UNIVERSIDAD DE LAS AMÉRICAS
Laureate International Universities®

FACULTAD DE CIENCIAS DE LA COMUNICACIÓN

CONDICIONES DE REEMBOLSO A USUARIOS DEL SISTEMA FINANCIERO PRIVADO, POR DELITOS INFORMÁTICOS EN LÍNEA EN EL DISTRITO METROPOLITANO DE QUITO

Trabajo de Titulación presentado en conformidad a los requisitos
establecidos para optar por el título de
Licenciada en Periodismo

Profesora Guía
Mónica Orozco Medina, Mgtr.

Autora
Mercedes Amelina Espinosa Altamirano

Año
2014

DECLARACIÓN DEL PROFESOR GUÍA

“Declaro haber dirigido este trabajo a través de reuniones periódicas con el/la estudiante, orientando sus conocimientos para un adecuado desarrollo del tema escogido, y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación.”

_____

Mónica Orozco Medina

Magíster

C.I.: 171635931-8

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

“Declaro que este trabajo es original, de mi autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes”.

_____

Mercedes Amelina Espinosa Altamirano

C.I.: 180428376-8

AGRADECIMIENTOS

Una de las frases que siempre tuve en mi mente desde el inicio de este estudio, es aquella de James Dean: “Vive como si fueras a morir mañana, aprende como si fueras a vivir para siempre”, frase compartida por mi padre, como un mensaje de aliento al iniciar este reto. Es por eso, que quiero agradecer eternamente a mis padres, porque a pesar de no acompañarme físicamente durante mi período estudiantil, con una llamada o visita inesperada, supieron darme el aliento necesario para seguir adelante y cumplir este sueño. También quiero agradecer a mi novio, por sus ideas y sugerencias siempre. Moni, para usted un agradecimiento muy especial e infinito por esa paciencia y guía en cada minuto que necesitaba de su ayuda, sin importar el día ni la hora. Por compartir conmigo sus conocimientos, una vez más mil gracias. Así como a los maestros y gente cercana que supieron ayudarme con una guía para el desarrollo de esta tesis.

RESUMEN

En este trabajo se realizó un análisis de las condiciones de reembolso a los usuarios del sistema financiero privado víctimas de los delitos informáticos en el Ecuador.

El trabajo parte de un análisis de los momentos históricos importantes de la banca del Ecuador, factores que explican el momento actual que vive el sector. A este estudio se sumó un análisis de los delitos informáticos, de la Ley de Comercio Electrónico Mensajes de Datos y Firmas Electrónicas y el Código Penal Ecuatoriano, leyes con las que se pudo evidenciar que existen vacíos al momento de tipificar los delitos informáticos en el país.

Mediante entrevistas y encuestas con los usuarios de la banca, se pudo evidenciar que estos no recuperan su dinero tras ser víctimas de la ciberdelincuencia. Hay que resaltar que esto ocurre actualmente por las falencias en seguridad de los sistemas bancarios, que son vulnerados por los ciberdelincuentes a diario.

Frente a esto, los afectados no tienen un respaldo como usuarios de la banca y a pesar de que las leyes y las entidades pertinentes existen, los afectados no reciben una guía clara de cómo realizar sus denuncias y las entidades encargadas del tema no dan una respuesta a todos los casos.

ABSTRACT

This work analyzed the conditions applied to the reimbursement to the users of the private financial system, who were victims of cyber attacks in Ecuador.

Various authors were studied in order to research the historical moments of Ecuador's banking system. These factors explain the current circumstance and the informatics crimes in general. To this study was added an analysis of the cyber attacks, of the Law of Electronic Commerce of Messages, Data and electronic signatures and the Ecuadorian legal code. The aforementioned laws helped demonstrate the existence of blank points that worsen the capability to typify the cyber crimes in Ecuador.

Through interviews and surveys with the accounting users it was possible indentify that said users didn't recover their money. This occurs because of the security mistakes on the banks.

The victims don't have a support as users and even though there are laws and entities in charge of supporting users, the victims don't have a clear guide as to how complaint and the entities in charge don't offer a clear answer in most cases.

ÍNDICE

INTRODUCCIÓN 1

1 CAPÍTULO I: ANTECEDENTES HISTÓRICOS, TEÓRICOS Y CONCEPTUALES DEL SISTEMA FINANCIERO **3**

1.1 TRAS LA HUELLA DE LA BANCA ECUATORIANA 3
1.1.1 Los inicios de la banca ecuatoriana 5
1.2 LOS INICIOS DE LA SUPERINTENDENCIA DE BANCOS Y SEGUROS DEL ECUADOR 8
1.3 SEGUNDO MOMENTO IMPORTANTE DE LA BANCA 9
1.4 CIFRAS DE LA EVOLUCIÓN DEL SISTEMA BANCARIO 15
1.5 BREVE HISTORIA DE LA OFERTA FINANCIERA EN EL ECUADOR 18

2 CAPÍTULO II: ANTECEDENTES HISTÓRICOS, TEÓRICOS Y CONCEPTUALES DE LOS DELITOS INFORMÁTICOS Y SUS TIPOS 21

2.1 DEFINICIÓN Y CONCEPTO DE LOS DELITOS INFORMÁTICOS 21
2.2 TIPOS DE DELITOS INFORMÁTICOS 25
2.2.1 Una propuesta de clasificación 27
2.2.1.1 Fraudes informáticos 27
2.2.1.2 El sabotaje informático 31
2.2.1.3 El espionaje informático y el robo a hurto de software 32
2.2.1.4 El robo de servicios 33
2.2.1.5 Acceso no autorizado a servicios informáticos 33
2.3 CARACTERÍSTICAS DE LOS DELITOS INFORMÁTICOS 35
2.3.1 Sujetos del delito informático 36
2.3.1.1 Sujeto activo 36
2.3.1.2 Sujeto pasivo 38
2.4 LEGISLACIÓN EXTRANJERA 40

3 CAPÍTULO III: ANÁLISIS DE LA SITUACIÓN ACTUAL Y LA LEGISLACIÓN ECUATORIANA FRENTE A LOS DELITOS INFORMÁTICOS 43

3.1 VACÍOS EN LA LEGISLACIÓN ECUATORIANA 43
3.2 LAS SANCIONES EN EL CÓDIGO PENAL ECUATORIANO 44
3.3 LOS DELITOS INFORMÁTICOS EN ECUADOR 47
3.3.1 Los delitos informáticos más frecuentes en el Ecuador 52

3.4 NUEVAS REFORMAS ENDURECEN LAS PENAS PARA DELITOS INFORMÁTICOS 53

4 CAPÍTULO IV: MEDIDAS DE SOLUCIÓN OPTADAS POR LAS ENTIDADES PARA LOGRAR FRENAR LOS DELITOS INFORMÁTICOS 57

4.1 LOS CASOS DE DELITOS INFORMÁTICOS TUVIERON UNA RESPUESTA TEMPORAL 57
4.2 CORE BANCARIO 61
4.3 LOS USUARIOS DE LA BANCA CUENTAN CON DEFENSORES DEL USUARIO 62
4.4 EL FRAUDE EN LÍNEA EN LA VOZ DE LOS AFECTADOS 66
4.5 EL IMPACTO DE LA DUPLICIDAD DE FUNCIONES EN LAS CAUSAS 74

5 CAPÍTULO V: RESULTADOS Y ANÁLISIS DE LAS ENCUESTAS A USUARIOS 79

5.1 DESARROLLO DE LA ENCUESTA A USUARIOS DE LA BANCA PRIVADA QUE HAN SIDO VÍCTIMAS DE LOS CIBERDELITOS 79
5.2 EXPOSICIÓN DE LA ENCUESTA REALIZADA A LAS VICTIMAS DE CIBERDELITOS 80

6 CAPÍTULO VI: CONCLUSIONES Y RECOMENDACIONES 90

6.1 CONCLUSIONES 90
6.2 RECOMENDACIONES 90

7 CAPÍTULO VII: PROPUESTA COMUNICACIONAL 92

7.1 RADIO-REVISTA: E-BANK 92
7.1.1 Descripción de la revista 92
7.1.2 Objetivos 93
7.1.3 Audiencia 93
7.1.4 Anunciantes 93
7.1.5 Secciones 94
7.1.6 Talentos humanos 94
7.1.7 Recursos técnicos 94
7.1.8 Guión 94
7.2 REPORTAJE TELEVISIVO 94
7.2.1 Objetivo 94
7.2.2 Requerimientos 95
7.2.3 Guión 95
7.3 PORTAL WEB “E-BANK” 95

REFERENCIAS 97

ANEXOS 100

INTRODUCCIÓN

Si bien la evolución de la era digital permite a los usuarios ser parte del ciberespacio también encierran altos niveles de inseguridad. Según la empresa internacional Kaspersky Lab, en Ecuador, hasta febrero del 2014 se registraron 20 mil ataques de malware por día, lo que significa que hubo 820 ataques de malware por hora y 14 ataques de malware por minuto.

Los usuarios de la red están expuestos a ser víctimas de la ciberdelincuencia, pero especialmente los usuarios de la banca en línea, quienes enfrentan hoy nuevas formas de delincuencia.

El delito informático opera desde un hogar hasta las mayores estructuras públicas o privadas. La globalización de la era digital permite expandir su alcance a escala internacional.

En el presente estudio se aborda el debate teórico en torno a los delitos informáticos. Además se detalla cómo operan los diversos tipos de delitos informáticos y se pone énfasis en los más recurrentes en el país.

Una vez estudiadas las bases teóricas e históricas, se expone un estudio sobre los vacíos que existe en la legislación local referente a los delitos informáticos. Los resultados de encuestas y entrevistas a usuarios de la banca, que fueron víctimas de delitos informáticos y que no recuperaron su dinero, también arrojan evidencia sobre estas falencias.

También se aborda el papel de las instituciones públicas y privadas encargadas de hacer el estudio de dichos casos, más cuando los delitos informáticos son difíciles de demostrar y resulta complicado hallar pruebas que ayuden a encontrar a los culpables.

Finalmente, con una metodología y con un sustento teórico se creó e-Bank, una línea de productos que busca informar a los usuarios sobre la información relacionada a la banca en línea. El objetivo es difundir y ser un servicio para los usuarios, especialmente aquellos que han sido víctimas de la ciberdelincuencia y evitar que nuevos usuarios de la tecnología lo sean.

1 CAPÍTULO I: ANTECEDENTES HISTÓRICOS, TEÓRICOS Y CONCEPTUALES DEL SISTEMA FINANCIERO

Para iniciar con este capítulo, es importante resumir los temas a tratar durante su desarrollo. Para poder entender la problemática de esta tesis, se ha decidido identificar los momentos históricos más importantes de la banca en el Ecuador. Desde sus inicios, sus años problemáticos y emblemáticos. Se explicará sobre la creación de las entidades como el Banco Central del Ecuador y la Superintendencia de Bancos y Seguros, parte fundamental del sistema como entidades de control de la oferta financiera existente.

Además, se abordará una etapa financiera que marcó la historia como es la crisis bancaria de 1999. Estos factores nos permitirán entender la evolución actual del sistema financiero.

1.1 TRAS LA HUELLA DE LA BANCA ECUATORIANA

El tema de la historia de la banca en el Ecuador ha sido abordado por varios autores, como Carlos Morlás (2004) o Luis Chiriboga Rosales (2010), entre otros. No todos los autores coinciden a la hora de definir a la banca o al momento de contar sus inicios.

En el artículo 2 de la Ley General de Instituciones del Sistema Financiero Ecuatoriano, promulgada el 12 de mayo de 1994, se menciona que:

> “Los bancos son instituciones financieras que se caracterizan principalmente por ser intermediarios en el mercado financiero, en el cual actúan de manera habitual, captando recursos del público para obtener fondos a través de depósitos o cualquier otra forma de captación, con el objeto de utilizar los recursos así obtenidos, total o parcialmente en operaciones de crédito e inversiones" (p. 1).

Luis Chiriboga Rosales (2010), quien publicó un libro denominado Sistema Financiero, que recoge la historia de los bancos en el país, agrega que los bancos son “sociedades anónimas que tienen como objetivo trasladar recursos de personas con exceso de liquidez a aquellas que necesitan dichos dineros para financiar sus inversiones” (p. 6).

Carlos Morlás Molina (2004), en su libro El ABC de la Banca, cita que la función de los bancos también es ofrecer un servicio técnico encaminado a satisfacer necesidades colectivas, básicas o fundamentales, mediante prestaciones individualizadas (p. 1). Añade que las instituciones del sistema financiero ecuatoriano se clasifican en instituciones financieras privadas, instituciones de servicios financieros y las instituciones de servicios auxiliares del sistema financiero.

Según Chiriboga (2007), este sector “se encarga de captar del público los recursos de capital y de transferirlos a los sectores productivos (intermediación financiera) y está conformado por entidades de carácter nacional y sucursales de bancos extranjeros” (p. 7).

El catedrático Morlás (2004, p. 1) menciona que el sistema financiero se clasifica en: bancos, sociedades financieras, asociaciones, mutualistas de ahorro y crédito para la vivienda y cooperativas de ahorro y crédito.

Los bancos, en definitiva, tienen como objetivo la captación de recursos y su colocación óptima en la cartera de créditos.

En el Régimen Financiero y Monetario Tomo 1, del Banco Central del Ecuador (2009), se cita el artículo 308 de la Constitución, que dice que el sistema financiero nacional se compone de tres sectores: público, privado y popular y solidario, que intermedian recursos del público. En este trabajo se estudiarán casos en el sistema financiero privado, por lo tanto se enfatizará más en este grupo.

1.1.1 Los inicios de la banca ecuatoriana

La banca tuvo un inicio desordenado en el Ecuador. El sector financiero estuvo compuesto por un reducido número de bancos privados, pero poco a poco fue ampliándose y actualmente comprende un gran número de partícipes. Los primeros bancos del país ecuatoriano pertenecieron a capitales privados y surgieron a mediados del siglo XIX. Los primeros bancos surgieron en la Costa, El primer banco fue fundado en Guayaquil por Manuel Antonio de Luzárraga en 1860 y se llamó Banco de Circulación y Descuento. En el apogeo de las exportaciones cacaoteras (1820-1920) creció más aún el sector financiero. Guayaquil era el eje del desarrollo bancario.

Hacia fines de 1875, la situación monetaria se normalizó. Los primeros bancos en el país, con el Banco del Ecuador a la cabeza, se transformaron inmediatamente en el eje del sistema financiero público y privado, según las obra Breve Historia Bancaria del Ecuador, del autor Wilson Miño Grijalba. Él dio a conocer los principales acontecimientos de la actividad bancaria nacional durante más de un siglo de historia bancaria (Grijalba, 2008).

En febrero de 1885 fue creado el Banco Internacional, como el banco de emisión y de depósito, lo que le posicionó como el principal rival del Banco del Ecuador. Este último, fue convertido en una verdadera fortaleza bancaria desde 1876 hasta 1917. El 31 de diciembre de este último año mencionado y tras la muerte de Eduardo Arosemena, ambos bancos pasaron a formar un frente común, en contra del proyecto de creación del Banco Central impulsado por Dillon.

Según el libro La Historia del Papel Moneda del Ecuador del autor Eduardo R. Trujillo (1984, p. 56), en 1920 surgió la propuesta de que los países tengan Bancos Centrales, durante la Conferencia Internacional de Bruselas.

En Ecuador, Luis Dillon, Ministro de Hacienda de la Junta de Gobierno, conformada por la Revolución Juliana del 9 de julio de 1925, fue quien propuso reformas del sistema bancario.

Dillon fue el pionero en varias gestiones: proponer y formular reformas al sistema bancario. Además, impulsó la creación del Banco Central del Ecuador. A pesar de eso, el proyecto Dillon pasó a segundo plano y las autoridades prefirieron la asesoría de expertos de afuera.

Este debate se daba en medio de la primera crisis de bancos que vivió el país en los años veinte.

Según la opinión de Luis N. Dillon, citado en la obra de Morlás (2004), la crisis causada en el país fue por varios factores:

> "Por la inconvertibilidad del billete, las emisiones sin respaldo, la inflación, la especulación, el abuso del crédito, el desnivel de la Balanza de Pagos, la falta de control oficial sobre los Bancos, la anarquía y rivalidad bancaria, debía enfrentare saneando la moneda y regularizando el cambio. La solución era la creación de un organismo llamado a cumplir estos fines, dentro de un complejo conjunto de reformas de la economía ecuatoriana, impulsadas por los militares y civiles congregados alrededor de las ideas julianas" (p. 173).

Morlás (2004) enfatiza el mérito de la Revolución Juliana fue iniciar el proceso de creación de un banco nacional de emisión con miras a poner fin a estos problemas. Con el apoyo de la Misión Kemmerer, el gobierno del presidente Isidro Ayora buscó, según una publicación del Diario Hoy del 12 de marzo de 1999, modernizar el Estado y reestructurar el sistema bancario del país (Hoy, 1999).

En el libro La Banca del Ecuador, una explicación histórica, del autor Mario Caness Oneto se indica que la propuesta del grupo de la Misión Kemmerer,

presidido por el profesor de Princeton, Edwin Walter Kemmerer, fue “corregir las deficiencias administrativas en el manejo de las finanzas, en un nuevo diseño económico, que lo pusiera a la altura de otros países del continente y del mundo” (2009, p. 1).

Finalmente, mediante Ley, se fundó el Banco Central del Ecuador, que abrió sus puertas el 10 de agosto de 1927 y el 25 del mismo mes se inauguró la Sucursal Mayor de Guayaquil. El Banco Central fue el único organismo que emitió legalmente monedas y billetes desde entonces.

Morlán (2004) menciona que por esta ley surgiría “una compañía anónima (BCE) autorizada durante 50 años para emitir dinero, redescontar préstamos a una tasa fija, constituirse en depositaria del dinero del Gobierno y de los bancos asociados, administrar el mercado de cambios y fungir de agente fiscal” (p. 174).

El historiador Juan Paz y Miño señala en su obra La Revolución Juliana en Ecuador, que el BCE se complementó con la Ley de Monedas que existía en Ecuador desde 1832 y Ley General de Bancos.

El BCE buscó estabilizar y unificar la moneda, que hasta entonces se emitía a libertad de cada banco. Para lograrlo, el Instituto Emisor se valió del “patrón oro de cambio”, que es el régimen monetario que fijaba el precio del sucre en términos del oro.

Según menciona Chiriboga (2007), el Banco Central es un ente jurídico de derecho público, de duración indefinida, con autonomía técnica y administrativa y patrimonio propio.

En la memoria anual 2003 del Banco Central del Ecuador, en el capítulo sexto del sistema de pagos ecuatoriano, se menciona que “bajo el esquema de dolarización de la economía ecuatoriana, la misión del Banco Central del

Ecuador, es promover y coadyuvar la estabilidad económica del país, tendiente a su desarrollo y crecimiento sostenido en el largo plazo" (p. 109, 2003).

Además, este autor agrega que esta entidad ya no puede conceder préstamos de última instancia a las instituciones del sistema financiero nacional.

1.2 LOS INICIOS DE LA SUPERINTENDENCIA DE BANCOS Y SEGUROS DEL ECUADOR

Paz y Miño (2013) resalta que Ley de Bancos fue presentada por Kemmerer y fue expedida por Decreto el 6 de septiembre de 1927.

> "Se creó una institución antes inexistente en Ecuador y que, con el paso del tiempo, se constituiría en una entidad fundamental para el control a los bancos al "Departamento Bancario", que nació en el Ministerio de Hacienda y cuyo jefe denominaría "Superintendencia de Bancos" (p. 70).

Antes de que exista el Superintendente, en 1914 se creó un "Comisario Fiscal de Bancos", pero según Paz y Miño (2013) sus actuaciones dejaron impune la plutocracia bancaria. Tras la presentación del proyecto de la Ley General de Bancos por la Misión Kemmerer y en la Exposición de Motivos se calificó como "infortunada" a la situación bancaria del Ecuador, añadiendo:

> "La Misión está convencida de que una supervisión eficaz de los bancos es un elemento esencial de cualquier plan de mejoramiento. La supervisión tiende a la prevención de desaciertos bancarios, antes que a la falsificación de delitos y al castigo de los delincuentes después de que los perjuicios se hayan producido".

Pero lo más contundente que resalta Paz y Miño (2013 p. 70) es que el cargo de Comisario Fiscal de Bancos fue creado como medida de emergencia en el

Decreto Ejecutivo de 1914 y que “nunca hubo supervisión eficaz de las operaciones de los bancos”.

A partir de la creación del BCE, se aprobaron leyes bancarias y la Superintendencia de Bancos, la Dirección General del Presupuesto, entre otras entidades, y además se logró regular la nueva estructura de la moneda. Con este organismo se logró regular la economía, las finanzas y la estabilidad de la moneda.

Durante la crisis financiera de los años veinte, aparte de la emisión de billetes sin respaldo, existieron otras causas financieras también poderosas. Como lo menciona Miño (2008), así se llega a otra de las causas fundamentales de la crisis.

Morlás (2004) define a la Superintendencia de Bancos como “el organismo técnico y autónomo encargado constitucionalmente y legalmente de la vigilancia y control de las instituciones financieras establecidas en el país” (p. 82).

El primer Superintedente de Bancos fue Harry L. Tompkins. Su primer informe lo presentó el 10 de septiembre de 1928. Entre la lista de los bancos que quedaron bajo la inaugurada Superintendencia estaban 22 bancos. En esta lista no se incluyó a las compañías de seguros. Entre algunos de los bancos estaban: Banco Anglo Sud Americano, Banco de Descuento, Banco de Manabí, Banco del Ecuador, Banco del Pichincha, Banco Territorial, entre otros.

1.3 SEGUNDO MOMENTO IMPORTANTE DE LA BANCA

En los años 90 surge otro de los momentos representativos de la banca donde se implementaron nuevas reglas. El libro La Banca de la Usura al Narcolavado, elaborado por Luis Torres Rodríguez, Presidente Ejecutivo de la Fundación Avanzar, aborda las reformas financieras de 1994, en el gobierno de Sixto Durán Ballén y Alberto Dahik.

> “(Las reformas) permitieron una enorme concentración del crédito en empresas vinculadas a los accionistas de los bancos hasta por el 60% de la cartera, lo que unido a la cómplice supervisión de los organismos de control, Superintendencia den Bancos y Banco Central, condujo a una situación de descontrol del sistema financiero” (p. 1).

Sin duda la crisis bancaria de 1999 fue el hecho de mayor trascendencia en la historia del sistema financiero ecuatoriano. Durante esta década, 17 de 40 bancos que en este entonces operaban en el país, colapsaron.

El Banco Central del Ecuador concedió en los dos últimos meses de 1995 y durante 1996, recursos a 12 bancos privados y 30 sociedades financieras. En el caso de los bancos privados, estos créditos alcanzaron hasta el 200% de su patrimonio técnico y, en el de las sociedades financieras, representaron hasta el 100% de ese indicador. A partir de agosto de 1996, en el gobierno de Bucaram, modificó las leyes para que los bancos no fueran liquidados inmediatamente.

Tras el cierre de bancos, Morlás (2004) menciona en su obra que el Superintendente de Bancos, Jorge Egas Peña, fue quien mediante una cadena nacional de radio y televisión, dio a conocer el diagnóstico del sistema financiero.

19 bancos continuarían operando normalmente en el país, cuatro recibirían el fortalecimiento patrimonial del Estado con créditos totales por cerca de USD 148 millones con plazo a un año, tres serían reestructurados y absorbidos por el Banco Continental (de propiedad del Banco Central del Ecuador) y dos entraron en saneamiento bajo el control de la Agencia de Garantías de Depósitos (AGD) (p. 78).

El Estado quiso salvar a los bancos con la Agencia de Garantía de Depósitos (AGD), pero no corrigió el problema y les dio más recursos en el llamado

“salvataje bancario”. Entre noviembre de 1999 y septiembre de 2002, los banqueros recibieron USD 212 millones, algo que algunos califican como una gran “ganancia” en plena crisis financiera.

El panorama para que esto sucediera se complicó desde el domingo 7 de marzo de 1999, cuando el Presidente de la República, Jamil Mahuad, decidió mediante decreto un feriado bancario.

El 9 de enero del 2000, el Gobierno decretó la dolarización en el país. Sin embargo, este sistema dolarizado fue impulsado por el mismo Banco Central del Ecuador, según afirma el autor Morlán (2004). Este autor enfatiza que esta decisión le llevó al país a estar al borde de la hiperinflación a causa del exceso de emisión inorgánica por cuenta del BCE, donde el sucre se lo hacía circular sin ningún respaldo, originándose depreciación acelerada de la moneda ecuatoriana.

Los primeros bancos en caer en la década de los 90 fueron: Continental, Préstamos, los Andes, Mercantil Unido, Solbanco y Tungurahua, que entraron en un proceso de saneamiento mientras el Filanbanco fue reestructurado. Además, por problemas de deficiencia, créditos vinculados, mala administración y falta de pagos quebraron los bancos Occidente, De Crédito, Unión, Financorp y Finagro, del Progreso, Popular, Azuay, Bancomex, Popular, Unión, La Previsora.

Torres (2007) hace también un recorrido de lo que fueron los bancos en el país. Una ley publicada en el Registro Oficial el 12 de mayo de 1994, puso las nuevas reglas para la banca: más “libertades” para conceder créditos vinculados y para obtener préstamos del Estado.

Para salvar a los bancos, el 1 de diciembre de 1998, por sugerencia del Banco Mundial y Guillermo Lasso, Ministro de Economía de Jamil Mahuad y una mayoría del Congreso Nacional, crearon la Agencia de Garantía de Depósitos,

(AGD) mediante la “Ley de Reordenamiento en materia económica, en el área tributaria financiera”.

En entrevista realizada para esta tesis, la ex Ministra de Economía y ex titular de la AGD, Wilma Salgado menciona que en 1994 se reformó la Ley de Instituciones Financieras, que buscaba desregular y liberalizar al sistema financiero, lo que incluyó medidas para permitir la libre circulación de capitales a escala internacional, incluidos de corto plazo, permitir la libre asignación del crédito por parte de los bancos, inclusive permitiendo en ciertos porcentajes la concesión de créditos a empresas vinculadas.

Al mismo tiempo que se achicaba el aparato del Estado, eliminando ciertas regulaciones que eran calificadas por los banqueros como de represión financiera, y se disminuía el tamaño del Estado, concretamente se despidió en forma masiva personal de la Superintendencia de Bancos.

Según Salgado, esto dio paso a la concentración del crédito en empresas relacionadas con los accionistas de los bancos, las empresas vinculadas, sin cumplir con las garantías legales. “Aquí la Superintendencia de Bancos no cumplió con su obligación de vigilar para que los créditos que conceda la banca cuenten con las respectivas garantías legales”.

El Fenómeno del Niño registrado en 1997/1998 y los efectos de la crisis asiática de los mismos años, fueron los detonantes de la crisis financiera y económica en el Ecuador y en varios países de América Latina. Sin embargo, la crisis fue más profunda en el Ecuador, debido a las políticas adoptadas por el gobierno del Presidente Jamil Mahuad, denominadas de salvataje bancario, que consistieron en la canalización masiva de recursos financieros a la banca:

- En un primer momento, entre Agosto 1998 hasta febrero de 1999, mediante créditos denominados de liquidez concedidos por el Banco Central, con el argumento de impedir la quiebra de los bancos. El Banco

Central concedió créditos masivos a la banca, en la moneda nacional de entonces, incumpliendo su obligación de “velar por la estabilidad cambiaria” que constaba en la Ley de Régimen Monetario.

- En marzo de 1999 se congelaron los ahorros de los depositantes en los bancos, privando de capital de trabajo a las empresas y de sus ahorros a las familias, empujando a la economía a una profunda recesión; y,

- Una vez creada la AGD, el Ministerio de Finanzas emitió los bonos AGD, que eran canjeados por la AGD con sucres de emisión del Banco Central, por alrededor de USD 1 700 millones, continuando con la inyección de moneda nacional sin respaldo en el mercado. La mayor parte de esos recursos no se utilizaron en la devolución de depósitos a los depositantes perjudicados por la quiebra de los bancos, sino que se canalizaron a otros bancos que, más tarde, también quebraron.

Una característica de esta política denominada de salvataje bancario, es que no impidió la quiebra de los bancos, sino que permitió que los banqueros reciban beneficios extraordinarios en la crisis. Quebraron los bancos, pero no los banqueros, porque éstos: Se quedaron con la propiedad de las empresas vinculadas en donde estaba concentrado el crédito concedido con los ahorros de los depositantes, puesto que no han pagado sus deudas; recibieron préstamos del Banco Central que no devolvieron en su totalidad; se congelaron los ahorros de los depositantes cuando la cotización del dólar era de 9 500 sucres por dólar y cuando se descongelaron, la cotización era de 25 000 sucres, beneficiándose los banqueros en perjuicio de los depositantes que tenían sus ahorros en moneda nacional; y, finalmente, el Estado se hizo cargo de pagar los pasivos de los bancos, tanto a los depositantes como a los acreedores internacionales con fondos públicos, esto es, con recursos de todos los ecuatorianos.

Frente a esto, Salgado afirma que, mientras fue Gerente de la AGD, impidió la prescripción de las deudas, iniciando los juicios de coactiva. Recuerda que la

citación a los deudores se realizó por la prensa, puesto que se desconocían las direcciones de los deudores dado el tiempo transcurrido desde la quiebra de los bancos.

“Empresas vinculadas no se acercaban a pagar sus deudas, conformé equipos de investigación, encontrando que la mayoría de dichas empresas ya habían sido liquidadas y disueltas, tratando de desaparecer a la figura del deudor”. (Salgado, 2014)

Tras eso, iniciaron las investigaciones sobre el destino de los ahorros de los depositantes, encontrando que habían sido transferidos los activos de las empresas vinculadas a terceras empresas creadas por lo general fuera del país, para disfrazarlas de extranjeras. “Habían sido escondidos en fideicomisos, de cuya existencia se desconocía; o habían sido transferidos a nombre de testaferros…”

Salgado considera que una de las consecuencias de esa época fue una enorme concentración del ingreso a favor de los accionistas de los bancos quebrados que no pagaron las deudas de sus empresas vinculadas, ni devolvieron los créditos recibidos desde el Banco Central y desde el Ministerio de Finanzas.

La contrapartida fue el violento empobrecimiento de la mayoría del pueblo ecuatoriano, estimándose que migraron alrededor de 1 millón de ecuatorianos fuera del país, en busca de sustento para sus familias, a tal punto que las remesas de los migrantes pasaron a convertirse en la segunda fuente de ingreso de divisas, después del petróleo.

La población ha intentado crear mecanismos alternativos para manejar sus ahorros, registrándose un auge del crecimiento de las cooperativas y de otras formas de organización social para el manejo de sus ahorros. Lamentablemente todos los delitos cometidos por los banqueros han quedado en la impunidad.

La vinculación de los gobiernos de turno y los partidos políticos con los banqueros, por sus aportes económicos a las campañas políticas, con el consecuente nombramiento de autoridades de los organismos de control, también “vinculados” a los banqueros fue otro problema, según Salgado. Además, otra razón, dice Salgado, es la “débil organización ciudadana, que no tuvo la capacidad de reacción frente a tanto abuso de autoridades y banqueros”.

1.4 CIFRAS DE LA EVOLUCIÓN DEL SISTEMA BANCARIO

Desde inicios de los años 2000, el Ecuador ha contado con una coyuntura internacional absolutamente favorable, por el incremento registrado en los precios del petróleo (de USD 6,9 el barril en agosto 1998 a bordear e incluso superar por momentos los USD 100 el barril desde el 2013). Esto es un factor del desarrollo del sistema bancario del país de los últimos años.

Además de esto, señala la ex Ministra Wilma Salgado han influido en este desarrollo el alza de los precios en el resto de productos primarios de exportación. Están también otros factores como las tasas de interés muy bajas en los mercados financieros internacionales, un dólar devaluándose frente al resto de divisas, ingreso de capitales al país atraídos por los diferenciales de tasas de interés y por las favorables condiciones de la economía.

En ese escenario internacional tan favorable, la banca ha registrado un crecimiento y desarrollado acelerado, aumentando tanto las captaciones como las colocaciones, dinamizando el crédito al conjunto de la economía, en particular al consumo.

Este escenario se evidencia en la evolución de los depósitos de la banca. Al registrarse 6.251 depósitos a la vista durante el 2006 y 18.254, se evidencia que en ocho años se triplicaron los depósitos en el país.

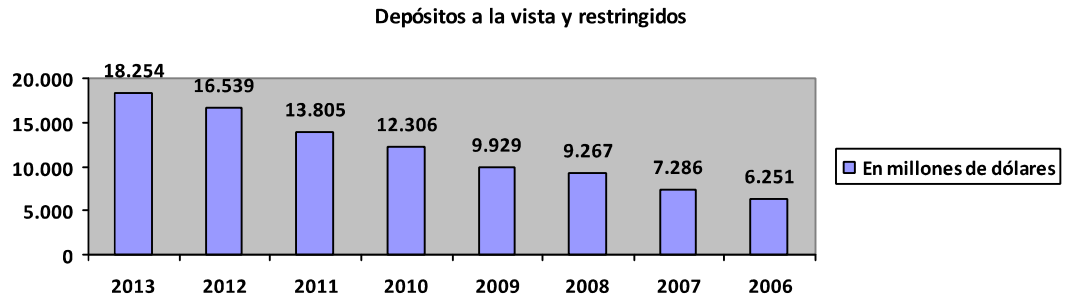


Figura 1. Depósito a la vista y restringidos
Tomado de SBS, 2013

En lo que respecta a las pérdidas y ganancias de los bancos privados del país, durante el período 2006-2013, se puede apreciar que los bancos han registrado ganancias que superan los USD 200 millones de dólares los últimos ocho años, incluso en dos años (2011-2012) esta cifra sobrepasó los USD 300 millones.

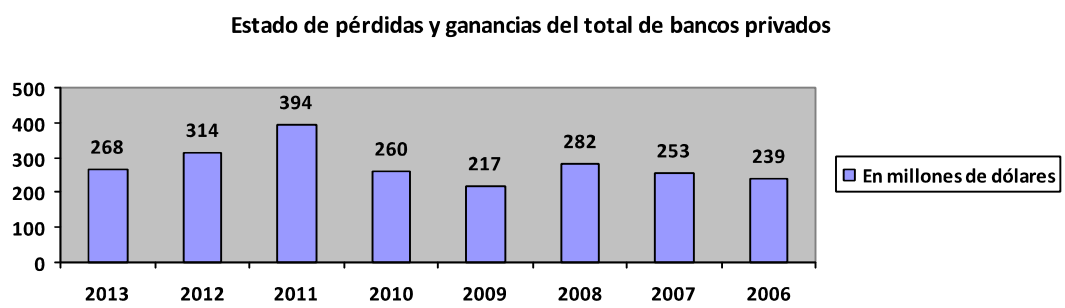


Figura 2. Estado de pérdidas y ganancias del total de bancos privados
Tomado de SBS, 2013

En lo que respecta a la composición de la cartera de créditos por vencimientos y líneas de negocio, se evidencia que durante el 2013 el total de la cartera bruta fue de USD 17 252 millones de dólares del total de bancos privados. De este monto, se evidencia que hubo más crédito comercial con USD 8 399 millones, seguido con el crédito de consumo, con USD 6 111 millones.

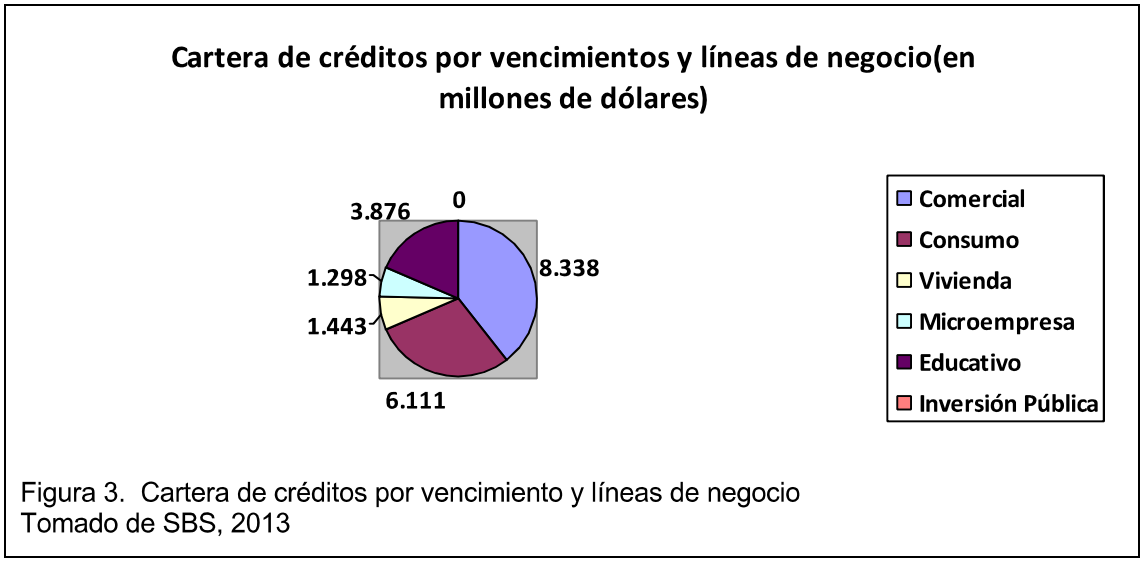


Figura 3. Cartera de créditos por vencimiento y líneas de negocio
Tomado de SBS, 2013

La calificación de riesgo de la banca privada del país, con un puntaje límite de 20 puntos, Citibank era el único banco con el puntaje más alto y con una calificación de AAA, que significa que la situación de la institución financiera es muy fuerte y ha registrado una buena trayectoria de rentabilidad. (SBS, Marzo 2013). Hay que resaltar que una entidad bancaria puede llegar a tener nueve calificaciones.

Seguido de este listado, se ubicó el Bolivariano, Pichincha y Produbanco con 18 puntos y calificación de AAA-/AAA. Los bancos de Guayaquil, Internacional y Procredit, tenían en cambio, una calificación de AAA/AAA-. Mientras que, entre la lista de los bancos con peores calificaciones, se ubicaron los bancos Cofiec con calificación C y puntuación 5, seguido del Banco Sudamericano, con calificación BB, que equivale a un puntaje de 4. (**Ver Anexo 1)**

Por otra parte, en lo que respecta a los indicadores financieros del sistema de bancos privados del Ecuador, relacionados a los resultados del ejercicio y patrimonio promedio del total de bancos privados, que permite medir la utilidad de la banca, se puede apreciar que durante el 2006 se registró un mayor porcentaje, que fue 24%, es decir más del doble que el porcentaje registrado en el 2013 que fue de un 11%. Salgado (2014) explica que las utilidades de la banca privada se han reducido en el último año, 2013, como consecuencia de

medidas de política económica adoptadas, en particular la adoptada por el Gobierno nacional para financiar el aumento del bono de desarrollo humano. Sin embargo, en general, cree que la situación de la banca es sólida, lo que no significa que esté exenta de riesgos macroeconómicos.

Figura 4. Indicadores financieros del sistema de bancos privados
Tomado de SBS, 2013

1.5 BREVE HISTORIA DE LA OFERTA FINANCIERA EN EL ECUADOR

En 1914 existían en Ecuador tres instituciones bancarias generadoras de crédito en forma de billetes y de cheques: Banco Comercial y Agrícola y Banco del Pichincha. Como lo cita Miño (2008) dicho año existían 18 instituciones de crédito.

La presencia de la banca privada cubría íntegramente la Sierra y Costa ecuatoriana y la provincia de Pastaza en el Oriente. Miño (2008) cita la base de datos de la Superintendencia de Bancos (1983) y menciona que en los años setenta se crearon ocho bancos, mientras que en 1979 el sistema de bancos privados estuvo integrado por 28 matrices.

La vigencia de la Ley General de Instituciones del Sistema Financiero, desde mayo de 1994, cambió la estructura del Sistema Financiero Nacional. A partir de ese año, el número de las entidades bancarias se ubicaron de la siguiente manera:

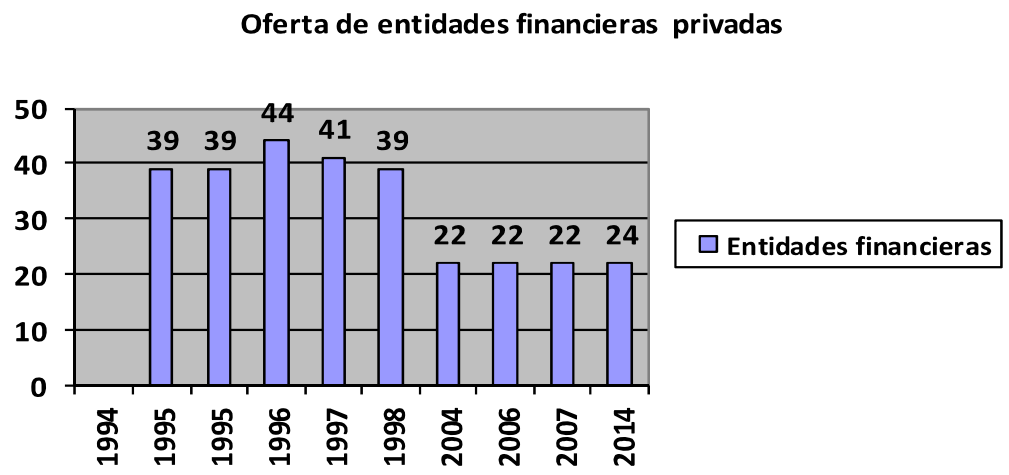


Figura 5. Oferta de entidades financieras privadas
Tomado de BCE, 2014

Es importante resaltar que en 1995 se seguía manteniendo un alto grado de concentración bancaria en las provincias de Pichincha, Guayas, Azuay y Tungurahua, lo cual ha contribuido a la mayor captación de ahorro.

El incremento de los depósitos de las instituciones bancarias fue de 35.5% entre 1997 y 1998, pasando de 21.511 mil millones de sucres a 29.154 mil millones de sucres, con una participación total en el Sistema Financiero Privado de 92,81% en 1998. Para diciembre de 1999, existieron 1952 depósitos a la vista y a plazo (en millones de dólares). Mientras que, la evolución de la cartera de crédito en estos mismos años, fue de USD 1 867 millones en 1999, USD 1 959 millones en el 2000 y USD 2 234 millones en el año 2001. A mediados de 2007, los depósitos ascendieron a USD 11 000 millones.

En los últimos diez años, se podría decir que el sector bancario, en particular, mostró una notable mejoría, producto también de un clima macroeconómico favorable para el Ecuador. Si bien la Superintendencia de Bancos tiene el reto de profundizar las reformas que se han llevado a cabo para determinar la real fortaleza del sector.

Pero también evidencia que a partir de la crisis bancaria de 1999 la Superintendencia de Bancos ha llevado a cabo esfuerzos significativos, con el apoyo de organismos multilaterales y el Gobierno Central, para modernizar y elevar sus controles a estándares internacionales. Se han emitido reglamentos que proveen lineamientos para el tratamiento de los diferentes riesgos financieros, y se ha profesionalizado y especializado en dicha área.

Este desarrollo también ha llevado a que en los últimos seis años se dé paso al sistema bancario en línea.

Las transacciones de dinero y consultas de estado de cuenta actualmente se efectúan a través de Internet, desde cualquier lugar del mundo, con accesos en clave otorgados por el banco a cada cliente. En la actualidad, toda entidad financiera oferta a sus clientes un servicio bancario en línea, lo cual contribuye en la mejora de la atención al usuario, de quien ya no se requiere una presencia física, que haga filas o papeleos en las agencias de su banca.

El Banco Pichincha, Banco de Guayaquil, Produbanco y Banco Bolivariano poseen tarjetas con coordenadas dinámicas (es un tipo de clave dinámica que permite autorizar operaciones por internet). Estas tarjetas son únicas y personales del cliente, cuentan con claves/coordenadas que son solicitadas para cada usuario).

Sin embargo, si bien este fue un gran avance de la banca, el acceso en línea ha dado paso a varios comportamientos ilícitos en la red, denominados en la actualidad como delitos informáticos. Al mismo tiempo que se extienden en la web varios servicios para el usuario como parte de una mejor de la calidad de vida y de progreso de la banca, se convierten en un incentivo para la delincuencia: robo y estafa en línea. A continuación, ampliaremos más sobre lo que engloban los delitos informáticos en línea.

2 CAPÍTULO II: ANTECEDENTES HISTÓRICOS, TEÓRICOS Y CONCEPTUALES DE LOS DELITOS INFORMÁTICOS Y SUS TIPOS

En el presente capítulo, se explicará qué es un delito informático, según las teorías de diferentes autores. Además se ampliará sobre los delitos informáticos más importantes para este estudio, ya que existen una gran variedad de tipos de delitos dentro de la literatura. Es importante que el lector diferencie lo que es un fraude, un *scam*, el *pishing* o *pharming*, que son algunos de los tipos de fraudes más comunes que sufren los usuarios de la banca electrónica.

Asimismo, se abordará en el estudio de este capítulo, las características de los delitos informáticos, más cuando estos son difíciles de demostrar y resulta complicado hallar pruebas que ayuden a encontrar a los culpables.

Se ampliará además sobre la diferencia de los sujetos de este tipo de delito, que son los activos que son aquellas personas comúnmente no identificadas, que cometen estos actos delictivos mediante la red. Mientras que, los sujetos pasivos, son los individuos de las instituciones afectadas que son víctimas de este tipo de fraude. Toda esta explicación nos ayudará a entender mejor sobre los delitos informáticos.

2.1 DEFINICIÓN Y CONCEPTO DE LOS DELITOS INFORMÁTICOS

La globalización tiene mucho que ver en los ámbitos políticos, militar, social y cultural. La revolución de tecnológica es uno de los motores de la globalización y en sus dominios crecen vertiginosamente nuevas modalidades de delito. En lo referente a la tecnología de la información, el delito también se “globaliza”, ya que el delito informático opera potencialmente desde un hogar, o hasta en las mayores estructuras públicas o privadas. La globalización permite expandir su alcance a lo internacional.

El acceso a una cuenta bancaria en línea ha dado paso a varios comportamientos ilícitos en la red, los cuales se han incrementado en los últimos cinco años, especialmente en Ecuador. Se trata de nuevas formas de delincuencia.

El término de delito informático no se encuentra tipificado en el Código Penal y es una limitante para comprender el concepto, características y las consecuencias con respecto a los actos irregulares o ilícitos informáticos que se cometen por medio del uso de un computador. Antes de entrar en este análisis, es importante definir el concepto de delitos informáticos.

La denominación de los delitos informáticos proviene de las expresiones inglesas *computer crime* y *computer-related crime* (delitos informáticos). Estas son definidas por la doctrina española como "aquellas conductas que ponen en peligro o lesionan la integridad, confidencialidad y/o disponibilidad de los datos y sistemas informáticos" (Rodríguez, 2002, p. 261).

Sin embargo, no existe una definición de consenso en el ámbito internacional de dicho término. En el caso de Ecuador, tampoco está definido en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, pese a que esta trata sobre las contravenciones y delitos relacionados a la actividad informática.

Existen tratadistas que lo han definido desde su aparición, hace más de 30 años. A continuación, se mencionan algunas definiciones de delito informático, que es importante comprender para esta tesis.

En el Convenio de Ciberdelincuencia (Consejo de Europa, 2001), o más conocido como convenio de cibercriminalidad, se define a los delitos informáticos como "los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos; así como el abuso de dichos sistemas, de redes y datos". (p. 2)

Este tratado internacional, elaborado por el Consejo de Europa en Estrasburgo, fue el primero en buscar soluciones a los delitos informáticos, con la aplicación de leyes que sancionen estos delitos.

Sin embargo, dentro de la delimitación del fenómeno de la delincuencia informática, se podría decir que la indebida utilización de cualquier medio informático de la tecnología moderna, da lugar a la conducta delincuencial en el ámbito de la cibernética (tecnología informática). Romeo Casabona en su obra Poder Informático y Seguridad Jurídica (Madrid, 1987), señala que si bien en la literatura de la lengua española se ha ido imponiendo la expresión de delito informático, es preferible hablar de delincuencia informática o delincuencia vinculada:

> "No se puede hablar de un delito informático, sino de una pluralidad de ellos, en los que encontramos como única nota común su vinculación de alguna manera con los computadores. El computador es en ocasiones el medio o el instrumento de la comisión del hecho, pero en otras es el objeto de la agresión en sus diversos componentes" (p. 204).

Para el autor español, el término delito informático debe usarse para designar una multiplicidad de conductas ilícitas y no una sola de carácter general (Casabona, 1987).

Pero además, el delito informático como acción dolosa provoca un perjuicio a personas o entidades en cuya comision intervienen dispositivos habitualmente utilizados en las actividades informáticas. Sin que necesariamente conlleve un beneficio material para su autor (Castillo y Romallo, 1989) (Camacho, 1997, p. 23).

Luis Camacho Losa (Madrid 1987), en su obra denominada El Delito Informático, coincide con Castillo y Ramallo, al mencionar que es una acción

dolosa, sin que necesariamente conlleve un beneficio material para su autor (p. 23).

Se podría decir que estas definiciones de una u otra manera son vagas, en cuanto no entregan una concreta delimitación de las fronteras en la que puede producirse los delitos infomáticos, desde un punto de vista jurídico.

De la literatura que se ha consultado para esta investigación, se entenderá como delito Informático a cualquier conducta criminal o acto ilícito en donde se utiliza al computador como instrumento o alguna herramienta informática que interfiera, destruya y hurte información.

Bajo la denominación de delitos informáticos o ciberdelitos, está la mala utilización de las computadoras, como medios para consumar el fraude, el espionaje, el sabotaje, la extorsión y otros ilícitos afines.

Entonces, existen varios tipos o géneros diferentes en gravedad y naturaleza, dependiendo de cuál sea el bien jurídico lesionado por el acto o de cómo y para qué se utilice la computadora; en tal virtud, cada caso merece ser analizado para determinar en forma la más exacta y posible la intención de la conducta.

Ecuador no se escapa de esta realidad. Es indispensable, por resguardo de la seguridad jurídica de las personas y de sus derechos, garantizar el uso lícito y adecuado de la informática en sus actuaciones públicas y privadas en el contexto de la globalización. El combate a esta nueva manifestación de delincuencia incumbe a todos los ciudadanos e instituciones del país, pero más directamente a la función judicial y a los entes públicos de control, más cuando las transacciones de dinero y consultas de estado de cuenta actualmente se efectúan a través de Internet, desde cualquier lugar del mundo, con accesos en clave otorgados por el banco a cada cliente.

Además, toda entidad financiera oferta a sus clientes un servicio bancario en línea, lo cual contribuye en la mejora de la atención al usuario, de quien ya no

se requiere una presencia física, que haga filas o papeleos en las agencias de su banca.

En ese contexto, los delitos informáticos se han incrementado, ya que los delincuentes ya no atacan a los bancos, sino a sus usuarios directamente. El acceso en línea ha dado paso a varios comportamientos ilícitos en la red. A medida que se extienden en la red varios servicios para el usuario, como parte de una mejor de la calidad de vida, crecen también las herramientas que motivan a la delincuencia: robo y estafa en línea.

2.2 TIPOS DE DELITOS INFORMÁTICOS

En 1990 la Organización de las Naciones Unidas (ONU), durante el Congreso sobre Prevención del Delito y Justicia Penal, celebrado en La Habana, Cuba, publicó un manual sobre prevención y control de los delitos informáticos. Allí se resalta una lista de los tipos de delitos informáticos, refiriéndolos en tres grupos.

Los fraudes por medio de manipulación de computadoras

Este tipo de delito es conocido también como sustracción de datos y es el delito informático más común, por ser fácil de cometer y difícil de descubrir. Para efectuarlo, no es necesario conocimientos técnicos de informática y puede cualquier persona que tenga acceso a las funciones normales de procesamiento de datos podría realizarlos.

Al atribuir la palabra manipulación, se refiere por ejemplo, a que un individuo estaría cometiendo un delito solo con el simple hecho de manipular datos personales de cualquier persona, o de programas, como en este caso, de programas de un sistema bancario en línea.

En este tipo también se le agrega al fraude realizado por manipulación informática, donde se aprovechan los procesos de cómputo. Esta es una

técnica especializada que se denomina "técnica del salchichón" apenas perceptibles como si se trataran de transacciones financieras, sacan repetidamente de una cuenta y se transfieren a otra. Incluso, cantidades mínimas como de un centavo de dólar, pasan a la cuenta de un tercero.

Para esto buscan diferentes victimas y esporádicamente retiran el dinero, sin que el usuario se dé cuenta. Con el tiempo, esta modalidad ha ido cambiando y ahora el atacante ahora prefiere sustraer ilícitamente cantidades significativas, de más de tres cifras, es decir ya no centavos, sino miles de dólares.

Los fraudes cometidos por manipulación de programas

Este delito se refiere a los fraudes realizados por manipulación informática. En este tipo de delito, es muy común usar las computadores como instrumento de falsificaciones de documentos de cualquier tipo, especialmente comercial. Por ejemplo, generalmente son las personas que alteran documentos en la Red, o que modifican datos sin autorización; cuando se aprovechan de las interacciones automáticas que se realizan en línea, para manipular y adquirir información confidencial.

Los daños o modificaciones de programas o datos computarizados

Este tipo de delito, engloba al sabotaje informático, que se refiere al acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema. Este tipo también incluye al acceso no autorizado a servicios y sistemas informáticos, que se pueden realizar por diversos motivos: desde la simple curiosidad hasta el sabotaje o espionaje informático. (Manual sobre prevención y control de los delitos informáticos ONU).

2.2.1 Una propuesta de clasificación

Acurio del Pino (2010) refuerza y amplía los tipos expuestos por la ONU y señala que los delitos informáticos se clasifica en: fraude, sabotaje informático, espionaje, robo de servicios y acceso no autorizado a servicios informáticos.

2.2.1.1 Fraudes informáticos

El fraude engloba lo referente a datos engañosos o falsos o también conocidos como Data diddling. El autor menciona que “es una manipulación de datos de entrada al computador con el fin de producir o lograr movimientos falsos en transacciones de una empresa” (P. 213). Es, además, uno de los delitos informático más comunes en el mundo y en el país, ya que como lo mencionamos anteriormente es fácil de cometer y difícil de descubrir.

Acurio del Pino detalla nueve subgrupos del fraude informático: scam, caballo de troya, técnica de salami, fasificaciones informáticas, manipulación de datos de salida, clonación de tajeras de crédito, débito, pishing y pharming. De este grupo, estudiaremos solo los más representativos para la realización de esta tesis.

‘Scam’

Es una especie de correo electrónico fraudulento que busca estafar económicamente al usuario mediante el “engaño”. Comúnmente ésta categoría busca un beneficio económico. Los más comunes scams son los conocidos como “Estafa a la Nigeria”, donde tratan de convencer al usuario que existen varios millones de dólares que no pueden salir del país por cualquier motivo, a no ser de que se transfiera a una cuenta extranjera y se entregue una comisión al receptor del correo electrónico. Por lo general, se hace creer que la transferencia es para una acción benéfica, que terminan en estafas.

Caballo de Troya

Su nombre es muy conocido y consiste en insertar nuevos programas, pero maliciosos, en los sistemas de computadoras. “Consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal” (Acurio del Pino, 2010, p. 213).

Técnica del Salami

Como lo mencionamos anteriormente, la ONU lo denomina la ténica del salchichón, donde esporádicamente el atacante roba cifras bajas, como centavos, para que los usuarios no se den cuenta. Para esto introducen un programa que transfiere el dinero de una cuenta bancaria a varias cuentas, de preferencia pequeñas cantidades de dinero.

Manipulación de los datos de salida

Este tipo de fraudes es aquel que se da mediante los cajeros automáticos. Se falsifican instrucciones de un computador y se adquieren datos personales de un usuario.

En un inicio este tipo de fraudes se cometía robando de manera física las tarjetas bancarias; sin embargo, hoy mediante programas de computadoras especializados en codificar información electrónica, pueden falsificar toda la información las tarjetas bancarias y de las tarjetas de crédito sin necesidad de sustraer estos documentos. Es muy común que en sitios comerciales como restaurantes o bares a la víctima le introduzca un chip en su tarjeta, que copia y almacena la información para luego ser descargada.

La clonacion de las tarjetas de débito sigue un proceso distinto. En primera instancia se clonan las denominadas bandas magnéticas de las tarjetas, o el

número de idenficación personal conocido como PIN (Personal Identification Number, por sus siglas en inglés).

Para cometer estos delitos, Acurio del Pino (2013) explica que se aplican carcasas junto a los lectores de los cajeros automáticos. También colocan cámaras que puedan registrar las claves, que posteriormente se graban en tarjetas en blanco.

Aunque la mayoría de estos delitos es mediante las tarjetas de crédito o débito, el fraude bancario en línea ha tomado la posta. En este estudio nos basaremos en los delitos en línea, donde se efectúan transferencias electrónicas.

'Phishing'

Este fraude informático también es conocido como "Phishing" o "Trapping", dependiendo si se han "pescado" claves de todo tipo mediante el Internet por correo electrónico, portales de chat, de tarjetas de crédito, etc. Este tipo de delito tiene como finalidad robar la identidad a una víctima que posea una cuenta bancaria. El delito consiste en obtener información como números de tarjetas de crédito, contraseñas, información de cuentas u otros datos personales, pero mediante engaños. (Acurio del Pino, 2010, p. 210)

La propia víctima puede caer en diferentes formas de engaño. Una de las maneras más comunes es mediante el envío de mails con formularios para obtener datos. Para esto, clonan una web oficial de una entidad bancaria, como si se tratara del portal original. Los usuarios reciben un mensaje electrónico que simula pertenecer a una entidad bancaria. La imagen corporativa de este sitio falso es idéntica con los logotipos, imágenes y textos que han sido recogidos del sitio real.

El autor Javier Fernández en su obra El cibercrimen y los delitos cometidos a través del internet, explica que para conseguir estos engaños los portales

fraudulentos piden al cliente que introduzca, como suele hacerlo en la web auténtica, sus contraseñas o números de tarjetas de crédito, de esta manera sus datos ya están en manos ajenas, listos para ser usados con fines delictivos (Fernández, 2009).

> “En ocasiones ni siquiera se redirige a la victima a la web falsa, sino que el mismo mail contiene un pequeño formulario en el que se pide al usuario que introduzca sus datos secretos de acceso y operaciones. Además, dependiendo del navegador que utilice el usuario, se llega a modificar la barra de direcciones, de tal modo que al seleccionarla se accede a la web suplantada” (p. 97).

Fernández añade que se han detectado otras formas de fraudes, como “encuestas falsas en organismos oficiales, páginas falsas de recargas móviles con tarjeta de crédito o de diversos productos a precios sospechosamente baratos”.

‘Pharming’

Una variable de ‘pishing’ es el ‘pharming’: “ataques a los computadores personales que consiste en modificar o sustituir el archivo del servidor de nombres de dominio DNS (Domain Name Server), cambiando al IP real de la entidad bancaria” (p. 218).

Los servidores DNS conducen a los usuarios a la página que desean ver. Pero mediante esta acción, quien pretende defraudar consigue que las páginas visitadas no correspondan con las auténticas, sino con otras creadas para recabar datos confidenciales, especialmente relacionados con la banca “on-line”.

Solo se necesita modificar un pequeño archivo llamado “hosts” que puede haber en cualquier máquina que funcione bajo Windows y que utilice Internet Explorer para navegar por Internet.

Con esto, si el usuario teclea en su navegador la dirección web que desea acceder, es reenviado a otra creada por el defraudante, que tiene el mismo aspecto que la original. De esta manera, el internauta introduce sus datos confidenciales con normalidad, sin conocer que los está remitiendo a un lugar inseguro.

Con las claves ya en su poder, suelen abrir de modo simultáneo una cuenta bancaria para remitir el dinero por medio de una transferencia "on-line". Aunque en realidad no es una sola transferencia, ya que comúnmente dividen el dinero en varias cuentas bancarias, que pueden estar en el mismo país o en diferentes, pero cercanos geográficamente.

El desarrollo tecnológico ha introducido nuevos términos para relacionarse con los delitos, que son los últimos dos tipos explicados anteriormente: "*pishing*" y 'pharming'. Estos casos son los más comúnmente utilizados en el país y que nos servirán de guía al momento de exponer los casos de esta tesis.

Los delitos pueden incluir a terceras personas para efectuar estas transacciones en diferentes cuentas bancarias. Estas se conocen como "mulas". Estos individuos reciben comisión a cambio de que se les haga una transferencia bancaria y que vuelvan a transferir a otra cuenta. A cambio, estas personas se quedan con un porcentaje de dinero.

Las "mulas" suelen ser captadas en Internet con supuestas ofertas de trabajo. Allí deben llenar formularios y facilitar un número de cuenta bancaria que posteriormente receptará transferencias de supuestos clientes ofreciendo, a cambio, una comisión del dinero recibido, por "préstamo de su cuenta".

2.2.1.2 El sabotaje informático

Este delito es un acto de suprimir o borrar e, incluso, modificar sin ninguna autorización algún dato de un computador para obstaculizar el funcionamiento

normal del sistema. Las técnicas que permiten cometer sabotajes informáticos son: bombas lógicas, gusanos, virus informáticos y 'malware', ciberterrrorismo, ataques de denegación de servicio y las redes robot. (Guibourg, 1996, p. 124) (Acurio del Pino, 2010, p. 218)

En todos esos casos son programas legítimos de procesamiento de datos que buscan modificar programas o destruir los datos de un computador. Aunque tienen diversos grados de malignidad, tienden a reproducirse y a extenderse dentro del sistema al que acceden, se contagian de un sistema a otro. En términos médicos podría decirse que un gusano es un tumor benigno, mientras que el virus es un tumor maligno. El primero es diferente del virus porque no puede regenerarse.

2.2.1.3 El espionaje informático y el robo a hurto de software

También llamados Data Leakage (fuga de datos) o divulgación no autorizada de datos reservados, este delito es una variedad del espionaje industrial que sustrae información confidencial de una empresa.

Según el Manual de Informática Jurídica, del autor Luis Camacho Losa, es "la facilidad existente para efectuar una copia de un fichero mecanizado es tal magnitud en rapidez y simplicidad que es una forma de delito prácticamente al alcance de cualquiera" (1987, p. 108).

Para evitar estos "ataques", la forma más sencilla de proteger la información confidencial es la criptografía o claves personales.

Sobre la reproducción no autorizada de programas informáticos de protección legal, Acurio del Pino (2010) dice que puede entrañar una pérdida económica sustancial para los propietarios legítimos.

"Algunas jurisdicciones han tipificado como delito esta clase de actividad y la han sometido a sanciones penales. El problema ha alcanzado dimensiones

transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones modernas" (p. 223).

El experto agrega que la reproducción no autorizada de programas informáticos no es un delito informático. Él cree que en primer lugar, el bien jurídico protegido es en este caso el derecho de autor y, en segundo lugar la protección al software.

2.2.1.4 El robo de servicios

En este grupo está el hurto de tiempo del computador que es muy común entre proveedoras de Internet y usuarios. El siguiente punto es la apropiación de informaciones residuales (scavenging). Puede efectuarse tomando la información residual que ha quedado en memoria o soportes magnéticos.

Y como tercer punto está el parsitismo informático y sumplatación de personalidad. Este ítem es muy importante explicarlo, ya que en estos casos, el delincuente utiliza la suplantación de personas para cometer otro delito informático, mediante organizaciones o empresas donde las personas depositan su confianza para que su identidad o cuentas bancarias sean protegidas y reservadas.

2.2.1.5 Acceso no autorizado a servicios informáticos

Dentro de este grupo están las puertas falsas, donde se introducen interrupciones en la lógica de los programas, para más adelante acceder a información condifencial. Por otra parte, están las llaves maestras, que es un programa informático que abre cualquier archivo del computador por muy protegido que esté, con el fin de alterar, borrar, copiar, insertar o utilizar, en cualquier forma no permitida, datos almacenados en el computador.

También está el pichado de líneas, que interfiere líneas telefónicas de transmisión de datos para recuperar la información que circula por ellas, por medio de un radio, un módem y una impresora.

Y, finalmente, están aquellos realizados por los piratas informáticos o ´hackers'. El acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones. El delincuente puede aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema. A menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sistema; esto suele suceder con frecuencia en los sistemas en los que los usuarios pueden emplear contraseñas comunes o contraseñas de mantenimiento que están en el propio sistema.

En la descripción de este 'modus operandi' coinciden el Perito en delitos informáticos Rafael Malgarejo y el experto en este tipo de delitos de la ESPE, Carlos Romero. Ellos comentan que debido al gran número de delitos informáticos que existen, s complicado tipificarlos. Ambos añaden que q pesar de eso, es importante empezar a sancionarlos, para que los casos sean resueltos y no perjudique a sus usuarios.

Inclusive, solo con capturar las claves bancarias de los usuarios, mediante programas especializados a través de Internet o enviando masivamente correos electrónicos con textos engañosos, cualquier persona puede caer en esta trampa. Esta situación se efectúa en cuestión de segundos, ya que cuando el usuario ingresa los datos de su cuenta real, estos son grabados en una base de datos que está bajo el control de los delincuentes informáticos.

Al momento que el usuario está ingresando sus datos se instala en el computador del usuario, un programa que captura los pulsos del teclado y luego envía a una dirección de Internet preestablecida que está también bajo el control de los sujetos activos.

Frente a esto, Javier Fernández Teruelo, en su libro, el Cibercrimen y los delitos cometidos a través de internet, agrega que la sustracción de las claves de acceso a un sistema informático sin el conocimiento de la víctima, son conocidos como “spyware”.

Entre las formulas significativas de fraude, según Fernández (2009), están aquellas mediante las cuales se logra la sustracción de datos.

> “El acceso a distancia al PC de la víctima puede tener lugar a través de múltiples vías. Actualmente dichos datos suelen obtenerse a través de spyware o archivos espía, que son pequeñas aplicaciones que se consiguen al introducir en el PC de la víctima y cuyo objetivo es el envío, a un lugar exterior de datos del sistema donde están instalados mediante la utilización subrepticia de la conexión a la red, sin el conocimiento del usuario” (p. 28).

Además en la obtención fraudulenta de las claves, es la propia víctima quien hace llegar al defraudador los datos necesarios para realizar las transacciones en línea (Fernández, 2009).

2.3 CARACTERÍSTICAS DE LOS DELITOS INFORMÁTICOS

Como lo mencionamos anteriormente, los delitos informáticos son difíciles de demostrar y complicado determinar las pruebas. Se pueden llevar a cabo de forma rápida y sencilla, en cuestión de segundos mediante un equipo informático sin necesidad de encontrarse físicamente en el lugar de los hechos. En esta clase de delitos tienden a proliferarse y evolucionar, situación que complica más aún su identificación y persecución.

De la literatura revisada, se pueden identificar al menos nueve características:

(1) Son conductas criminógenas de cuello blanco, ya que solo determinan el número de personas con ciertos conocimientos técnicos. (2) Son acciones

ocupacionales, por que comúnmente se efectúan cuando el sujeto está trabajando. (3) Provocan serias pérdidas económicas (4) Son muchos los casos y pocas las denuncias, y todo ellos debido a la misma falta de regulación por parte del derecho. (5) Por el momento, muchos siguen siendo ilícitos impunes de manera manifiesta ante la ley. (6) En el aspecto temporal, por tratarse de categorías penales tan efímeras, fructuales y volátiles como la propia telecomunicación. (7) Manipulación informática es cuando se usa la conducta de alterar, modificar u ocultar datos informáticos. (8) La transferencia no consentida del patrimonio de otra persona sin utilizar violencia. (9) El perjuicio a terceros, ya que no es la propia víctima la que realiza la transferencia económica, sino que es el propio autor del delito el que la lleva a cabo. (Téllez, 2003, pp. 105 y 106) (Palomino, 2009, p. 56)

2.3.1 Sujetos del delito informático

En material penal, la comisión de un delito supone la existencia de dos sujetos: un activo y otro pasivo. Los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y su situación laboral se encuentra en lugares estratégicos donde se maneja información de carácter sensible, mientras que los sujetos pasivos, en este caso son las víctimas.

Solamente las personas naturales pueden delinquir y por el contrario, el ofendido puede ser una persona natural o jurídica, agravándose la situación en este último caso, por ejemplo, cuando se trata del delito de traición a la patria.

2.3.1.1 Sujeto activo

Según el catedrático chileno, Mario Garrido Montt, se entiende como sujeto activo a quien realiza toda o una parte de la acción descrita por el tipo penal.

Las personas que cometen los llamados delitos informáticos son aquellas que poseen ciertas características que no presentan el denominador común de los

delincuentes, que como se mencionó anteriormente, poseen habilidades para el manejo de los sistemas informáticos.

> “Con el tiempo se ha podido comprobar que los autores de los delitos informáticos son muy diversos y que lo que los diferencia entre sí es la naturaleza de los delitos cometidos. De esta forma, la persona que “entra” en un sistema informático sin intenciones delictivas es muy diferente del empleado de una institución financiera que “desvía fondos” de las cuentas de sus clientes”. (Acurio del Pino 2010, p. 185).

Según un estudio que se publicó en el Manual de las Naciones Unidas para la prevención y control de delitos informáticos (ONU 2012, pp. 43 y 44), un 90% de los delitos realizados a través de un computador, fueron elaborados por los mismos trabajadores de la compañía afectada. A este grupo se los denomina “insiders”, que son los trabajadores disconformes o individuos externos, pero que tienen algún acceso a los sistemas dentro de la compañía.

De igual manera, en un estudio efectuado en América del Norte y Europa, se menciona que el 73% de las infracciones informáticas suscitadas, fueron atribuibles a personas internas y un 23% a la actividad delictiva externa, o llamados “outsiders” (ONU 2012).

En 1943 el criminólogo norteamericano Edwin Sutherland introdujo por primera vez el término de delitos informáticos, refiriéndose a aquellos que precisan unos determinados conocimientos para su realización.

Con base en estas premisas, se puede concluir que la cualificación del sujeto activo es un elemento determinante para medir la gravedad en la delincuencia informática, ya que solo aquellos delitos cometidos por hackers, podrían ser realizados por sujetos y considerarse como calificados y peligrosos.

2.3.1.2 Sujeto pasivo

El sujeto pasivo puede ser: individuos, instituciones financieras, de gobierno, o en general instituciones que manejen sistemas automatizados de información y que, sean titulares de los bienes jurídicos protegidos que el legislador protege y sobre la cual recae la actividad típica del sujeto activo.

> “Mediante él podemos conocer los diferentes ilícitos que cometen los delincuentes informáticos, con objeto de prever las acciones antes mencionadas debido a que muchos de los delitos son descubiertos casuísticamente por el desconocimiento del modus operandi de los sujetos activos” (Acurio del Pino, 2010, P. 206).

Está claro entonces que el fraude informático se realiza mediante manipulaciones informáticas que ocasionan perjuicios económicos, cuyos autores lo realizan con ánimo de lucrar aprovechando sus conocimientos de los sistemas informáticos a los que acceden.

Por esta razón, dentro del fenómeno de la delincuencia informática, el fraude informático es el delito considerado más impune y que mayores obstáculos para su prevención, represión y detención enfrenta en casi todo el mundo.

Si bien la gestión del sistema ha evolucionado conjuntamente con la gestión bancaria, teniendo como objetivo solucionar los casos de los usuarios afectados, muchos quedan sin resolverse.

De hecho, y es que uno de los factores que más incide en este alto índice delincuencial y que individualmente incita a la persona que quiere delinquir es la impunidad. La principal causa generadora de la impunidad es la falta de investigación y seguimiento a los casos.

Según el estudio Visión de Consumidores Latinoamericanos de Easy Solutions, 53% de quienes no utilizan Internet para transacciones bancarias o pagos tienen como razón principal el miedo al fraude. El 40% de los encuestados no recuerda ninguna campaña que su banco haya realizado acerca del fraude electrónico.

El Registro de Direcciones de Internet para América Latina y el Caribe, Lacnic, calcula que las pérdidas anuales en Latinoamérica debido al fraude electrónico llegan a USD 39 billones. Estos montos, según Silvia López, directora de marketing de Easy Solutions pueden ser mediante el robo a muchos clientes de poco dinero, para que los usuarios no se den cuenta.

Los colombianos perdieron USD 40 millones en el 2013 por fraude financiero, según David Castañeda, Director de investigación y desarrollo de Easy Solutions. En total, casi 10 millones de usuarios colombianos fueron víctimas de algún tipo de fraude en las plataformas virtuales, según el portal web del periódico La República de Colombia. En este país, el 'phising' (suplantación de identidad) es el más usado, con 60% de los casos; le sigue el 'pharming' (suplantación web), 25%, y el 'malware' (código malicioso), con 15% de ejecución en los entornos digitales y plataformas online (Alzate, 2012).

Si bien en la legislación de algunos países, en la actualidad se tipifica y sanciona el delito del fraude informático, lo más óptimo sería que en todas las legislaciones exista una figura penal, ya que actualmente es más común realizar transacciones interbancarias utilizando medios tecnológicos como Internet.

Es vital que la legislación penal ecuatoriana incursione de la mejor manera posible en la tipificación de fraude informático para evitar la impunidad de este tipo de delitos que hasta ahora no se pueden sancionar en el país.

En el país, gran porcentaje de estas denuncias se archivan sin adelantar la mínima búsqueda de pruebas y otras fracasan porque las investigaciones son cortas y a paso lento, y no se las realizan oportunamente (Ver capítulo IV).

2.4 LEGISLACIÓN EXTRANJERA

Desde hace 15 años la mayoría de los países europeos y en Latinoamérica, han hecho todo lo posible para incluir dentro de la ley de conducta penal, este tipo de delitos. Poco a poco esto se ha ido difundiendo en los países por la preocupación de contar con comunicaciones electrónicas y transacciones confiables y seguras, tanto como sea posible.

En 1983, la Organización de Cooperación y Desarrollo Económico (OCDE), mediante un estudio buscaba “aplicar y armonizar en el plano internacional las leyes penales, con el objetivo de luchar contra el problema del uso indebido de los programas computacionales” (Acurio del Pino, 2010, P. 30).

El Parlamento Europeo aprobó en noviembre del 2013, la nueva legislación sobre protección de datos a nivel europeo. Cuando entre en vigor esta normativa será vinculante para todos los Estados miembros y se encargará de que se haga un correcto uso de los datos personales, buscando la transparencia en relación a las personas afectadas.

España a pesar de ser un país miembro de la Unión Europea ha sufrido más robos de identidad a través de Internet muy por encima de la media europea según los datos de Eurostat, que es la oficina de estadísticas de la Unión Europea.

En una publicación del portal web Periodista Digital, en dicho país, un 18 % de los ciudadanos ha sido víctima de este delito, lo que signfiica más de 4,5 millones de personas. Se enfatiza que “las pérdidas económicas por el uso fraudulento de la identidad ascienden a los 8 000 euros de media por caso”

(Periodista Digital). Esta cifra en promedio significa unos USD 10 800 americanos.

En el portal web se agrega, además, el Departamento de Justicia de EE.UU., ha determinado que 12 millones de familias americanas se han visto afectadas por el robo de identidad. Las pérdidas generadas por este delito en el país del norte superaron los USD 50 000 millones hasta el 2013 (Periodista Digital).

Desde el Observatorio Legálitas, una entidad con servicio de abogacía a los ciudadanos, se están adoptando una serie de medidas para proteger a los clientes de este delito. Este es el primer y único servicio de protección de Identidad integral que existe en el mercado Español.

En el Nuevo Código Penal de España (artículo 264-2), establece que se aplicará la pena de prisión de uno a tres años y multa, a quien por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.

El Convenio sobre la ciberdelincuencia Nº 185 del Consejo de Europa, elaborado por dicho Consejo y con la participación de Canadá, Estados Unidos, Japón y Sudáfrica, en vigor desde julio 2004, promueve una norma mundial que mejore la legislación en estos delitos.

Por su parte, Alemania sancionó en 1986 la Ley contra la Criminalidad Económica, que contempla los siguientes delitos: Espionaje de datos, estafa informática, alteración de datos y sabotaje informático. Mientras que en Austria, la Ley de reforma del Código Penal, en su artículo 148, sanciona a aquellos que causen un perjuicio patrimonial a un tercero. Además, contempla sanciones para quienes comenten este hecho utilizando su profesión de especialistas en sistemas.

En Gran Bretaña, debido a un caso de hacking en 1991, rigió la Computer Misuse Act (Ley de Abusos Informáticos). Quienes alteren datos informáticos es penado con hasta cinco años de prisión o multas. Los virus están incluidos en esa categoría. El liberar un virus tiene penas desde un mes a cinco años, dependiendo del daño que causen. En Holanda, en Marzo de 1993, entró en vigencia la Ley de Delitos Informáticos, en la cual se penaliza el 'hacking'.

Finalmente en Francia, en enero de 1988, se dictó la Ley relativa al fraude informático, la cual prevé penas de dos meses a dos años de prisión y multas por la intromisión fraudulenta que suprima o modifique datos.

La legislación alemana, en el párrafo 263 de su Código Penal, tipifica el fraude informático de la siguiente manera:

> "Quien con la intención de procurar para sí o para un tercero una ventaja patrimonial ilícita, perjudique el patrimonio de otro influyendo en el resultado de un proceso de elaboración de datos por medios del uso de datos incorrectos o incompletos, a través del uso no autorizado de datos o a través de intervención desautorizada en el proceso, será castigado con pena de privación de de libertad de hasta cinco años o con multa".

Este tipo de penalización extranjera podría ser optada como una opción a seguir para nuestra legislación, logrando de esta manera tener más claro el concepto y las penalizaciones de los delitos informáticos.

3 CAPÍTULO III: ANÁLISIS DE LA SITUACIÓN ACTUAL Y LA LEGISLACIÓN ECUATORIANA FRENTE A LOS DELITOS INFORMÁTICOS

Durante el desarrollo de este capítulo, se hará una explicación y análisis de la legislación ecuatoriana sobre delitos informáticos. Dentro de este tratamiento, se abordará las reformas al nuevo Código Penal, que fue aprobado el pasado 17 de diciembre del 2013 en la Asamblea Nacional. Este documento, se analizará con la Ley de Comercio Electrónico, Firmas Electrónicas y Mensaje de Datos (LCEFEMD), que fue creada para regular este tipo de delitos, artículos que fueron replicados en el antiguo Código Penal Ecuatoriano.

Además, se abordará un análisis sobre la situación de estos delitos en Ecuador, haciendo énfasis sobre los más frecuentes en el país.

Este capítulo también es muy relevante, por las cifras que se expondrán, en cuanto al crecimiento de la oferta bancaria en el país, el crecimiento de sus usuarios y las denuncias receptadas por los usuarios en las diferentes instituciones encargadas de responder sobre este tipo de delitos. Cifras que ayudarán a comprender y analizar de una mejor manera el estudio de esta tesis.

3.1 VACÍOS EN LA LEGISLACIÓN ECUATORIANA

Si bien los delitos informáticos se conocieron desde hace 30 años en casi todos los países del mundo, en el Ecuador aparecieron con la expedición y promulgación en el Registro Oficial de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, promulgada en abril del 2002.

Por primera vez en la legislación se tomó en cuenta a este delito, para tipificarlos en el Ecuador. Hay que resaltar que en dicha ley mencionada anteriormente, a estos delitos los denominaron infracciones informáticas. Sin

embargo, estos delitos se encuentran como reformas dispersas en el Código Penal antiguo, pero que aún está en vigencia.

En este punto, los legisladores tampoco fueron claros con la redacción de los tipos penales que se relacionan con los delitos informáticos, lo que en la actualidad genera varios problemas al momento de determinarlos, ya que el contenido de los artículos es muy general y ambiguo, situación que ampliaremos en el siguiente capítulo. Además, no se mencionaba ninguna sanción relacionada a los delitos por medio de la banca electrónica.

El antecedente de esta norma fueron los primeros ataques a páginas electrónicas en el país, en especial, a la página del Municipio de Quito (Diario Hoy, 2001).

En el artículo 1 de Ley de comercio electrónico se menciona que:

> "Esta ley regula los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos a través de redes de información, incluido el comercio electrónico y la protección al usuario de estos sistemas" (p. 5).

3.2 LAS SANCIONES EN EL CÓDIGO PENAL ECUATORIANO

En marzo del 2009, la Asamblea Nacional realizó reformas al Código Penal vigente a esa fecha, para establecer sanciones y multas a los siete artículos de las infracciones establecidas en la Ley de Comercio Electrónico.

Las infracciones tienen que ver con conductas ilícitas, acceso ilegal a sistemas informáticos, interceptación ilegal de las comunicaciones, daños en sistemas informáticos, fraude electrónico, fraude en las telecomunicaciones, entre otros.

En el artículo 57 de la LCEFEMD, se precisa que se considerarán infracciones informáticas, a las de carácter administrativo y además a las tipificadas en

Código Penal. Hasta el 10 de febrero el Código Penal establecía 14 sanciones (carcelarias y pecuniarias) por delitos e infracciones informáticas.

Tabla 1. Sanciones cancelarias y pecuniarias del código penal antiguo

ART. 58: DELITOS CONTRA LA INFORMACIÓN PROTEGIDA (art.202 CP):	***SANCIÓN CARCELARIA***	***SANCIÓN PECUNIARIA***
1.- Violentando claves o sistemas	6 meses a un año	US$ 500.- a US$ 1.000.-
2.- Información obtenida sobre la Seguridad nacional, secretos comerciales o industriales:	3 años	US$ 1.000.- a US$ 1.500.-
3.- Divulgación o utilización fraudulenta de los rubros anteriores:	3 a 6 años	US$ 2.000.- a US$ 10.000.-
4.- Divulgación o utilización por funcionarios a cargo de dicha información.	6 a 9 años	US$ 2.000.- a US$ 10.000.-
5.- Obtención y uso no autorizados de datos personales para cederla o utilizarla :	2 meses a 2 años	US$ 1.000.- a US$ 2.000.-
ART. 59: DESTRUCCION MALICIOSA DE DOCUMENTOS POR FUNCIONARIOS DE SERVICIO PÚBLICO (Art. 262 CP)	3 A 6 AÑOS	xxx
ART. 60: FALSIFICACIÓN ELECTRÓNICA SEGÚN EL SIGUIENTE DETALLE Y CON ÁNIMO DE LUCRO CON PERJUICIO A TERCEROS (Art. 353 CP):	Serán juzgados de acuerdo a lo que se dispone en este capítulo, o sea, 6 años	xxx
1.- Alterar un mensaje de datos		
2.- Simulación de mensaje.		
3.- Suposición de intervención en actos, declaraciones, etc.		
ART. 61: DAÑOS INFORMÁTICOS (Art. 415 CP) SEGÚN:		
1.- Daño doloso de información contenida en un sistema.	6 meses a 3 años	US$ 60,oo a US$ 150,oo
2.- Cometido por funcionario público o vinculado a la defensa nacional.	3 a 5 años	US$ 200.- a US$ 600.-
3.- Si no se tratare de un delito mayor, la destrucción, alteración o inutilización de infraestructura para la transmisión.	8 meses a 4 años	US$ 200.- a US$ 600.-
ART. 62: APROPIACIÓN ILÍCITA (Art. 553 CP) SEGÚN LO SIGUIENTE:	6 meses a 5 años	US$ 500.- a US$ 1.000.-
1.- Uso fraudulento o ilícito para apropiación de un bien ajeno, etc.		
2.- Uso fraudulento mediante la utilización de los siguientes medios: 1) Inutilización de sistemas de alarma o guarda; 2) Descubrimiento descifrado de claves secretas o encriptadas; 3) de tarjetas magnéticas, carding o perforadas; 4) de controles o instrumentos de apertura a distancia y 5) violación de seguridades electrónicas u otras semejantes	Uno a cinco años	US$ 1.000.- a US$ 2.000.-
ART. 63 ESTAFA (ART.363 CP) A TRAVÉS DE MEDIOS ELECTRÓNICOS	Uno a cinco años	US$ 500.- a US$ 1.000.-
ART. 64 DERECHO A LA INTIMIDAD (art.606 #19°CP) Si no fuere delito	La sanción aún está en sucres, equivalente a casi centavos.	De dos a cuatro días

Tras lo expuesto anteriormente, podemos hacer un análisis de las reformas del Código Penal ecuatoriano, dadas a través de esta ley registrada en el 2002. Si bien el propósito de los legisladores de dicha época, tuvieron la intención de crear diferentes tipos penales en esta legislación, para sancionar los delitos informáticos en el país, se podría decir que se realizó de una manera muy ambigua y confusa.

Como se puede observar en las tablas expuestos anteriormente, el análisis recae en que, aparentemente no existió el apoyo de técnicos en sistemas, o de programadores, que expongan a los legisladores de todos los tipos y clases de delitos informáticos que pueden existir.

El autor de dichos delitos es un experto en ejecutar actos injuriosos a través de la manipulación fraudulenta de un computador. Esto podría producir varios resultados como el espionaje y sabotaje informático, apropiación no autorizada de programas y archivos, entre otros (Ver capítulo II).

Por lo dicho anteriormente, las reformas introducidas en el Código Penal junto con la Ley de Comercio Electrónico, Firmas y Mensajes de Datos, son ambiguas al momento de ser aplicadas por un agente fiscal o juez penal, al calificar la conducta delictiva o al determinar el tipo penal correspondiente. Hay que resaltar que los elementos que configuran los nuevos tipos penales mal llamados por la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos como “infracciones informáticas”, son muy ambiguos.

Por otra parte, se podría decir que existe una falta de conocimientos técnicos y se puede distinguir que existió quizás una ligereza de parte de los legisladores al tratar la redacción de las reformas introducidas al Código Penal, como nuevos tipos penales. Esto es un error, ya que se confunde al fraude informático como la apropiación indebida y la estafa.

Además, el inciso agregado al artículo 563 del Código Penal produce confusiones, ya que la estafa tradicional tiene elementos que no pueden asimilarse a una “estafa por medios electrónicos”.

Por lo tanto, una nueva reforma al Código Penal y al Título V de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, fue siempre una necesidad para que no queden impunes todas las formas de defraudación informática que se pueden cometer y que se delimite y especifique de mejor manera lo relacionado a los delitos informáticos que se crearon con dicha Ley.

Además, se evidenció la necesidad de que se tipifiquen nuevos delitos informáticos que no están tipificados todavía en nuestra legislación penal, pero que en otros países ya cuentan con sanciones y sus elementos están debidamente determinados y especificados.

3.3 LOS DELITOS INFORMÁTICOS EN ECUADOR

La informática ha reemplazado muchos de los documentos tradicionales, en soportes que constan como operaciones y saldos de los clientes. Estos son más conocidos como “anotaciones en cuenta”, por ser registros en sistemas informáticos sin la utilización del papel. Esta es una de las razones por la delincuencia se ha centrado en la manipulación de datos informáticos. Tal es así, que desde noviembre del 2010, la Policía Nacional del Ecuador empezó a conocer e investigar este tipo de delitos a través de la Unidad de Investigación de delitos tecnológicos de la Policía Judicial del Ecuador.

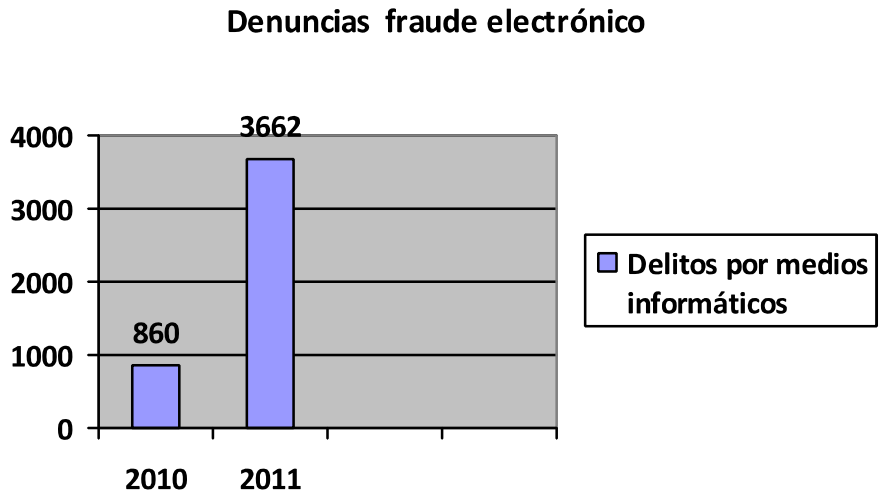


Figura 6. Denuncias fraude electrónico
Tomado de Policía Judicial

De las denuncias receptadas en el 2010, 679 fueron apropiación ilícita. De estas, 82 denuncias correspondieron a delitos informáticos como vulneración a páginas de servicio privado y apenas 1 por estafa.

En el 2011, como se puede apreciar en la figura anterior, el número de delitos se multiplicó por cuatro frente al 2010. Estos fueron cometidos mediante redes telemáticas, pornografía infantil, cyberbulling y grooming;

Frente a este fenómeno, el sistema financiero ecuatoriano empezó a establecer medidas de seguridad estándar. En lo que respecta a la banca electrónica, hasta el 30 de junio del 2012 los bancos del país debían "contratar coberturas de seguro contra fraudes informáticos en los servicios entregados mediante canales electrónicos", con base en la resolución No. JB-2012-2090 emitida por la Junta Bancaria, el 17 de enero del 2013.

Dicha resolución, en su artículo 41, establece que: "(...) las instituciones financieras contratarán anualmente con las compañías de seguro, coberturas que aseguren a la entidad contra fraudes generados a través de su tecnología

de la información, sistemas electrónicos, sistemas telemáticos, electrónicos o similares...” (Junta Bancaria, 2012)

Sin embargo, pese a que la gente afectada realiza denuncias de sus casos y están protegidos por una legislación, no todos los usuarios consiguen la devolución del dinero sustraído de sus cuentas, en los llamados delitos informáticos (Ver capítulo IV).

Según César Robalino, presidente de la Asociación de Bancos Privados del Ecuador, hasta el 2013 el número de clientes de la banca en el país, ascendió a 7 millones, de los cuales 4 millones y medio de usuarios corresponden a la Banca Privada y Cooperativas, (Asociación de Bancos, 2012). Esto significa que la mitad de la población ecuatoriana posee al menos una cuenta bancaria, y un tercio de la población de Ecuador tiene una cuenta en un banco privado.

Según la Asociación de Bancos Privados del Ecuador, entre el 2006 y 2012, el número de clientes bancarios creció en un 96,3 %.

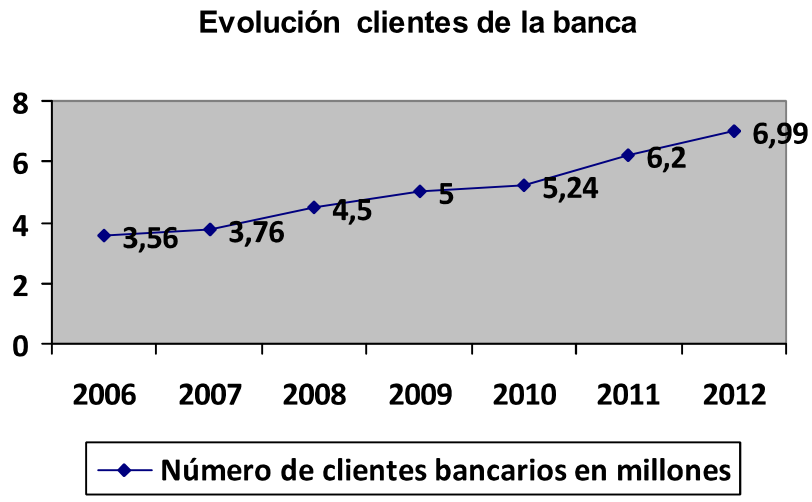


Figura 7. Evolución de clientes de la banca
Tomado de Asociación de Bancos Privados del Ecuador, 2013, p. 2

La Dirección Nacional de Atención y Educación al Usuario de la Superintendencia de Bancos, registran otras cifras por delitos informáticos.

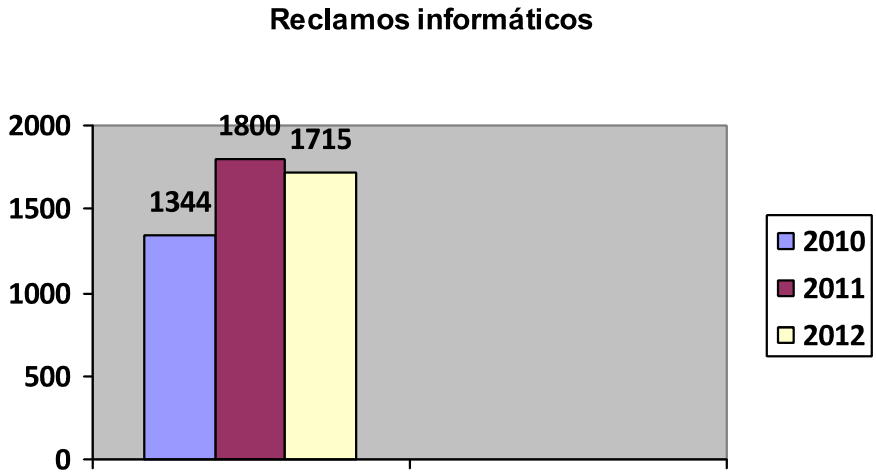


Figura 8. Reclamos informáticos
Tomado de SBS, 2012

La Superintendencia de Bancos y Seguros tiene bajo su control a 94 entidades financieras que se dividen en: entidades privadas, entidades públicas, mutualistas, cooperativas de ahorro y crédito, sociedades financieras y otras entidades. Lo que significa que los usuarios de este grupo objetivo son vulnerables a ser víctima de un delito informático.

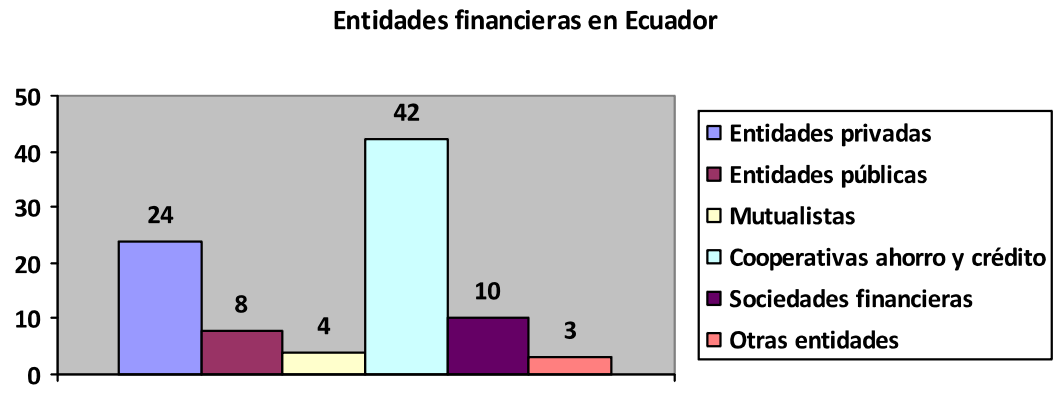


Figura 9. Entidades financieras
Tomado de SBS, 2014

La Fiscalía General del Estado también recepta denuncias sobre este tipo de delitos. Durante el 2009, el organismo recibió 168 denuncias por apropiación ilícita a través del sistema informático. Un año más tarde (2010), la cifra

aumentó a 1 099. y para 2011 la cifra se triplicó a 3 129 denuncias de delito de apropiación ilícita, utilizando medios informáticos. Esto significa que en el 2011 hubo 163,88% más casos que se registraron en el 2010. De las 3 129, unas 2 928 ingresaron a indagación previa y 63 a instrucción fiscal. Pero de estas últimas, solo 27 llegaron a dictámenes acusatorios, en cuatro hubo abstenciones y en seis dictámenes mixtos, según datos de la Fiscalía. Es decir, que del total de causas solo alrededor del 1% llegó a un dictamen judicial.

Mientras que, para el 2012, la cifra se redujo a 2 682. Hasta agosto del 2013, se registraron 1 089 denuncias. (Fiscalía General del Estado).

Según Jorge San Lucas, director de Tecnología de Información de la Fiscalía General del Estado, en el 2011 fue el año con más casos registrados; sin embargo, cree que la disminución de casos desde el 2012, fue por la campaña de información a los usuarios por parte de la Fiscalía y la banca privada a sus clientes. Agrega que en dicha campaña se informó a los usuarios que ninguna entidad bancaria solicita información a sus clientes, mediante correos electrónicos o mensajes de texto.

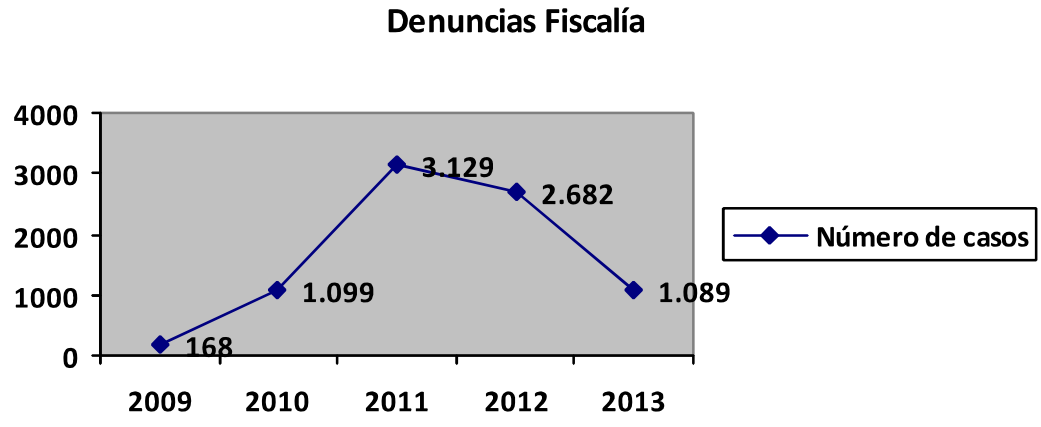


Figura 10. Denuncias fiscalía
Tomado de Fiscalía, 2013

Según el Banco Central del Ecuador, al año en el país se registran unos 27 millones de transacciones en línea, es decir unas 75 342 transacciones diarias, 31 39 por hora y 52 transacciones vía internet por minuto (Banco Central del Ecuador, 2012).

3.3.1 Los delitos informáticos más frecuentes en el Ecuador

La Superintendencia de Telecomunicaciones del Ecuador, en su Revista Informática “Delitos en telecomunicaciones”, publicó una clasificación de los delitos informáticos más frecuentes en Ecuador que son: pishing, pharming, spam, Hacking, Hoax o correos no deseados y keyloggers. Todos ellos fueron definidos en el capítulo anterior.

Fernández (2009) agrega que los programas más utilizados para sustracción de claves, son los denominados ‘keyloggers’, que registran todo lo que el usuario teclea en su ordenador. Sin embargo, también se puede acceder a información ajena sin que el usuario teclee nada y abriendo puertos y accediendo a la información cuando el usuario accede a un enlace determinado. Así acceden a información personal, que pueden ser datos bancarios y claves que posteriormente suelen ser utilizados para transferencias bancarias a su favor o de un tercero.

Según datos del Instituto Nacional de Estadísticas y Censos (INEC), hasta julio del 2013, en el Ecuador el 65% de la población tenía acceso a internet. De esta cifra, el 44,5% fueron habitantes de Pichincha que usan el Internet, siendo esta la provincia con más número de usuarios.

Cabe resaltar que la plataforma de Internet constituye el principal medio para realizar las transacciones bancarias, compra y venta de artículos e inclusive entrega de información personal, situación que conlleva la vulnerabilidad de este medio para la comisión de delitos.

Para finalizar este capítulo, es importante resaltar un estudio de la Superintendencia de Telecomunicaciones del Ecuador, que midió el grado de conocimiento de la población, relacionado al tema de delitos cibernéticos.

En la encuesta se preguntó: ¿Cómo califica su nivel de conocimiento sobre los delitos cibernéticos? En los resultados, se conoció que solo el 43% de la población conocía sobre los delitos informáticos.

Este trabajo fue realizado en el 2012. Los encuestados podían calificar del 1 al 5 (1=pésimo y 5=excelente). Respecto al índice de conocimiento sobre delitos cibernéticos, el 57% de la población no conocía sobre los delitos informáticos. Solo un 43% de la población puso una calificación del 1 al 5, confirmando que sí conocía que eran los delitos informáticos.

Quienes sí respondieron conocer sobre delitos cibernéticos, el 13% califican su conocimiento en una escala de 3, mientras que un 9% y 4% respondieron que tienen un alto conocimiento sobre delitos cibernéticos.

El estudio se realizó mediante una investigación cuantitativa y a través de una muestra probabilística de 2 220 entrevistas, representadas a nivel de hogares del área urbana, tomada en 15 ciudades de la Costa, Sierra y Amazonía.

3.4 NUEVAS REFORMAS ENDURECEN LAS PENAS PARA DELITOS INFORMÁTICOS

Dentro del proyecto de Código Orgánico Integral Penal del Ecuador, aprobado el pasado 17 de diciembre del 2013 en la Asamblea Nacional ya se citan algunos tipos de delitos informáticos. Los artículos que los tipifican están en la sección tercera y van desde el 229, hasta el artículo 234. En esta lista se toman en cuenta aquellos delitos por revelación ilegal de base de datos, transferencia electrónica por activo patrimonial, intercepción ilegal de datos, ataque a la integridad de sistemas informáticos, delitos contra la información

pública reservada, y acceso no consentido a un sistema informático. (pp. 85-327)

En dichos artículos del Proyecto de Código Orgánico Integral Penal del Ecuador, que están citados textualmente posterior a este análisis, nos podemos dar cuenta que sí existe una modificación en los artículos que tipifican los delitos informáticos.

Haciendo un análisis, con el Código Penal anterior, existe mucha relación con el nuevo proyecto. Es decir, son muy similares los delitos, pero modificados los títulos de los artículos. Además, en la mayoría de artículos la sanción carcelaria aumentó, a diferencia del Código Penal antiguo que se sancionaba con privación de la libertad por tres meses, el nuevo código tiene penas carcelarias que llega hasta a 10 años de prisión.

En lo que respecta a la pena monetaria, en el artículo 70, literal 6, del proyecto del Código Penal, en cuanto a la aplicación de multas, se aplica además la pena de multa dependiendo de las infracciones mencionadas por delitos informáticos.

Cabe resaltar que un salario mínimo o básico en el Ecuador, para e 2014, es de USD 340. En este nuevo proyecto del Código Penal, se refleja que la multa monetaria, también aumenta, ya que en el antiguo, uno de los valores máximos era de USD 2 000. Mientras que, en el nuevo proyecto, sobrepasa los USD 6 000.

En este nuevo Código Penal establece 15 sanciones (carcelarias y pecuniarias) por delitos e infracciones informáticas, es decir un delito más que el Código Penal anterior.

Tabla 2. Tabla explicativa de cada artículo con su sanción carcelaria y pecuniaria

ART. 229: REVELACIÓN ILEGAL DE BASE DE DATOS Quien revele información registrada mediante sistema electrónico	**SANCIÓN CARCELARIA** 1 a 3 años	**SANCIÓN PECUNIARIA** 4 a 10 salarios básicos unificados (Entre 1360 y 3400 dólares)
1. Si es funcionario público, empleados bancarios	3 a 5 años	10 a 12 salarios básicos (Entre 3400 y 4800 dólares)
ART. 230: INTERCEPTACIÓN ILEGAL DE DATOS 1. Quien intercepte, escuche, desvíe, grabe u observe un dato informático para obtener información registrada. 2. Quien diseñe, desarrolle, venda, ejecute, programe o envíe mensajes, páginas electrónicas con enlaces maliciosos. 3. Quien copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico de tarjetas de crédito, débito. 4. Quien produzca, fabrique, distribuya, posea o facilite materiales para delitos informáticos.	3 a 5 años	10 a 12 salarios básicos (Entre 3400 y 4800 dólares)
ART. 231: TRANSFERENCIA ELECTRÓNICA DE ACTIVO PATRIMONIAL 1. Quien con ánimo de lucro, altere, manipule o modifique el funcionamiento de programa o sistema informático de transferencias bancarias 2. Quien facilite datos de su cuenta bancaria para obtener de forma ilegítima un activo patrimonial a través de una transferencia electrónica	3 a 5 años	10 a 12 salarios básicos (Entre 3400 y 4800 dólares)
ART. 232: ATAQUE A LA INTEGRIDAD DE SISTEMAS INFORMÁTICOS		
1. Quien destruya, dañe, borre, deteriore, altere o cause mal o suprima datos informáticos, mensajes de correo electrónico. 2. Quien diseñe, desarrolle, programe, adquiera, envíe, ejecute, venda o distribuya programas informáticos maliciosos o programas destinados a causar los efectos señalados anteriormente. 3. Quien destruya o altere sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general. Si es sobre bienes de un servicio público o vinculado con la seguridad ciudadana serán de 5 a 6 años.	3 a 5 años	10 a 12 salarios básicos (Entre 3400 y 4800 dólares)
ART. 233: DELITOS CONTRA LA INFORMACIÓN PÚBLICA RESERVADA LEGALMENTE		
1. Quien destruya o inutilice información clasificada de conformidad con la Ley 2. La o el servidor público que, utilizando cualquier medio electrónico o informático, obtenga este tipo de información 3. Cuando se trate de información reservada que pueda comprometer gravemente a la seguridad del Estado o al servidor público.	5 a 7 años 3 a 5 años 7 a 10 años (inhabilitación para ejercer un cargo o función pública por 6 meses, siempre que no sea grave)	12 a 20 salarios básicos (Entre 4080 y 6800) 10 a 12 salarios básicos
ART. 234: ACCESO NO CONSENTIDO A UN SISTEMA INFORMÁTICO, TELEMÁTICO O DE TELECOMUNICACIONES		
Quien sin autorización acceda a un sistema informático o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para modificar un portal web, desviar o redireccionar de tráfico de datos	3 a 5 años	10 a 12 salarios básicos (Entre 3400 y 4800 dólares)

Tomado deCPI

Un artículo importante que es parte de este estudio es el artículo 229 sobre la revelación ilegal de base de datos, donde se menciona que si en este caso, el acto es cometido por “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”. Esta sanción por ejemplo, no existía en el antiguo Código, que aún está en vigencia.

Esto es importante porque la Fiscalía General del Estado no descarta que los funcionarios de las entidades bancarias estén involucrados en este tipo de delitos.

Otro artículo importante es el artículo 230, literal 2 sobre la interceptación ilegal de datos que enfatiza que una persona que de alguna manera desarrolle, venda o ejecute páginas electrónicas o enlaces emergentes, o dominios de un servicio financiero, envié a otro sitio de internet diferente y libre de seguridad, tendrá una pena privativa de libertad de tres a cinco años. Este punto es importante debido a la clonación de portales web, especialmente de instituciones bancarias, que son clonadas para engañar a sus usuarios y acceder a sus cuentas bancarias.

En este mismo artículo, pero en el literal 3 se hace hincapié que la persona que copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico, que esté soportada en las tarjetas de crédito, débito, pago o similares, tendrá la misma pena. Es importante citarlo en este estudio, ya que es otra de las estrategias que los maleantes informáticos utilizan para sustraer dinero de cuentas bancarias.

Tras este pequeño análisis, considero que sí es un gran avance la aprobación del Proyecto de Código Orgánico Integran Penal en el Ecuador, ya que ayudaría de alguna manera a resolver varios casos que con el antiguo Código Penal han quedado muchas veces en la impunidad **(Ver Capítulo IV).**

4 CAPÍTULO IV: MEDIDAS DE SOLUCIÓN OPTADAS POR LAS ENTIDADES PARA LOGRAR FRENAR LOS DELITOS INFORMÁTICOS

Para finalizar, en este capítulo hablaremos sobre las diferentes resoluciones que la Junta Bancaria tuvo que establecer, tras el índice de afectados por delitos informáticos. Algo muy significativo en el desarrollo de este capítulo, es la exposición de los casos de las víctimas de estos delitos, así como el análisis de las respuestas que recibe cada usuario afectado, por parte de sus entidades bancarias y la Superintendencia de Bancos y Seguros del Ecuador.

Se realizará, además, una explicación de dos temas importantes que muchos de los usuarios de la banca desconocen, como son los seguros con los que cuentan los bancos para este tipo de fraude y el Defensor del Usuario que tiene cada institución bancaria, con el fin de ayudar a los afectados con la resolución de sus casos, tras no tener una respuesta favorable a sus solicitudes, por haber sido víctimas de estos delitos.

4.1 LOS CASOS DE DELITOS INFORMÁTICOS TUVIERON UNA RESPUESTA TEMPORAL

El 21 de marzo del 2011 el ex El Fiscal Washington Pesántez y el superintendente de Bancos y Seguros, Pedro Solines, firmaron la resolución 001-FGE-SBS- 2011 para ordenar a las diferentes entidades financieras, devolver el dinero a los depositantes que fueron perjudicados por delitos informáticos. Esto frente a la cifra de afectados por delitos informáticos en ese año (Ver capítulo II).

Pero la medida fue solo temporal. En la norma se ordenó a los bancos restituir parcial o completamente el dinero que los usuarios perdieron por delitos informáticos solo desde el 1 de enero del 2010 hasta la fecha de publicación de esa medida. Es decir, estuvo vigente solo durante 15 meses.

En el artículo 4 de dicha resolución, además, estableció que los bancos debían devolver el 100% del dinero a los depositantes que hayan sufrido estafas en cantidades de entre USD 1 y USD 2 000 en este período. Si el perjuicio superaba ese monto, las entidades deberían pagar solo el 60% de la cantidad.

Aunque la iniciativa tuvo acogida en la Superintendencia de Bancos, quien la impulsó fue Pesantez. La disposición tuvo un carácter de obligatorio. Pesantez advirtió que si la banca no cumplía iniciaría una instrucción.

El mismo día que se firmó el acuerdo, Pesantez incluso dejó abierta la posibilidad de que “los perjudicados inicien las acciones civiles o penales que crean en caso de no estar de acuerdo con la devolución” (Hoy, 2011). Según dijo, la medida beneficiaba al 98% del total de perjudicados a escala nacional.

Esta ha sido hasta ahora la única medida efectiva que ha permitido resolver de manera efectiva los casos relacionados con este tipo de delitos. Pero las dos autoridades coincidieron en ese entonces en que la medida tomada debía ser temporal mientras los bancos tomaban medidas para evitar que el delito informático siga en aumento.

César Robalino, presidente de la Asociación de Bancos Privados del Ecuador (ABPE), no vio con buen ojo la medida con la disposición, ya que, según el gremio, eso solo multiplicaría este tipo de delitos y el autorobo.

En su momento, Solines sugirió a las entidades bancarias debían contratar un seguro para cubrir el perjuicio a los clientes, y dijo que ese servicio no necesariamente debían pagar los bancos.

Pero para Pesantez, esto no era algo que debía ser costeado por los usuarios, sino que deberían ser los bancos los que corran con ese gasto, por ser estas entidades las responsables de custodiar los ahorros y depósitos de los clientes.

La medida tuvo impacto. Tras la resolución, el sistema financiero ecuatoriano efectivamente empezó a establecer medidas de seguridad estándar.

Esto se reforzó más tarde con una nueva resolución emitida por la Junta Bancaria el 17 de enero del 2012. Esta norma, bajo el nombre JB-2012-2090, dio seis meses a los bancos para contratar coberturas de seguro contra fraudes informáticos en los servicios entregados mediante canales electrónicos.

Dicha resolución, en su artículo 41, establece que "(...) las instituciones financieras contratarán anualmente con las compañías de seguro, coberturas que aseguren a la entidad contra fraudes generados a través de su tecnología de la información, sistemas electrónicos, sistemas telemáticos, electrónicos o similares..." (Resolución Junta Bancaria, 2012). Se dio una nueva prórroga a los bancos y el plazo para cumplir esta disposición vence en junio de 2014.

Según César Robalino, representante de la Asociación de Bancos Privados, los bancos tienen una póliza global que incluye delitos informáticos que puedan afectar a la entidad y cree que eso es suficiente, "a menos que la autoridad diga que no es suficiente (...), porque uno no puede pagarle por descuido de los clientes" (El Universo, 2012).

Robalino hace hincapié en que si el banco no reembolsa el dinero del usuario afectado, dicha disposición solo cubre contingencias por un límite de USD 600, en los casos de las entidades que cuenten con un seguro por delitos.

Francisco Miño, vicepresidente de Marketing de Banco Pichincha, aseguró que la entidad tiene una póliza para delito informático y cibercrimen, pero aclaró que "esa cobertura está enfocada a cubrir eventos de gran materialidad que podrían atentar contra la estabilidad de las instituciones" (El Universo, 2012).

En efecto, como veremos más adelante, estas medidas no han constituido una respuesta para los usuarios perjudicados por estos delitos. Es importante

resaltar, que en una entrevista solicitada al actual Fiscal General de la Nación, Galo Chiriboga, al preguntarle sobre casos y cifras de delitos informáticos, respondió desconocer del tema.

Mediante la resolución interinstitucional (No. 001-FGE-SBS-2011) promulgada el 21 de marzo del 2011, la Junta Bancaria consideró que las entidades financieras debían, además, contratar una "póliza de fidelidad bancaria" que incluya la cobertura de delito informático y cibercrimen. En su artículo número 7 se menciona que esta "brindaría un amparo contra fraudes informáticos bajos condiciones pactadas entre los clientes y la institución y que aseguren la cobertura necesaria sobre estos hechos". (Resolución Junta Bancaria, 2011).

Sin embargo, pese a que la gente afectada realiza denuncias de sus casos y están protegidos por una legislación, no todos los usuarios consiguen la devolución del dinero sustraído de sus cuentas en los llamados delitos informáticos.

Según cifras oficiales de la Superintendencia de Bancos y Seguros, durante el período 2010,2011 y septiembre del 2012, esta entidad registró 204 resoluciones desfavorables al usuario, de 378, por motivo de phishing, o más conocido como robo en línea.

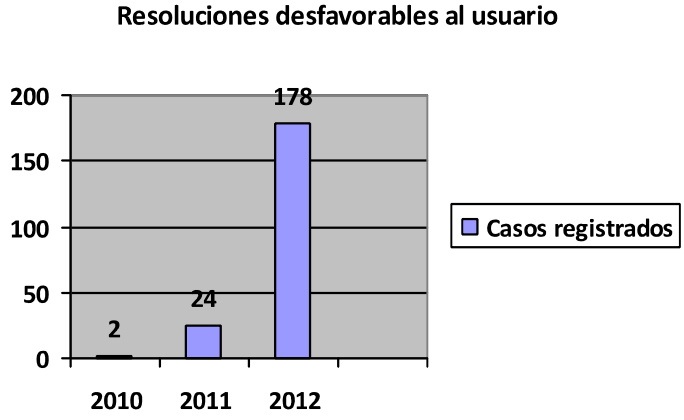


Figura 11. Resoluciones desfavorables al usuario
Tomado de SBS, 2014

Estas reclamaciones receptadas registraron una suma de dinero no reembolsado a los usuarios de USD 228.709, 29.

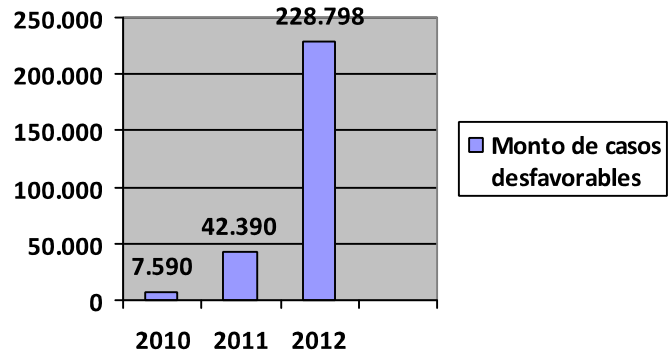


Figura 12. Dinero no reembolsado a usuarios
Tomado de SBS, 2014

Cabe resaltar que, con base al artículo 308 de la Constitución, se establece que la finalidad fundamental de los bancos es preservar los depósitos. Además, la Ley General de Instituciones del Sistema Financiero, dice que tienen la obligación legal de custodia del dinero del depositante.

4.2 CORE BANCARIO

El core bancario, o más conocido como soluciones integrales bancarias, se está implementando poco a poco en el país. Según el portal Web (www.nasoft.com) “el Core Bancario representa el corazón de la operación financiera, y la decisión de seleccionar una plataforma de última generación, que asegure un soporte operativo a mediano y largo plazo”.

El Banco Pichincha fue el primero en implementar en abril del 2012, en toda su red de oficinas en el Ecuador, un software llamado TCS BaNCSS. Esta es una herramienta de core bancario, que ayuda a generar niveles de seguridad.

Esta tecnología de TCS BaNCS es operada en la actualidad en más de 170 entidades financieras en Europa, Medio Oriente, Asia y Oceanía. En América Latina, el Ecuador será fue el primer país en operarla. Esta herramienta pertenece a Tata Consultancy Services (TCS).

Por su parte, Produbanco implementó un nuevo aplicativo bancario Prometeus sobre plataforma Microsoft Windows 2000 Server. Este proyecto inició en Septiembre del 2001 y culminó en febrero del 2004.

A este proyecto se lo denominó Prometeus Core Banking, que ayudó a mejorar la calidad de servicio a los clientes y disminuir los costos de operación. Además, según explican sus autoridades en su portal web, permitió mantener controles preventivos en línea.

El titular de Cobiscorp, Richard Moss, dirigió el proyecto de core bancario del Banco Nacional de Fomento, que finalizó en noviembre del 2010. El valor de este proyecto le costó a la institución USD 4,8 millones.

En síntesis, este sistema ayuda a mejorar la seguridad y el servicio de las instituciones financieras, a pesar que no han ayudado a frenar totalmente los inconvenientes que continúan en la red. Sin embargo, es importante mencionar, que en el país, de los 17 bancos que integran la Asociación de Bancos Privados del Ecuador, solo dos han hecho público que cuentan con este sistema, del resto no existe información pública disponible.

4.3 LOS USUARIOS DE LA BANCA CUENTAN CON DEFENSORES DEL USUARIO

Desde febrero del 2013, los 7 millones de usuarios de la banca cuentan con Defensores del Cliente Financiero. Su principal función es precautelar los derechos de los clientes de la banca. En total son 43 agentes, quienes además cuentan con un suplente en cada banco, que actuaría en casos específicos.

En su portar web, cada entidad bancaria cuenta con el listado de los defensores. **Ver Anexo 2**

Estos Defensores del Cliente financiero, fueron elegidos de acuerdo a la Ley General de Instituciones del Sistema Financiero, la cual establece que su designación la debe efectuar el Consejo de Participación Ciudadana y Control Social, Institución que luego de tres convocatorias culminó con el proceso de selección.

Las funciones, atribuciones y obligaciones de los Defensores del Cliente están normadas en la Constitución de la República del Ecuador, la Ley General de Instituciones del Sistema Financiero así como la normativa expedida por la Junta Bancaria, en su resolución No. JB-2012-2226. Ellos desarrollarán sus funciones en la oficina matriz de cada institución financiera para la cual fueron designados.

Según se especifica en el portal de la Superintendencia de Bancos y Seguros, los defensores del cliente "son las personas naturales designadas en un proceso eleccionario organizado por el Consejo de Participación Ciudadana y Control Social, cuya función principal es la protección de los derechos e intereses particulares de los clientes".

Las instituciones financieras privadas, incluidas las sucursales de instituciones financieras extranjeras, están sujetas a la obligación de contar con un defensor del cliente, independientemente de que todos sus clientes sean personas jurídicas. Esto está incluido en la resolución No. JB-2012-2293 del 13 de septiembre del 2012. **Ver Anexo 3**

El artículo 8 hace énfasis en que los usuarios podrán someter un reclamo al defensor de clientes, tras haber presentado su queja por escrito a su institución financiera y no tuvieron una respuesta favorable.

Cintia Sánchez es una de las defensoras del cliente, que representa al Banco Pichincha. Esta ingeniera añade que entre los requisitos para este proceso se requiere: carta del reclamo que se dirige al banco, respuesta por escrita del banco dirigida al usuario afectado, autorización del clienta para acceder a toda información del usuario, copia de cédula y datos en general.

“Luego de esto analizo el caso para ver si puedo aceptarlo, porque hay varios tipos de reclamos. Lo acepto o no, hago mis oficios y pido al banco una respuesta”, relató Sánchez.

Este proceso dura entre unos 15 o 20 días. Sánchez asegura que el mayor número de reclamos es por problemas en los cajeros. En esos casos, debe pedir videos o cuadres en caja. Posteriormente realiza un análisis a esa información para determinar cuándo y dónde ocurrieron los retiros sospechosos.

Durante el 2013, Sánchez recibió aproximadamente 10 reclamos por problemas en transacciones en línea y afirma que desconoce cuántos se presentan en total en la institución. “Por lo general el Banco y yo nos abstenemos porque es responsabilidad de cada cliente cuidar sus claves. Hay pocos casos que se devuelve el dinero”.

La defensora no descarta que la culpa es de los usuarios. “Realizar este tipo de fraudes es difícil porque la persona que hace el fraude debe tener la tarjeta con la numeración, las preguntas de seguridad, la tarjeta con las coordenadas, etc.”.

Es importante resaltar en este punto, que cada defensor del cliente representa a cada banco a nivel nacional. Es decir, que una sola persona es la encargada de ayudar con la solución de las respuestas negativas de las instituciones financieras, a los reclamos presentados por los usuarios.

Magno Bohórquez es el defensor del Banco de Guayaquil. Este funcionario coincide con Sánchez en que tampoco tienen cifras específicas de las personas que presentan los reclamos en sus oficinas. Bohórquez agrega que un defensor por cada banco es insuficiente ya que los casos que atienden son a nivel nacional y, además, resulta complicado para varias personas que viven en otras ciudades trasladarse a la matriz de su banco para presentar su requerimiento.

“Hay personas que desconocen de este servicio, o las que conocen, por ejemplo, su lugar de residencia no es en el mismo lugar donde está la matriz bancaria, a pesar que los defensores pueden atender por videoconferencias”.

Este defensor del cliente agrega que entre los casos más fáciles de resolver están aquellos que se realizaron mediante cajeros automáticos, ya que se puede solicitar pruebas de cámaras a los bancos, lo que no es posible cuando son transferencias en línea.

En cambio, Fanny Tomalá, defensora del cliente de Produbanco, dice que entre la mayoría de reclamos que ha recibido son los relacionados con compras electrónicas en el exterior con tarjetas de crédito que, según los usuarios, nunca las realizaron.

Tomalá resalta que hay ocasiones en que las denuncias presentadas no son tramitadas porque los clientes no siguieron el órgano regular, como es en primera instancia, solicitar solución a su entidad bancaria.

Si no existe una respuesta positiva entre las partes, el defensor debe remitir un informe dirigido al cliente y al banco, que si no es acogido por las partes será enviado a la Superintendencia de Bancos.

Sin embargo, si bien estos funcionarios son los encargados de “precautelar los derechos de los clientes de la banca”, como lo mencionamos anteriormente, en

los casos de robos en línea, resulta más complicado la devolución del dinero, como lo afirman los mismos defensores.

Los usuarios de la banca desconocen la existencia de los Defensores del Usuario y conocen más sobre las funciones que realiza la Defensoría del Pueblo.

Un solo Defensor del Usuario por banco y a nivel nacional parece ser insuficiente para dar el seguimiento a este tipo de casos, como lo aseguraron los agentes de este departamento, durante las entrevistas realizadas. Esta puede ser otra de las razones por la que los casos no tienen el seguimiento necesario y por ende quedan en la impunidad.

4.4 EL FRAUDE EN LÍNEA EN LA VOZ DE LOS AFECTADOS

La falta de respuesta y de coordinación entre entidades encargadas para brindar una solución a este tipo de casos, y la demora en los procesos de denuncias por delitos informáticos, son los principales problemas y malestares que enfrentaron al menos 384 usuarios de la banca privada del país, que presentaron su reclamo en la Superintendencia de Bancos y Seguros, durante el periodo 2010, 2011 y septiembre del 2012, tras ser víctimas de “phishing” o robo en línea.

Hay que resaltar que de este grupo, para mi investigación trabajé con la muestra de 200 casos de usuarios de la banca privada, ya que el universo no es infinito. De este grupo, el 10 % de los casos fueron registrados en un análisis de estudio mediante encuestas y entrevistas.

Uno de los casos de estudios fue la historia de Juan Francisco Suquillo, de 29 años. Este quiteño recuerda que un viernes del mes de julio del 2012, sacó una parte de sus ahorros de uno de los cajeros ubicados en el valle de Cumbayá, en Quito. Al siguiente día trató de hacer un nuevo retiro en otro

cajero de la ciudad, pero el cajero reportó “fondos insuficientes”. Más tarde comprobó que le habían sustraído USD 1 283 de su cuenta. Esperó al lunes para hacer la denuncia.

Desde entonces y hasta diciembre del 2013, pasaron 17 meses sin una respuesta del banco. Suquillo asistía continuamente a la entidad en busca de una solución, pero nunca tuvo una respuesta favorable. “Es como una burla porque se pasan la pelotita entre todos y nadie ayuda a resolver los casos de los usuarios. Primero esperé una respuesta del banco y tampoco me ayudaron”.

Tras no tener ayuda, este quiteño acudió a la Defensoría del Pueblo, quienes hicieron un llamado al banco para una cita, pero no asistió ningún funcionario de la entidad bancaria a dar una justificación. Posteriormente, la Defensoría le guió a Suquillo para poner una denuncia en la Fiscalía y en la Superintendencia de Bancos y Seguros (SBS). En la Fiscalía el caso se estancó por otros siete meses más.

Luego fue a la SBS donde la funcionaria encargada de procesar su solicitud, le respondió que estaba resolviendo procesos de un año atrás, por lo tanto su caso se iba a demorar unos tres o cuatro meses más.

“Fue indignante. Me fui a varias instituciones y nadie me ayudó. En una cita con el Banco Pichincha, me indicaron ‘vouchers’ de las supuestas compras y no se comprobó q era mi firma, sin embargo ni eso sirvió como prueba de mi denuncia”.

Hasta el momento Suquillo o ha tenido respuesta, y tras tantos meses de espera, y ajetreo por varias instituciones, decidió abandonar el reclamo. Con los registros de su estado de cuenta, se determinó que con el dinero que le robaron los delincuentes hicieron pagos de gasolina en Latacunga y transferencias a dos cuentas bancarias diferentes.

“Es muy injusto que las autoridades no den respuesta, deberían investigar más. Es frustrante porque uno tiene planificado sus ahorros y de la noche a la mañana me quedé sin nada en la cuenta”.

Otro problema es que los afectados no saben a dónde acudir. Al menos seis entidades son a las que acuden los clientes, las cuales actúan sin coordinación generando confusión y falta de respuesta.

Este es el caso de Alberto Castro, de 42 años, quien visitó al menos al menos tres entidades y en ninguna le dieron respuesta tras ser víctima de delitos informáticos. Este padre de familia hacía compras junto a su esposa y sus gemelas (quienes tenían 11 meses aquel día), la cajera del supermercado le informó que el saldo de su cuenta no era suficiente para cancelar su compra.

Sorprendido por lo que escuchó, este vendedor de productos químicos se acercó a un cajero cercano para verificar y efectivamente su cuenta bancaria tenía solo USD 5. “Eran USD 300 dólares en compras que tuvimos que dejar al no tener con qué dinero pagar. Nos quedamos sin comida. No tenía ni leche para darles a las gemelas esa noche, ya no tenían ni pañales”.

Castro cuenta que nunca recibió un mensaje o correo de alerta de las transferencias que hicieron desde su cuenta. En las indagaciones, se pudo constatar que le cambiaron el correo electrónico y el número telefónico registrado para recibir las alertas. Previo a ser víctima de un robo electrónico, en su cuenta de ahorros del Banco de Guayaquil, tenía USD 3 400.

Este quiteño, quien se traslada al oriente ecuatoriano cada 21 días por trabajo, cuenta que cuando ingresó al portal web de su banco, le apareció el mensaje de alerta y posteriormente ingresó normalmente las claves de seguridad.

En este punto es importante resaltar que la SBS emite, por escrito, en la mayoría de oficios de los casos estudiados para esta tesis, una respuesta estándar para todos los casos.

En estos oficios entregados a los usuarios afectados, se menciona que la banca ha venido alertando públicamente por múltiples medios de comunicación que los clientes no deben entregar nunca o facilitar sus datos personales, claves biométricas o coordenadas de tarjeta “E-key”, por correo electrónico, mensajes de celular, SMS, teléfono, página web u otros medios.

De igual manera, en el informe de respuesta al usuario, se hace referencia que al momento previo al ingreso a la banca electrónica se despliega la siguiente alerta, a la cual el usuario debe tener en cuenta cuando ingrese al portal web:

Figura 13. Alerta de portal web
Tomado de Banco Pichincha, 2014

Castro asegura que, aunque la banca en línea agilita los procesos y ahorra tiempo a los usuarios, las falencias y la falta de gente preparada en sistemas informáticos han provocado que este servicio, actualmente, tenga más falencias, a diferencia de asistir personalmente a un banco para realizar dichas gestiones.

Asegura que previo a ser víctima de este delito, durante el último pago en línea que realizó, no observó ninguna anomalía en el portal de su entidad bancaria. Incluso, asegura que con el tiempo se ha familiarizado con el sistema y recuerda que aquel día sí apareció la altera de seguridad con las precauciones que los usuarios deben tener en cuenta.

Ninguna de las entidades le ha dado respuesta hasta el momento. Ya han pasado 18 meses (hasta febrero del 2014), y su caso quedó en la impunidad.

Recibió un análisis de su denuncia por parte de la Fiscalía, donde se informó el número de cuenta de la persona a la que transfirieron el dinero era de Esmeraldas. Dicha cuenta era del Banco Pichincha y el dinero transferido fue cobrado de manera inmediata.

“El número IP tiene el banco, al igual que el nombre de la persona que me robó, números de cuenta de los involucrados. La denuncia está hecha, todos tienen la información necesaria para actuar, pero no hacen nada”, agregó Castro.

Este usuario concluye que aunque han implementado medidas de seguridad en la banca, el sistema sigue vulnerable. “Yo sugiero que si es necesario se cobre a los usuarios un valor extra para implementar mejores sistemas, pero que frenen este fraude, porque nos roban a gente inocente”.

Es más, en los oficios desfavorables de la SBS se menciona que los bancos no son responsables del fraude informático del cual son víctimas los usuarios y se hace referencia al artículo 5, Sección 1, Capítulo III, Título XXV, Libro 1 de la Codificación de Resoluciones de la Superintendencia de Bancos y Seguros y de la Junta Bancaria, que establece lo siguiente y que se cita en las respuestas de los oficios de los afectados:

> “Es responsabilidad exclusiva del cliente respecto de las transacciones que efectuare a través de estos medios; y la responsabilidad del cliente de mantener en secreto la clave o seguridades a él asignadas, así como los cambios de claves que efectuaren. Igual responsabilidad tendrá con respecto a las claves o seguridades adicionales por él solicitadas y otorgadas por el banco” (SBS, 2013).

Esta cita forma parte de las respuestas que la SBS emite a los usuarios afectados. **(Ver Anexo 4).** Hay que resaltar que los oficios emitidos como respuesta, comúnmente dicen lo mismo, y solo cambian datos como fecha, nombre del usuario y el monto del dinero reclamado.

La cita mencionada anteriormente, incluyó en el informe de Marcelo Mejía, quien es otro de los afectados, a quien le jaquearon su cuenta en el Banco Pichincha. Sin embargo, aunque el robo fue de USD 3 400, logró recuperar USD 1600 de este monto. Pero hay que resaltar que este último monto fue reembolsado, porque era un dinero que estaba en su cuenta de ahorro programado o conocida también como ahorro futuro.

Este último es un servicio opcional gratuito que ofrece el banco. Es una cuenta de ahorros con la que el usuario no puede hacer ninguna transferencia bancaria, ni retirar dinero, sea por ventanilla o cajero automático. El resto del monto que Mejía perdió en su cuenta fue de USD 1 800, cifra que estaban en su cuenta corriente.

Mejía recuerda que el dinero que tenía en su cuenta era de unos negocios que realizó días anteriores y que le pagaron en cheques. El cree que esperaron a que se haga efectivo el dinero, para robarle.

El 9 de mayo del 2010 le robaron a las 16:00. Tras recibir una alerta en su celular intentó ingresar a su mail, pero la red de trabajo no le permitió ingresar al sistema. Tras eso decidió acercarse a la agencia de su banco más cercana y presentó una carta con su denuncia. Tras no tener respuesta de su banco, el 4 de julio del 2010 presentó una nueva denuncia en la SBS. A los dos meses le llegó una respuesta, donde se mencionaba que el valor a reembolsar solo sería el de su cuenta de ahorro programado.

“El muerto, muerto está. Recuperar algo más a estas alturas ya no creo. Además que para mí fue muy tedioso trasladarme todo el tiempo a estas instituciones para presionar. Tiempo era lo que menos tenía”

Este contador coincide con otros usuarios afectados por estos delitos, que los bancos se excusan en decir que la culpa de cada usuario y que cada uno es responsable y guardián de sus claves.

Esto a decir que, en la respuesta del caso, se añade una cita donde la banca no se hace responsable de lo sucedido y que el usuario es el culpable por no cuidar sus claves:

> "Concomitantemente con lo anteriormente expuesto y de acuerdo al contenido del análisis integral del presente caso, se presume que no se tomaron los debidos cuidados en las claves asignadas a usted, lo cual produjo que terceras personas accedieran por usted a este canal electrónico, incumpliendo de esta manera lo referido en el contrato de Servicios Electrónicos – Asignación de Tarjeta E-Key, suscrito por usted". (Banco Pichincha, 2013)

Este usuario relata que sacó su cuenta y tarjeta bancaria, por ser práctico, por facilidad y para pagar impuestos en línea. "Esa comodidad me resultó más cara. Ahora prefiero no usar ni la tarjeta e-key y hacerlo todo mediante ventanilla".

La Unidad de Delitos Informáticos se encarga de indagar estos casos a través de peritos especializados en la materia, para hacer un análisis del caso y encontrar a los responsables.

Jorge San Lucas dice que, en caso de hallar falencias en las seguridades de las entidades bancarias, son los bancos quienes están en la obligación de reembolsar el dinero sustraído de sus cuentas.

Sin embargo, como se puede evidenciar en los casos expuestos anteriormente, esto no ocurre. Investigar y comprobar que existió fraude informático puede llevar varios meses e incluso años.

Ese es el caso de María Elena Cárdenas, de 55 años, quien tras presentar la denuncia ante varias instituciones incluido el banco y luego de 22 meses de investigación que concluyó en diciembre del 2013, su caso tuvo una respuesta desfavorable. Ella sostiene que alguien sustrajo de su cuenta corriente de Produbanco, USD 2 600 en febrero del 2012. Era el único valor que tenía en su cuenta, tras haber recibido el sueldo de su último mes de trabajo.

En un cajero ubicado en Tumbaco se informó que su saldo era insuficiente para realizar la transacción. Fue allí cuando se dio cuenta que le habían robado. Al siguiente día fue al banco a dejar la carta de denuncia y en seis meses no tuvo respuesta. Presentó una nueva carta en la SBS y desde agosto del 2012 ha visitado con frecuencia esta institución, pero su caso no se resolvió.

En la atención al usuario de la SBS, le dijeron que su caso se había demorado, por no tener una respuesta de su banco. Esta situación fue difícil para esta arquitecta, quien a los dos meses de lo sucedido dejó de trabajar y no disponía ni ingresos fijos ni dinero ahorrado. Tenía deudas, por lo que tuvo que hacer un préstamo para pagar.

En los estados de cuenta que solicitó se reflejaba que el dinero que le robaron fue transferido a una cuenta extranjera. A ella le cobraron hasta los impuestos de salida de capital. Su cuenta fue hackeada vía internet.

“Todo fue una infamia. Cuando he regresado a estas instituciones me he topado con más afectados. Un gran número de afectados han reclamado en conjunto, pero no hay respuesta. Uno más pierde tiempo”, enfatiza.

Ella dice que como “premio consuelo”, le dieron una nueva tarjeta de débito pero la tiene guardada en su escritorio. “Ahora prefiere hacer la fila en el banco y no volver a ser engañada. Hasta me sentí ofendida que me den una nueva tarjeta, para ver si así dejaba de insistir con mi solicitud. Sí dejé de insistir,

pero por dignidad y porque es fastidioso ir cada semana a preguntar si tienen respuesta de mi caso".

El estudio de estos casos evidencia que la investigación tarda hasta años y los usuarios, aunque apenados por perder su dinero, dejan pasar la situación debido a la falta de respuesta de las entidades. Los afectados se agotan de tanto papeleo que deben realizar y de acudir a las entidades de control que no siempre ayudan a resolver estos casos.

El catedrático Acurio del Pino rechaza la política de ciertas instituciones bancarias de trasladar la responsabilidad de los fraudes informáticos a sus clientes, haciéndoles responsables de las pérdidas sufridas.

"Desde un enfoque de servicio al cliente, se da una ruptura entre el banco y el usuario financiero. Es decir, desde el momento en que éste reporta a la institución financiera el posible fraude, aquel pasa a ser el principal sospechoso y se le delega toda la carga de la prueba", enfatiza el experto (p. 238).

Acurio del Pino agrega que a esto se suma que las instituciones financieras realizan una escueta investigación de los casos y, violando el debido proceso, niegan los reclamos de sus clientes, sin que una sola evidencia demuestre la negligencia o dolo del peticionario, "unicos casos en que la institución financiera podría liberarse de la responsabilidad de restituir los dineros defraudados" (P. 241).

4.5 EL IMPACTO DE LA DUPLICIDAD DE FUNCIONES EN LAS CAUSAS

Dentro de los organismos encargados de receptar denuncias están las intendencias, donde se encuentran los intendentes de policía encargados entre otras cosas, de receptar denuncia y la comisaría de la Policía. Estas entidades, la Superintendencia de Bancos y Seguros y la Fiscalía General del Estado son las principales instituciones encargadas de receptar este tipo de denuncias, además de cada entidad bancaria a la que pertenece cada usuario.

Sin embargo, a pesar de que estas entidades son las primeras opciones a las que asisten los usuarios no siempre los afectados reciben una ayuda eficaz, ya que o no responden sus solicitudes o simplemente sus funcionarios cierran los casos sin dar una respuesta favorable a los usuarios.

María José Troya, Directora de la Tribuna del Consumidor, al igual que Ramiro Ribadeneira, Defensor del Pueblo, coinciden en que ambas instituciones no están autorizadas para recibir denuncias de este tipo.

Sin embargo, agregan que, cuando llegan personas con este tipo de denuncias, indican a los usuarios el procedimiento deben realizar frente a estos casos.

En ese caso, se les recomienda acercarse a cualquier sucursal de su entidad bancaria y presentar su denuncia por escrito, en el balcón de servicios. Allí les darán un documento con el número del reclamo y la fecha límite en la que el banco debe emitir una respuesta. **(Ver Anexo 5)**

Es importante resaltar que esa fecha límite que emite la entidad bancaria no se cumple. Esta aseveración se refleja en los casos estudiados para esta tesis, porque las respuestas de las entidades bancarias llegan a durar entre seis meses y más de un año.

Como recomendación, cuando el usuario se acerca a la ventanilla para denunciar es importante que solicite, temporalmente, la cancelación de su tarjeta bancaria y el congelamiento de la misma. Esto evitará, mientras se estudia el caso, que los ciberdelincuentes no realicen más trasferencias sin su consentimiento.

Además, la Defensoría del Pueblo informa a los usuarios que en caso de no tener una respuesta por su entidad bancaria, puede presentar una nueva denuncia en la Superintendencia de Bancos o acudir al Defensor del Usuario

de su entidad bancaria. Si el tema pasa a mayores, también puede ser presentado en la Fiscalía.

En la Superintendencia de Telecomunicaciones (Supertel), Patricio Jarrín, Director Nacional de Imagen y Comunicación, también agrega que dicha institución guía a los usuarios de la banca sobre cuál es el proceso a seguir tras ser víctima de este tipo de delitos. Jarrín indica que institución es responsable de remitir los códigos IP (Protocolo de Internet) a la Fiscalía cuando esta así lo ha requerido, según se estableció desde julio del 2012 a través del reglamento para usuarios de telecomunicaciones.

Jorge San Lucas, Director de Tecnologías de la Información de la Fiscalía General del Estado, enfatiza que es importante que los usuarios afectados no presenten únicamente sus denuncias en su entidad bancaria y recomienda asistir a la Fiscalía para presentar su denuncia.

En esta institución existen Peritos en Delitos Informáticos que hacen un seguimiento a los casos y a las bandas que operan en línea, incluso desde fuera del país. Frente a esto, Malgarejo explica que aunque tras estas investigaciones, las entidades de control como la Fiscalía logra encontrar a los implicados, o al menos identifican los números de IP de los computadores desde los que se operan las transacciones fraudulentas es muy difícil que puedan detener a las bandas que efectúan estos delitos.

Según Malgarejo estas bandas suelen tener como domicilio de este delito a otros países, especialmente de Latinoamérica.

“Para la Fiscalía es difícil apresar a estos implicados tras hacer una investigación con los números IP, porque el Fiscal General de la Nación es quien debe emitir un oficio al Fiscal General del país donde se registra tal IP. Son procesos largos, que frente a la demanda de casos, es complicado ejecutarlos” (Meljarejo, entrevista, 2014).

Si bien ahora el nuevo Código Integral Penal tiene artículos modificados que ayudarían de alguna manera a que estos delitos se resuelvan, hay que preguntarse, ¿qué va a pasar con los casos registrados durante el período 2009-2014, previo a la aprobación de esta legislación? Son muchas las interrogantes que quedan, al igual que los casos de los usuarios afectados.

Las personas afectadas por este tipo de delitos manifestaron que las instituciones bancarias guardaron hermetismo frente a sus casos y también han mostraron poca colaboración para información y las razones que justificaban la declinación de algunos reclamos, por ende los casos quedan en la impunidad.

En este punto es importante enfatizar, que no solo en Ecuador los usuarios no recuperan su dinero. Así lo aseguró mediante una entrevista Dmitry Bestuzhev (Bestuxhev, 2014), Director de Investigación y Análisis para la empresa Karpersky Lab.

Bestuzhev señaló que un estudio realizado en verano del 2013 en el ámbito global, denominado “Riesgos de Seguridad para el Consumidor”, mostró que el 41 % de los usuarios que perdieron su dinero por ser víctimas de fraude financiero en línea, no recuperaron un solo centavo de su dinero.

El experto agregó que a pesar de que ese dinero puede ser reembolsado por la entidad bancaria al usuario, incluso en algunos casos tras un procedimiento judicial, eso no era una garantía para los usuarios. “Sólo el 45% de los usuarios recuperó totalmente su dinero. Un 14% solo recuperó una parte del dinero perdido y el 41% de las víctimas restantes no recuperaron ni un centavo”, explicó el experto.

En este estudio se determinó además que en un 33 % de casos de delitos informáticos en línea, el dinero corre más riesgo de ser irrecuperable si es sustraído fraudulentamente durante una transacción de pago electrónico. En el

17% de los casos el dinero desapareció durante sesiones de banca electrónica y un 13% de las víctimas eran clientes de tiendas en línea.

Además, el estudio muestra que el 54% de los encuestados cree que el banco es responsable de pagar cualquier cantidad de dinero perdido durante transacciones en línea y el 68% de los encuestados cree que el banco debe proporcionar herramientas de seguridad para proteger las transferencias de dinero.

Entre las soluciones que se debe adoptar frente a estos casos, son en primera instancia, obligar a los bancos a invertir en tecnología que mejore la seguridad bancaria, para que los usuarios no continúen siendo víctimas de estos delitos.

Pero los usuario también deben colaborar y proteger sus computadores. Según un artículo publicado por PCWord, se muestra que según “las previsiones de PandaLabs, existirían alrededor de 637 000 antivirus falsos logrando ventas por semana de antivirus de hasta USD 90 000 por cada delincuente” (Herranz, Julio 2009). Es decir, que se podría prevenir o minimizar el riesgo de los ataques por la red, buscando acuerdos y soluciones de seguridad en los contratos de Internet de banda ancha que ofrecen las operadoras.

5 CAPÍTULO V: RESULTADOS Y ANÁLISIS DE LAS ENCUESTAS A USUARIOS

Finalmente, en el desarrollo de este capítulo, expondremos los resultados obtenidos tras una encuesta realizada a los usuarios de la banca, que han sido afectados por la ciberdelincuencia. Tras las cifras obtenidas, se realizará un análisis explicativo de cada resultado, que ayudará a entender de una mejor manera una parte importante del desarrollo de este estudio.

5.1 DESARROLLO DE LA ENCUESTA A USUARIOS DE LA BANCA PRIVADA QUE HAN SIDO VÍCTIMAS DE LOS CIBERDELITOS

Mediante una encuesta realizada a los usuarios de bancos, víctimas de delitos informáticos en línea se pudo obtener cifras que ayudan a complementar el estudio de esta investigación.

Cada encuesta contó con 10 preguntas **(Ver Anexo 6)**, que fueron realizadas a 200 personas domiciadas en la ciudad de Quito.

El promedio de edad de las víctimas de robos en línea es de entre 29 y 55 años. De este grupo, el 70 % son hombres y el 30% son mujeres. Los robos fueron registrados entre mayo del 2010 y ooctubre del 2012.

A continuación, se expone cada pregunta de la encuestra, complementada con una tabla que refleja los resultados obtenidos.

5.2 EXPOSICIÓN DE LA ENCUESTA REALIZADA A LAS VICTIMAS DE CIBERDELITOS

1. ¿Bajo qué modalidades fue víctima de fraude informático?

A) Ingreso de todas las coordenadas
B) Página web bancaria clonada
C) Correo electrónico con oferta laboral o promocional
D) Otros

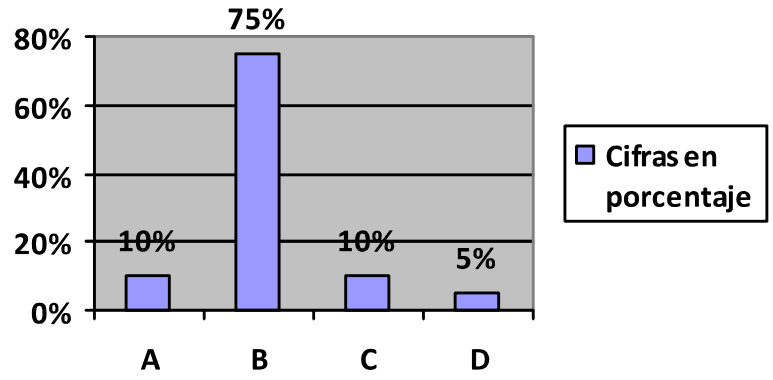


Figura 14. ¿Bajo qué modalidades fue víctima de fraude informático?

El delito más común a través del cual se cometen estos delitos es phishing, como lo muestra la figura anterior. Así el 75% de los encuestados fue víctima de fraude informático tras ser clonada la página web de su entidad bancaria. Solo un 10% cayó en la trampa de responder información mediante correo electrónico y a un 5 % se le clonó su tarjeta mediante un cajero automático, con lo que luego se realizaron transferencias bancarias no autorizadas por el usuario.

2. El monto de su perjuicio fue de:

A) 0- 500
B) 500-1000
C) 1000-5000
D) 5.000-10.000

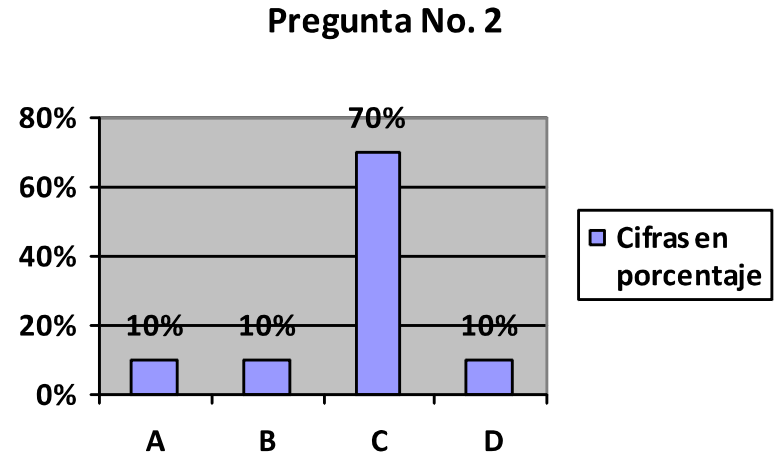


Figura 15. El monto de su perjuicio

En esta pregunta, se evidenció que el mayor porcentaje de usuarios perdió dinero entre 1000 y 5000 dólares. Las cifras no alcanzan más de 10.000 dólares, debido a que las entidades bancarias tienen un límite de transferencias en línea. Cuando las transferencias necesitan ser más altas, los usuarios deben acercarse a la ventanilla de su banco a realizar el trámite personalmente.

3. ¿A qué institución asistió primero para hacer su reclamo?

A) Su entidad bancaria
B) Superintendencia de Bancos
C) Fiscalía General del Estado
D) Superintendencia de Telecomunicaciones
E) Policía Nacional

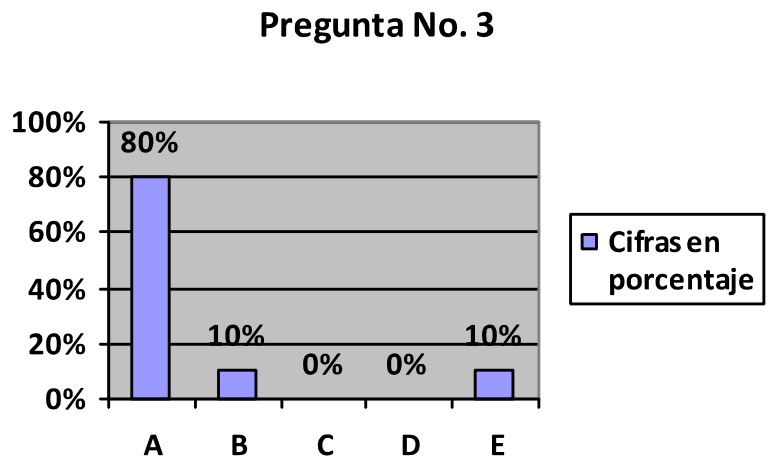


Figura 16. ¿A qué institución asistió primero para hacer su reclamo?

Tras ser víctimas de este tipo de delito, los entrevistados, en su mayoría (80%) coincidieron en que la primera entidad donde presentaron su denuncia fue en su entidad bancaria. Tras no tener respuesta, el resto acudió a la Superintendencia de Bancos y Seguros y a la Policía.

4. ¿Qué tipo de respuesta recibió respecto a su denuncia?

A) Positiva
B) Negativa

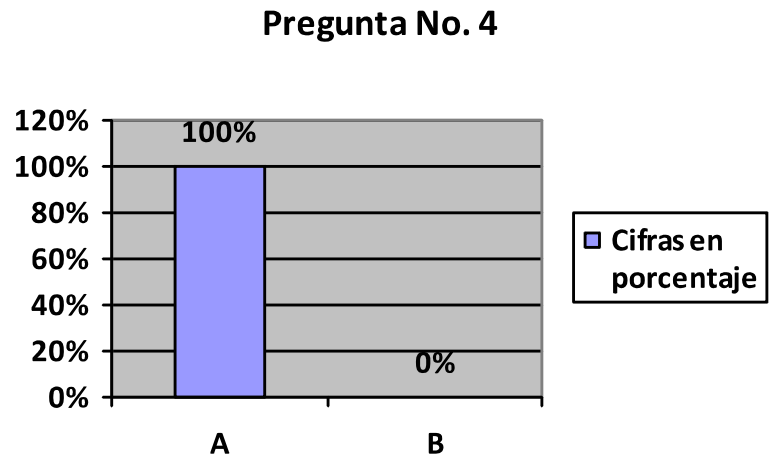


Figura 17. ¿Qué tipo de respuesta recibió respecto a su denuncia?

Como ya lo analizamos anteriormente, como respuesta a denuncias, los usuarios reciben respuestas negativas de las entidades de control, donde se les niega el reembolso de su dinero, tras justificar que no fue favorable su resolución.

5. ¿De qué entidad bancaria fue sustraído su dinero?

A) Banco Pichincha
B) Banco Guayaquil
C) Produbanco
D) Banco Internacional

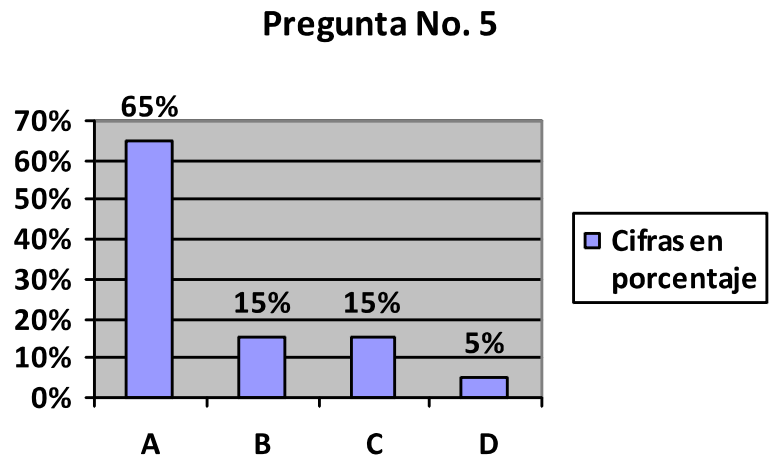


Figura 18. ¿De qué entidad bancaria fue sustraído su dinero?

En esta pregunta, se puede apreciar que el Banco del Pichincha registra en este estudio más número de casos de los usuarios afectados, con un 65%, seguido de un 15% el Produbanco y Banco de Guayaquil.

6. Su dinero fue sustraído de una cuenta de:

A) Ahorros
B) Corriente

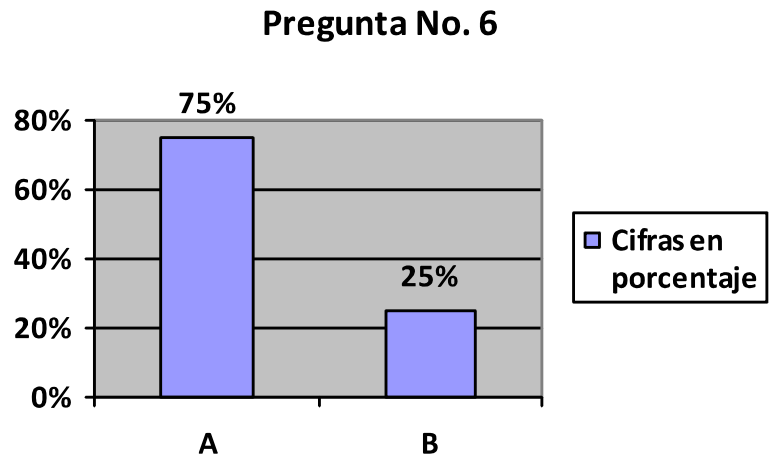


Figura 19. Su dinero fue sustraído de una cuenta

El 75% de los encuestados, afirmó que la cuenta de la que fue sustraído su dinero sin su consentimiento, fue de una cuenta de ahorros.

7. ¿Desde qué lugar realizó su transferencia bancaria, por la que se presume que fue víctima de delito informático?

A) Casa
B) Cibercafé
C) Oficina

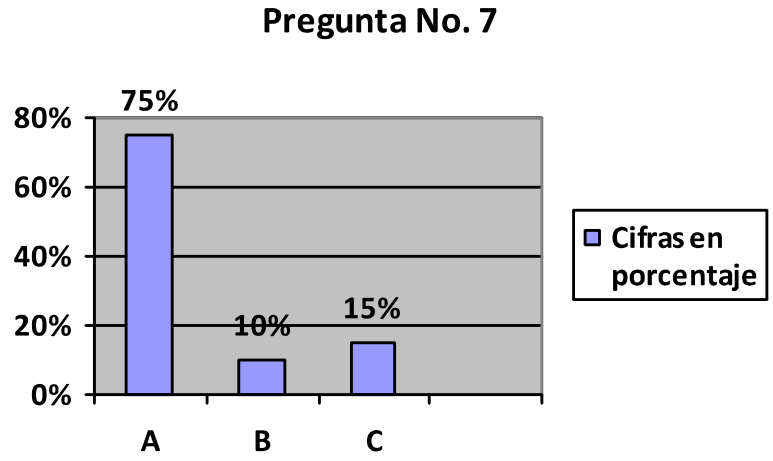


Figura 20. ¿Desde qué lugar realizó su transferencia bancaria, por la que se presume que fue víctima de delito informático?

Si bien en la mayoría de los entrevistados aseguraron tener una profesión y trabajar en diferentes oficios en esta pregunta se puede observar que el 75% de las personas prefiere realizar sus transferencias desde su hogar y que cuando fueron víctimas de la ciberdelincuencia estuvieron en sus domicilios.

8. ¿Cuánto tiempo se demoró el estudio de su caso?

A) 1-3 meses
B) 3-6 meses
C) 6-12 meses
D) Más de un año

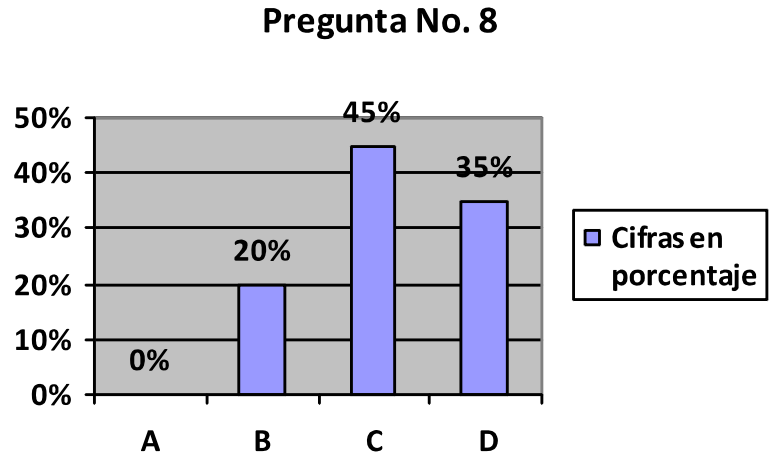


Figura 21. ¿Cuánto tiempo se demoró el estudio de su caso?

Durante el estudio del capítulo IV, se expuso los casos de este estudio, donde se evidenciaba el tiempo que puede llegar a tardar el proceso de estos casos. Como se puede observar, un 45% de los casos llegó a durar hasta un año. Un 35% incluso, duró más de un año y a pesar de la espera, resultó negativa su solicitud.

9. ¿Tras concluir el proceso, le devolvieron su dinero?

A) Sí ()
B) No ()

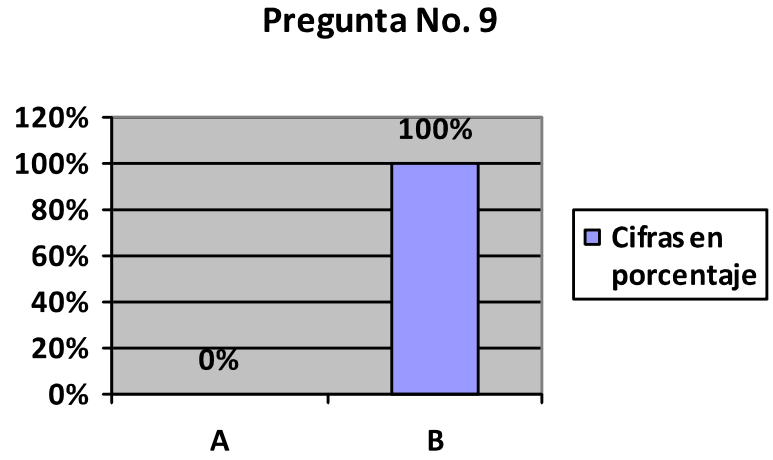


Figura 22. ¿Tras concluir el proceso, le devolvieron su dinero?

El 100% de los encuestados de este estudio no recuperó su dinero, tras recibir un informe negativo de su denuncia.

10. ¿Después de ser víctima de un fraude informático continúa haciendo transferencias en línea?

A) Si ()
B) No ()

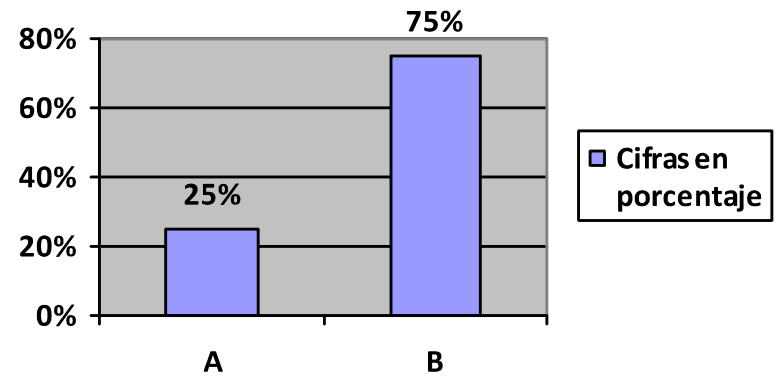


Figura 23. ¿Después de ser víctima de un fraude informático continúa haciendo transferencias en línea?

Esta problemática ha influido en que un 75% prefiera dejar de hacer transferencias en línea, tras ser víctimas de este delito informático.

6 CAPÍTULO VI: CONCLUSIONES Y RECOMENDACIONES

6.1 CONCLUSIONES

- Uno de los factores que más incide en este alto índice delincuencial es la impunidad. La causa se archiva en muchos de los casos sin realizar la búsqueda de pruebas. Otra cantidad fracasa porque las investigaciones no se realizan oportunamente.

- Si bien son, al menos, seis entidades de control encargadas de resolver y hacer un seguimiento de estos casos, los usuarios deberían tener un canal más claro para realizar sus denuncias, pero esto no ocurre y en las entidades públicas y privadas se señala, muchas veces, al propio usuario como el responsable de los casos.

- La falta de una cultura informática en el país sobre el uso y consumo de las nuevas tecnologías es otro problema. No hay madurez en el usuario para clasificar la información y determinar su utilidad, lo que lleva a cometer este tipo de delitos.

- La normativa legal ecuatoriana, en cuanto a los delitos informáticos, aún requiere de ajustes para tipificar este tipo de delitos, ya que pese a que la gente afectada realiza denuncias de sus casos y están protegidos por una legislación no todos los usuarios consiguen la devolución del dinero sustraído de sus cuentas.

6.2 RECOMENDACIONES

- Tras el estudio de esta tesis, considero que es necesario que los usuarios utilicen herramientas de seguridad avalados por proveedores de servicios locales que incluyan banda ancha segura en hogar. Se requieren servicios con un un amplio portafolio de antivirus.

- Ecuador debe adherirse al Convenio de “Cibercriminalidad de la Unión Europea”, lo que le permitiría contar con una legislación adecuada sobre el tema y beneficiarse de la cooperación internacional en la protección contra este problema social.

- Pese a la falta de profesionales especializados en el área de la computación forense sería recomendable incorporar en el pensum de estudios de la Carrera de Ingeniería en Sistemas, una materia relacionada a Computación Forense y a la Prevención y detención de delitos informáticos. Como sugirió Acurio del Pino durante una entrevista para esta tesis: “No tienen que ser fiscales expertos en tecnología, pero deben saber cómo iniciar el proceso de investigación”.

- Es importante que se logre profundizar el conocimiento en las tecnologías informáticas, actualizando y capacitando constantemente a fiscales, jueces, peritos y abogados para combatir el cibercrimen.

7 CAPÍTULO VII: PROPUESTA COMUNICACIONAL

Este capítulo también cumple un rol importante en el desarrollo de esta tesis, ya que mediante los productos se busca informar y educar de alguna manera a los usuarios del ciberespacio, pero especialmente de banca. Este espacio sirve para plasmar los resultados obtenidos durante el desarrollo de esta tesis.

7.1 RADIO-REVISTA: E-BANK

Misión:

Somos un espacio de información sobre la banca en línea en la ciudad de Quito, que tiene como objetivo informar a los usuarios de la banca, para prevenir que sean víctimas de los delitos informáticos.

Visión:

Lograr ser una guía y un referente de información sobre la banca, para las personas que están expuestos a ser víctimas de la ciberdelincuencia.

Valores: Veracidad, Aprendizaje, Contribución, Servicio

7.1.1 Descripción de la revista

La radiorevista “e-Bank” tiene una emisión semanal de 30 minutos, que busca ser un espacio de información y guía con las víctimas de la ciberdelincuencia. De igual manera, busca difundir en su audiencia lo importante que es denunciar los casos de delitos informáticos a las autoridades pertinentes. La periodicidad de esta radio revista es semanal.

7.1.2 Objetivos

Guiar sobre las precauciones que deben tener los usuarios de Internet, especialmente con sus claves y portales web.

Exponer los métodos utilizados por los ciberdelincuentes para atacar a usuarios.

Generar información sobre las responsabilidades que tienen las instituciones pertinentes frente a denuncias por delitos informáticos.

7.1.3 Audiencia

Usuarios de Internet del Ecuador y que especialmente posean una cuenta bancaria y prefieran evitar las filas de los bancos, para utilizar los servicios de la banca en línea. Además, durante la encuesta realizada se evidenció que los usuarios tenían entre 29 y 55 años.

Público 18 a 50 años (Adolescentes y Adultos)

18-19 Adolescentes
20-29 Adultos jóvenes
30-44 Adultos medios
45-64 Adultos
65- Adultos mayores

7.1.4 Anunciantes

Se aspira contar con el Aval de la Asociación de Bancos Privados del Ecuador, así como la Superintendencia de Bancos y Seguros del Ecuador.

7.1.5 Secciones

- Perfil 2.0
- En la red
- Infobank
- El experto on-line

7.1.6 Talentos humanos

- Productora y conductora
- Técnico operador

7.1.7 Recursos técnicos

- Estudio de Grabación
- Material de audio

7.1.8 Guión

Ver Anexo 7 y 8

7.2 REPORTAJE TELEVISIVO

Dentro de los productos propuestos para este proyecto, está un reportaje televisivo al que se le ha denominado “La ciberdelincuencia”. Con este reportaje se buscar brindar a la ciudadanía una radiografía de los delitos informáticos.

7.2.1 Objetivo

El objetivo es que los usuarios del mundo cibernético, conozcan cómo opera la ciberdelincuencia y sepan cómo prevenir ser víctimas. Durante el desarrollo de

este reportaje, se puede observar desde testimonios de los afectados, hasta expertos que brindan su aporte sobre el tema.

Dicho reportaje tiene una duración de 9 minutos.

7.2.2 Requerimientos

- Un trípode
- Cámara CANON 7D
- Un micrófono corbatero
- Equipo de iluminación
- Una computadora Mac
- Software de edición

7.2.3 Guión

Como soporte de la filmación, se utilizó un guión, que fue estructurado a partir del planteamiento del tema, desarrollo y cierre. **(Ver Anexo 9 y 10).**

7.3 PORTAL WEB "E-BANK"

El producto digital propuesto es un sitio web que fusiona texto, audio, video y fotografía. Su diseño buscar exponer a la audiencia digital una guía de prevención a la ciberdelincuencia y de educación on-line a la ciudadanía.

Los usuarios podrán conocer cómo hacer una denuncia, las precauciones que se deben tener al navegar en un portal web, especialmente de las entidades bancarias que son las más vulneradas, compartir sus testimonios e inquietudes, así como también, observar infografías y videos educativos sobre la banca. Además, podrán tener acceso al audio de cada programa semanal de la radiorevista.

En el portal web también se podrá observar un menú principal. Este menú de navegación estará dividido en secciones: “Quiénes somos”, “Infobank”, “En la red”, “Expertos on-line”, “Multimedia” y “Contactos”.

La plataforma utilizada para este portal web se realizó en formato HTML, que permite visualizarse en cualquier computador. Como parte del diseño, se cuenta con un espacio sencillo, pero a su vez interactivo, donde se podrán dejar denuncias o interactuar con otros afectados de la ciberdelincuencia. A pesar de ser la página principal, las direcciones de las redes sociales como Facebook y Twitter estarán relacionadas al portal web, para interactuar entre usuarios cualquier duda o sugerencia. Los posteos en las redes sociales especialmente, serán diarios.

El nombre del portal web, al igual que el resto de productos, es “e-bank” y su URL www.ebank.com.

REFERENCIAS

Acosta, S. (s.f.). Recuperado el 19 de enero de 2014, de http://www.larepublica.co/finanzas/conozca-y-evite-el-phising-pharming-y-malware-principales-delitos-financieros_101236

Acurio del Pino, S. (2010). Derecho y Nuevas Tecnologías. Quito.

Alzate, S. (s.f.). *La Repúbica*. Recuperado el 17 de enero de 2014, de http://www.larepublica.co/finanzas/conozca-y-evite-el-phising-pharming-y-malware-principales-delitos-financieros_101236

Banco Central del Ecuador. (1957). *Boletín*. Obtenido de www.bce.gob.ec

Banco Central del Ecuador. (2003). Memoria Anual 2003. Obtenido de www.bce.gob.ec

Cabello, A. (1999). *La globalización y liberación financiera y la bolsa mexicana de valores, del auge a la crisis*. México.

Camacho, L. (1987). *El Delito Informático*. Madrid.

Caness, M. (2009). *La Banca del Ecuador, una explicación histórica*.

Castillo, M. & Ramallo, M. (1989). *El delito informático*. Madrid: Congreso sobre Derecho Informático. Facultad de Zaragoza.

Chiriboga, L. (2010). *Sistema Financiero*. Quito.

Consejo de Europa. (2001). *Convenio sobre la Ciberdelincuencia*. Madrid: Convenio Núm. 185.

Diario El Universo. (2012). *Bancos deben tener seguros contra delitos informáticos*. Recuperado el 15 de enero de 2014, de http://www.eluniverso.com/2012/06/29/1/1356/bancos-deben-tener-seguros-contra-delitos-informaticos.html

Diario Hoy. (12 de Marzo de 1999). *Economía monetaria ecuatoriana previo a la Misión Kemmerer.* Recuperado el 12 de enero de 2014, de http://www.hoy.com.ec/noticias-ecuador/bancos-devolveran-dinero-por-delitos-informaticos-465384.html

Fernández, J. (2009). *El Cibercrimen y los delitos comeditos a través de Internet.* Madrid.

Garrido, M. (1992). *Nociones Fundamentales de la Teoría del Delito*. Chile.

Grijalba, W. (2008). *Breve Historia Bancaria del Ecuador*. Quito.

Guibourg, R., Alende, J., & Campanella, E. (1996). *Manual de Informática Jurídica*. Argentina.

Herranz, A. (2009). Revista PC Word, España, 12-13.

Jiménez de Asúa, L. (2001). *La Ley y el Delito*. (13va. Ed.). México, Hermes.

Junta Bancaria SBS. (2013). Artículo 5, Sección 1, Capítulo III, Título XXV, Libro 1 de la Codificación de Resoluciones. Quito.

Junta Bancaria. (17-01-2012). No. JB-2012-2090. Quito.

López, S. (2013). *Directora de marketing de Easy Solutions*. Madrid.

Loza, C., & Camacho, L. (1987). *Manual de Informática Jurídica*. Madrid.

Malgarejo, R. (2013). Entrevista. *Perito en delitos informáticos*.

Marcel, P., & Ripert, G. (2006). *Tratado elemental de Derecho Civil*. Bogotá.

Morlás, C. (2004). *El ABC de la Banca*. Guayaquil.

Nasoft. (s.f.). Recuperado el 9 de enero de 2014, de http://www.nasoft.com/site/home/soluciones/portecnolog%c3%ada/corebancario/tabid/97/default.aspx

Noruega, N. (2013). Recuperado el 7 de enero del 2014, de http://www.delitosinformaticos.com/10/2013//danos-informaticos/ataque-informatico-mediante-bomba-logica-o-bomba-de-tiempo#.UtQeKtIW1ac

Organización de las Naciones Unidas (ONU). (1990). *Congreso sobre Prevención del Delito y Justicia Penal.* La Habana, Cuba.

Palomino, J. (2006). *Derecho penal y nuevas tecnologías*. Valencia.

Periodista Digital. (2014). Recuperado el 20 de enero del 2014, de http://www.periodistadigital.com/economia/empresas/2014/01/20/atento-momento-pueden-robando-identidad.shtml

Rodríguez, G. (2002). *Derecho penal e Internet*. Madrid: La Ley.

Romeo, C. (1987). *Poder Informático y Seguridad Jurídica*. Madrid: Fundesco.

Romero, C. (2013). *Experto en delitos informáticos de la ESPE*. Quito.

Superintendencia de Bancos y Seguros. (2012). *Reclamos informáticos*. Obtenido de http://www.sbs.gob.ec/practg/sbs_index?vp_art_id=&vp_tip=5&vp_lang=1&vp_buscr=Reclamos+inform%C3%A1ticos&x=15&y=12

Superintendencia de Bancos y Seguros. (2013). *Estados de situación remitidos por las entidades*. Obtenido de http://www.sbs.gob.ec/

practg/sbs_index?vp_art_id=&vp_tip=5&vp_lang=1&vp_buscr=Estados+de+situaci%C3%B3n+remitidos+por+las+entidades&x=6&y=8

Superintendencia de Bancos y Seguros. (2014). *Oferta de entidades financieras privadas*. Obtenido de http://www.sbs.gob.ec/practg/sbs_index?vp_art_id=&vp_tip=5&vp_lang=1&vp_buscr=Oferta+de+entidades+financieras+privadas&x=14&y=14

Superintendencia de Telecomunicaciones del Ecuador. (2011). *Delitos informáticos más frecuentes en el país.* Obtenido de http://www.supertel.gob.ec/pdf/publicaciones/supertel13_2012.pdf

Téllez, J. (2003). *Derecho Informático*. México.

Temperini, M. (2012). *Delitos Informáticos en Latinoamérica: Un estudio de derecho comparado.* Argentina.

Torres, L. (2007). *La Banca de la Usura al Narcolavado*. Quito.

Trujillo, E. (1984). *La Historia del Papel Moneda del Ecuador*. Guayaquil.

ANEXOS

ANEXO 1

Calificación de riesgo de la banca privada

ENTIDAD	CALIFICACIÓN MARZO-13	PUNTAJE CALIFICACIÓN	PARTICIPACIÓN DIC-12	ENTIDAD
AMAZONAS	**AA**	5	0,5	AMAZONAS
AUSTRO	**AA-/AA-**	10	4,5	AUSTRO
BOLIVARIANO	**AAA-/AAA-**	18	8,7	BOLIVARIANO
CAPITAL	**AA-**	14	0,5	CAPITAL
CITIBANK	**AAA**	20	2,0	CITIBANK
COFIEC	**C**	5	0,1	COFIEC
COMERCIAL DE MANABI	**A-**	8	0,2	COMERCIAL DE MANABÍ
COOP. NACIONAL	**A+**	13	0,6	COOP. NACIONAL
DELBANK	**BBB**	4	0,0	DELBANK
D-MIRO S.A.	**BBB+**	14	0,1	D-MIRO S.A.
FINCA	**BBB-**	6	0,0	FINCA
GENERAL RUMIÑAHUI	**AA**	14	1,9	GENERAL RUMIÑAHUI
GUAYAQUIL	**AAA / AAA-**	16	11,6	GUAYAQUIL
INTERNACIONAL	**AAA-/AAA-**	16	8,3	INTERNACIONAL
LITORAL	**A**	10	0,1	LITORAL
LOJA	**AA+**	15	1,4	LOJA
MACHALA	**AA+**	15	2,4	MACHALA
PACIFICO	**AAA-**	12	11,9	PACIFICO
PICHINCHA	**AAA- / AAA-**	18	29,4	PICHINCHA
PROCREDIT	**AAA- / AAA-**	16	1,2	PROCREDIT
PRODUBANCO	**AAA- / AAA-**	18	9,7	PRODUBANCO
PROMERICA	**AA+**	12	2,8	PROMERICA
SOLIDARIO	**AA+**	14	2,1	SOLIDARIO
SUDAMERICANO	**BB**	4	0,0	SUDAMERICANO
TERRITORIAL		6	-	TERRITORIAL
UNIBANCO		12	-	UNIBANCO

Tomado de SBS, 2013

ANEXO 2

Listado de los defensores del usuario por entidad bancaria y sus domicilios

Representantes por institución financiera

Institución financiera	Principal	Suplente
BANCO PICHINCHA	Cintia Vaneza Sánchez	Carlos Iván Muñoz Aguilar
BANCO DE GUAYAQUIL	Magno Rafael Bohórquez	Rosa Piedad Tapia Andino
BANCO DEL PACÍFICO	Roberto Xavier Guerrero	Francisco Xavier Gálvez
BANCO DEL AUSTRO	Cristian Mauricio Tello Moreno	María Gabriela Zurita Castillo
BANCO BOLIVARIANO	Claudia Lorena Sigcha	Jacqueline del Rocío Cuadrado
BANCO CAPITAL	Juan Carlos Terán Almeida	Eva María Cañarte Bosch
BANCO COOPNACIONAL	Jorge Enrique Rivas Triviño	David Ricardo Matías Meza
BANCO DE LOJA	Verónica del Cisne Pineda	Joffre Juan Villalva Casanello
BANCO DE MACHALA	Ernesto Vicente Guadalupe	Alfredo de Jesús López
BANCO DEL BANK	Silvana Inés Escalante	Gicella Magdalena Bravo
BANCO DE LA VIVIENDA	Gisella Katherine Rangel Mora	Miguel Ángel Enrique Espinoza
BANCO INTERNACIONAL	José Andrés Mármol Revelo	Tania Lorena Coello Vásquez
BANCO LITORAL	Susana Janeth Rodríguez León	Luis Armando Chisaguano
PROCREDIT	Diana Roxana Astudillo	Cristian Isabel Campoverde
PRODUBANCO	Fanny Goretty Tomalá	Diana Alejandra Mijas Castillo
BANCO PROMERICA	Oswaldo Alfonso Abad	María Mercedes Mero Cortez
BANCO SOLIDARIO	Dexis Cecilia Vergara López	Cristian Darwin Reibán Quito
BANCO TERRITORIAL	Ketty Elizabeth Vega Tola	Saskya Miosotis Falconí Plaza
BANCO AMAZONAS	Kléver Catón Coello Bajaña	Sol María Faytong Hernández
COFIEC	Manuel Mesías Dávila Proaño	Marco Gonzalo Cevallos Cazar

Tomado de Participación Ciudadana

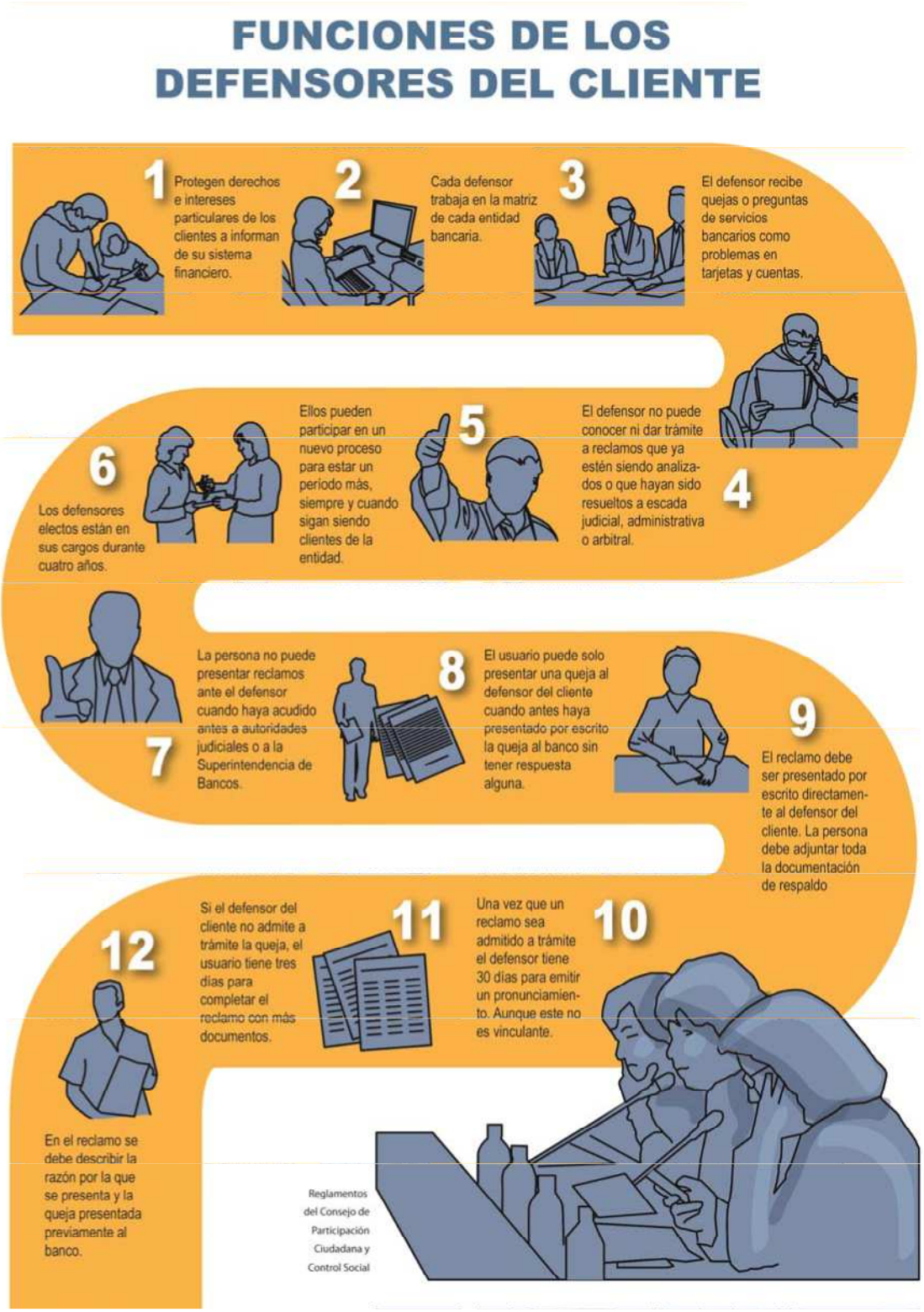
Domicilios de los defensores del cliente

ESTADO	NOMBRE INSTITUCION	CIUDAD	DIRECCION
	ENTIDADES PÚBLICAS		
ACTIVA	BANCO DEL INSTITUTO ECUATORIANO DE SEGURIDAD SOCIAL	QUITO	Amazonas N35 - 181 y Japón
ACTIVA	BANCO DEL ESTADO	QUITO	Av. Atahualpa OE1-109 y Av. 10 de Agosto
ACTIVA	BANCO ECUATORIANO DE LA VIVIENDA	QUITO	Av. 10 de Agosto 2270 y Cordero
ACTIVA	BANCO NACIONAL DE FOMENTO	QUITO	Antonio Ante Oe 1-15 y Av. 10 de Agosto
ACTIVA	CORPORACION FINANCIERA NACIONAL	GUAYAQUIL	Av. 9 de Octubre 200 y Pichincha
ACTIVA	INST.ECUAT.CREDITO EDUCATIVO Y BECAS	QUITO	Alpallana E7-183 entre Diego de Almagro y Whymper
	BANCOS PRIVADOS		
ACTIVA	BANCO AMAZONAS	GUAYAQUIL	Av. Francisco de Orellana No. 238
ACTIVA	BANCO DEL AUSTRO	CUENCA	Sucre y Antonio Borrero, esquina
ACTIVA	BANCO DE GUAYAQUIL	GUAYAQUIL	P. Icaza 200 e/ Pedro Carbo y Pichincha
ACTIVA	BANCO BOLIVARIANO	GUAYAQUIL	Junin 200 Y Panama Esq. Guayaquil
ACTIVA	BANCO COFIEC	QUITO	Av. Patria E4-21 y 9 de Octubre
ACTIVA	BANCO CAPITAL S.A.(antes Corfinsa S.A.)	QUITO	Amazonas Nº 34-311 y Avenida Atahualpa
ACTIVA	BANCO COOPNACIONAL S.A.	GUAYAQUIL	Capitan najera 4210 y La 14,
ACTIVA	BANCO D-MIRO	GUAYAQUIL	García Goyena 4826, entre la 24 ava. y 25 ava.
ACTIVA	DELBANK (antes Baninco)	GUAYAQUIL	P- Ycaza 454 Y Baquerizo Moreno
ACTIVA	BANCO COMERCIAL DE MANABI	PORTOVIEJO	18 de Octubre y 10 de Agosto
ACTIVA	BANCO FINCA S.A.	QUITO	Av. Amazonas N 39-123 y José Arizaga
ACTIVA	BANCO DEL LITORAL S.A.	GUAYAQUIL	Malecón 514 e Imbabura
ACTIVA	BANCO GENERAL RUMIÑAHUI S.A.	QUITO	Av.Republica E6-573 Y Eloy Alfaro
ACTIVA	BANCO INTERNACIONAL	QUITO	Av. Patria E4-21 y 9 de Octubre
ACTIVA	BANCO DE LOJA	LOJA	Bolivar y Rocafuerte Esquina
ACTIVA	BANCO DE MACHALA	MACHALA	9 de Mayo y Rocafuerte Esquina
ACTIVA	BANCO DEL PACIFICO S.A.	GUAYAQUIL	Capitán Nájera 4210 y la 14ava
ACTIVA	BANCO PICHINCHA C.A.	QUITO	Av.amazonas 4560 Y Pereira Quito
ACTIVA	BANCO PROCREDIT S.A.	QUITO	AVS. ATAHUALPA Y AMAZONAS ESQUINA
ACTIVA	PRODUBANCO	QUITO	Av. Amazonas N35-211 y Japón
ACTIVA	BANCO PROMERICA S.A.	QUITO	Amazonas y Colón, Esquina
ACTIVA	BANCO SOLIDARIO	QUITO	Av. Amazonas y Corea
ACTIVA	BANCO SUDAMERICANO	QUITO	Av. Amazonas y Rumipamba

Tomado de SBS

ANEXO 3

Infografía de las funciones de los defensores del cliente



ANEXO 4

Oficios de la SBS a los usuarios afectados por delitos informáticos

OFICIO No. DNAE-SAU-2012-6644
Quito D.M., 06 de noviembre de 2012
Doctor
WILSON HERNÁN ANDRADE DÁVILA
El Condado, calle H 239 e intersección B
Quito.-
De mi consideración:
Mediante Resolución No. ADM-2012-11043, se emitió la Acción de Personal No. 1309 de 17 de julio de 2012, en la que fui nombrada Subdirectora de Atención al Usuario, en tal virtud, avoco conocimiento del presente reclamo administrativo.

I. ANTECEDENTES

Me refiero a su comunicación ingresada en este organismo de control el 20 de junio de 2012, mediante la cual presentó un reclamo administrativo en contra de Banco Pichincha C.A., manifestando lo siguiente:

> *"(...) El día de 19 de junio de 2012, a las 22h12 minutos, ingresé vía internet a realizar una CONSULTA DE MOVIMIENTOS de mi cuenta corriente 3214691104, del BANCO PICHINCHA. Sorpresivamente, aparece que el día 18/06/2012, han realizado una TRANSFERENCIA INTERNET de mi referida cuenta, por un valor de 4,898.39 dólares de los Estados Unidos de Norteamérica., transferencia que jamás realizó o autorizó el suscrito, con lo cual se habría producido el presunto delito de APROPIACIÓN ILÍCITA DE BIENES AJENOS, VIOLACIÓN DE SEGURIDADES ELECTRÓNICAS, INFORMÁTICAS U OTRAS SEMEJANTES, previsto en nuestra legislación (...). "*

De lo referido solicita:

> *"disponga que el Banco Pichincha me reverse (reintegre) el valor ilegalmente extraído de mi cuenta corriente y transferido seguramente a la cuenta de quien haciendo uso de medios ilícitos realizó esta "TRANSFERENCIA". Como el hecho es tan evidente, aspiro que la citada institución financiera, BANCO PICHINCHA, sea sancionada con todo el rigor de la Ley, pues no es justo que los usuarios de estas entidades, sigamos siendo objeto de varios tipos de delitos"*

Al respecto, cumplo en informar que su reclamo fue trasladado a la institución financiera con comunicaciones de 4 de julio de 2012, tanto al representante legal como a Auditoría Interna, en observancia a lo dispuesto en el artículo 76 de la Constitución de la República, en concordancia con el artículo 2, sección I, capítulo IV "Procedimiento para la atención de los reclamos contra las instituciones del sistema financiero", título XX, libro I, de la Codificación de Resoluciones de la Superintendencia de Bancos y

Seguros y de la Junta Bancaria; las mismas fueron contestadas por la entidad financiera el 7 y 28 de agosto de 2012 por las unidades antes referidas, de los cuales se desprende los siguientes aspectos relevantes que son motivo de análisis.

II. ANÁLISIS DE LA INFORMACIÓN

Del análisis realizado a la documentación que consta en el expediente, se desprende lo siguiente:

1. Conforme a la información reportada y registrada en el sistema del banco, la cuenta corriente No. 3214691104 fue aperturada a su nombre en la Agencia Amazonas el 22 de diciembre del 2004, y registra su nombre como único titular de la misma. En la cuenta corriente está ligada la tarjeta E-Key No. 654394.

2. En caso de que el ingreso a la banca electrónica no coincida con las características y patrones de comportamiento y entorno que se encuentran registrados en el sistema biométrico de la entidad, se procede a solicitar de manera aleatoria que responda una de sus preguntas secretas y que seleccione la figura secreta, datos que usted previamente registró.

3. Se evidencia que la transferencia reclamada, fue procesada en forma exitosa el día 18 de junio de 2012, con validación de códigos de la tarjeta de coordenadas E-Key No. 654394, por una valor de USD$ 4.898.39 y con débito a la cuenta corriente No. 3214691104, según el siguiente detalle:

Fecha y Hora	Valor	Cta. Origen	Cta. Destino	Beneficiario	No. IP. y ubicación
18/06/2012	4.898,39	3214691104	4820499200	Meza Castro Ricardo Rafael	190.118.173.217

   Conforme al movimiento de cuenta de la reclamante, se evidencia que de la cuenta de ahorros No. 4820499200 beneficiaria de la transferencia, que pertenece al señor Ricardo Rafael Meza Castro el dinero fue retirado el mismo día 18 de junio del 2012, a través de una transacción efectuada en ventanilla en la Agencia Reales Tamarindos por el valor de de USD 4.890,00.

   Al realizar transferencias electrónicas o pagos de cualquier índole vía internet, es necesario que el cliente active su tarjeta E-Key. El monto diario asignado y habilitado por parte de la entidad financiera para este tipo de servicio es de hasta US$ 5.000,00; el sistema le permite escoger la cuenta a la que desee ingresar el cupo por el cliente previamente definido dentro de los parámetros precitados.

4. Se reitera, que las transferencias por internet realizadas a través del canal de Banca Virtual para ser consideradas como "**exitosas**", se deben cumplir, las siguientes condiciones: 1) Ingresar el usuario y clave biométrica registrada por el cliente. 2) De ser el caso responder a la pregunta e imagen seleccionada, información que es de **exclusivo conocimiento del cliente** y constituye el único mecanismo para acceder a

los servicios ofrecidos por medios electrónicos. 3) Como medida complementaria de seguridad, la entidad financiera otorga a sus clientes que realizan transferencias por éste canal la tarjeta de coordenadas E-key que solicita el sistema para aceptar la transacción. 4) Finalmente el sistema dentro del procedimiento, en este tipo de transacciones le solicita el ingreso de un correo electrónico y número de celular, estos campos son obligatorios debido a que toda la información proporcionada por usted, permite notificar automáticamente a través de un mensaje SMS al número celular y dirección de e-mail las transferencias realizadas vía internet.

Según el Log de transacciones, se observa que previo a la transacción de la transferencia reclamada, se registra un ingreso a su cuenta, a las 12:45:44 del 18 de junio de 2012, bajo el concepto de "Activación de cuentas para transferencias", presumiblemente, en este momento se actualizaron sus datos, lo que explicaría el hecho de que no haya recibido notificación vía SMS o vía e-mail.

Es importante hacer referencia a la disposición reglamentaria vigente a esa fecha referida en el artículo 5, Sección 1, Capítulo III, Título XXV, Libro 1 de la Codificación de Resoluciones de la Superintendencia de Bancos y Seguros y de la Junta Bancaria, que establece lo siguiente:

> "*Los depósitos, retiros de fondos, créditos, débitos y cualquier otra transacción permitida en cuentas de depósitos monetarios, efectuados a través de medios electrónicos o electromecánicos, deberán estar sustentados por un acuerdo escrito entre el banco y el titular de la cuenta, en el que deberán constar, por lo menos, las siguientes condiciones:*
>
> *5.1 La responsabilidad exclusiva del cliente respecto de las transacciones que efectuare a través de estos medios; y,*
>
> *5.2* ***La responsabilidad del cliente de mantener en secreto la clave o seguridades a él asignadas, así como los cambios de claves que efectuaren. Igual responsabilidad tendrá con respecto a las claves o seguridades adicionales por él solicitadas y otorgadas por el banco.****"* (la negrilla es mía).

5. En la "Solicitud de Servicios Electrónicos" suscrita por usted, en el numeral 3 se establece:

"(...) En el caso de acceder a los servicios brindados a través de medios electrónicos, (Banca electrónica-internexo) deberé (emos) crear un usuario y clave biométricos, así como preguntas y figura secreta en el Sistema de Ingreso Biométrico, por lo que el prolijo cuidado que tenga(mos) con esta(s) tarjeta(s), clave(s) e información relacionada, constituye una obligación de mi(nuestra) parte y es de fundamental importancia para evitar actos dolosos en mi(nuestra) contra, que puedan causarme(nos) perjuicios especialmente por transacciones, transferencias, retiros operaciones, conocimiento de información y en general otros actos que pudieran efectuar personas inescrupulosas que lleguen a tener dicha información y/o

tarjetas por descuido mío(nuestro); el cuidado que debemos tener busca también proteger a la(s) institución(es) de actos dolosos, con mi(nuestra) responsabilidad de acuerdo con la ley. "

Por lo cual el uso y la debida custodia de su usuario, clave, figura y tarjeta de coordenadas es de su exclusividad responsabilidad.

6. El Banco Pichincha C.A. ha venido alertando públicamente por múltiples medios de comunicación entre estos la página web de acceso a la plataforma de servicios bancarios, que los clientes no entreguen nunca o faciliten sus datos personales, claves biométricas o coordenadas de tarjeta "E-key", por correo electrónico, mensajes de celular, sms, teléfono, página web u otros medios. Por lo cual se ha podido evidenciar el siguiente mensaje:

   "Banco Pichincha NO envía mails solicitando descarga de archivos"

   De igual manera, en el momento previo al ingreso a la banca electrónica se despliega la siguiente alerta:

   Concomitantemente con lo anteriormente expuesto y de acuerdo al contenido del análisis integral del presente caso, se presume que no se tomaron los debidos cuidados en las claves asignadas a usted, lo cual produjo que terceras personas accedieran por usted a este canal electrónico, incumpliendo de esta manera lo referido en el contrato de Servicios Electrónicos – Asignación de Tarjeta E-Key, suscrito por usted.

III. CONCLUSIÓN

Ante el análisis expuesto, se puede concluir lo siguiente:

- No se ha comprobado que en el presente caso exista responsabilidad del Banco Pichincha C.A. en la transferencia de dinero reclamada.

- La transferencia reclamada por usted, fue realizada con la utilización de las claves personales "E Key" y la serie de validaciones requeridas por la entidad financiera para el acceso al sistema de Banca Virtual, y autorizada ingresando los dígitos de la tarjeta de coordenadas en el momento de la transferencia, mismas que son únicas para cada cliente, y es su responsabilidad el custodiarla adecuadamente, conforme lo descrito en el numeral 5 del presente oficio.

- Banco de Pichincha C.A., cumplió con los procedimientos internos de servicios electrónicos en referencia a la validación y registro de la transferencia reclamada, la cual fue debidamente procesada y registrada, utilizando todos los controles implementados para el efecto.

- Banco Pichincha C.A., por motivos de seguridad **no registra en ningún archivo o medio, las claves o coordenadas de seguridad.**

- Se presume que usted fue víctima de un delito, tal y como se señala en su escrito de reclamo, sin embargo, esta Superintendencia de Bancos y Seguros no puede pronunciarse al respecto, al ser una competencia exclusiva del juez correspondiente determinar la existencia del mismo.

IV. RESOLUCIÓN

Por todo lo expuesto, participo a usted que de conformidad con el análisis y las conclusiones precitadas, no es posible atender su solicitud favorablemente ya que Banco Pichincha C.A., no ha vulnerado sus derechos financieros ni ha incumplido sus obligaciones de custodio de sus fondos.

Por los antecedentes ya indicados y en cumplimiento de la normativa legal vigente este despacho ha realizado el trámite correspondiente solicitado. En tal virtud, se concluye el presente caso.

Atentamente,

Ab. María Verónica Cevallos V.
SUBDIRECTORA DE ATENCION AL USUARIO

Quito D.M., 09 de Noviembre de 2012

Señor
WUELFOR ROBERTO JACOME CORAL
Huigra S14-28, Pasaje S14, Barrio Coop. IESS-FUT
Ciudad.-

De mi consideración:

Mediante resolución No. ADM-2012-10779, de 6 de febrero de 2012, se creó la Dirección Nacional de Atención y Educación al Usuario; y, con Resolución No. ADM-2012-11043, se emitió la Acción de Personal No.1309, de 17 de julio de 2012, en la que fui nombrada Subdirectora de Atención al Usuario, en tal virtud, avoco conocimiento del presente reclamo administrativo.

I. ANTECEDENTES

En atención a su comunicación recibida en este organismo de control el 22 de junio de 2012, mediante la cual presentó su reclamo en contra del Banco Pichincha C.A., en el que manifestaba:

> *"(...) El dá 24 de mayo deposite en mi cuenta de ahorros N.- 5936609100 del Banco del Pichincha la suma de 1500,00 dólares en efectivo, el día 25 de mayo fui a retirar dinero del cajero y mi sorpresa fue que me habían hecho 2 transferencias la una por 46 dólares, y la otra por el valor de 1498,45 transferencias que yo nunca la he realizado (...)"*

De lo referido solicitó:

> *"(...) ayuda en este caso ya que son mis ahorros y me he quedado sin nada viviendo de mi sueldo."*

En cumplimiento a lo dispuesto en el artículo 76 de la Constitución de la República del Ecuador y en concordancia con el artículo 2, sección I, capítulo IV, título XX, libro I, de la Codificación de Resoluciones de la Superintendencia de Bancos y Seguros y de la Junta Bancaria, la Directora Nacional de Atención y Educación al Usuario, dando trámite a su reclamo, requirió a la entidad financiera, la información necesaria para proceder con el análisis de la misma y emitir la resolución correspondiente.

II. ANÁLISIS DE LA INFORMACIÓN

Del análisis realizado a la documentación adjuntada en el reclamo y la remitida por la entidad financiera, se desprende lo siguiente:

1. La transferencia electrónica que usted reclama, se produjo mediante el canal de banca electrónica de la entidad financiera, el 24 de mayo de 2012 aproximadamente a las 13:56 por el valor de USD 1498.45 desde la cuenta corriente No. 5936623900, hacia la cuenta de ahorros No. 5168465000 del mismo banco, cuyo titular es el señor José Leonardo Procel Orellana, con la validación del usuario, clave biométrica y tarjeta de coordenadas No. 1498741, información que es de conocimiento exclusivo del titular de la cuenta.

2. En caso de que el ingreso a la banca electrónica no coincida con las características y patrones de comportamiento y entorno que se encuentran registrados en el sistema biométrico de la entidad, se procede a solicitar de manera aleatoria que responda una de sus preguntas secretas y que seleccione la figura secreta, datos que usted previamente registró.

3. Para que las transacciones realizadas a través del canal de banca electrónica sean consideradas como exitosas, se deben cumplir, las siguientes condiciones: 1) El ingreso del usuario creado por el cliente, 2) El ingreso de la clave personal de seguridad de 12 a 16 caracteres, con combinaciones entre letras y números, 3) Confirmar la transferencia interbancaria digitando el número de la tarjeta de coordenadas solicitado, dichas herramientas se encuentran bajo la custodia del titular de la cuenta.

De igual manera, es importante hacer referencia a la disposición reglamentaria vigente contenida en el Artículo 8, Sección II, Capítulo III, Título XXV, Libro I de la Codificación de Resoluciones de la Superintendencia de Bancos y Seguros y de la Junta Bancaria, que establece:

> "*Los depósitos, retiros de fondos, créditos, débitos y cualquier otra transacción permitida en cuentas de depósitos monetarios, efectuados a través de medios electrónicos o electromecánicos, deberán estar sustentados por un acuerdo escrito entre el banco y el titular de la cuenta, en el que deberán constar, por lo menos, las siguientes condiciones:*
>
> *8.1 La responsabilidad del cliente respecto de las transacciones que efectuare a través de estos medios; y,*
>
> *8.2 La responsabilidad del cliente de mantener en secreto la clave o seguridades a él asignadas, así como los cambios de claves que efectuaren. Igual responsabilidad tendrá con respecto a las claves o seguridades adicionales por él solicitadas y otorgadas por el banco."*

4. En la "Solicitud de Servicios Electrónicos" suscrita por usted y la entidad el 15 de junio de 2011, en el numeral 3 se establece:

"(...) En el caso de acceder a los servicios brindados a través de medios electrónicos, (Banca electrónica-internexo) deberé (emos) crear un usuario y clave biométricos, así como preguntas y figura secreta en el Sistema de Ingreso Biométrico, por lo que el prolijo cuidado que tenga(mos) con esta(s) tarjeta(s), clave(s) e información relacionada, constituye una obligación de mi(nuestra) parte y es de fundamental importancia para evitar actos dolosos en mi(nuestra) contra, que puedan causarme(nos) perjuicios especialmente por transacciones, transferencias, retiros operaciones, conocimiento de información y en general otros actos que pudieran efectuar personas inescrupulosas que lleguen a tener dicha información y/o tarjetas por descuido mío(nuestro); el cuidado que debemos tener busca también proteger a la(s) institución(es) de actos dolosos, con mi(nuestra) responsabilidad de acuerdo con la ley. "

Por lo cual el uso y la debida custodia de su usuario, clave, figura y tarjeta de coordenadas es de su exclusividad responsabilidad.

5. Se ha podido evidenciar que Banco del Pichincha C.A. a través de varios medios de comunicación como radio, prensa y televisión alerta a sus clientes sobre las seguridades que deben mantener al transaccionar en canales electrónicos, inclusive en su página web se aprecia el siguiente mensaje:

"Banco Pichincha NO envía mails solicitando descarga de archivos"

De igual manera, en el momento previo al ingreso a la banca electrónica se despliega la siguiente alerta:

III. CONCLUSIONES

Ante el análisis expuesto, se puede concluir que:

- No se ha comprobado que en el presente caso exista responsabilidad del Banco Pichincha C.A. en la transferencia de dinero reclamada.

- No se encontraron indicios ni pruebas que demuestren que en la transacción no reconocida, se produjeron omisiones de las responsabilidades de control y mitigación del riesgo operativo que la entidad financiera está obligada a cumplir; por lo cual no existen evidencias que permitan a esta Superintendencia imputar responsabilidades administrativas al banco.

- Se presume que usted fue víctima de los delitos contra la inviolabilidad del secreto y falsificación electrónica, tipificados en el Código Penal, por lo tanto, los mismos recaen en un ámbito fuera de la competencia de este organismo de control.

IV. RESOLUCIÓN

Por lo antes expuesto, y cumpliendo con el debido proceso consagrado en la Constitución de la República del Ecuador, participo a usted que de conformidad con el análisis y las conclusiones citadas, no es posible atender su solicitud favorablemente ya que no se ha comprobado que Banco Pichincha C.A. haya incumplido con las leyes, normativa, y procedimientos vigentes relacionados con éste caso.

De esta manera, el reclamo presentado por usted ha sido atendido, por lo cual se declara concluido el presente trámite administrativo.

Atentamente,

Ab. Ma. Verónica Cevallos V.
SUBDIRECTORA DE ATENCIÓN AL USUARIO

OFICIO No. DNAE-SAU-2012-6069
Quito D.M., 18 de Octubre de 2012

Señor
MANUEL FAUSTO ROLANDO REMACHE QUIZHPI, y/o
Abogada
BEATRIZ RIERA ULLOA
Cooperativa Santa Martha, Sector #3, Cl. Alfredo Pareja, Casa 407
Ciudad.-

De mi consideración:

Mediante resolución No. ADM-2012-10779, de 6 de febrero de 2012, se creó la Dirección Nacional de Atención y Educación al Usuario; y, con Resolución No. ADM-2012-11043, se emitió la Acción de Personal No.1309, de 17 de julio de 2012, en la que fui nombrada Subdirectora de Atención al Usuario, en tal virtud, avoco conocimiento del presente reclamo administrativo.

I. ANTECEDENTES

En atención a su comunicación recibida en este organismo de control el 23 de marzo de 2012, mediante la cual presentó su reclamo en contra del Banco Pichincha C.A., en el que manifestaba:

> *"(...) de mi cuenta fue transferido a otra cuenta y lo único que el Banco manifiesta es que para el día 26 marzo -2012 se sabrá que ha pasado; es decir no se tiene ningún apoyo, ni explicación (...) También quiero dejar constancia ante su autoridad que en el mes de julio del 2011 presenté un reclamo porque se me sustrajeron mi tarjeta de débito la misma que solicité al banco la anulación, lo único que hicieron es bloquearla por 24 horas activándole el fin de semana, donde fui estafado por un valor de $ 1600,00 (...)"*

De lo referido solicitó:

> *"que el Banco sea responsable y devuelva el valor que se transfirió sin autorización de 3.200,00 dólares americanos."*

En cumplimiento a lo dispuesto en el artículo 76 de la Constitución de la República del Ecuador y en concordancia con el artículo 2, sección I, capítulo IV, título XX, libro I, de la Codificación de Resoluciones de la Superintendencia de Bancos y Seguros y de la Junta Bancaria, la Directora Nacional de Atención y Educación al Usuario, dando trámite a su reclamo, requirió a la entidad financiera, la información necesaria para proceder con el análisis de la misma y emitir la resolución correspondiente.

II. ANÁLISIS DE LA INFORMACIÓN

Del análisis realizado a la documentación adjuntada en el reclamo y la remitida por la entidad financiera, se desprende lo siguiente:

1. La transferencia electrónica que usted reclama, se produjo mediante el canal de banca electrónica de la entidad financiera, el 01 de marzo de 2012 aproximadamente a las 11:32 por el valor de USD 3200.00 desde la cuenta corriente No. 3272161004, hacia la cuenta de ahorros No. 4208866900 del mismo banco, cuya titular es la señora Gladis Lelia Escobar Zapata, con la validación del usuario, clave biométrica y tarjeta de coordenadas No. 1497757, información que es de conocimiento exclusivo del titular de la cuenta.

2. En caso de que el ingreso a la banca electrónica no coincida con las características y patrones de comportamiento y entorno que se encuentran registrados en el sistema biométrico de la entidad, se procede a solicitar de manera aleatoria que responda una de sus preguntas secretas y que seleccione la figura secreta, datos que usted previamente registró.

3. Para que las transacciones realizadas a través del canal de banca electrónica sean consideradas como exitosas, se deben cumplir, las siguientes condiciones: 1) El ingreso del usuario creado por el cliente, 2) El ingreso de la clave personal de seguridad de 12 a 16 caracteres, con combinaciones entre letras y números, 3) Confirmar la transferencia interbancaria digitando el número de la tarjeta de coordenadas solicitado, dichas herramientas se encuentran bajo la custodia del titular de la cuenta.

De igual manera, es importante hacer referencia a la disposición reglamentaria vigente contenida en el Artículo 8, Sección II, Capítulo III, Título XXV, Libro I de la Codificación de Resoluciones de la Superintendencia de Bancos y Seguros y de la Junta Bancaria, que establece:

> "*Los depósitos, retiros de fondos, créditos, débitos y cualquier otra transacción permitida en cuentas de depósitos monetarios, efectuados a través de medios electrónicos o electromecánicos, deberán estar sustentados por un acuerdo escrito entre el banco y el titular de la cuenta, en el que deberán constar, por lo menos, las siguientes condiciones:*
>
> *8.1 La responsabilidad del cliente respecto de las transacciones que efectuare a través de estos medios; y,*
>
> *8.2 La responsabilidad del cliente de mantener en secreto la clave o seguridades a él asignadas, así como los cambios de claves que*

efectuaren. Igual responsabilidad tendrá con respecto a las claves o seguridades adicionales por él solicitadas y otorgadas por el banco."

4. En la "Solicitud de Servicios Electrónicos" suscrita por usted y la entidad, en el numeral 3 se establece:

> *"(...) En el caso de acceder a los servicios brindados a través de medios electrónicos, (Banca electrónica-internexo) deberé (emos) crear un usuario y clave biométricos, así como preguntas y figura secreta en el Sistema de Ingreso Biométrico, por lo que el prolijo cuidado que tenga(mos) con esta(s) tarjeta(s), clave(s) e información relacionada, constituye una obligación de mi(nuestra) parte y es de fundamental importancia para evitar actos dolosos en mi(nuestra) contra, que puedan causarme(nos) perjuicios especialmente por transacciones, transferencias, retiros operaciones, conocimiento de información y en general otros actos que pudieran efectuar personas inescrupulosas que lleguen a tener dicha información y/o tarjetas por descuido mío(nuestro); el cuidado que debemos tener busca también proteger a la(s) institución(es) de actos dolosos, con mi(nuestra) responsabilidad de acuerdo con la ley. "*

Por lo cual el uso y la debida custodia de su usuario, clave, figura y tarjeta de coordenadas es de su exclusividad responsabilidad.

5. Se ha podido evidenciar que Banco del Pichincha C.A. a través de varios medios de comunicación como radio, prensa y televisión alerta a sus clientes sobre las seguridades que deben mantener al transaccionar en canales electrónicos, inclusive en su página web se aprecia el siguiente mensaje:

> *"Banco Pichincha NO envía mails solicitando descarga de archivos"*

De igual manera, en el momento previo al ingreso a la banca electrónica se despliega la siguiente alerta:

III. CONCLUSIONES

Ante el análisis expuesto, se puede concluir que:

- No se ha comprobado que en el presente caso exista responsabilidad del Banco Pichincha C.A. en la transferencia de dinero reclamada.

- No se encontraron indicios ni pruebas que demuestren que en la transacción no reconocida, se produjeron omisiones de las responsabilidades de control y mitigación del riesgo operativo que la entidad financiera está obligada a cumplir; por lo cual no existen evidencias que permitan a esta Superintendencia imputar responsabilidades administrativas al banco.

- Se presume que usted fue víctima de un delito de falsificación electrónica, tipificado en el Código Penal, por lo tanto, recae en un ámbito fuera de la competencia de este organismo de control.

IV. RESOLUCIÓN

Por lo antes expuesto, y cumpliendo con el debido proceso consagrado en la Constitución de la República del Ecuador, participo a usted que de conformidad con el análisis y las conclusiones citadas, no es posible atender su solicitud favorablemente ya que no se ha comprobado que Banco Pichincha C.A. haya incumplido con las leyes, normativa, y procedimientos vigentes relacionados con éste caso.
De esta manera, el reclamo presentado por usted ha sido atendido, por lo cual se declara concluido el presente trámite administrativo.

Atentamente,

Ab. Ma. Verónica Cevallos V.
SUBDIRECTORA DE ATENCIÓN AL USUARIO

OFICIO No. DNAE-SAU-2012-7217
Quito D.M., 27 de noviembre de 2012
Señor
JOSÉ SANTOS CUYO MAIGUA
Casillero Judicial No. 4938, Palacio de Justicia
Quito.-

De mi consideración:

I. ANTECEDENTES

Me refiero a su comunicación ingresada en este organismo de control el 21 de septiembre de 2012, mediante la cual presentó un reclamo administrativo en contra de Banco Pichincha C.A., manifestando lo siguiente:

> *"(...) El día de 18 de mayo de 2012, a eso de las 16h00, me disponía a realizar un retiro del cajero automático del Banco Pichincha ubicado en la Plaza Granda de esta ciudad de Quito, de mi cuenta de ahorros número 3026630300, encontrándome con la novedad que no disponía de fondos en mi cuenta, más que un saldo de $5 usd, por lo que ingresé a un internet y verifiqué mi saldo, desprendiéndose que a las 12h14pm, habían realizado una transferencia bancaria a la Agencia Norte, retirando de mi cuenta el valor de CUATRO MIL CIENTO OCHENTA Y SEIS CON SETENTA Y DOS CENTAVOS DÓLARES AMERICANOS ($ 4186,72 USD)*

De lo referido solicita:

> *"...La devolución de mi dinero hurtado fraudulentamente..."*

Al respecto, cumplo en informar que su reclamo fue trasladado a la institución financiera con comunicaciones de 2 de octubre de 2012, tanto al representante legal como a Auditoría Interna, en observancia a lo dispuesto en el artículo 76 de la Constitución de la República, en concordancia con el artículo 2, sección I, capítulo IV "Procedimiento para la atención de los reclamos contra las instituciones del sistema financiero", título XX, libro I, de la Codificación de Resoluciones de la Superintendencia de Bancos y Seguros y de la Junta Bancaria; las mismas fueron contestadas por la entidad financiera el 24 de octubre de 2012 por las unidades antes referidas, de los cuales se desprende los siguientes aspectos relevantes que son motivo de análisis.

II. ANÁLISIS DE LA INFORMACIÓN

Del análisis realizado a la documentación que consta en el expediente, se desprende lo siguiente:

1. Conforme a la información reportada y registrada en el sistema del banco, la cuenta de ahorros No. 3026630300, fue aperturada a su nombre en la Agencia Amazonas el 9 de diciembre del 2003.

2. La transacción objeto de reclamo, se realizó mediante el canal internexo con la Cédula de Ciudadanía No. 0502023708, perteneciente al señor José Santos Cuyo Maigua, con el siguiente detalle:

Fecha y Hora	Valor	Cta. Origen	Cta. Destino	Beneficiario	No. IP. y ubicación
2012/05/18	4.186,67	3026630300	6326391000	Rosado Chilán Pedro Pablo	201.240.96.58

Conforme al movimiento de cuenta de la reclamante, se evidencia que de la cuenta de ahorros No. 6326391000 beneficiaria de la transferencia, que pertenece al señor Pedro Pablo Rosado Chilán, realiza un retiro por ventanilla por un valor total de 4,186.67 USD.

Así mismo en relación a lo descrito, la Unidad de Análisis de Riesgos Físicos manifiesta lo siguiente:

La institución financiera ha certificado que el monto máximo asignado para realizar transferencias a través de canal internexo está definido en USD 5.000,00, y que sin embargo primero se debe habilitar la cuenta con un monto igual o menor al valor indicado, por lo que el cliente define su propio monto de dinero habilitado para la realización de transferencias.

3. Se ha remitido el log de transacciones realizadas a través del canal internexo de la Cédula de Ciudadanía No. 0502023708 perteneciente al señor Cuyo Maigua, del cual se desprende lo siguiente:

   - El día 18 de mayo de 2012 se realiza un acceso desde la dirección IP 201.240.96.58 para la activación de la cuenta No. 3026630300, para transferencias por un valor de USD 5.000,00
   - A continuación, se realiza una transferencia por un valor total de USD 4,186.67 a la cuenta No. 6326391000 a las 12:37.

4. Se reitera, que las transferencias por internet realizadas a través del canal de Banca Virtual para ser consideradas como "**exitosas**", se deben cumplir, las siguientes condiciones: 1) Ingresar el usuario y clave biométrica registrada por el cliente. 2) De ser el caso responder a la pregunta e imagen seleccionada, información que es de **exclusivo conocimiento del cliente** y constituye el único mecanismo para acceder a los servicios ofrecidos por medios electrónicos. 3) Como medida complementaria de seguridad, la entidad financiera otorga a sus clientes que realizan transferencias por éste canal la tarjeta de coordenadas E-key, que en el presente caso es la No. 1248093, perteneciente al señor Cuyo Maigua, que solicita el sistema para aceptar la transacción. 4) Finalmente el sistema dentro del procedimiento, en este tipo de transacciones le solicita el ingreso de un correo electrónico y número de celular, estos campos son obligatorios debido a que toda la información proporcionada por usted, permite

notificar automáticamente a través de un mensaje SMS al número celular y dirección de e-mail las transferencias realizadas vía internet.

Es importante hacer referencia a la disposición reglamentaria vigente a esa fecha referida en el artículo 5, Sección 1, Capítulo III, Título XXV, Libro 1 de la Codificación de Resoluciones de la Superintendencia de Bancos y Seguros y de la Junta Bancaria, que establece lo siguiente:

"*Los depósitos, retiros de fondos, créditos, débitos y cualquier otra transacción permitida en cuentas de depósitos monetarios, efectuados a través de medios electrónicos o electromecánicos, deberán estar sustentados por un acuerdo escrito entre el banco y el titular de la cuenta, en el que deberán constar, por lo menos, las siguientes condiciones:*

5.1 La responsabilidad exclusiva del cliente respecto de las transacciones que efectuare a través de estos medios; y,

5.2 ***La responsabilidad del cliente de mantener en secreto la clave o seguridades a él asignadas, así como los cambios de claves que efectuaren. Igual responsabilidad tendrá con respecto a las claves o seguridades adicionales por él solicitadas y otorgadas por el banco.***" (la negrilla es mía).

5. En la "Solicitud de Servicios Electrónicos" suscrita por usted, en el numeral 3 se establece:

"(...) En el caso de acceder a los servicios brindados a través de medios electrónicos, (Banca electrónica-internexo) deberé (emos) crear un usuario y clave biométricos, así como preguntas y figura secreta en el Sistema de Ingreso Biométrico, por lo que el prolijo cuidado que tenga(mos) con esta(s) tarjeta(s), clave(s) e información relacionada, constituye una obligación de mi(nuestra) parte y es de fundamental importancia para evitar actos dolosos en mi(nuestra) contra, que puedan causarme(nos) perjuicios especialmente por transacciones, transferencias, retiros operaciones, conocimiento de información y en general otros actos que pudieran efectuar personas inescrupulosas que lleguen a tener dicha información y/o tarjetas por descuido mío(nuestro); el cuidado que debemos tener busca también proteger a la(s) institución(es) de actos dolosos, con mi(nuestra) responsabilidad de acuerdo con la ley. "

Por lo cual el uso y la debida custodia de su usuario, clave, figura y tarjeta de coordenadas es de su exclusividad responsabilidad.

6. El Banco Pichincha C.A. ha venido alertando públicamente por múltiples medios de comunicación entre estos la página web de acceso a la plataforma de servicios bancarios, que los clientes no entreguen nunca o faciliten sus datos personales, claves biométricas o coordenadas de tarjeta "E-key", por correo

electrónico, mensajes de celular, sms, teléfono, página web u otros medios. Por lo cual se ha podido evidenciar el siguiente mensaje:

"Banco Pichincha NO envía mails solicitando descarga de archivos"

De igual manera, en el momento previo al ingreso a la banca electrónica se despliega la siguiente alerta:

Concomitantemente con lo anteriormente expuesto y de acuerdo al contenido del análisis integral del presente caso, se presume que no se tomaron los debidos cuidados en las claves asignadas a usted, lo cual produjo que terceras personas accedieran por usted a este canal electrónico, incumpliendo de esta manera lo referido en el contrato de Servicios Electrónicos – Asignación de Tarjeta E-Key, suscrito por usted.

III. CONCLUSIÓN

Ante el análisis expuesto, se puede concluir lo siguiente:

- No se ha comprobado que en el presente caso exista responsabilidad del Banco Pichincha C.A. en la transferencia de dinero reclamada.

- La transferencia reclamada por usted, fue realizada con la utilización de las claves personales "E Key" y la serie de validaciones requeridas por la entidad financiera para el acceso al sistema de Banca Virtual, y autorizada ingresando los dígitos de la tarjeta de coordenadas en el momento de la transferencia, mismas que son únicas para cada cliente, y es su responsabilidad el custodiarla adecuadamente, conforme lo descrito en el numeral 5 del presente oficio.

- Banco de Pichincha C.A., cumplió con los procedimientos internos de servicios electrónicos en referencia a la validación y registro de la transferencia reclamada, la cual fue debidamente procesada y registrada, utilizando todos los controles implementados para el efecto.

- Banco Pichincha C.A., por motivos de seguridad **no registra en ningún archivo o medio, las claves o coordenadas de seguridad.**

- Se presume que usted fue víctima de un delito, tal y como se señala en su escrito de reclamo, sin embargo, esta Superintendencia de Bancos y Seguros no puede pronunciarse al respecto, al ser una competencia exclusiva del juez correspondiente determinar la existencia del mismo.

IV. RESOLUCIÓN

Por todo lo expuesto, participo a usted que de conformidad con el análisis y las conclusiones precitadas, no es posible atender su solicitud favorablemente ya que Banco Pichincha C.A., no ha vulnerado sus derechos financieros ni ha incumplido sus obligaciones de custodio de sus fondos.

Por los antecedentes ya indicados y en cumplimiento de la normativa legal vigente este despacho ha realizado el trámite correspondiente solicitado. En tal virtud, se concluye el presente caso.

Atentamente,

Ab. Ma. Verónica Cevallos
SUBDIRECTORA DE ATENCIÓN AL USUARIO

OFICIO No. DNAE-SAU-2012-7310

Quito D.M., 28 de noviembre de 2012

Señor
LEONARDO XAVIER MORILLO GARCÉS
Rafael León Larrea N24-78 y Vizcaya
Floresta – Mariscal Sucre
Quito.-

De mi consideración:

I. ANTECEDENTES

Me refiero a su comunicación ingresada en este organismo de control el 17 de agosto de 2012, mediante la cual presentó un reclamo administrativo en contra de Banco Pichincha C.A., manifestando lo siguiente:

> *"(...) El siguiente día (jueves) a las tres de la madrugada recibo un mensaje de texto por el celular "Ha realizado un intento de ingreso a banca electrónica" por sorpresa no sé que es lo que está pasando, desde esa hora hasta las siete de la mañana recibí cinco mensajes de intento de ingreso a la banca electrónica y finalmente a las diez horas con quince minutos del mismo día recibo un mensaje de texto. "Ha realizado una transacción exitosa de $4,995,23 (...)."*

De lo referido solicita:

> *"(...) La devolución de mi dinero, porque no es justo y no está apegado a la verdad (...)"*

Al respecto, cumplo en informar que su reclamo fue trasladado a la institución financiera con comunicación de 7 de septiembre del 2012, en observancia a lo dispuesto en el artículo 76 de la Constitución de la República, en concordancia con el artículo 2, sección I, capítulo IV "Procedimiento para la atención de los reclamos contra las instituciones del sistema financiero", título XX, libro I, de la Codificación de Resoluciones de la Superintendencia de Bancos y Seguros y de la Junta Bancaria; el requerimiento realizado fue contestado por la entidad financiera el 24 de octubre de 2012 y del cual me permito destacar lo siguiente:

II. ANÁLISIS DE LA INFORMACIÓN

Del análisis realizado a la documentación que consta en el expediente, se desprende lo siguiente:

1. Conforme a la información reportada y registrada en el sistema del banco, la cuenta de ahorros No. 4876456100, fue aperturada a su nombre en la Agencia Amazonas el 6 de junio del 2001.

2. La transacción objeto de reclamo, se realizó de la cuenta No. 4876456100, aperturada a nombre de Leonardo Xavier Morillo Garcés, desde la dirección IP. 200.25.222.23, con el siguiente detalle:

Fecha y Hora	Valor	Cta. Origen	Cta. Destino	Beneficiario	No. IP. y ubicación
2012/06/21	4.995,23	4876456100	4640623100	Chiriguaya Eslao Gregorio-Isido	200.25.222.23

Conforme al movimiento de cuenta de la reclamante, se evidencia que la cuenta de ahorros No. 4640623100 beneficiaria de la transferencia pertenece al señor Pedro Pablo Rosado Chilán.

La institución financiera ha certificado que el monto diario habilitado para este tipo de servicios está definido en USD 5.000,00, y que sin embargo el sistema permite al usuario titular de la(s) cuenta(s), registrar el monto por hasta USD 5,000.00 y escoger la cuenta a la que desee ingresar el cupo por el cliente definido.

3. Se ha remitido el log de transacciones realizadas con la tarjeta E-Key, efectuadas en la cuenta de ahorros No. 4876456100, durante el período comprendido entre el 21 de diciembre del 2011 hasta el 07 de septiembre del 2012; de dicho log, se evidencian las notificaciones respectivas sobre las transacciones reclamadas.

4. Se reitera, que las transferencias por internet realizadas a través del canal de Banca Virtual para ser consideradas como "**exitosas**", se deben cumplir, las siguientes condiciones: 1) Ingresar el usuario y clave biométrica registrada por el cliente. 2) De ser el caso responder a la pregunta e imagen seleccionada, información que es de **exclusivo conocimiento del cliente** y constituye el único mecanismo para acceder a los servicios ofrecidos por medios electrónicos. 3) Como medida complementaria de seguridad, la entidad financiera otorga a sus clientes que realizan transferencias por éste canal la tarjeta de coordenadas E-key, que solicita el sistema para aceptar la transacción. 4) Finalmente el sistema dentro del procedimiento, en este tipo de transacciones le solicita el ingreso de un correo electrónico y número de celular, estos campos son obligatorios debido a que toda la información proporcionada por usted, permite notificar automáticamente a través de un mensaje SMS al número celular y dirección de e-mail las transferencias realizadas vía internet.

Al respecto, y remitiéndonos al texto de su comunicación, usted claramente indica que recibió varios mensajes de texto, en este caso como alerta de que se había intentado ingresar a "banca electrónica" previo a la realización de la transacción

reclamada, por lo cual, si usted tuvo conocimiento de estos "intentos" debió haber comunicado el particular inmediatamente a la institución financiera, para evitar el perjuicio posterior causado.

Es importante hacer referencia a la disposición reglamentaria vigente a esa fecha referida en el artículo 5, Sección 1, Capítulo III, Título XXV, Libro 1 de la Codificación de Resoluciones de la Superintendencia de Bancos y Seguros y de la Junta Bancaria, que establece lo siguiente:

> "*Los depósitos, retiros de fondos, créditos, débitos y cualquier otra transacción permitida en cuentas de depósitos monetarios, efectuados a través de medios electrónicos o electromecánicos, deberán estar sustentados por un acuerdo escrito entre el banco y el titular de la cuenta, en el que deberán constar, por lo menos, las siguientes condiciones:*
>
> *5.1 La responsabilidad exclusiva del cliente respecto de las transacciones que efectuare a través de estos medios; y,*
>
> *5.2* ***La responsabilidad del cliente de mantener en secreto la clave o seguridades a él asignadas, así como los cambios de claves que efectuaren. Igual responsabilidad tendrá con respecto a las claves o seguridades adicionales por él solicitadas y otorgadas por el banco.****"* (la negrilla es mía).

5. En la "Solicitud de Servicios Electrónicos" suscrita por usted, en el numeral 3 se establece:

"(...) En el caso de acceder a los servicios brindados a través de medios electrónicos, (Banca electrónica-internexo) deberé (emos) crear un usuario y clave biométricos, así como preguntas y figura secreta en el Sistema de Ingreso Biométrico, por lo que el prolijo cuidado que tenga(mos) con esta(s) tarjeta(s), clave(s) e información relacionada, constituye una obligación de mi(nuestra) parte y es de fundamental importancia para evitar actos dolosos en mi(nuestra) contra, que puedan causarme(nos) perjuicios especialmente por transacciones, transferencias, retiros operaciones, conocimiento de información y en general otros actos que pudieran efectuar personas inescrupulosas que lleguen a tener dicha información y/o tarjetas por descuido mío(nuestro); el cuidado que debemos tener busca también proteger a la(s) institución(es) de actos dolosos, con mi(nuestra) responsabilidad de acuerdo con la ley. "

Por lo cual el uso y la debida custodia de su usuario, clave, figura y tarjeta de coordenadas es de su exclusividad responsabilidad.

6. El Banco Pichincha C.A. ha venido alertando públicamente por múltiples medios de comunicación entre estos la página web de acceso a la plataforma de servicios bancarios, que los clientes no entreguen nunca o faciliten sus datos personales, claves biométricas o coordenadas de tarjeta "E-key", por correo

electrónico, mensajes de celular, sms, teléfono, página web u otros medios. Por lo cual se ha podido evidenciar el siguiente mensaje:

"Banco Pichincha NO envía mails solicitando descarga de archivos"

Concomitantemente con lo anteriormente expuesto y de acuerdo al contenido del análisis integral del presente caso, se presume que no se tomaron los debidos cuidados en las claves asignadas a usted, lo cual produjo que terceras personas accedieran por usted a este canal electrónico, incumpliendo de esta manera lo referido en el contrato de Servicios Electrónicos – Asignación de Tarjeta E-Key, suscrito por usted.

III. CONCLUSIÓN

Ante el análisis expuesto, se puede concluir lo siguiente:

- No se ha comprobado que en el presente caso exista responsabilidad del Banco Pichincha C.A. en la transferencia de dinero reclamada.

- La transferencia reclamada por usted, fue realizada con la utilización de las claves personales "E Key" y la serie de validaciones requeridas por la entidad financiera para el acceso al sistema de Banca Virtual, y autorizada ingresando los dígitos de la tarjeta de coordenadas en el momento de la transferencia, mismas que son únicas para cada cliente, y es su responsabilidad el custodiarla adecuadamente, conforme lo descrito en el numeral 5 del presente oficio.

- Banco de Pichincha C.A., cumplió con los procedimientos internos de servicios electrónicos en referencia a la validación y registro de la transferencia reclamada, la cual fue debidamente procesada y registrada, utilizando todos los controles implementados para el efecto.

- Banco Pichincha C.A., por motivos de seguridad **no registra en ningún archivo o medio, las claves o coordenadas de seguridad.**

- Se presume que usted fue víctima de un delito, tal y como se señala en su escrito de reclamo, sin embargo, esta Superintendencia de Bancos y Seguros no puede pronunciarse al respecto, al ser una competencia exclusiva del juez correspondiente determinar la existencia del mismo.

IV. RESOLUCIÓN

Por todo lo expuesto, participo a usted que de conformidad con el análisis y las conclusiones precitadas, no es posible atender su solicitud favorablemente ya que Banco Pichincha C.A., no ha vulnerado sus derechos financieros ni ha incumplido sus obligaciones de custodio de sus fondos.

Por los antecedentes ya indicados y en cumplimiento de la normativa legal vigente este despacho ha realizado el trámite correspondiente solicitado. En tal virtud, se concluye el presente caso.

Atentamente,

Ab. Diego F. Villavicencio G.
SUBDIRECTOR DE ATENCIÓN AL USUARIO, SUBROGANTE

OFICIO No. DNAE-SAU-2012-6238

Quito D.M., 24 de octubre del 2012
Señora
MARÍA SOLEDAD CHÁVEZ CHACÁN
Calle Museo Solar S/N
Conjunto Marifer 2, Casa 26 San Antonio de Pichincha
Ciudad.-

De mi consideración:

I. Antecedentes

Me refiero a su comunicación presentada ante este organismo de control el 19 de marzo del 2012, en la cual manifestaba lo siguiente:

> *"(...)denuncio al Banco del Pichincha por robo, ya que de mi cuenta corriente No. 3010476904 se efectuó una transferencia no autorizada por un valor de $1622USD(mil seiscientos veinte dos) dólares el 15 de julio del 2012 (...)".*

De lo referido, solicita:

> *"(...) me ayuden con este caso y me sea devuelto el dinero robado de mi cuenta por parte del Banco Pichincha (...)".*

II. Acciones emprendidas por la Superintendencia de Bancos y Seguros

Al respecto, cumplo en informar a usted que su reclamo fue trasladado a la institución financiera BANCO PICHINCHA C.A. mediante oficio de 14 de septiembre del 2012, en cumplimiento a lo dispuesto en el artículo 76, de la Constitución de la República, en concordancia con la sección I, capítulo IV "PROCEDIMIENTO PARA LA ATENCIÓN DE LOS RECLAMOS CONTRA LAS INSTITUCIONES DEL SISTEMA FINANCIERO", título XX, libro I, de la Codificación de Resoluciones de la Superintendencia de Bancos y Seguros y de la Junta Bancaria; el mismo que fue contestado por la entidad con oficio de 08 de octubre del 2012, de las cuales se desprenden los siguientes aspectos relevantes que son motivo de análisis:

III. Análisis De La Información

1.- El Banco Pichincha C.A. remitió la documentación requerida sobre el reclamo formulado por usted, en lo pertinente a la respuesta otorgada, manifiesta que:

"(...)Conforme la información reportada en nuestro sistema, la cuenta corriente No. 3105020604 fue aperturada en la Agencia Alameda,el 03 de mayo del 2001 y registra como titular a la señora María Soledad Chavez Chacán.

Según la herramienta de reclamos del Banco, con fecha 16 de julio del 2012, la señora María Chávez, en la Agencia Eloy Alfaro, presentó un reclamo por transferencias a través de internet realizada desde su cuenta corriente por USD 1,622.

Luego de la revisión y de acuerdo con los procedimientos internos para atención de reclamos, se determinó que el caso no procede por cuanto la transferencia fue ejecutada cumpliendo con los requisitos indispensables que se requieren para acceder al canal electrónico internet y procesar este tipo de transacciones, como son: usuario y clave biométrica ;y, adicionalmente, las coordenadas de una tarjeta E-key cuyo cuidado y custodia es responsabilidad única del cliente.

Al validar los archivos proporcionados por el área de tecnología, se observa que el 16 de julio del 2012, se realizó la transferencia a través del canal electrónico internet, desde la cuenta corriente No. 3010476904 de propiedad de la reclamante, por el valor de USD 1,622 con destino a la cuenta de ahorros No. 4114606400 del Banco Pichincha y que de acuerdo con la información del sistema, pertenece al señor Wilson Oswaldo Correa Rueda. Esta transferencia se realizó desde la dirección IP, 199.192.206.212.

Según se observa en los movimientos de la cuenta de ahorros No. 4114606400, beneficiaria de la transferencia, el dinero fue retirado el mismo día 16 de julio del 2012, a través de un retiro de USD 1,400 realizado por ventanilla en la Agencia Huaquillas y un retiro de USD 200 a través de cajero automático realizado en la misma agencia.

De acuerdo con la investigación realizada por el Banco, no se ha logrado ubicar al señor Wilson Correa. Actualmente la cuenta de ahorros se encuentra cancelada.

De acuerdo al reporte del área de sistemas, señalamos que dicha transferencia fue procesada con la información y coordenadas de la tarjeta E-Key No. 1188974 correspondiente a la señora María Chavez. Debemos mencionar que para acceder al canal electrónico internet, es necesario el ingreso de un usuario y clave biométrica y que el cliente disponga de una tarjeta E-key para procesar las transferencias, en el presente caso, la tarjeta E-key, por solicitud de la reclamante, fue cancelada el 16 de julio del 2012, posterior a la realización de la transferencia objeto del presente reclamo.

Es importante, explicar que el Banco por motivos de seguridad no registra en ningún archivo o medio, las claves o coordenadas de la tarjeta E-key (...)".

2.- Del Contrato de Servicios Electrónicos (personas naturales) se desprende que en su numeral 3 dice lo siguiente:

> *"Conozco(cemos) y acepto(amos) que la(s) clave(s) de la (s) mencionada(s) tarjeta(s) y/o, clave(s) asignada(s), con el número de cédula de ciudadanía/ identidad/ pasaporte extranjero, según el caso, constituyen la información necesaria para acceder a los servicios brindados a través de medios electromecánicos o telefónicos, que solicito(mos). En el caso de acceder a los servicios brindados a través de medios electrónicos, (Banca electrónica-*

Internexo), deberé (emos) crear un usuario y clave confidencial biométricos, así como preguntas y figura secreta en el Sistema de Ingreso Biométrico, ***por lo que el prolijo cuidado que tenga(mos) con esta(s) tarjeta(s), clave(s) e información relacionada, constituye una obligación de mi (nuestra) parte y es de fundamental importancia para evitar actos dolosos en mi (nuestra)contra, que puedan causarme(nos)perjuicios especialmente por transacciones, transferencias, retiros, operaciones, conocimiento de información y en general otros actos que pudieran efectuar personas inescrupulosas que lleguen a tener dicha información y/o tarjetas por descuido mío (nuestro); el cuidado que debe(mos) tener busca también proteger a la(s) institución(es), por mi (nuestra) cuenta, responsabilidad y riesgo, a brindarme(nos) los servicios electrónicos a los que se pueda acceder con la(s) tarjeta(s) y/o clave(s) y/o registros biométricos e información relacionada, y los que llegue a brindar en el futuro, consintiendo yo(nosotros), expresamente, que la(s) institución (es), no deben para ello efectuar ninguna verificación sobre las órdenes electrónicas que se realicen con la información que me(nos) corresponde; ni deben, según su criterio, exigir ninguna nueva autorización, pedido, instrucción, firma, ni documento adicional de ninguna clase de mi(nuestra) parte, para brindar los servicios electrónicos que sean solicitados por cualquiera de los mecanismos a mi(nuestra) disposición. Notificaré(mos) expresa y físicamente por escrito a la(s) respectiva(s) institución(es), si eventualmente deseara(mos) excluir alguno de los servicios electrónicos, de manera que no me(nos)sea brindado.***

Su numeral 4 dice lo siguiente:

> *"****Una vez realizadas las transacciones u operaciones solicitadas, y realizados los débito que correspondan de mis (nuestras) cuentas, valores, inversiones y/o derechos de cualquier tipo, se entenderán hechas por mi (nuestra) expresa instrucción y consentimiento"****.*

Su numeral 10 dice lo siguiente:

> ***"En caso de pérdida, destrucción o sustracción de la (s) tarjeta (s); o, en caso de que terceras personas no autorizadas hayan obtenido la citada información o clave(s), me(nos) obligo(mos) a comunicar a la Institución respectiva inmediatamente del suceso. Acepto expresamente que dicha(s) Institución(es) no será(n) responsable(s) de ninguna transacción u operación realizada dentro de las 48 horas posteriores a la fecha en que comunique(mos) el suceso, mediante documento escrito en que deberá constar la recepción de la(s) respectiva(s) institución(es), o mediante comunicación electrónica, debidamente recibida por la(s) Institución(es), según las respectivas políticas y procedimientos"***

Toda vez que los contratos suscritos de cuenta corriente y de Servicios Electrónicos (personas naturales) ambos son ley para las partes, tanto así el compromiso adquirido en cuanto a las transacciones efectuadas, que son obligaciones contractuales y mantienen concordancia con las condiciones pactadas.

4.- El artículo 5, capítulo III, título XXV "Disposiciones Generales", libro I "Normas generales para la aplicación de la Ley General de Instituciones del Sistema Financiero" de la Codificación de Resoluciones de la Superintendencia de Bancos y Seguros y de la Junta Bancaria, vigente al momento del evento, señala:

> *"Artículo 5.- Los depósitos, retiros de fondos, créditos, débitos y cualquier otra transacción permitida en cuentas de depósitos monetarios, efectuados a través de medios electrónicos o electromecánicos, deberán estar sustentados por un acuerdo escrito entre el banco y el titular de la cuenta, en el que deberán constar, por lo menos, las siguientes condiciones:5.1 La responsabilidad exclusiva del cliente respecto de las transacciones que efectuare a través de estos medios; y, 5.2 La responsabilidad del cliente de mantener en secreto la clave o seguridades a él asignadas, así como los cambios de claves que se efectuaren. Igual responsabilidad tendrá con respecto a las claves o seguridades adicionales por él solicitadas y otorgadas por el banco"*

5.- En virtud de lo manifestado, se ha evidenciado documentadamente que el asunto específico que motiva el reclamo se enmarca en un caso característico de delincuencia común en el ámbito informático, llamado ***"Phishing"***, por lo tanto la Superintendencia de Bancos y Seguros carece de competencia para juzgar y determinar el supuesto ilícito y menos para establecer responsabilidades sobre tales hechos.

El **"Phishing" es cuando l**os delincuentes obtienen información confidencial a través de un correo electrónico en el que engañan al usuario haciéndole creer que debe enviar sus claves o datos para confirmación o actualización de datos.

Otra forma es suplantar la página web de la institución financiera, es decir, colocar otra página en su lugar, que se ve muy parecida.

Los fraudes más conocidos son:

1. Fraudes relacionados con las claves de banca electrónica de los usuarios. Con estas claves, los delincuentes realizan transferencias de cuentas de clientes hacia otras personas y luego realizan retiros en efectivo.

2. Ofertas en página web de productos o servicios que no existen

3. Suplantación de identidad, es decir que los delincuentes abren cuentas o realizan transacciones a nombre de las personas a las que les han robado su cédula o pasaporte.

6.- El Artículo 8, Sección II, Capítulo III, Título XXV, Libro 1 de la Codificación de Resoluciones de la Superintendencia de Bancos y Seguros y de la Junta Bancaria, que señala lo siguiente:

> ***"8.2 La responsabilidad del cliente de mantener en secreto la clave o seguridades a él asignadas, así como los cambios de claves que efectuaren. Igual responsabilidad tendrá con respecto a las claves o seguridades adicionales por él solicitadas y otorgadas por el banco."*** (la negrilla me corresponde).

Como es de su conocimiento. Dentro de los procedimientos de la entidad financiera para el proceso de transferencias por internet, es necesario ingresar al usuario biométrico y clave biométrica por usted generados, además, de ser el caso responder a la pregunta e imagen seleccionada, información que es de exclusivo conocimiento del cliente y constituye el único mecanismo para acceder a los servicios ofrecidos por medios electrónicos.

Además, se evidencia por parte del Banco Pichincha C.A. la implementación de la tarjeta de carácter personal e intransferible denominada "E-key", en la cual se registra la coordenada solicitada por el sistema para aceptar la transacción, siendo igualmente de responsabilidad exclusiva del cliente mantener en secreto las coordenadas constantes en su tarjeta "E-key", bajo su más estricta custodia.

IV. Conclusiones y Resolución.

Ante el análisis expuesto, se puede concluir lo siguiente:

- No existen evidencias que permitan determinar que las transacciones efectuadas en internet no fueron hechas por usted, ya que del monitoreo de las referidas transacciones estas son realizadas por el titular de la cuenta, no obstante de ello, en el momento que el cliente solicita el usuario la clave biométrica el sistema requiere el ingreso de un correo electrónico y número celular, estos campos son obligatorios debido que la información proporcionada, se encuentra bajo su custodia, permite notificar automáticamente a través de un SMS al número celular y dirección de e-mail las transferencias realizadas vía internet.

- No se encontraron evidencias ni pruebas que demuestren que se haya cometido alguna omisión en el procedimiento de las operaciones sobre las transacciones reclamadas; por lo cual no existen pruebas que permitan a esta Superintendencia, imputar responsabilidades administrativas a la entidad financiera.

- En el presente reclamo, este organismo de control no puede atender su solicitud favorablemente ya que no se ha evidenciado que BANCO PICHINCHA C.A. haya vulnerado sus derechos financieros o haya incumplido normativas, procesos y procedimientos internos y externos.

En el presente reclamo, este organismo de control no puede atender su solicitud favorablemente motivo por el cual se declara concluido el presente reclamo.

Atentamente,

Ab. Ma. Verónica Cevallos V.
SUBDIRECTORA NACIONAL
DE ATENCIÓN AL USUARIO

OFICIO No DNAE-SAU-2012- 05421

Quito D.M., 19 de septiembre de 2012
Señora
CARMELA SUSANA ERAZO ROSERO
Pasaje Los Juncos No. 523 y Eloy Alfaro, Conjunto Siglo XXI
Quito.-

De mi consideración:

Mediante resolución No. ADM-2012-10779, de 6 de febrero de 2012, se creó la Dirección Nacional de Atención y Educación al Usuario; y, con Resolución No. ADM-2012-11043, se emitió la Acción de Personal No.1309, de 17 de julio de 2012, en la que fui nombrada Subdirectora de Atención al Usuario, en tal virtud, avoco conocimiento del presente reclamo administrativo.

I. ANTECEDENTES

Me refiero a su comunicación presentada ante este organismo de control el 23 de julio de 2012, en la cual, manifestó lo siguiente:

> *"(..) Se realizaron una transferencia desde mi cuenta de ahorros a una cuenta de ahorros de un Señor Jorge Yambay, cuenta (...) persona que mantiene cuenta en el Banco Pichincha por el valor de 2.800,00 vía electrónica (...)"*

De lo referido solicita: *"(..) ayudarme a solucionar este problema, guiándome en los pasos a seguir (..)"*.

Por lo que, en observancia de lo dispuesto en el Artículo 76, numeral 7; literales b) y d) de la Constitución de la República del Ecuador, se remitió copias del mencionado reclamo a la entidad financiera para que presente las explicaciones y descargos que pudieran asistirle, garantizando así el debido proceso.

II. ANÁLISIS DE LA INFORMACIÓN

Del análisis realizado a la documentación que consta en el expediente, se desprende lo siguiente:

1. De acuerdo al contenido en el reclamo, los documentos adjuntos y la información sustentada, remitida por el Banco Pichincha C.A., se evidencia que la transferencia reclamada, fue procesada en forma exitosa el día 13 de junio de 2012 a las 12h22m01s., con la Tarjeta "E-key" que tiene asignada la Señora Erazo Rosero, la misma es: la No. 213224, la cual efectuó un débito a la cuenta de ahorros No.3006219700, por un valor de USD ($ 2.800,00).

2. La entidad financiera ha asignado como monto máximo para transferencias a través del canal internexo USD $ 5.000,00, para la fecha en la cual se ejecutó la transacción. Sin embargo de esto, primero se debe autorizar a la cuenta con un monto similar o menor al valor indicado, por lo que el usuario puntualiza su propio monto de dinero autorizado para la realización de transferencias a través de este canal.

3. La entidad financiera indica que en el log del canal internexo de la Cédula de Ciudadanía No. 1710789908, perteneciente a la Señora Erazo Rosero, se puede observar que él día 13 de junio del año dos mil doce se realiza un acceso desde la dirección IP 190.113.196.1, desde la cual se registra un intento fallido de transferencia debido a que el monto supera el valor permitido. A continuación utilizando la misma sesión y la misma dirección IP 190.113.196.1, se procede a la activación de la cuenta No. 3006219700 para transferencia por un valor total de USD $ 2,800,00 a la cuenta No. 4948166000 a las 12h22m01s.

4. El la ejecución de estas transacciones no se evidencia el ingreso errado tanto de la clave de acceso como de la clave de coordenada de la tarjeta "E-key" (necesarias para realizar transferencias). Lo que muestra que el individuo que realizó las transacciones, tenía conocimiento de las diferentes claves requeridas para la obtención de transferencias.

5. Según se puede apreciar en los registros de la entidad financiera la transacción fue procesada correctamente, de acuerdo al reporte del área de sistemas, señalando que dicha transferencia fue procesada con la información y coordenadas de la tarjeta "E-key" No. 213224, correspondiente a la señora Silvana Valdivieso.

6. La institución financiera implementó la tarjeta de carácter personal e intransferible denominada "E-key", en la cual se registra la coordenada solicitada por el sistema para aceptar la transacción, siendo igualmente de responsabilidad exclusiva del cliente mantener en secreto las coordenadas constantes en su tarjeta, y la más estricta custodia de la misma.

7. Al respecto, es importante recordarle la disposición reglamentaria vigente a esa fecha referida en el artículo 5, Sección 1, Capítulo III, Título XXV, Libro 1 de la Codificación de Resoluciones de la Superintendencia de Bancos y Seguros y de la Junta Bancaria, que establece: "*Los depósitos, retiros de fondos, créditos, débitos y cualquier otra transacción permitida en cuentas de depósitos monetarios, efectuados a través de medios electrónicos o electromecánicos, deberán estar sustentados por un acuerdo escrito entre el banco y el titular de la cuenta, en el que deberán constar, por lo menos, las siguientes condiciones:*

7.1. La responsabilidad exclusiva del cliente respecto de las transacciones que efectuare a través de estos medios; y,

*7.2. "**La responsabilidad del cliente de mantener en secreto la clave o seguridades a él asignadas, así como los cambios de claves que efectuaren. Igual responsabilidad tendrá con respecto a las claves o seguridades adicionales por él solicitadas y otorgadas por el banco."** (La negrilla me pertenece).*

8. De acuerdo a lo establecido en el documento de Servicios Electrónicos – Asignación de Tarjeta, suscrito por su persona, usted *"se obliga a custodiar con diligencia y cuidado la tarjeta"*. Además, de conformidad con la Ley de Comercio Electrónico y su respectivo Reglamento y de acuerdo con los principios de neutralidad tecnológica y autonomía privada:

"El Cliente reconoce, desde ya, la calidad de firma electrónica a las Claves, códigos de aceptación a través del sistema y demás seguridades que tengan por objeto ser utilizadas en las transacciones y servicios proporcionados por el Banco. El Cliente es responsable de todas las operaciones o transacciones que se realicen mediante la utilización de su dispositivo de seguridad. La sola utilización de este dispositivo de seguridad en las respectivas transacciones, serán para el Banco instrucciones impartidas por el Cliente que conllevan, implícitamente, la manifestación de su voluntad, y, por lo que tales instrucciones son válidas, integras, correctas e irrevocable. El cliente se responsabiliza y libera al Banco de toda responsabilidad por el uso indebido de los dispositivos de seguridad por parte de personas distintas al cliente. ***El hecho de que cualquier tercero haya utilizado la clave que le sea requerida por nuestro sistema, será considerado como si dicha transacción fue realizada por el Cliente, quien la reconoce como propia y sin reservas y asume frente al Banco, toda responsabilidad derivada de su uso indebido****" (La negrilla me pertenece).*

9. De acuerdo a la documentación remitida por la entidad financiera, esta manifiesta que: *"[...] Con la finalidad de minimizar la realización de fraudes en la página web de Banca Electrónica de Banco Pichincha, se publican constantemente Tips para no ser víctima de Fraude Informático".*

10. Como se puede apreciar, la transacción fue procesada correctamente, en donde se evidencia que usted accede con frecuencia a la Banca "E-key",l y realiza transferencias interbancarias mediante este canal, adicionalmente se observa que la Cuenta de Ahorros No 3006219700, disponía de un saldo promedio de USD $ 4.000,00. Durante el mes de de junio del 2012.

11. Por lo manifestado y debido a la transaccionalidad observada en la cuenta no se refleja comportamientos inusuales que haya hecho posible que se generen alertas a la entidad financiera.

III. CONCLUSIONES Y RESOLUCIÓN

Ante el análisis expuesto, se puede concluir que:

- La transferencia objeto del reclamo fue realizada con la utilización de las claves de acceso al sistema de carácter personal e intransferible denominada "E-key", en la cual se registra la coordenada solicitada por el sistema para aceptar la transacción, mismas que son únicas y es responsabilidad del cliente custodiarla.

- Se recomienda mantener el cuidado y resguardo necesario de su información, así como no ingresar coordenadas cuando no efectúe operaciones de carácter personal e intransferible denominada "E-key".

Por lo manifestado, este organismo de control no puede atender su solicitud favorablemente ya que no se ha evidenciado que Banco Pichincha C. A., haya vulnerado sus derechos financieros o haya incumplido normativas, procesos y procedimientos internos y externos; motivo por el cual se declara concluido el presente reclamo.

Atentamente,

Ab. Ma. Verónica Cevallos V.
SUBDIRECTORA DE ATENCIÓN
AL USUARIO (SAU)

ANEXO 5

Oficios de los usuarios que han sido víctimas de delitos informáticos

SBS
Superintendencia de Bancos y Seguros del Ecuador

Oficio No. DNAE-SAU-2012- 2556

Quito, D.M. 20 de junio del 2012

Asunto **Acuse recibo**
Producto: **Tarjeta de débito**
Subproducto :Débito no realizados por el usua.
Reclamo No. 2012- 006073
Estado: **En trámite**

Señorita Arquitecta
MARIA CARDENAS VALENZUELA
Francisco Sanz Barrio La Dolorosa Parroquia Tumbaco
Teléfono Nº092861385
Ciudad.-

De mi consideración:

Me refiero a su comunicación presentada ante este organismo de control el 20 de abril 2012, en la cual manifiesta lo siguiente:

"..solicito a Ustedes se me atiendan en el reclamo sobre dineros sustraídos de mi cuenta de ahorros Nº12000124635 de PRODUBANCO a través del cajero automático, de acuerdo a la descripción adjunta (copia), que hiciera en el reclamo al mencionado Banco y que ha sido atendida desfavorablemente..."

Atendiendo a su requerimiento, esta Dirección ofició a la entidad financiera, a fin de que presente los descargos que me pudiera asistir en el presente caso. Luego del análisis a la información remitida por la institución financiera, se le comunicará lo que en derecho corresponda.

Atentamente,

Dra. María Gabriela Mayorga
DIRECTORA NACIONAL DE ATENCION Y EDUCACION AL USUARIO
H.R. (040538)
Func. Resp. Dra. Y. Morejón
Revisado por: Ing. Nancy Conde

Quito
Avenida 12 de Octubre N24-185 y Madrid
Tel.: (593 2) 299 7600
(593 2) 299 6100

Guayaquil
Chimborazo 412 y Aguirre
Tel.: (593 4) 370 4200

Cuenca
Antonio Borrero 710 y Presidente Córdova
Tel.: (593 7) 283 5961
(593 7) 283 5726

Portoviejo
Calle Olmedo y Alajuela, esquina
Tel.: (593 5) 263 4951
(593 5) 263 5810

www.sbs.gob.ec

SOLICITUD DE RECLAMO/REQUERIMIENTO

No: 1873384

Reclamo ● Requerimiento ○

1	Nombres/Apellidos:	[redacted]		
2	Cedula/Ruc:	1804283768		
3	Fecha Reclamo/Requerimiento:	2012-06-01 15:46	Fecha Solución:	2012-6-27
4	Tipo de Reclamo/Requerimiento:	Casos de Investigación		
5	Orden de Trabajo	1873384 Adjuntar Archivos	Monto ($)	344
6	Nombre del Asesor	NAJERA BUITRON PAMELA ALEJANDRA		
7	Oficina Receptora:	INAQUITO AGENCIA	Notificación:	CALL CENTER

BANCO PICHINCHA C.A.
Pamela Nájera B.
Ejecutivo de Servicios
Agencia Inaquito

Firma del Cliente 631937-PMNB

Estimado Cliente, si Usted desea conocer el estatus de su reclamo o requerimiento, por favor comuníquese 02 2999-999 para Quito y Región Andinatel, al 1 700 - 800 800 Guayaquil y Región Pacifictel y al 07 2848-888 para Cuenca y Región Austro con referencia a su orden de trabajo. En caso de retiro de documento, dirigirse a la caja de servicios de la oficina de entrega.

2999999

BANCO PICHINCHA C.A.
Ejecutivo de Servicios
Agencia Inaquito

BANCO PICHINCHA C.A.

Quito, 25 de julio de 2012
BP – RRCI – 2012 – 0034

Señor
[redacted]
Presente.-

De nuestra consideración:

En atención a su reclamo No. 1873407 por el valor de $ 261.00 debitados de su cuenta No. 5889366700, mismo que se relaciona con transferencia realizada a través de Internet, nos permitimos manifestar lo siguiente:

Como es de su conocimiento, dentro del procedimiento establecido por el Banco para el proceso de transferencias por Internet, es necesario ingresar el usuario biométrico y clave biométrica por Usted generados, además, de ser el caso, responder a la pregunta e imagen seleccionada, información que es de exclusivo conocimiento del cliente y constituye el único mecanismo para acceder a los servicios ofrecidos por medios electrónicos.

Como medida complementaria de seguridad, el Banco implementó la tarjeta de carácter personal e intransferible denominada "E-key", en la cual se registra la coordenada solicitada por el sistema para aceptar la transacción, siendo igualmente de responsabilidad exclusiva del cliente mantener en secreto las coordenadas constantes en su tarjeta "E-key", y la más estricta custodia de la tarjeta.

Una vez realizados los debidos análisis y verificaciones, se establece que la transferencia por Usted reclamada ha sido efectuada por medios electrónicos, sin ninguna responsabilidad del Banco Pichincha, ni de sus funcionarios y empleados. Lamentamos lo ocurrido, sin embargo no podemos asumir su reclamo.

Es necesario mencionar adicionalmente que Banco Pichincha ha venido alertado públicamente, por múltiples medios, a sus clientes para que nunca entreguen o faciliten sus datos personales usuario y claves biométricas, o coordenadas de tarjeta "E-key".

A efectos de atender su pedido y con el fin de evitar que mi representada pueda incurrir en cualquier violación legal relacionada con sigilo bancario, solicitamos que la información de las cuentas y beneficiarios, sea solicitada a través de la forma prevista en la Ley General de Instituciones del Sistema Financiero o por orden de autoridad competente.

Atentamente,
Banco Pichincha C.A.

Gerente de Negocios
Ag. Pana Sur

ANEXO 6

Encuesta realizada a los usuarios afectados

Encuesta

Los datos de esta encuesta serán utilizados expresamente para la realización de una tesis de grado.

Sobre las "Condiciones de reembolso a usuarios del sistema financiero privado, por delitos informáticos en línea, en el Distrito Metropolitano de Quito.

Nombre:
Edad:
Ocupación:
SEXO: F ( ) M ( )
Fecha en que ocurrió el robo

Escoger una opción de cada pregunta y señalar con una X en el paréntesis.

1.- ¿Bajo qué modalidades fue víctima de fraude informático?

A) Ingreso de todas las coordenadas ( )
B) Página web bancaria clonada ( )
C) Correo electrónico con oferta laboral o promocional ( )
D) Otros ( )

Si su respuesta fue otros, especifique a continuación……

2.- El monto de su perjuicio fue de:

A) 0- 500 ( )
B) 500-1000 ( )
C) 1000-5000 ( )
D) 5.000-10.000 ( )

3. ¿A qué institución asistió primero para presentar su reclamo?

A) Su entidad bancaria ( )
B) Superintendencia de Bancos ( )
C) Fiscalía General del Estado ( )
D) Superintendencia de Telecomunicaciones ( )
E) Policía Nacional ( )

4. ¿Qué tipo de respuesta recibió respecto a su denuncia?

A) Positiva
B) Negativa

5.- ¿De qué entidad bancaria fue sustraído su dinero?

A) Banco Pichincha ( )
B) Banco Guayaquil ( )
C) Produbanco ( )
D) Banco Internacional ( )

6.- Su dinero fue sustraído de una cuenta de:

A) Ahorros ( )
B) Corriente ( )

7.- ¿Desde qué lugar realizó su transferencia bancaria, por la que se presume que fue víctima de delito informático?

A) Casa ( )
B) Cibercafé ( )
C) Oficina ( )

8.- ¿Cuánto tiempo se demoró el estudio de su caso?

A) 1-3 meses ( )
B) 3-6 meses ( )
C) 6-12 meses ( )
D) Más de un año ( )

9.- ¿Tras concluir el proceso, le devolvieron todo su dinero?

A) Sí ( )
C) No ( )
Por qué: ……

10.- ¿Después de ser víctima de un fraude informático continúa haciendo transferencias en línea?

A) Si ( )
B) No ( )

ANEXO 7

Libreto de la Radio revista e-Bank

001 CONTROL: PRESENTACIÓN

002 PRESENTADORA: Muy buenos días amigos radioescuchas Bienvenidos a e-
003 Bank, la radio revista que le informa. sobre todo lo relacionado a la banca en
004 línea y especialmente buscamos guiarle con precauciones que usted debe
005 tener, para que se proteja y evite ser víctima del robo a través de internet.

006 Esta mañana tendremos un programa muy especial, porque abordaremos a fondo sobre la ciberdelincuencia y cómo prevenir este fenómeno, que continúa creciendo con el avance de la tecnología.

007 Como siempre les recordamos que deben atentos con lo que publicamos en nuestras redes sociales y tener cuidado con los portales web que visitamos y los sitios desde donde nos conectemos para navegar en línea.

008 Este mismo instante sus claves personales, redes sociales o cuentas bancarias pueden estar siendo vulneradas.

009 Soy Amelina Espinosa, y durante 30 minutos exploraremos los riesgos en el mundo del ciberespacio, bienvenidos.

010 CONTROL:(INTRO TECLAS)

011 Gracias amigos por continuar con nosotros. Para iniciar, les presentamos el segmento PERFIL 2.0.

012 En esta ocasión tenemos la historia de dos “hackers” aficionados, que por curiosidad aprendieron a vulnerar sistemas en línea.

013 Ellos aseguran que sus habilidades en la red sólo las aplican para jugar y no para hacer daño.

014 Antes de dar paso a este segmento quisiera contarles amigos que un hacker o también llamados como piratas informáticos, son personas apasionadas por la informática. Estos pueden aprovechar la falta de rigor de las medidas de seguridad de la informática para acceder a las redes.

015 Tras esta breve introducción, damos paso a esta nota, que de seguro les ayudará a entender mejor sobre el perfil que puede tener un hacker.

CONTROL: (BITE 1)

CONTROL: (CORTINA)

016 Continuamos amigos con más información. Qué les pareció este segmento? No olviden que pueden compartirnos sus opiniones inquietudes a través de Facebook y Twitter de e-Bank.

017 Escucharon lo fácil que es vulnerar una red? Pero no se alarme, solo tener las debidas precauciones para evitar ser víctimas de este tipo de intromisión.

018 Bueno amigos, luego de presentarles estos perfiles, nos vamos a nuestro primer corte comercial. Regresamos, no te despegues de tu programa e-Bank.

019 CONTROL (SOSTENIMIENTO DE SALIDA)

020 CONTROL: MENSAJE DE LA ASOCIACIÓN DE BANCOS PRIVADOS DEL ECUADOR

021 CONTROL: (SOSTENIMIENTO DE REGRESO)

022 Seguimos amigos en esta mañana, cargados de mucha información. Ahora les quiero preguntar, cuántos de ustedes tienen una red social?

023 El portal de mediciones de popularidad de las redes sociales en el mundo, denominado Socialbakers, menciona algunos datos interesantes. Sabía usted que hasta mayo del 2013, Ecuador tenía 5.641.540 de usuarios de facebook. Esto hizo que Ecuador se ubique en la posición 35 a nivel mundial de países con más usuarios de esta red social.

024 Con este dato amigos radioescuchas, les presentamos el siguiente segmento en la RED, donde queremos compartirles un reportaje sobre las medidas de seguridad en redes sociales, donde queremos mostrarles que una red social puede ser un producto muy cotizado entre los ciberdelincuentes.

025 CONTROL: (CORTINA)

026 CONTROL: (BITE 2)

027 Amigos radioescucha debemos estar atentos con lo que publicamos en las redes sociales ya que hacen un seguimiento a los usuarios. Incluso para adquirir información, inventan perfiles falsos en las redes sociales y agregan como amigos a las víctimas, con el fin de enlazar una amistar y poco a poco conseguir información de nuestras cuentas bancarias.

028 Ahora cambiamos de tema, porque es momento de informarnos en nuestro segmento INFOBANK. Entre las noticias que queremos compartirles esta mañana es cómo los usuarios de la banca pueden actuar si fueron víctimas de fraude informático sobre todo si usted no ha tenido una respuesta

favorable de su banco. Ahora ustedes pueden presentar su caso a los defensores del usuario. Estas y otras noticias, a continuación.

029 CONTROL: (CORTINA)

030 CONTROL: (BITE 3)

031 Noticia 1: Desde febrero del 2013, los 7 millones de usuarios de la banca cuentan con Defensores del Cliente Financiero. La principal función de estas personas es precautelar los derechos de los clientes de la banca. En total son 43 agentes, quienes además cuentan con un suplente que actúa en casos específicos.

032 Estos Defensores del Cliente financiero fueron elegidos a través del Consejo de Participación Ciudadana y Control Social, Institución que luego de tres convocatorias culminó con el proceso de selección. Ellos desarrollan sus funciones en la oficina matriz de cada institución financiera para la cual fueron designados.

033 Noticia 2. El core bancario, o más conocido como soluciones integrales bancarias, se está implementando poco a poco en el país. Según el portal Web (www.nasoft.com) “el Core Bancario representa el corazón de la operación financiera, y la decisión de seleccionar una plataforma de última generación, que asegure un soporte operativo a mediano y largo plazo”.

034 El Banco Pichincha fue el primero en implementar en abril del 2012, en toda su red de oficinas en el Ecuador, un software llamado TCS BaNCSS. Esta es una herramienta de core bancario, que ayuda a generar niveles de seguridad.

035 Produbanco implementó un nuevo aplicativo bancario Prometeus sobre plataforma Microsoft Windows 2000 Server. Este proyecto inició en Septiembre del 2001 y culminó en febrero del 2004.

036 A este proyecto se lo denominó Prometeus Core Banking, que ayudó a mejorar la calidad de servicio a los clientes y disminuir los costos de operación. Además, según explican sus autoridades en su portal web, permitió mantener controles preventivos en línea.

037 Pero no todos los bancos informan si disponen de estos sistemas. Saberlo podría ayudar a los usuarios a tomar decisiones sobre sus transacciones en línea y conocer cuán protegidos están al realizar sus pagos por intrnet.

038 En síntesis, este sistema ayuda a mejorar la seguridad y el servicio de las instituciones financieras, a pesar que no han ayudado a frenar totalmente los inconvenientes que continúan en la red.

039 CONTROL: (CORTINA)

040 CONTROL (SOSTENIMIENTO DE SALIDA)

041 CONTROL: MENSAJE DE LA ASOCIACIÓN DE BANCOS PRIVADOS DEL ECUADOR (PUBLICIDAD)

042 CONTROL: (SOSTENIMIENTO DE REGRESO)

043 Estamos ya de regreso con nuestro segmento ENTREVISTA CON EL EXPERTO ON-LINE.

044 Esta semana el invitado es Dmitry Bestuzhev, quien es Director de Investigación del laboratorio Kaspersky. Muy buenos días Dmitry bienvenido.

045 PREGUNTAS:

1. ¿Cuáles son los delitos informáticos más comunes en Ecuador?
2. ¿En cuanto a las principales causas de los ataques cibernéticos a las entidades bancarias, cómo se comenten estos delitos?
3. ¿Cifras actuales, hasta febrero del 2014, demuestra que en el Ecuador han aumentados este tipo de delitos?
4. Actualmente hay más ataques que demuestren que el Ecuador está subiendo en el ranking Latinoamericano por ataque informáticos?
5. Cuáles son las provincias más afectadas en el Ecuador por estos delitos?
6. Mediante un estudio ustedes determinaron que la mayoría de usuarios no recuperaban su dinero tras ser víctimas por delitos informáticos, cuéntenos sobre este estudio.
7. ¿Qué recomendaciones qué nos puede compartir frente a este tema, tanto para las entidades bancarias como para los usuarios?
8. ¿Los ciberdelincuentes aprovechan la coyuntura noticiosa para crear virus que conllevan al fraude?

046 CONTROL: (CORTINA)

047 Muchísimas gracias Dmitry por acompañarnos esta mañana y ayudarnos a resolver algunas dudas sobre este tipo de delitos.

048 Estamos llegando amigos radioescuchas a la parte final de nuestro programa, pero antes de despedirnos, les queremos compartir algunas

recomendaciones para tener en cuenta y prevenir ser víctimas de la ciberdelincuencia, a continuación en nuestro segmento CIBERSEGURIDAD.

049 CONTROL: (CORTINA)

050 Cómo proteger nuestras claves para dejar de ser víctimas de la ciberdelincuencia? A continuación.

051 Para protegerse de los ciberdelincuentes usted debe tomar algunas medidas importantes. Como no guardar sus claves y tarjetas de crédito y de débito, en ningún archivo del computador.

052 CONTROL: (CORTINA)

053 Como ya pudieron escuchar esta mañana, la ciberdelincuencia es una nueva forma de atacar a la sociedad y que también es asediada por la delincuencia común y organizada. Como ustedes vieron en este programa, es importante informarse y saber cómo protegerse para ser menos vulnerable frente a este tipo de delitos.

054 Cuidar nuestras claves electrónicas, utilizar mecanismos de bloqueo y protección de nuestros computadores, actualizarse todo el tiempo con las últimas tecnologías, seleccionar la información que publicamos en las redes sociales o páginas web, esas son algunas de las recomendaciones que nos han compartido los expertos, para combatir a los ciberdelincuentes.

055 Recuerde que si usted fue víctima, debe hacer su denuncia en su entidad bancaria, en la Superintendencia de Bancos y en la Fiscalía. Es obligación de estas entidades investigar su caso y emitir una pronta respuesta y solución.

056 Muchísimas gracias por acompañarnos en su programa e-Bank, informando sobre la seguridad de la banca en línea. Estuvo con ustedes durante la conducción de este programa, Amelina Espinosa. Hasta la próxima emisión.

057 CONTROL: (CORTINA)

058 CONTROL: DESPEDIDA

ANEXO 8

Tabla Guión de Radio: e-Bank

RESPONSABLE	ACTIVIDADES	TIEMPO
Controles	Presentación del programa	12s''
Locutor 1	Saludo	1 min
Controles	Intro e-bank	5s''
Locutor 1	Desarrollo del segmento	1,29 min
Controles	BITE 1 PERFIL 2.0.	5,03 min
Controles	Cortina	4 s''
Locutor 1	Desarrollo del segmento	1 min
Controles	Sostenimiento de Salida	13 s''
Controles	Comerciales: Mensaje ABPE	36s''
Controles	Sostenimiento de regreso	11 s''
Locutor 1	Desarrollo del segmento	1,44 min
Controles	BITE 2 Reportaje En la red	4,50 min
Locutor 1	Conclusiones del segmento	50 s''
Controles	BITE3 Infobank	3,20 min
Controles	Sostenimiento de Salida	13 s''
Controles	Comerciales: Mensaje ABPE	33s''
Controles	Sostenimiento de regreso	11 s''
Locutor 1	Desarrollo del segmento: Entrevista con el experto on-line.	8 min
Locutor 1	Desarrollo del segmento Ciberseguridad	10 s''
Controles	Cortina	4s''
Locutor 1	Ciberseguridad	1 min'
Locutor 1	Despedida	1,20 min
Controles	Cortina	4s''
Controles	Sostenimiento despedida	12 s''
TOTAL		30,02 Min

ANEXO 9

Escaleta Reportaje Multimedia

Tema: Reportaje "Ciberdelincuencia"

Objetivo: Mostrar las diferentes formas a las que un usuarios del ciberespacio está expuesto a ser víctima de la ciberdelinciencia.

Sinopsis:

Si bien el alcance a la tecnología facilita a los usuarios su día a día, esto también encierra altos niveles de inseguridad a los que están expuestos sus usuarios. Es por eso, que mediante este reportaje, se demostrará lo fácil que resulta que los ciberdelincuentes vulneren los sistemas para hallar víctimas en el ciberespacio, que incluso esas víctimas llegar a tener un alto consto en el mercado negro del internet, tras acceder a sus cuentas, especialmente bancarias.

Entrevistas:

1. Dmitry Bestuzhev
   Director de Investigación del laboratorio Kaspersky
   Tema a tratar: - el costo de los usuarios en internet y cifras de la ciberdelincuencia
2. Pablo Córdova
   Presidente del Comité de seguridad bancaria
   Tema a tratar: las mejoras de seguridad de la banca para prevenir estos delitos
3. Jorge San Lucas
   Director en Tecnología e información de la Fiscalía General del Estado
   Tema a tratar: Denuncias por delitos informáticos

4. Arturo De la Torre
   Docente de la ESPE
   Tema a tratar: Cómo operan los ciberdelincuentes en el Ecuador
5. Juan Armendariz
   Especialista en Seguridad Informática
   Tema a tratar: Medidas de seguridad para prevenir estos delitos
6. Testimonios
   Usuarios que fueron víctimas de a ciberdelincuencia
   Tema a tratar: Cómo se robaron el dinero de sus cuentas bancarias

Requerimientos:

1. Técnicos: Cámara CANON 7, un micrófono corbatero, equipo de iluminación, una computadora Mac, software de edición, trípode, tarjeta de memoria, pilas AA, micrófono de bola, cable de micrófono.

2. Transporte: Las grabaciones se realizarán dentro de la ciudad de Quito y al ser el equipo técnico grande y costoso, se utilizará taxis, para lo cual se utilizará un promedio de 40 dólares para pagar el servicio.

ANEXO 10

Guión Reportaje Multimedia "Ciberdelincuencia"

Ciberdelincuencia **Amelina Espinosa**	
AUDIO	**VIDEO**
LOCUCIÓN Según la empresa internacional Kaspersky Lab, en Ecuador, de acuerdo al crimen cibernético y los ataques de malware, hasta febrero del 2014 se registraron 20 mil ataques de malware por día, lo que significa que hubo 820 ataques de malware por hora y 14 ataques de malware por minuto.	Tomas internet, computadores, cibercafés
ENTREVISTA Dmitry Bestuzhevnos Muestra cómo operan los ciberdelincuentes a través de ellas.	Plano Medio
LOCUCIÓN Para comprobar si esto sucede en la práctica, concurrí a un centro comercial de Quito junto a un hacker que dice ser ético, porque su fin no es hacer daño….Él nos muestra cuán fácil es sustraerse la información.	Plano medio y subjetivo de lo que realiza el hacker
LOCUCIÓN Los grafittis políticos eran en los años noventas parte del paisaje urbanístico de la capital del Ecuador.	Tomas de archive Quito año 90
ENTREVISTA hacker Demuestra el peligro del acceso a redes wifi	Plano detalle
LOCUCIÓN El hacker inició con la ayuda de un programa básico y gratuito de seguridad en redes, le tomó tan solo segundos saber el número y el tipo de equipos electrónicos que estaban conectados a la misma red wifi.	Tomas de distintos sitios webs y computador
ENTREVISTA hacker Indica lo encontrado en la red desde su computador	Plano detalle
LOCUCIÓN El proceso es sencillo y el usuario ni si quiera se da cuenta de lo que está sucediendo. Los expertos dicen que es porque en la máquina del usuario no aparece ninguna alerta o aviso de que alguien extraño se haya conectado a su máquina.	Tomas de computadores e informática en general

LOCUCIÓN usuarios Victoria y Daniel son dos de los 384 víctimas que llegaron a la Superintendencia de Bancos y Seguros, entre el 2010 y 2013, para presentar una denuncia por phishing.	Plano general y medio de los usuarios
LOCUCIÓN En el caso de Daniel, a través de una transferencia electrónica, se le sustrajeron USD 1000 dólares de su cuenta bancaria.	Planos generales y medios del usuario
ENTREVISTA Diego Explica qué sucedió con su cuenta bancaria	Plano medio y detalle
LOCUCIÓN Pintura, rodillos, aerosoles y stickers y hasta escultupintura, son parte de este festival.	Planos detalle y generales de los materiales del Detonarte
LOCUCIÓN Cada año millones de dólares son robados de las cuentas bancarias a los usuarios. Para cometer estos fraudes, los ciberdelincuentes se valen de la clonación de tarjetas de crédito, o por el robo de usuario y contraseña de la banca.	Planos detalles de usuarios de internet
GRÁFICO FISCALÍA Durante el 2011, la fiscalía receptó 168 denuncias por delitos informáticos, el 2010 fueron 1111 y el 2013 registraron 3129 denuncias. Es decir que se incrementó un 1800 %.	Infografía
ENTREVISTA Pablo Córdova Habla sobre las medias de seguridad de la banca privada	Plano medio
LOCUCIÓN El código penal ecuatoriano, sanciona este tipo de delitos con prisión de libertad de 3 a 10 años dependiendo de la gravedad. Además la sanción monetaria mínima va desde 4 a 20 salarios básicos unificados, que significa entre 1360 y 6800 dólares.	Imágenes animadas
LOCUCIÓN Si usted fue víctima de este delito, lo primero que debe hacer es notificar a su entidad bancaria, si no tiene respuesta presentar una nueva denuncia en la Superintendencia de Bancos y a la Fiscalía. Pero esto, no le garantiza la devolución de su dinero	Planos generales usuarios e imágenes de informática

ENTREVISTA Pablo Córdoba Comenta, que a diferencia de años atrás, actualmente la banca en línea del país tiene mayores filtros que protegen al cliente.	Planos medios y detalle
LOCUCIÓN Los ciberdelincuentes hacen negocios con cada cuenta electrónica que llega a su poder. Esto tiene un gran valor en el mercado negro de venta de información	Imágenes animadas
LOCUCIÓN Para cometer estos ilícitos existe una red organizada.	Imágenes animadas
LOCUCIÓN Para evitar ser víctimas de estos delitos Expertos nos dan algunas recomendaciones.	Planos generales de usuarios de internet
LOCUCIÓN Victoria y Daniel no recuperaron su dinero, Daniel por su parte agrega que ha dejado de utilizar la banca en línea.	Planos medios y detalle de los dos usuarios