento o modificación de los datos. Las penas pueden ser de hasta 4 años.

3. Los Artículos siguientes (285 y 286) agravan las penas por la naturaleza de la persona jurídica depositaria de la información (Bancos, aseguradoras, casas de bolsa, empresas de servicio público, Estado) o por las funciones que correspondían al ofensor.

Paraguay

Ver el Proyecto de Ley que está estudiando el Congreso Nacional y que es lo único que se tiene con relación al tema.

Perú

En el Perú no se han tipificado como delitos, las conductas ("pishing", "loop libanes", "skimming", etc.; sin embargo, existen en el Capítulo X, tres artículos, el 207 A, 207 B y 207 C del Código Penal, referidos a delitos informáticos en general.

Asimismo, existe un Proyecto de Ley promovido por el Programa Integral de Seguridad Bancaria de ASBANC (PISB) para discusión en la Comisión de Justicia del Congreso de la República, que trata sobre la incorporación de tales delitos dentro del Código Penal del país.

República Dominicana

En República Dominicana no están tipificados los delitos cometidos a través de los canales electrónicos, aunque se cuenta con la ley de Comercio Electrónico No.126-02, la misma no trata sobre los delitos realizados por dichos medios.

Uruguay

En Uruguay resultan aplicables las normas del Código Penal, no existiendo normativa especial con respecto a las novedosas figuras delictivas que se mencionan. A título de ejemplo, la reciente Ley Nº 18.600, por la que se reconoce la admisibilidad, validez y eficacia jurídicas del documento electrónico y de la firma electrónica al describir actitudes ilícitas, remite para la tipificación delictiva al mencionado Código (Arts. 236 a 245).

Como podemos observar en algunos de estos países no existe una ley que regule este tipo de delitos la mayoría son proyectos de ley que aún están en estudios pero que no son concretados.

A medida que se incremente el fraude y la población siga siendo afectada por este tipo de situaciones los legisladores se verán obligados a contemplar una ley con carácter de urgente ya sea estos delitos se incorporen a un Código Penal ya existente o que se promulgue una nueva ley.

2.2 Marco Teórico Referencial

En relación a los aspectos teóricos la investigación corresponde al estudio de algunos autores que han analizado e investigado sobre el tema con relación al fraude electrónico y al Derecho Informático y algunos antecedentes que se han dado con el pasar del tiempo.

¿Qué es el derecho informático?

El Derecho Informático se lo ha catalogado como una rama autónoma del Derecho que abarca el estudio de la doctrina legislativa y jurisprudencia relativas al control y regulación de la informática y sus derivados en su expansión y desarrollo y a la aplicación idónea de las herramientas informáticas.

1|Para Emilio Suñé Linas, "Derecho de la Informática es el conjunto de normas reguladoras del objeto informática o de problemas directamente relacionados con la misma….el Derecho Informático, al que la mayoría de los autores asimilan sin más con el Derecho de la Informática, es la disciplina que engloba, a la Informática Jurídica y al propio Derecho de la Informática".

El fraude electrónico se va generando con el progreso tecnológico que ha experimentado la sociedad, supone una evolución en las formas de infringir la ley.

> 2| Julio Téllez Valdés conceptualiza al delito informático en forma típica y atípica, entendiendo que en la forma típica son "las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como

instrumento o fin" y la forma atípica "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin".

3| El Convenio de Cyber-delincuencia del Consejo de Europa, define a los delitos informáticos como "los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas redes y datos" Conviene destacar entonces, que diferentes autores y organismos han manifestado diferentes apreciaciones para señalar las conductas ilícitas en las que se utiliza la computadora, esto es "delitos informáticos", "delitos electrónicos", "delitos relacionados con la computadora", "crímenes por computadora", "delincuencia relacionada con el computador".

Tal como podemos notar en las definiciones establecidas por autores anteriores, no existe una definición de carácter universal propia de delito informático. Es preciso señalar que la última definición brindada por el Convenio de Cyber-delincuencia del Consejo de Europa anota especial cuidado en los pilares de la seguridad de la información: la confidencialidad, integridad y disponibilidad. El delito informático involucra acciones criminales que en primera instancia los países han tratado de poner en figuras delictivas típicas, tales como: robo, fraudes, falsificaciones, estafa, sabotaje, entre otros, por ello, es primordial mencionar que el uso indebido de las computadoras es lo que ha creado la necesidad imperante de establecer regulaciones por parte de la legislación.

A continuación podemos ver un antecedente y los diferentes medios utilizados para cometer fraude electrónico

> En 1996 un hacker se hizo pasar por técnico de una compañía y envió mensajes haciendo uso de la ingeniería social en los que solicitaba que el usuario verificase su cuenta o confirmase una factura y así poder solicitar las credenciales personales de la víctima. Con estos datos ya podía realizar acciones como el envío de spam. Para intentar solucionarlo, la compañía incluyó como texto *by default* en el intercambio de mensajes: "XYZ nunca le solicitará contraseñas o información de facturación".

Este es un claro ejemplo de cómo funciona el phsing y de cómo los hackers utilizan sus mañas para que por medio de engaños y con la imagen de una entidad o de una compañía falsa o fantasma, se entregue información personal y relevante para cometer fraude o estafa a nivel financiero.

Los diferentes medios y técnicas que se usaron a partir de entonces se enfocan hacia intentos de fraude como:

- Correos electrónicos
- Mensajería instantánea
- Sitios web
- Buscadores
- Redes sociales
- Mensajes en foros/chats
- Plataformas de juegos online
- Falsos antivirus
- Teléfonos móviles

El objetivo de estas mafias es la búsqueda de usuarios y los datos de sus cuentas bancarias. Entrando en las redes sociales como Facebook o Twitter. Los usuarios y las entidades deben tener una actitud responsable y utilizar medidas de protección. Se debe concienciar y educar al ciudadano para estar alerta y evitar que sus datos personales y bancarios sean vulnerados o sustraídos.

1.- Suñé Llinás Emilio.- Tratado de Derecho Informático, Volumen I, Pag, 1 y 2
2.-Julio Téllez Valdés- Derecho Informático- Biblioteca Jurídica Virtual - biblio.juridicas.unam.mx
3.- Convenio de Ciberdelicuencia del Consejo de Europa - www.agpd.es

2.3 Marco Legal

Para profundizar en el estudio del marco legal de esta investigación haremos mención de algunas leyes que existen en el Ecuador sobre el fraude electrónico tales como:

1. Constitución de la República del Ecuador
2. Ley de Comercio Electrónico, firmas electrónicas y mensajes de datos
3. Código Orgánico Integral Penal (COIP)
4. Tratados Internacionales
5. Resolución de la Superintendencia de Banco

2.3.1. Constitución de la República del Ecuador

Art. 92.- Toda persona, por sus propios derechos o como representante legitimado para el efecto, tendrá derecho a conocer de la existencia y a acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, en soporte material o electrónico. Asimismo tendrá derecho a conocer el uso que se haga de ellos, su finalidad, el origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos. Las personas responsables de los bancos o archivos de datos personales podrán difundir la información archivada con autorización de su titular o de la ley. La persona titular de los datos podrá

solicitar al responsable el acceso sin costo al archivo, así como la actualización de los datos, su rectificación, eliminación o anulación. En el caso de datos sensibles, cuyo archivo deberá estar autorizado por la ley o por la persona titular, se exigirá la adopción de las medidas de seguridad necesarias. Si no se atendiera su solicitud, ésta podrá acudir a la jueza o juez. La persona afectada podrá demandar por los perjuicios ocasionados.

Con el análisis de la Constitución del Ecuador en su Art. 92 hace referencia sobre el acceso a la Información pública que es un derecho que tenemos todos los ciudadanos de este país debidamente tipificado en la ley, pero así mismo se debe conocer cuál es el uso y la finalidad que tendrá dicha información, las instituciones públicas o privadas deberán proporcionar la información solicitada debidamente autorizada por un juez o por la autoridad competente en caso que resistencia la persona puede demandar por perjuicios ya que no se puede negar ni ocultar ninguna información de carácter público como lo indica el Art.92 en mención.

Art.92.- Constitución Política de la República del Ecuador – Sección V- Acción de habeas data

2.3.2. Ley de Comercio Electrónico, Firmas Electrónicas y mensaje de datos

La ley de Comercio electrónico fue publicada oficialmente en el año 2002 bajo el No. 2002-67. Esta ley se divide en cinco títulos con disposiciones generales, transitorias y finales y un glosario de términos para la mejor compresión del significado de algunos términos empleados en esta ley.

Titulo I.- De los mensajes de Datos

Título II.- De las Firmas Electrónicas, Certificados de firma electrónica, entidades de certificación de información, organismos de promoción de los servicios electrónicos, y de regulación y control de las entidades de certificación acreditadas.

Título III.- De los servicios electrónicos, la contratación electrónica y telemática, los derechos de los usuarios e instrumentos públicos.

Título IV.- De la prueba y notificaciones electrónicas.

Titulo V.- De las Infracciones informáticas.

En las disposición derogativa novena del COIP manifiesta Deróguese el Título V, desde el artículo 57 al artículo 64, de la Ley de Comercio Electrónico, Firmas y Mensaje de Datos publicada en e1 Suplemento del Registro Oficial No. 557 de 77 de abril de 2OO2. Entonces la entrada en vigencia del Código Orgánico Integral Penal quedaría eliminado el título de las DE LAS INFRACCIONES INFORMÁTICAS.

2.3.3. Código Orgánico Integral Pena (COIP)

El Código Orgánico Integral Penal publicado en el Registro Oficial Suplemento N° 180 el 10 de Febrero de 2014.

Sección tercera.- delitos contra la seguridad de los Activos de los sistemas de información y comunicación. De los Arts. 229 hasta el 234 nos hace mención sobre:

- Revelación ilegal de base de datos
- Interpretación ilegal de datos
- Transferencia Electrónica de activo patrimonial
- Ataque a la integridad de sistemas informáticos
- Delitos contra la información pública reservada legalmente
- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.

En estos artículos hace mención a las penas y al tipo penal como tal, mas no hace referencia a la forma de cometer el delito ni los medios que se utilizan para llegar a delinquir en este tipo de fraudes, es por ese motivo que se estudia esta ley para hacer una comparación más exacta y exhaustiva de las modificaciones que se implementaron en este nuevo código, para sancionar y penalizar de una forma más adecuada y con severidad de todo el peso de la ley.

Tabla 2.- Delitos incluidos en el nuevo Código Orgánico Integral Penal

DELITOS INCLUIDOS EN EL CODIGO ORGANICO INTEGRAL PENAL		
TIPO PENAL	**ARTICULO COIP**	**SANCION**
Revelación ilegal de bases de datos	**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.	1 a 3 años
Interceptación Ilegal de datos	**Artículo 230**.- 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,	3 a 5 años

	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.	
Transferencia electrónica de activo patrimonial	**Artículo 231.-** 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.	3 a 5 año
Ataque a la integridad de sistemas informáticos	**Artículo 232**.- .- La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años. Con igual pena será sancionada la persona que: 1. Diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados a causar los efectos señalados en el primer inciso de este artículo. 2. Destruya o altere sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general. Si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana, la pena será de cinco a siete años de privación de libertad.	3 a 5 años 5 a 7 años

Delitos contra la información pública reservada legalmente	**Artículo 233.-** La persona que destruya o inutilice información clasificada de conformidad con la Ley, será sancionada con pena privativa de libertad de cinco a siete años. La o el servidor público que, utilizando cualquier medio electrónico o informático, obtenga este tipo de información, será sancionado con pena privativa de libertad de tres a cinco años. Cuando se trate de información reservada, cuya revelación pueda comprometer gravemente la seguridad del Estado, la o el servidor público encargado de la custodia o utilización legítima de la información que sin la autorización correspondiente revele dicha información, será sancionado con pena privativa de libertad de siete a diez años y la inhabilitación para ejercer un cargo o función pública por seis meses, siempre que no se configure otra infracción de mayor gravedad.	5 a 7 años
Acceso no consentido a un sistema informático, telemático o de telecomunicaciones	**Artículo 234**.- La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años.	3 a 5 años

Fuente.- Código Orgánico Integral Penal

Elaborado por Autora

2.3.4. Tratados Internacionales

En 1990 la Organización de las Naciones Unidas (ONU) en el Octavo Congreso sobre Prevención del Delito y Justicia Penal, celebrado en La Habana,
Cuba, se dijo que la delincuencia relacionada con la informática era consecuencia del mayor empleo del proceso de datos en las economías y burocracias de los distintos países y que por ello se había difundido la comisión de actos delictivos.
En 1992 elaboró un conjunto de normas para la seguridad de los sistemas de información, con intención de ofrecer las bases para que los Estados y el sector privado pudieran erigir un marco de seguridad para los sistemas informáticos.

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

Hay otros Convenios no ratificados aún por nuestro País, realizados por la Organización Mundial de la Propiedad Intelectual (OMPI), de la que nuestro país es parte integrante a partir del 8/10/1980.

En el Ecuador se han suscrito varios convenios internacionales de protección de datos así tenemos:

- Convenio de la Unión Internacional de Telecomunicaciones
- Acuerdo Relativo a la Organización Internacional de Telecomunicaciones por Satélite INTELSAT;
- Convenio de Acción de Sistemas Informáticos Nacionales
- Acuerdo Relativo a la Organización Andina de Telecomunicaciones por Satélite OATS.

2.3.5. Resolución de la Superintendencia de Bancos y Seguros

Resolución JB-2012-2148- Junta Bancaria del Ecuador

Como resultados a la evidente tendencia de fraude a los que han sido víctimas los clientes de la banca en estos últimos cinco años, la Junta Bancaria del Ecuador junto a la Superintendencia de Bancos y Seguros emitieron la Resolución JB-2012-2148 en donde se resuelve efectuar algunos cambios e implementar medidas de seguridad en la Ley General de Instituciones del Sistema Financiero como:

ARTÍCULO 1.- En el capítulo I "Apertura y cierre de oficinas en el país y en el exterior, delas 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 (Antimalware) 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;”

Las medidas de seguridad que se incluyeron en los canales electrónicos es establecer mecanismos de monitoreo en cajeros automáticos en donde las bandas delictivas hacen de estos el uso más frecuente.

La información que transmita el canal electrónico deberá estar en todo momento protegida usando técnicas de encriptación para claves, cifras, etc. Esto conlleva a la implementación de una buena plataforma de seguridad donde al principio a la mayoría de los clientes se les dificulte su uso.

Se tomaron medidas de restricciones en los montos máximos con los que los clientes pueden transaccionar como en consumos nacionales, consumos en el exterior, compras por internet, entre otros, manteniendo siempre informado al cliente de todo movimiento realizado ya sea vía móvil o vía correo electrónico.

En esta misma resolución se dispuso sobre las tarjetas de crédito y de débito que emiten las instituciones financieras, estas deberán ser tarjetas inteligentes es decir tarjetas con microprocesador o chip, ya que las tarjetas comunes con bandas magnéticas son de fácil clonación. Esta medida tuvo un periodo considerable para que la banca genere y entregue a todos sus clientes nuevas tarjetas con chip y para que realice cambios en todos sus dispositivos como cajeros automáticos y POS que sean aptos de leer este tipo de tarjetas, el plazo asignado para este proceso según la SBS vence a final de este año 2015.Con estas medidas se espera que el fraude disminuya en un 90%, no a totalidad ya que estos delincuentes siempre encontraran la forma de cometer fraude a toda hora. Esta resolución presentada por la Superintendencia de Bancos y Seguros tiene un tiempo de implementación que da a todas las entidades bancarias del Ecuador para proceder con el cambio de las tarjetas con bandas magnéticas a tarjetas inteligentes, a continuación se detalla en una tabla las fases de migración de estas tarjetas.

Tabla 3.- Tiempo de Migración de las tarjetas

	FASE DE MIGRACION DE TARJETA CON BANDAS MAGNETICAS A TARJETAS INTELIGENTES	
FASE	**DESCRIPCION**	**TIEMPO(MESES)**
0	Diagnóstico inicial de la entidad para implementar Tarjetas con Chip	6
1	Implementar adecuaciones para operar con tarjetas inteligentes en	12
	Cajeros Automáticos	
	Adquirencias	
	Tarjetas de Crédito	
	Tarjetas de Debito	
2	Entrega de Tarjetas con Chip	18

Fuente.- Superintendencia de Bancos y Seguros

Elaborado por: Autora

Este es un cambio que tienen que implementar dispositivos en cajeros automáticos, y a los diferentes comercios donde se utilizan el dinero electrónico. Este es un cambio que genera un gran gasto para los bancos pero así mismo tenemos que ver los resultados a futuro después de la implementación de estas tarjetas, dejaran de tener grandes pérdidas económicas.

2.4 Marco Conceptual

¿Cómo se genera el fraude electrónico?

En la actualidad en pleno siglo XXI mas del 90% de la población utiliza el internet como medio facilitador, ya que nos ofrece una gran ayuda y de la forma más sencilla a realizar compras, transferencias, pagos de servicios básicos entre otros, que nos ahorra mucho tiempo y nos evita largas filas en los bancos, trafico, etc.

Las bandas delictivas siempre están al acecho de cualquier oportunidad para hacer de las suyas, y el campo de la informática es el más vulnerado ya que está al alcance de todo el mundo. Al momento de utilizar una tarjeta de crédito, de débito o de contestar un correo electrónico estamos expuestos a que estos maleantes sustraigan datos de nuestra información bancaria como claves, saldos, usuarios, entre otros, tan solo con un dispositivo o por medio de engaños. El fraude electrónico ha crecido tanto que estas bandas delictivas viven del dinero que obtienen de una forma ilegal y en otras ocasiones intercambian, venden o compran información al mejor postor y es así como se expande el fraude cada día más en nuestro país y en otros lugares del mundo.

¿Qué roban al clonar las tarjetas?

Como se menciona anteriormente lo que buscan es la información tales como números de tarjetas de créditos que permiten a los delincuentes realizar cargos a nuestro nombre, no solo para adquirir mercancías o realizar consumos, sino

también para suplantar nuestra identidad a la hora de registrarse en algún sitio u organización.

Buscan obtener acceso al sistema de la banca electrónica tales como usuarios y contraseñas, algunos bancos ya han tomado medidas al respecto utilizando los famosos tokens o implementando una plataforma de seguridad donde se solicita digitar los últimos cuatro dígitos de su número de cedula para mayor seguridad a la hora de transaccionar en los cajeros automáticos, también se implementó preguntas de seguridad con información personal que solo el titular de la cuenta conoce y pueda lograr identificarse en la banca virtual.

¿Cómo se obtiene la información de las tarjetas?

Lamentablemente, los atacantes tienen una amplia gama de opciones para obtener información. Se valen de engaños (phishing, pharming), espían nuestras actividades diarias y, en algunos casos incluso nos atacan directamente (gusanos, virus).

Manipulan los cajeros automáticos insertando cámaras lectoras diminutas de claves y copian las bandas magnéticas de las tarjetas para posteriormente sacar el dinero con tarjetas falsas, representa más del 70% de fraude de ATM. El skimmer, es un dispositivo hecho para colocarse en la boca de un cajero automático y secretamente sacar la información de tarjeta de crédito y débito cuando los clientes deslizan sus tarjetas en las máquinas para sacar dinero.

PROCESO DEL SKIMING

En el skiming podemos encontrar cuatro fases fundamentales que consiste en el proceso utilizado por delincuentes para clonar las tarjetas en los cajeros automáticos, como lo habíamos mencionado anteriormente utilizan pequeñas cámaras que son instaladas sin que los usuarios se dieran cuenta cómo lo podemos observar en las gráficas más explicitas que se adjunta en los anexos.

1. **Instalación Fraudulenta**
2. **Ingreso del cliente al cajero automático**
3. **Copia de la Clave**
4. **Clonación de la Banda Magnética**

PROCESO DEL PHISHING

Cuando hablamos del Phishing intervienen los famosos Hackers que son los encargados de enviar un sin número de correos electrónicos engañando al usuario para que le proporcione información de sus cuentas bancarias con una falsa imagen, dicha información puede ser vendida a otras bandas delictivas o utilizadas por los mismos Hackers para obtener ganancias. Este proceso de Phising se puede observar de una manera más explícita en la gráfica que se adjunta en los anexos.

ROBO O SUPLANTACION DE IDENTIDAD

El robo de identidad es un delito que comete una persona que suplanta a otra valiéndose de documentación o datos personales de un tercero para operar

bancariamente, o de documentación falsa para comprar bienes o contratar servicios y cargárselos a la cuenta de quién es sustituido.

Decimos que es un delito porque se trata de una conducta delictual que engloba varias figuras penales: defraudación, falsificación de documento entre otros.

En muchos casos esto sucede cuando una persona pierde su cedula de identidad o es robada y no pone la respectiva denuncia ante las autoridades competentes, los delincuentes aprovechan para utilizar sus nombres y para actuar de forma ilegal haciéndose pasar por la persona que no es.

Algunas entidades financieras en el momento de otorgar créditos, ventas a crédito, tarjetas y operaciones similares, que no ejercen un adecuado control de la identidad de sus futuros clientes. Una vez que el ladrón de identidad no paga la deuda del crédito obtenido, la persona a quien le suplantaron la identidad comienza a recibir llamadas y estados de cuentas de consumos y compras que jamás han realizado lo cual causa un daño en del buró de crédito.

Por los múltiples casos que han existido de robo de identidad la Superintendencia de Bancos y Seguros dispuso a todas las instituciones financieras que conozca a su cliente un novedoso método de investigación y validación datos básicos como lugar de residencia, lugar de trabajo, firmas, planillas de servicios básicos que son documentos primordiales para poder abrir una cuenta bancaria pero esto no basta la entidad financiera es responsable se puede decir que del 80 % de este tipo de delitos la mayoría de las veces es porque solo están interesado en cumplir metas y ganar un número mayor de clientes para ser mejor que la competencia cuando no se dan cuentan del alto riesgo y daño que causa a terceras personas.

Se puede mencionar la responsabilidad y la intervención del Estado ya que se están creando cedulas de identidad falsas con material robado, dentro de los cuales tiene que hacerse responsable y expandir medidas preventivas para que no ocurra este tipo de delitos en una institución pública con la más alta responsabilidad de emitir números de cedulas, partidas, entre otros. Es así como vemos una participación triangular donde interviene el delincuente, la entidad financiera y el Estado.

MEDIDAS DE PRECAUCION

Para evitar este tipo de fraudes a los que estamos expuestos tenemos que considerar tomar en cuenta algunas precauciones como:

- Proteger la cartera o bolsa manteniendo bien vigilados
- No llevar tarjetas demás solo la que va a utilizar
- En caso de robo, perdida o extravío, comunicarse de inmediato con su entidad financiera y proceder con el bloqueo.
- Evite el fraude por correo electrónico, no llene campos donde le soliciten información bancaria.
- Comunicarse con su entidad financiera para corroborar si es verídica la información solicitada por páginas web o correos electrónicos.
- Si usted realiza operaciones bancarias en línea, no use “firmas automáticas" en sitios bancarios o de tarjeta de crédito.
- No deje su clave del cajero o de acceso a la banca virtual anotada en algún lugar, memorícelo.

- No le dé su clave ni envié a terceras personas a realizar retiros, solo en caso de que sea de su extrema confianza.
- No acepte ayuda de ningún extraño al momento de realizar transacciones en los cajeros automáticos, muchas veces esas son las oportunidades que los delincuentes esperan para atacar.
- Vigile bien cuando empleados de tiendas y restaurantes utilizan su tarjeta y asegúrese que no están copiando o “skimming" su número de tarjeta de crédito. A veces los dispositivos usados para copiar se parecen a teléfonos móviles.
- Después de que usted hace una compra y le devuelven su tarjeta, verifique que efectivamente es su tarjeta.
- Si usted va a salir de viaje y piensa usar su tarjeta fuera de casa, notifique a su compañía de tarjeta de crédito. Esto puede evitar que le marquen la cuenta por posible
- Revise su estado de cuenta el mismo día que le llegue.

CAPÍTULO III

METODOLOGÍA DE LA INVESTIGACIÓN

3.1. Métodos de la investigación

Para el trabajo de investigación realizado se utilizó los siguientes métodos:

Método Inductivo-Deductivo.- Se aplicó un proceso analítico sintético estudiando aspectos particulares de casos de fraudes bancarios, para llegar a un aspecto general que es la rectificación de la Ley de Comercio Electrónico, estableciendo un sustento teórico general. En este método la encuesta, entrevista, y la observación directa de las actividades desarrolladas por las empresas e individuos, fueron de fundamental importancia, pues permitieron recabar de una manera satisfactoria y ordenada toda la información.

Método Deductivo-Inductivo.- Partimos de lo general a lo particular, es decir, mediante un aspecto general que es la rectificación a una Ley nacional, se pueden obtener o disminuir los casos de fraudes de robo de dinero por medio de redes informáticas.

Método Analítico.- Porque relaciona las variables totalmente aisladas y se formula una teoría que unifica los diversos elementos. Variables como: externalidades, medioambientales, incentivos gubernamentales, etc. Variables exógenas que están inmersas en la investigación y que son tratadas para el estudio basadas en un marco legal.

Método Sintético.- El tema a tratar es real, el cual permite la comprensión de un hecho o fenómeno concreto, fenómenos y problemas estructurales abordados en la

investigación, sociales, financieros, tecnología, entre otros. Todos estos fenómenos comprenden la realidad del tema abordado.

Método Cualitativo.- se desarrolla en cuanto a lo social y razones del comportamiento, con el propósito de explorar las relaciones sociales y describir la realidad que se especifican en el caso de los delitos de fraudes electrónicos, tomando en cuenta que se lo hace por afectar el patrimonio de los usuarios de la banca privada, problema que se presenta a las personas que utilizan diversos canales de tecnología, para sus actividades diarias, y esto no solo se desarrolla en el Ecuador si no a nivel mundial.

Método Cuantitativo.- se enfoca principalmente en los resultados numéricos, de investigaciones realizadas, se aplicará a la muestra la encuesta y se comprobará los resultados con la hipótesis.

3.2. Población y muestra

La población que hemos decidido tomar para este trabajo, se concentra en los clientes de la Banca privada de la ciudad de Guayaquil, la cual actualmente está conformada por 24 Instituciones Financieras legalmente registradas y autorizadas por la Superintendencia de Bancos y Seguros y de las cuales se ha escogido como muestra a los 5 bancos más grandes durante la última década.

Tabla 4.- Población

BANCOS	NUMERO DE CLIENTES AÑO 2014	% DE POBLACION
Banco Pichincha	2.933.012	35%
Banco Guayaquil	1.360.994	27%
Banco Bolivariano	883.905	18%
Produbanco	804.977	15%
Banco del Pacifico	643.030	5%
Total	**6.625.918**	**100%**

Fuente: Superintendencia de Bancos y Seguros - Revista Ekos

Elaborado por: Autora

Por lo expuesto en virtud del tamaño de la muestra es demasiado extenso, la población de estudio se determinó a través de la fórmula de población infinita.

N = 6.625.918

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

n = Tamaño de la muestra = ¿?

Z = Nivel de confianza 95% = 1,96

p = variabilidad positiva = 80% aceptables

q = Variabilidad negativa = 20% no aceptables

N = Tamaño de la población = 6.625.918

e = Precisión o error = 5%

n = 390

La población utilizada fue los clientes promedio que tiene varios Bancos en la ciudad de Guayaquil en el año 2014, aplicando la fórmula para obtener el tamaño de la muestra para poder realizar las encuestas, se obtuvo una muestra de 390 personas a encuestar, con un error de la fórmula del 5% y un nivel de confianza del 95% en la muestra obtenida.

Tabla 5.- Muestra

BANCOS	MUESTRA
Banco Pichincha	112
Banco Guayaquil	98
Banco Bolivariano	75
Produbanco	65
Banco del Pacifico	40
Total	**390**

Fuente: Resultados de la Investigación

Elaborado por: Autora

3.3. Técnicas e instrumentos de recolección de datos

El presente estudio se enmarcará dentro de los siguientes tipos de investigación: cuantitativa, cualitativa, descriptiva, de campo y bibliográfica.

Encuesta.- A través de ella se lograra saber la opinión de los encuestados sobre el tema a tratar, y comprobar si la solución del problema es la tipificación del fraude electrónico como delito informático.

Entrevista.- A través de ella se lograra saber la opinión de los encuestados sobre el tema a tratar, y comprobar si la solución del problema es la tipificación del fraude electrónico como delito informático.

Descriptiva.- La investigación se circunscribe a un estudio descriptivo, la recolección de datos sobre la base de una teoría ha permitido describir las actividades de servicio de un Banco en este país. Los resultados se exponen de manera sistemática y se interpretan objetivamente.

El diseño de investigación es descriptiva, asociativa, no experimental, de tipo transversal. Es científica porque se utiliza métodos investigativos científicos, la investigación no es exploratoria, ni explicativa, es una investigación descriptiva.

Por otro lado, de acuerdo a las clasificaciones de investigaciones científicas descriptivas, la investigación no es univariada, sino más bien es una investigación asociativa.

Finalmente, de acuerdo con el tratamiento de las variables, la investigación es no experimental, y de acuerdo a esta clasificación es de tipo transversal. Es decir, la

investigación científica es: descriptiva, asociativa, no experimental, de tipo transversal.

Es descriptiva porque lo que busca es describir independientemente las variables expuestas, y es asociativa, ya que lo que busca es medir el grado de asociación entre las variables expuestas.

Es no experimental, debido a que no se manipulan las variables, y de tipo transversal, porque se utilizó una muestra para realizar la encuesta.

De campo.-La investigación se desarrolló directamente en un Banco de la ciudad de Guayaquil, y personas en general. Se enfocó principalmente en la prevención del fraude, estrategias de competitividad. La encuesta realizada a personas ecuatorianas tuvo como objetivo obtener una perspectiva más humana y real acerca de la visión financiera y económica de los ciudadanos en el Ecuador.

Se realizó también visitas de campo para sustentar el estudio investigativo, estas visitas de campo fueron de observación científica, y por medio de las entrevistas a funcionarios estratégicos de los bancos se pudo obtener información más real y acorde al tema tratado.

Estos funcionarios estratégicos son especialistas en análisis y prevención, analizan tendencias y factores inmersos e implícitos de cara a un desarrollo del incremento al fraude electrónico, lo que hace justificable el estudio.

Bibliográfica.- La base teórica de la investigación se sustentó mediante consultas a: fuentes bibliográficas, revistas, apuntes, textos, documentos varios, periódicos,

folletos, así como también fuentes informáticas de internet las cuales permitieron establecer parámetros y matrices que generaron resultados en la investigación

3.4 Procesamiento y Análisis Personal de la Propuesta

En este estudio de la investigación sobre fraudes electrónicos lo que queremos proponer como una medida de solución alternativa y de implementación a nuestro sistema legislativo y financiero es el reformar la Ley de Comercio Electrónico tipificando los artículos con la definición de los fraudes más comunes cometidos en nuestro país y que tengan concordancia y relación con el nuevo Código Orgánico Integral Penal.

Además realizar como prueba la implementación de un departamento de capacitación en una de las instituciones financieras del país, para los clientes de la banca capacitándolos en el buen manejo y la debida forma de realizar transacciones utilizando la tecnología que hoy en día nos facilita la vida cada vez más.

Culturizar a la población con respecto a los nuevos productos de la banca y al buen uso de los mismos evitando de cierta forma que disminuya el fraude en nuestro país.

3.5 Tratamiento de la Información

Los resultados arrojados por las técnicas que se aplicaran, serán estadísticos de forma cuantitativa y cualitativa, lo que nos llevara a figurar en cuadros estadísticos con porcentajes y cantidades para posterior realizar un análisis de los resultados.

Luego de haber cumplido con la obtención de datos se procederá a la representación de los resultados por medio de gráficos de pasteles, para visualizar mejor las técnicas aplicadas.

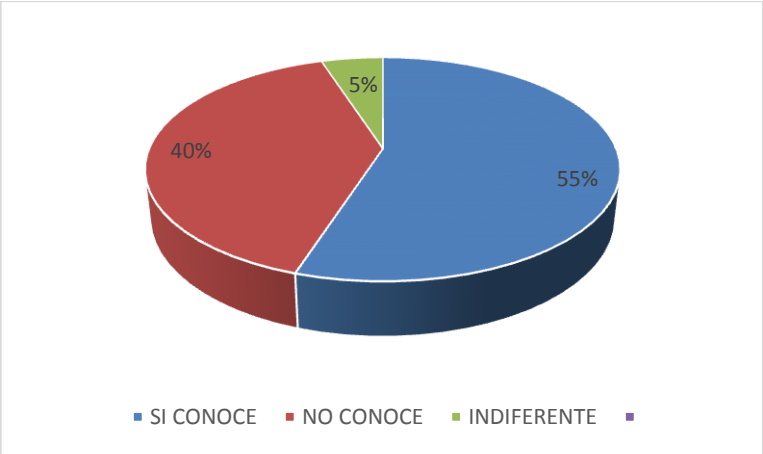
3.6 Procesamiento y Análisis

A continuación mostraremos los porcentajes de respuestas de cada una de las preguntas realizadas a los clientes cuando se acercaban a realizar retiros en los cajeros automáticos de los diferentes bancos de la ciudad de Guayaquil.

1.- ¿Conoce usted que es el fraude electrónico?

Tabla 1

	TABLA DE FRECUENCIA	
DETALLE	**DATOS**	**PORCENTAJE**
SI CONOCE	**234**	**55%**
NO CONOCE	**132**	**40%**
INDIFERENTE	**24**	**5%**
TOTAL	**390**	**100%**



Fuente: Resultados de las Encuestas

Elaborado por: Autora

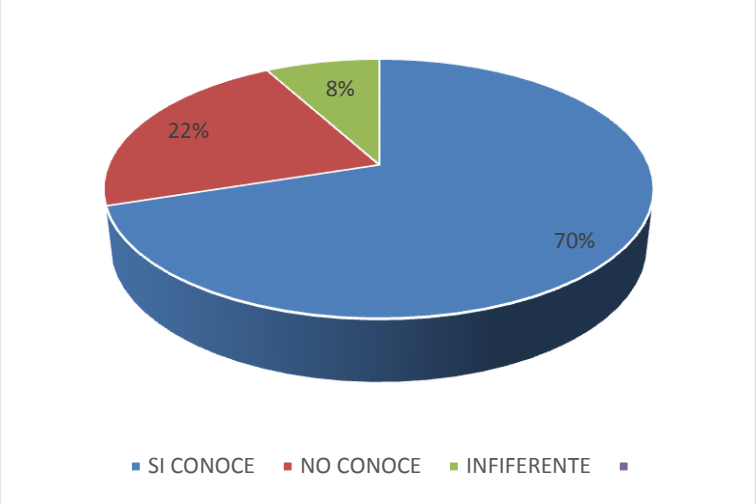
Análisis:

Con respecto a la primera pregunta de la población encuestada el 55% que si conoce o tiene una idea sobre lo que es el fraude electrónico quizás porque han sido víctimas directas de este tipo de delitos, el 40% no conoce o no han escuchado nada sobre el fraude electrónico.

2.- ¿Conoce usted alguna persona que ha sido víctima de algún tipo de fraude en tarjeta de crédito o débito?

Tabla 2

	TABLA DE FRECUENCIA	
DETALLE	**DATOS**	**PORCENTAJE**
SI CONOCE	256	70%
NO CONOCE	112	22%
INDIFERENTE	22	8%
TOTAL	**390**	**100%**



Fuente: Resultados de las Encuestas

Elaborado por: Autora

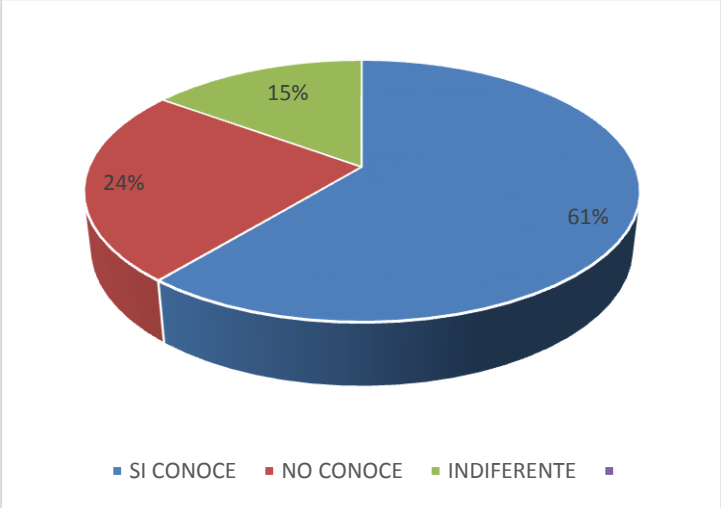
Análisis:

El 70% de la población encuesta indica que conoce a alguien como familiar o amigos que han sido víctimas del fraude electrónico con tarjetas de crédito pero con mayor frecuencia en las tarjetas de débito, como podemos observar en la gráfica existe un 22% que no conoce a ninguna persona.

3.- ¿Conoce usted en que consiste el skiming o clonación de tarjeta?

Tabla 3

	TABLA DE FRECUENCIA	
DETALLE	**DATOS**	**PORCENTAJE**
SI CONOCE	**182**	**61%**
NO CONOCE	**164**	**24%**
INDIFERENTE	**44**	**15%**
TOTAL	**390**	**100%**



Fuente: Resultados de las Encuestas

Elaborado por: Autora

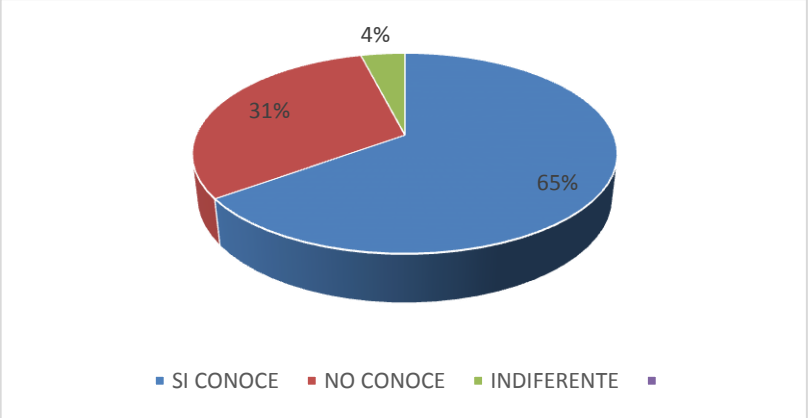
Análisis:

Como se observa en los resultados obtenidos, el 61% contesto que si conoce en que consiste el skiming o clonación de tarjeta y cuáles son las causas o motivos por los cual se da este tipo de delito, pero el 24% y el 15% indica que no conoce o que le es indiferente conocer sobre el skiming.

4.- ¿Conoce usted, si en el Código Orgánico Integral Penal se encuentra tipificado el fraude electrónico?

Tabla 4

	TABLA DE FRECUENCIA	
DETALLE	**DATOS**	**PORCENTAJE**
SI CONOCE	**190**	**65%**
NO CONOCE	**170**	**31%**
INDIFERENTE	**30**	**4%**
TOTAL	**390**	**100%**



Fuente: Resultados de las Encuestas

Elaborado por: Autora

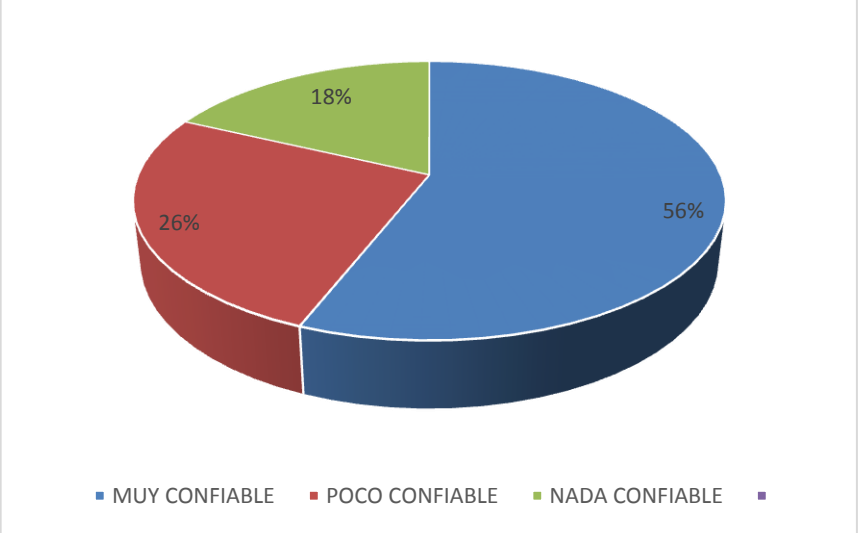
Análisis:

El 65% indica que conoce y ha leído sobre la tipificación de este delito en el nuevo Código Orgánico Integral Penal pero indican que aun así se sigue cometiendo estos fraudes en la Banca Privada. El 31% contesto que no conoce y un 4% indican que le es indiferente si existe o no la tipificación de estos delitos.

5.- ¿Cómo calificaría usted la plataforma de seguridad utilizada en las instituciones financieras sobre los diferentes canales o dispositivos de tecnología?

Tabla 5

	TABLA DE FRECUENCIA	
DETALLE	**DATOS**	**PORCENTAJE**
MUY CONFIABLE	148	56%
POCO CONFIABLE	52	26%
NADA CONFIBLE	46	18%
TOTAL	**390**	**100%**



Fuente: Resultados de las encuestas

Elaborado por: Autora

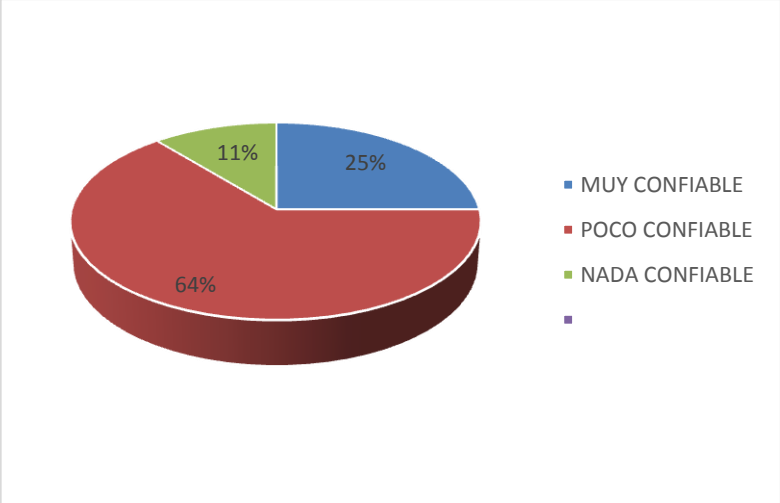
Análisis:

Como observamos en la gráfica el 56% califica a la plataforma de seguridad utilizada es muy confiable por que se han implementado nuevas técnicas en los cajeros automáticos y en la banca virtual como los últimos 4 dígitos de su cedula de identidad, el 26 % indica que es poco confiable y un 18% contesto no es nada confiable porque cualquier persona hoy en día puede saber tus datos personales.

6.- ¿Cuanta seguridad o confianza le inspira transaccionar actualmente con tarjeta de crédito o de débito?

Tabla 6

	TABLA DE FRECUENCIA	
DETALLE	**DATOS**	**PORCENTAJE**
MUY CONFIABLE	**158**	**25%**
POCO CONFIABLE	**200**	**64%**
NADA CONFIABLE	**32**	**11%**
TOTAL	**390**	**100%**



Fuente: Resultados de las encuestas

Elaborado por: Autora

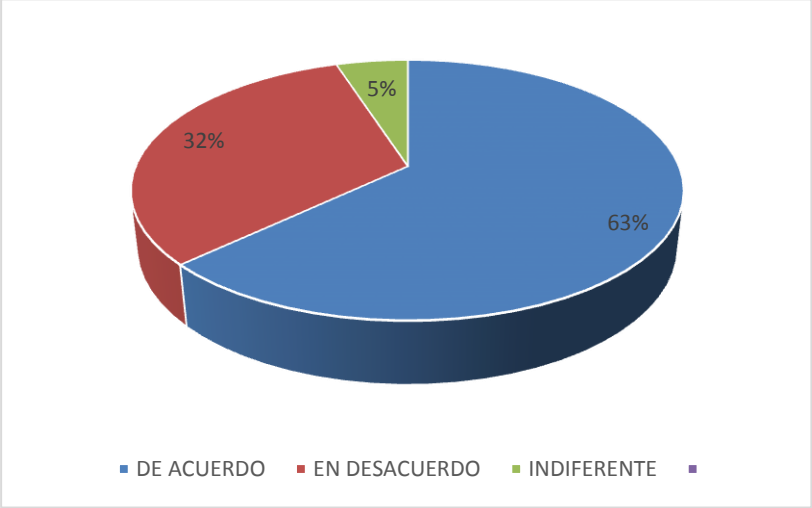
Análisis:

El 25% contesto que actualmente se siente muy confiable al realizar transacciones con sus tarjetas de crédito o de débito pero al mismo tiempo existe todavía un 64% que se siente poco confiable ya que siguen existiendo este tipo de delitos y que aun así no están seguros y toman todas las precauciones en cualquier situación.

7.- ¿Considera usted que la falta de tipificación del delito informático es causa para que se siga produciendo el fraude electrónico?

Tabla 7

	TABLA DE FRECUENCIA	
DETALLE	**DATOS**	**PORCENTAJE**
DE ACUERDO	**197**	**63%**
EN DESACUERDO	**168**	**32%**
INDIFERENTE	**25**	**5%**
TOTAL	**390**	**100%**



Fuente: Resultados de las encuestas

Elaborado por: Autora

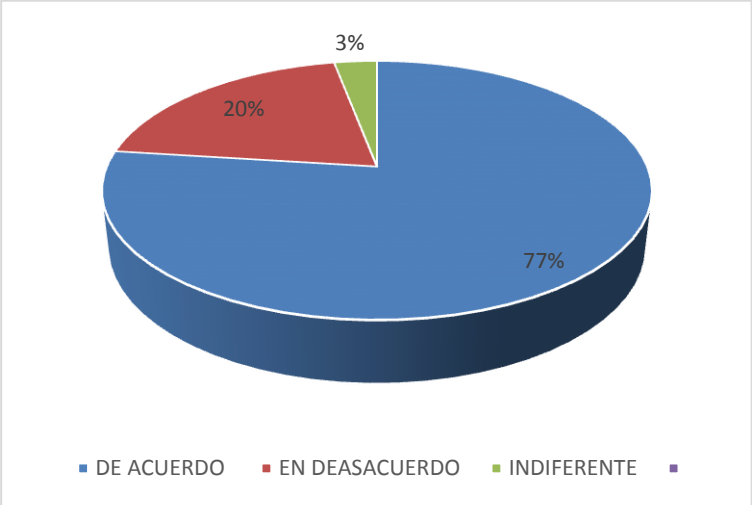
Análisis:

El 63% de la población encuestada contesto que está de acuerdo y considera que la falta de tipificación de los delitos informáticos en nuestra legislación causa que el fraude electrónico siga con su tendencia de incrementar cada día más, el 32% está en desacuerdo y no considera que la falta de tipificación sea un factor para corregir y reducir el fraude.

8.- ¿Cree usted que es adecuado la conceptualización de los tipos de fraude en la Ley de Comercio Electrónico para reducir y regular este tipo de delitos?

Tabla 8

	TABLA DE FRECUENCIA	
DETALLE	**DATOS**	**PORCENTAJE**
DE ACUERDO	**213**	**77%**
EN DESACUERDO	**147**	**20%**
INDIFERENTE	**30**	**3%**
TOTAL	**390**	**100%**



Fuente: Resultados de las encuestas

Elaborado por: Autora

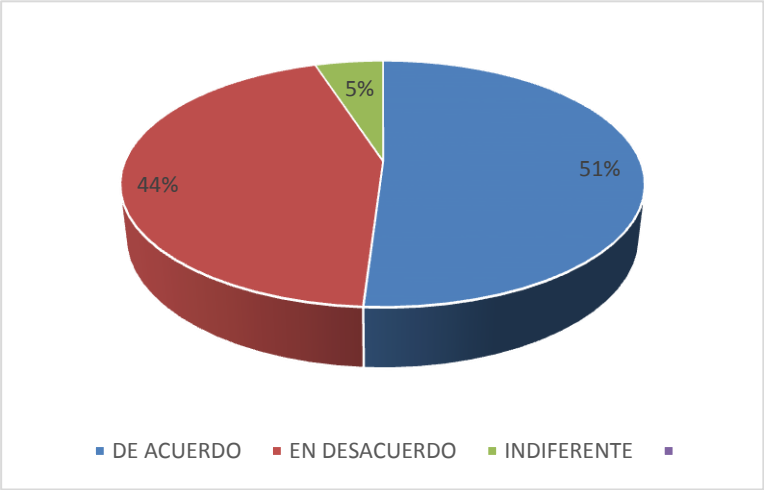
Análisis:

De acuerdo a los resultados de la encuesta en la presente interrogante el 77% estuvo de acuerdo y considera adecuado la conceptualización y la reforma a la Ley de Comercio Electrónico para regular estos delitos informáticos ya que no existe una normativa clara que sea de conocimiento público para conocer en que consiste cada uno de los fraudes electrónicos.

9.- ¿Considera que los jueces y fiscales de nuestro país deben de estar mejor informados de este tipo de delitos para la aplicación de la ley?

Tabla 9

	TABLA DE FRECUENCIA	
DETALLE	**DATOS**	**PORCENTAJE**
DE ACUERDO	**245**	**51%**
EN DESACUERDO	**100**	**44%**
INDIFERENTE	**45**	**5%**
TOTAL	**390**	**100%**



Fuente: Resultados de las encuestas

Elaborado por: Autora

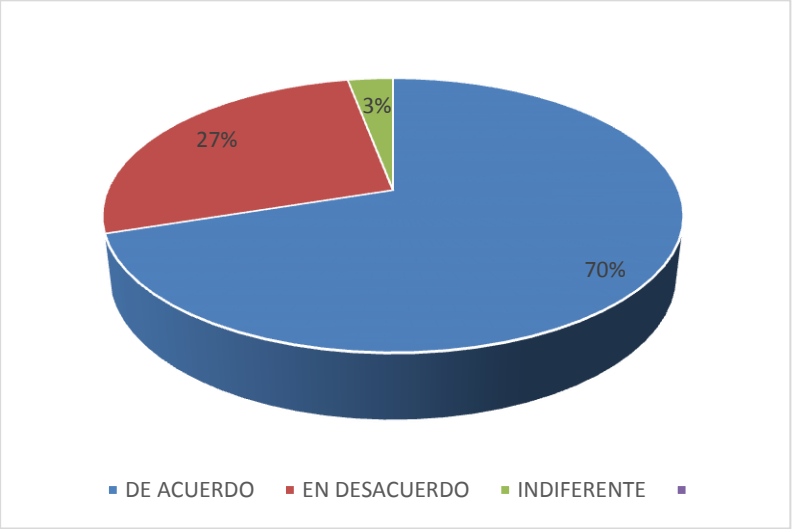
Análisis:

Como observamos en la gráfica tenemos una respuesta casi pareja con el 51% y el 44% que están en acuerdo y en desacuerdo sobre el tema de que los jueces y fiscales deben de estar mejor informados, algunas personas indican que es fundamental ya que son ellos los encargados de regular y aplicar la ley para este tipo de delitos, en cambio otras personas consideran que no solo basta que ellos estén informados si no también la sociedad.

10.- ¿Considera conveniente que el fraude electrónico debe tener una sanción más severa en nuestra legislación penal?

Tabla 10

	TABLA DE FRECUENCIA	
DETALLE	**DATOS**	**PORCENTAJE**
DE ACUERDO	**215**	70%
EN DESACUERDO	**124**	27%
INDIFERENTE	**51**	3%
TOTAL	**390**	**100%**



Fuente: Resultados de las encuestas

Elaborado por: Autora

Análisis:

Según el resultado de la encuesta el 70% está de acuerdo con se sancione de una forma más severa a los delincuentes que cometan este tipo de delitos y que dicha sanción esté debidamente tipificada en nuestra legislación ecuatoriana, el 27 % está en desacuerdo ya que considera que la sanción que se tipifica en el COIP es suficientemente severa para su aplicación.

3.7 Resultados de la Observación (Entrevistas)

De las entrevistas realizadas a tres funcionarios de la banca privada y a un fiscal de delitos informáticos obtuvimos varias respuestas de acuerdo a las preguntas realizadas y que tienen relación con la tipificación del fraude electrónico.

La entrevista tendrá un cuestionario de preguntas de fácil compresión y sobre todo importantes comentarios y punto de vista para la realización de este trabajo investigativo, porque el tema es una realidad latente que ocurre en todas las personas que usan la tecnología como medio facilitador.

Luego de haber realizado las entrevistas es necesario realizar un pequeño análisis de los resultados obtenidos y observar el común denominador en las respuestas de los entrevistados.

Entrevistado 1.- A.- Ing. Gary Rivas- Jefe de Prevención de Fraudes del Banco Bolivariano.

Entrevistado 2.- B.- Ing. Carmen Zambrano- Analista Senior de Tarjetas de crédito del Banco del Pacifico

Entrevistado 3.- C.- Sr. Christopher Lara- Analista Junior de Tarjetas de débito del Banco de Guayaquil

Entrevistado 4.- D.- Dr.- Walter Suarez- Fiscal de la Unidad 2 Patrimonio Ciudadano.

1.- ¿Cuál es su punto de vista sobre la evolución del fraude informático durante el periodo 2009 al 2014?

A.- El fraude hace un par de años atrás más se daba por skiming en tarjetas de crédito o tarjetas de débito, actualmente con el tema de la implementación del sistema MB o la tecnología chip, el fraude con lectura de banda no se está dando mucho y ahora más bien se están presentando casos de suplantación de identidad en ventanillas y compras a través de internet en los comercios electrónicos.

B.- Mi punto de vista sobre la evolución del fraude como analista de tarjetas de crédito en los últimos años es que siempre se está incrementando, surgiendo nuevas formas y métodos de obtener información.

C.- Bueno el fraude electrónico ha evolucionado mucho con la llegada de las nuevas tarjetas con chip, estos últimos meses no hemos atendido tantos reclamos por retiros con tarjetas de débitos, pero anteriormente los reclamos era una cantidad impresionante de atender, más que todo se daba skiming en los días de feriado cuando había mayor transaccionalidad de los clientes**.**

D.- El fraude informático ha crecido indudablemente porque son delitos que a través de los sistemas informáticos las personas pueden alterar datos y de lo que tenemos conocimiento los fiscales este delito va en aumento en cuanto a las estadísticas e ingresos que diariamente las causas que nosotros conocemos.

Análisis.- Según las respuestas de los entrevistados podemos observar que todos concuerdan con que la tendencia del fraude siempre ha sido incrementarse e ir en aumento con el pasar del tiempo.

2.- ¿Cree usted que existe una falencia en nuestra legislación ecuatoriana con respecto a la tipificación del fraude electrónico?

A.- No, yo pienso que con la nueva legislación actual es mejor de la que teníamos porque por lo menos ahora se encuentran contemplados los delitos informáticos, básicamente creería yo que falta un poco más de conocimiento por la parte de los fiscales y jueces con respecto a este tipo de delitos para que puedan proceder con la debida aplicación de la ley.

B.- Bueno nosotros manejamos una parte más operativo pero lo que puedo deducir es que si hace falta una sanción más severa, porque hemos conocido de casos de delincuentes que son capturados pero que a la semana los liberan por falta de denuncias o pruebas entonces nunca tienen un castigo o sentencia adecuada.

C.- Bueno con el nuevo Código Orgánico Integral Penal, podemos decir que no existe falencia porque está tipificado, cosa que anteriormente no existía pero creo yo que existe una clara falta de aplicación de la ley porque son pocos los casos que llegan a ser sentenciados.

D.- Yo pienso que no existe falencia lo que no hay es la debida información, lo que debo señalar es que con el nuevo Código Orgánico Integral Penal, las instituciones financieras o personas jurídicas también son responsables y también respondan por este tipo de delitos que se ha estado evadiendo.

Análisis.- Con respecto a la pregunta algunos de los entrevistados indican que la llegada del nuevo Código Integral Penal no existe falencia porque por lo menos se encuentra tipificado pero que existe algún tipo de desinformación en la sociedad.

3.- ¿Considera usted conveniente una reforma a la Ley de Comercio Electrónico, implementando la conceptualización de los diferentes tipos de fraude electrónico?

A.- Claro que estoy de acuerdo, eso sería muy bueno y de gran ayuda para que los jueces de nuestro país tengan una mejor aplicación de la ley.

B.- Si yo creo que si, ya que no es una norma que se utiliza mucha actualmente pero no estaría mal que los fraude estén conceptualizados para que la sociedad tenga conocimiento, ya que es un tema que nos afecta a todos.

C.- Si sería bueno una norma que regule y conceptualice a estos delitos.

D.- La ley de Comercio Electrónico es una ley que se encuentra en el olvido, considero yo que sería bueno implementar artículos que mencione al fraude electrónico al delito como tal y que se complemente con el COIP en sus sanciones.

Análisis.- Con las respuestas de los entrevistados obtenemos un resultado positivo con respecto a la pregunta, indican que sería una reforma interesante y de gran ayuda para todos.

4.- ¿Cree usted que el Código Orgánico Integral Penal tiene las normas suficientes para sancionar el fraude electrónico?

A.- Nunca será suficiente, ni las normas, ni las sanciones, nada detiene a los delincuentes que siempre están buscando nuevas formas de cometer el fraude, como por ejemplo hoy en día está en boga el famoso cambiazo que consiste en engañar a las personas que se encuentran transaccionando para que les entregue la tarjeta y devolverles una falsa para así ellos realizar los retiros con la tarjeta original.

B.- Las normas y sanciones ayuda mucho pero como lo mencione anteriormente el fraude nunca va a detenerse, nunca conseguiremos llegar a un fraude cero a nivel nacional eso es imposible.

C.-Si las normas establecidas fueran suficientes hoy en día no existiría el fraude, lo que si debe existir es una regularización para el uso del internet creería yo que eso se debe encargar el Ministerio de Telecomunicaciones.

D.- Como fiscalía órgano de investigación es difícil la aplicación de dichas sanciones eso le corresponde específicamente a los jueces que les ha sido asignado el proceso, pero dentro de mi experiencia y de los casos vistos es muy difícil identificar e imponer una sanción a estos delincuentes, dichas sanciones sirven para limitar las acciones delincuenciales que se siguen produciendo mas no para liberarse por completo del delito.

Análisis.- Las personas encuestadas indican que ninguna sanción será suficiente, que son de gran ayuda para limitar las acciones de los delincuentes que se dedican a cometer acciones fraudulentas.

5.- ¿Cómo cree usted que se puedan evitar que se siga produciendo ataques por parte de delincuentes informáticos?

A.-Nosotros como banco hacemos todo lo posible para evitar el fraude, contamos con un departamento de monitoreo quienes son los encargados que monitorear las transacciones de los clientes, consumos entre otros, esto nos ayuda mucho ya que si ellos detectan algo inusual previenen al cliente llamándolo para confirmar la transacción o el consumo o simplemente nos envían una alerta para proceder con el bloqueo de las tarjetas.

B.- Si claro que se puede evitar, informando a los usuarios de la banca privada para que tomen todas las medidas de seguridad correspondientes.

C.- si se puede evitar ser víctima del fraude teniendo en cuenta las medidas de precaución, cambiando nuestra clave en ciertos periodos de tiempo o simplemente teniendo un buen uso o custodio de la tarjeta, con todas estas recomendaciones podemos evitar ser víctimas potenciales de los delincuentes

D.- La fiscalía siempre ha pedido que se difunda a través de los medios de comunicación las medidas preventivas para evitar el fraude electrónico, el año pasado estuvo el diario el Universo y sacaron ampliamente una nota donde se hacía advertencia a la población pero no se ha realizado ninguna gestión más durante este año.

Análisis.- Con respecto a la pregunta realizada los entrevistados indican que si se puede evitar ser víctima del fraude tomando las medidas necesarias preventivas para lograrlo.

6.- ¿Quién cree usted que puede estar más propensos o ser víctimas de fraude electrónico?

A.- Normalmente son personas que se dejan llevar por publicidad en el internet como por ejemplo las agencias o aerolíneas que venden pasajes baratos o de ofertas y son víctimas de este tipo de delitos quizás por los precios o por las rebajas pero lo que venden es el riesgo de la procedencia de esas publicidades que son inusuales.

B.- Las personas que tienden a ser demasiado confiadas y creen que con una llamada telefónica diciéndoles que se ha ganado un premio y resulta ser falso solo con el fin de obtener información y es así como resultan ser víctimas de fraudes.

C.- Principalmente las personas más vulnerables a este tipo de delitos son los adultos mayores que no saben utilizar un cajero automático y piden ayuda a terceras personas o que se encuentran preocupados por algún tema, y ese es el momento donde aprovechan para realizar los retiros sin que sospechen nada.

D.- De los casos que han llegado a la Fiscalía el mayor número de personas que han sufrido son los mayores adultos ya que muchas veces solicitan ayuda a terceras personas o desconocidos y entregan sus datos como claves y saldo que tiene en la cuenta, es así como son las victimas más vulnerables para estos delincuentes.

Análisis.-La mayoría contesta que las personas más propensas son los mayores adultos que solicitan ayuda a terceros para poder transaccionar en un cajero automático.

CAPÍTULO IV

LA PROPUESTA

4.1.TITULO DE LA PROPUESTA

Reformar el Título V, Capítulo I de la Ley de Comercio Electrónico para combatir el delito informático e informar a los usuarios de la banca privada en que consiste el fraude electrónico.

Se propone lo siguiente:

- ✓ Fortalecer la Ley de Comercio Electrónico que no considera la definición de los tipos de fraudes. considerando los 3 casos planteados en el problema.
- ✓ Condensar y sintetizar regulaciones en las leyes ecuatorianas que provengan o hagan referencia al fraude y a la forma de hacer fraude electrónico.
- ✓ Incentivar la implementación de un departamento de capacitación para los clientes de la Banca en cada una de las entidades financieras, donde se informe y enseñe el uso correcto de realizar transacciones tanto por medio del internet como el uso de cajeros automáticos multifuncionales que existen en algunas instituciones financieras actualmente.

4.2.Justificación de la Propuesta

La tecnología ha sido usada para relevantes objetivos como el desarrollo de la ciencia así como para causar daño, los ataques más frecuentes se ven dirigidos a los clientes de bancos. El comportamiento de los delincuentes informático ha causado pérdidas económicas al sistema financiero y se ha creado la inseguridad con el uso del internet, los usuarios de la banca privada ya no siente la confianza y ha perdido la credibilidad cuando ha sido víctima de unos de los ataques por medio de fraude electrónico.

4.3.Objetivo General de la Propuesta

Determinar si la reforma presentada en la Ley de Comercio Electrónico permite reducir el fraude electrónico en nuestro país y evitar la forma de que aumente o busquen nuevas formas de hacer fraude, imponiendo sanciones acorde a lo tipificado en el Código Orgánico Integral Penal y tomando las medidas de seguridad correspondiente.

4.4.Objetivos Específicos de la Propuesta

- ✓ Analizar las reformas en el Título V, Capítulo I, Sección de las Infracciones Informáticas de la ley N° 2002-67 (Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos).

- ✓ Presentar una propuesta de implementar un departamento especializado en capacitación a usuarios y que se dedique únicamente ayudar a los clientes el manejo de los diferentes medios electrónicos que se utilizan actualmente.

4.5.Hipótesis de la Propuesta

La Ley de Comercio Electrónico no tipifica ni conceptualiza el fraude electrónico que atenta contra la sustracción del dinero resguardado en las entidades financieras, a través de la conceptualización de los diferentes tipos de fraude electrónico más comunes se lograra disminuir la problemática y obtener una normativa más clara y precisa sobre el tema.

4.6.Desarrollo de la Propuesta

PROPUESTA DE REFORMA

REPÚBLICA DEL ECUADOR

ASAMBLEA NACIONAL

EL PLENO

CONSIDERANDO:

QUE.- Es obligación del Estado ecuatoriano precautelar las garantías constitucionales de los ecuatorianos y que todos tengan los mismos derechos, y amparados en la Declaración de Derechos Humanos y en el artículo 66 numeral 20. El derecho a la intimidad personal y familia.

QUE.- Es obligación general de la Asamblea Nacional aprobar leyes, normas generales de interés común, y tipificar infracciones y establecer sanciones que ejercen la autoridad de administración justicia, hacer respetar lo manifestado en la Constitución de la República del Ecuador y en la ley, con miras del bien común,

del principio del buen vivir, equidad y la justicia. Es necesario criminalizar el fraude electrónico, con el objetivo de garantizar la estabilidad de los ecuatorianos.

QUE.- El uso de las tecnologías no sea un impedimento para generar seguridad jurídica.

LEY REFORMATORIA A LA LEY DE COMERCIO ELECTRONICO, FIRMAS ELECTRONICAS Y MENSAJES DE DATOS.

Refórmese al Art. 1 de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos; agregar la palabra **Fraude electrónico** en el Objeto de esta ley la misma que dirá:

Art.1.- Objeto de la Ley.- Esta ley regula los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, **el fraude electrónico**, a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas.

Añádase

Reformar el Título V, de las infracciones informáticas, la misma que dirá:

TITULO V

DEL FRAUDE ELECTRONICO

CAPITULO I

Agregar

Art….- Fraude electrónico.- Es el uso indebido de tecnologías de información, valiéndose de cualquier manipulación en sistemas o cualquiera de sus componentes, en la data o información en ellos contenida, consiga insertar instrucciones falsas o fraudulentas, que produzcan un resultado que permite obtener provecho injusto en perjuicio ajeno.

Art…..- Skiming.- Es el copiado de la banda magnética de forma ilegal de la información como claves de una o varias tarjeta de crédito o de débito usando un dispositivo lector y reproductor de dicha información llamado skimmer. La persona que cometa de forma infraganti o se descubra que forma parte de bandas delictivas que realizan este delito será sancionadas con pena privativa de libertad de tres a cinco años en concordancia con el Art. 230 numeral 3 del Código Orgánico Integral Penal.

Art….- Phising.- Consiste en enviar una cantidad enorme de mensajes por correo electrónico haciéndole conocer al consumidor o usuario que los mensajes vienen de su institución financiera, tratando de conseguir que la víctima potencial revele la información personal, como los números de cuentas, cifras, claves, entre otros.

Art….- Robo de identidad.- Es el uso fraudulento de la información personal de una persona como su número de Seguro Social, fecha de nacimiento, cedula de identidad, entre otros, para cometer fraude financiero.

Art…..- Manejo Fraudulento de Tarjetas Inteligentes.- Toda persona que por cualquier medio, cree, capture, grabe, copie, altere, duplique o elimine información contenida en una tarjeta inteligente o en cualquier instrumento destinado a los mismos fines será sancionado acorde el art. 230 del Código Orgánico Integral Penal.

En la misma pena incurrirá quien adquiera, comercialice, posea, distribuya, venda, o realice cualquiera tipo de intermediación de tarjetas inteligentes destinadas al mismo fin.

Disposición Final.- Esta ley entrara en vigencia a partir de su publicación en el registro oficial. Dado y firma en el Pleno de la Asamblea Nacional de la República del Ecuador.

Quito, a los …….. días del mes de ……. del año dos mil…..

F…… F…….

Presidente El Secretario

PROPUESTA PARA LA IMPLEMENTACIÓN Y CREACIÓN DEL DEPARTAMENTO DE CAPACITACIÓN A USUARIOS EN CADA UNO DE LOS CINCO BANCOS MÁS IMPORTANTES DE LA CIUDAD.

Objetivo

El objetivo principal de la creación de este departamento de capacitación a usuarios es educar e informar a los usuarios de la banca privada, enfocado únicamente a prevenirlos de las múltiples circunstancias y formas de hacer fraude y así evitar y seguir combatiendo este delito comenzando en la ciudad de Guayaquil para luego expandir este departamento en otras sucursales y agencias del país.

Recursos

Las personas necesarias para comenzar este proyecto serian de cuatro con los siguientes cargos:

- Jefe del Departamento
- Asistente Senior
- Asistentes Junior

Métodos

Los métodos que se utilizaran serán dirigidos para clientes y funcionarios de la banca privada

- Folletos
- Cursos virtuales

- Charlas
- Seminarios
- Redes Sociales

Nombre del Departamento: Capacitación de Usuarios

Descripción de Perfiles y Funciones

CARGO	PERFIL	FUNCIONES
Jefe del Departamento de Capacitación de Usuarios	Ingeniero en carreras afines de Administración, Gestión y Finanzas. Conocimientos en: Políticas y procedimientos Bancario, Servicio al Cliente. Utilitarios de Office Experiencia: Experiencia laboral mínimo cinco años en entidades bancarias Género: Indistinto	Monitorear el estado de los casos de fraude que ha sufrido el Banco, controlando la gestión de sus subordinados. Instruir, capacitar e informar a la Gerencia los objetivos y resultados alcanzados con la creación del departamento; conforme a lo definido en los manuales de políticas y procedimientos de la Institución.

CARGO	PERFIL	FUNCIONES
Asistente Senior	Egresado(a) en carreras afines de Administración, Gestión y Finanzas. Conocimientos en: Políticas y procedimientos Bancario, Servicio al Cliente, y Gestión de Calidad. Utilitarios de Office Experiencia: Experiencia laboral mínimo tres años en entidades bancarias Género: Indistinto	Brindar soporte y apoyo al Jefe Inmediato del Departamento. Coordinar charlas preventivas para los usuarios que serán dictadas por el Jefe del Departamento; publicar los cursos online, fechas y lugares de realización; entre otros.

CARGO	PERFIL	FUNCIONES
Asistente Junior	Estudiante de carreras afines de Administración, Gestión y Finanzas, Talento Humano, Trabajo Social. Conocimientos en: Políticas y procedimientos Bancario, Servicio al Cliente, y Gestión de Calidad. Utilitarios de Office Experiencia: Experiencia laboral mínimo un año en entidades bancarias Género: Indistinto	Brindar la información y guía respectiva a los usuarios que se acerquen a las agencias para la apertura una cuenta bancaria, y también a los clientes que se acercan a realizar retiro por medio de los cajeros automáticos para así prevenirlos de cualquier tipo de fraude.

4.6.1.1.IMPACTO/PRODUCTO/BENEFICIO OBTENIDO

El beneficio que conlleva mi propuesta que es la de proponer una reforma a la Ley de Comercio Electrónico en el Título V, servirá para prevenir, capacitar, combatir y erradicar el fraude electrónico en nuestro país, por medio de charlas de prevención dirigidas a los usuarios y funcionarios de la banca privada como para jueces y fiscales, con la ayuda de entidades públicas como la fiscalía, la policía nacional y el apoyo de instituciones privadas como las entidades financieras.

4.7.VALIDACION DE LA PROPUESTA

Según las personas entrevistadas indican que con la llegada del nuevo Código Orgánico Integral Penal se ha podido regularizar este tipo de delitos de fraude electrónico pero que igual se necesita fortalecer la ley para su aplicación y que con la reforma presentada a la Ley de Comercio Electrónico en esta investigación, los jueces y fiscales del país estarán mayor informados y tendrán una mejor guía para llevar los procesos con prontitud y aceleración que se exige.

CONCLUSIONES

Como finalidad de este estudio investigativo podemos concluir que el fraude electrónico es una forma de vida de adquirir lo que desea de un modo más fácil y sencillo para muchos delincuentes que se dedican a crear y buscar nuevas formas de engañar y estafar a las personas. Esto ocurre porque no existe una normativa más clara que regule este delito.

Las estadísticas a cerca de los delitos informáticos en el Ecuador, han ido en aumento porque las personas no denuncian, o desconocen la existencia de tipos penales en que puedan basar su denuncia, el desinterés impiden que se pueda contabilizar los casos de perjuicio.

Como conclusión podemos observar en esta investigación que todos somos responsables de mantener la seguridad de nuestro dinero, inversiones e información personal, tanto las entidades bancarias como los órganos que las regularan, y de la misma forma la fiscalía y el estado en una fase investigativa y preventiva para la sociedad.

Existen muchas leyes en nuestro país que se encuentran en abandono y que no son tomadas en cuenta para regular, es por eso que este proyecto de investigación presenta la propuesta de reforma a una ley que se encontraba en el olvido y que debe ser de conocimiento para la comunidad y para los funcionarios que laborar en las diferentes entidades financieras del país.

RECOMENDACIONES

Se recomienda realizar la prueba con un piloto de la creación del departamento de capacitación a usuarios presentados en la propuesta de este proyecto durante el periodo de un año en uno de los bancos de la ciudad para estandarizar los resultados y los beneficios obtenidos con la creación de dicho departamento. Si los resultados son positivos expandir dicho departamento en otras agencias y sucursales del Banco en otras provincias del país para de este modo lograr la disminución del fraude electrónico.

También presentar la propuesta de reforma a la ley de Comercio Electrónico para que se implemente en nuestra legislación actual y así pueda ser utilizada en procesos de este tipo de delitos junto con el Código Orgánico Integral Penal para así respetar el debido proceso y obtener la igualdad de justicia.

Por parte de la Fiscalía tener un mayor apoyo en realizar seminarios, charlas de capacitación para los funcionarios judiciales para que se familiaricen con tipos penales relacionados con el delito informático y no se los confunda con otros ya existentes.

BIBLIOGRAFIA

TEXOS LEGALES

- Constitución de la Republica (2008) .- Registro Oficial 449 de 20 de Octubre de 2008.
- Código Orgánico Integral Penal
- Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de datos, Ley No. 200267, Registro Oficial Suplemento No. 557 de 17 de abril del 2002, Editorial: CEP, Quito- Ecuador.

TEXTOS Y PAGINAS WEB

- Aboso, Gustavo Eduardo (2010).- "La nueva regulación de los llamados delitos informáticos en el Código Penal Argentino": un estudio comparado. Argentina- Santa fe. Editorial Rubizal- Culzoni.
- Asamblea Nacional Constituyente. "Agenda de la Política Económica para el Buen Vivir" 2011-2013
- Andrés Gómez Díaz "El delito informático, su problemática y la cooperación internacional como paradigma de su solución: el convenio de Budapest" (Disponible en URL: http://www.unirioja.es/dptos/dd/redur/numero8/diaz.pdf) (10 de octubre de 2013).
- Banco Bolivariano S.A. www.bolivariano.com
- Banco Central del Ecuador. "Boletines estadísticos #1880 y 1898", octubre 2008-abril 2010. Quito-Ecuador.

- Banco Central del Ecuador. “Revistas cuestiones económicas”, volumen 23, 2007. Quito-Ecuador.
- Benavides Espíndola Olga. “Competencia y competitividad” Editorial McGraw-Hill, 2002, Medellín-Colombia.
- Bello Galindo, José de Jesús (2012).- “Manual de medidas preventivas de seguridad”; Editorial Trillas. México-México
- BUENO ARÚS, Francisco, “El delito informático”, Actualidad Informática Aranzadi Nº 11 de abril 199
- Cámara de Industria de Guayaquil. “Indicadores macroeconómicos y políticas aplicadas en Ecuador” documento, 2012. Guayaquil-Ecuador.
- Cisneros Baquero, Edison Adrián (2009).- “Los Delitos Informáticos”. Editorial Universidad Andina Simón Bolívar Sede Ecuador
- Fiscalía de Guayaquil www.fiscalia.gob.ec
- Guerrero, Diego (2010).- “Fraude en la red aprenda a proteger contra el fraude en internet”; Editorial: Ra-Ma: Madrid-España.
- http://www.derechoecuador.com/articulos/detalle/archive/doctrinas/derechoinformatico/ 2009/05/27/derecho-informático (15 de octubre de 2013).
- http://www.derechoecuador.com/articulos/detalle/archive/doctrinas/derechoinformatico/ 2005/11/24/delitos-informáticos.
- Marqués Escobar, Carlos Pablo (2003).- “El Delito Informático la Información y la Comunicación en la Esfera Penal”. Editorial Leyer. Bogotá-Colombia.
- Medina Frisancho, José Luis (2011).- “La imputación a la víctima en los delitos de defraudación patrimonial”. Editorial Grijley. Lima- Perú

- MUÑOS NAVARRO, Patricio, "Derecho e Informática", actos y congreso Iberoamericano de Informática Jurídica, 1989.
- Pérez Rodríguez, Ángela M. (2010).- "Derecho del Sistema Financiero y Tecnología". Editorial Marcial Pons; Madrid- España.
- Revista Ekos- Negocios.- Edición Raking financiero 2015.
- Rovira del Canto, Enrique (2002).- "Delincuencia informática y fraudes informáticas". Editorial Comares. Granada-España.
- RODRÍGUEZ CARAMELO, Luis Miguel, "Informática y Ordenadores, Conceptos Básicos y aplicaciones jurídicas". Facultad de Derecho de la Universidad Complutense. 1986.
- Superintendencia de Bancos y Seguros del Ecuador - www.sbs.gob.ec
- Salazar Andrade, Oswaldo Ricardo (2008).- "Análisis del delito de fraude informática". Editorial Universidad Andina Simón Bolívar Sede Ecuador
- Téllez Valdez, Julio (2009).- "Derecho Informático". Cuarta Edición. Editorial Mc Graw Hill
- Vallejo Delgado, Vicente E. (2010).- "El delito informático en la legislación ecuatoriana". Editorial: Corporación de Estudios y Publicaciones. Quito-Ecuador.

ANEXOS

UNIVERSIDAD LAICA VICENTE ROCAFUERTE DE GUAYAQUIL

DIRECCION DE INVESTIGACION

FACULTAD DE JURISPRUDENCIA

ENCUESTA MATRIZ

OBJETIVO:

Determinar el conocimiento de la población sobre los diferentes tipos de fraude electrónico, sobre las leyes que sancionan estos delitos y la falta de normativa en nuestra legislación.

INTRUCCIONES:

Leer determinadamente y no dejar ninguna pregunta sin contestar

Marque únicamente una opción

La información brindada es estrictamente confidencial

ENCUESTA GENERAL

SEXO: MASCULINO FEMENINO

PREGUNTAS		CALIFICACION	
Conocimiento del Fraude	**SI CONOCE**	**NO CONOCE**	**INDIFERENTE**
1.- ¿Conoce usted que es el fraude electrónico?			
2.- ¿Conoce usted alguna persona que ha sido víctima de algún tipo de fraude en tarjeta de crédito o débito?			
3.- ¿Conoce usted en que consiste el skiming o clonación de tarjeta?			
4.- ¿Conoce usted, si en el Código Orgánico Integral Penal se encuentra tipificado el fraude electrónico?			
Seguridad	**MUY CONFIABLE**	**POCO CONFIABLE**	**NADA CONFIABLE**
5.- ¿Cómo calificaría usted la plataforma de seguridad utilizada en las instituciones financieras sobre los diferentes canales o dispositivos de tecnología ?			
6.- ¿Cuanta seguridad o confianza le inspira transaccionar actualmente con tarjeta de crédito o de débito?			
Normativa	**DE ACUERDO**	**EN DESACUERDO**	**INDIFERENTE**
7.- ¿Considera usted que la falta de tipificación del delito informático es causa para que se siga produciendo el fraude electrónico?			
8.- ¿Cree usted que es adecuado la conceptualización de los tipos de fraude en la Ley de Comercio Electrónico para reducir y regular este tipo de delitos?			
9.- ¿Considera que los jueces y fiscales de nuestro país deben de estar mejor informados de este tipo de delitos para la aplicación de la ley?			
Sanción	**DE ACUERDO**	**EN DESACUERDO**	**INDIFERENTE**
10.-¿Considera conveniente que el fraude electrónico debe tener una sanción más severa en nuestra legislación pena?			

Cómo funciona el sistema

1 INSTALACIÓN FRAUDULENTA

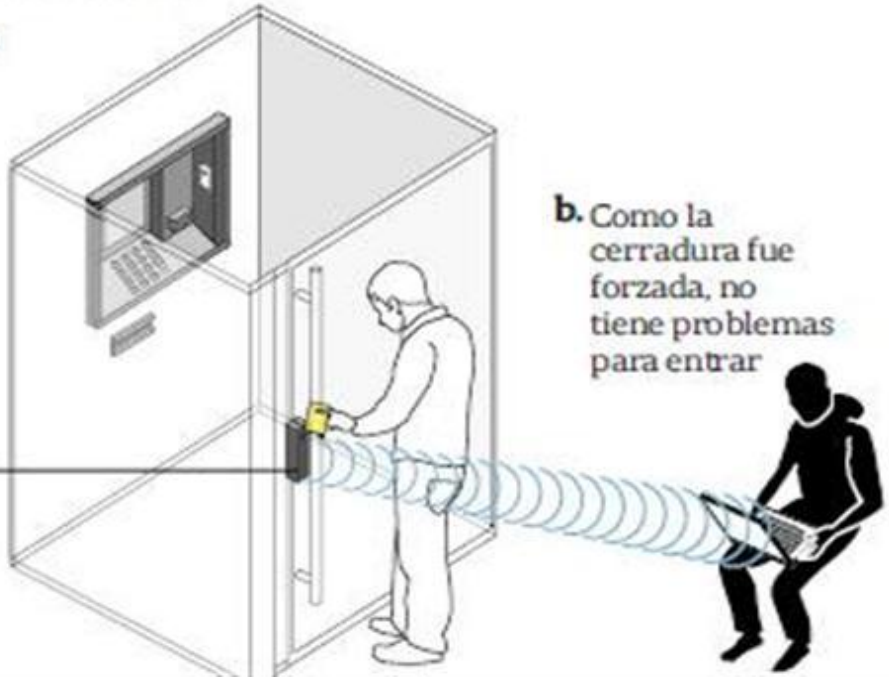
Los ladrones llegan al cajero y fuerzan la cerradura para que no sea necesaria la tarjeta para abrir

b. Colocación de una minicámara

a. Colocación de un lector de ingreso falso

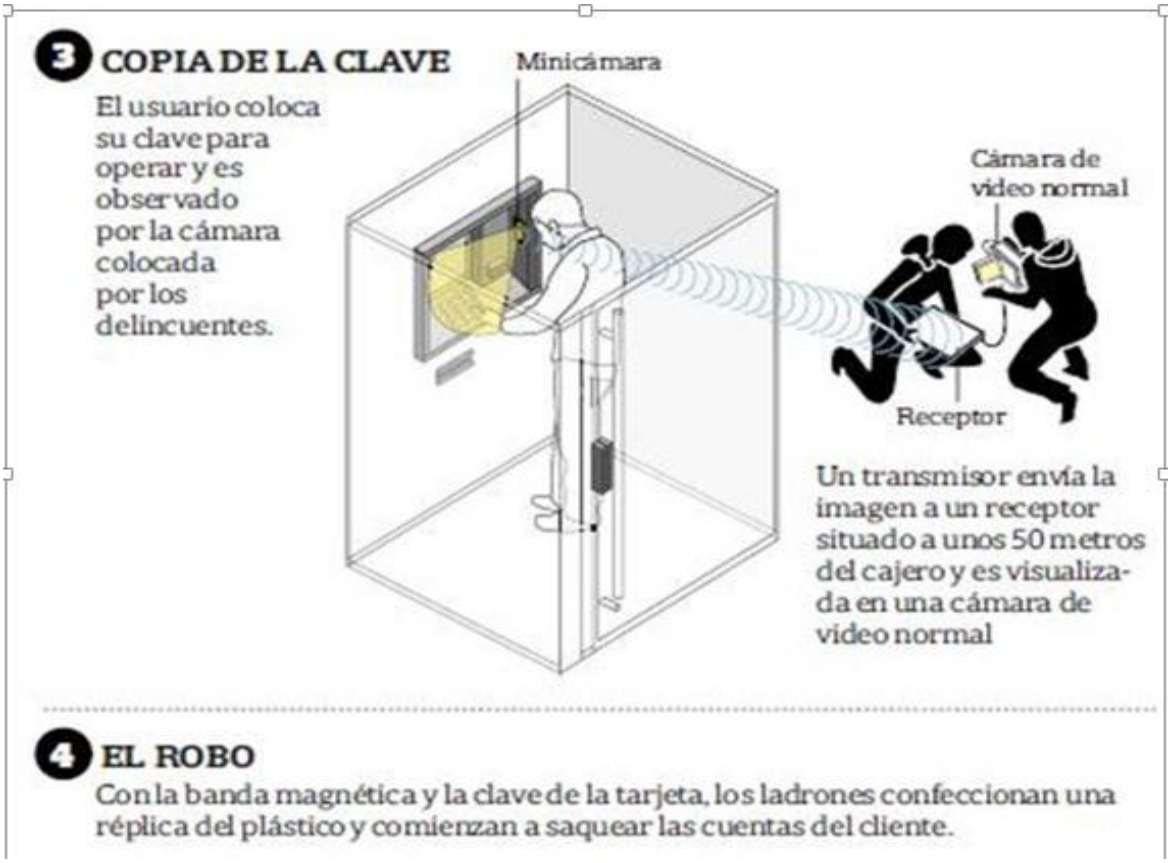
2 INGRESO DEL CLIENTE

El usuario pasa su tarjeta por el lector falso de entrada del banco para ingresar.



a. La banda magnética es copiada.

b. Como la cerradura fue forzada, no tiene problemas para entrar


3 COPIA DE LA CLAVE
El usuario coloca su clave para operar y es observado por la cámara colocada por los delincuentes.
Minicámara
Cámara de video normal
Receptor
Un transmisor envía la imagen a un receptor situado a unos 50 metros del cajero y es visualizada en una cámara de video normal
4 EL ROBO
Con la banda magnética y la clave de la tarjeta, los ladrones confeccionan una réplica del plástico y comienzan a saquear las cuentas del cliente.


Proceso de un Phishing
1 El atacante crea el email falso y la web falsa
2 Le envia el email falso con el link de la web falsa al correo de los usuarios
3 Los usuarios víctimas reciben el email falso
4 Acceden al email falso con el link de la web falsa
5 Los usuarios son engañados con la web falsa y completan los datos solicitados
Atacante (Hacker)
Credenciales (usuario y clave)
Datos personales (nombre, cédula de identidad, dirección
No. Cuenta bancaria, No. Tarjeta de crédito
Los datos solicitados y completados por los usuarios víctimas en la web falsa con enviados al atacante