**UNIVERSIDAD CATÓLICA**
**DE SANTIAGO DE GUAYAQUIL**

**FACULTAD DE CIENCIAS ECONÓMICAS Y ADMINISTRATIVAS**
**CONTADURÍA PÚBLICA E INGENIERÍA EN CONTABILIDAD Y AUDITORÍA CPA.**

**TÍTULO:**
# "ESTABLECIMIENTO DE MEDIDAS DE CONTROL EN CONTRA DEL FRAUDE EN TARJETAS DE CRÉDITO Y DÉBITO COMO UNA OPCIÓN DE PREVENCIÓN DE RIESGOS"


**AUTORAS:**

**ACOSTA VELASQUEZ, YANINA MADELAYNE**
**REYES SERRANO, PATRICIA LISSETTE**


**Trabajo de Titulación previo a la Obtención del Título de:**
**INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA.**

**TUTOR:**
**CPA. HIDALGO TACURI JOHN LUIS, MSC**

**Guayaquil, Ecuador**

**2014**

**UNIVERSIDAD CATÓLICA**
**DE SANTIAGO DE GUAYAQUIL**

**FACULTAD DE CIENCIAS ECONÓMICAS Y ADMINISTRATIVAS**
**CONTADURÍA PÚBLICA E INGENIERÍA EN CONTABILIDAD Y AUDITORÍA CPA.**

## CERTIFICACIÓN

Certificamos que el presente trabajo fue realizado en su totalidad por **PATRICIA LISSETTE REYES SERRANO Y YANNINA MADELAYNE ACOSTA VELASQUEZ**, como requerimiento parcial para la obtención del Título de **INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA**.

**TUTOR:**

_____
**CPA. HIDALGO TACURI JOHN LUIS, MSC.**

**DIRECTOR DE LA CARRERA:**

_____
**ING. ÁVILA TOLEDO ARTURO ABSALÓN, MSC.**

**Guayaquil, Octubre del 2014**

**UNIVERSIDAD CATÓLICA**
**DE SANTIAGO DE GUAYAQUIL**

**FACULTAD DE CIENCIAS ECONÓMICAS Y ADMINISTRATIVAS**
**CONTADURÍA PÚBLICA E INGENIERÍA EN CONTABILIDAD Y AUDITORÍA CPA.**

## DECLARACIÓN DE RESPONSABILIDAD

Nosotras**, Patricia Lissette Reyes Serrano y Yannina Madelayne Acosta Velásquez.**

**DECLARAMOS QUE:**

El Trabajo de Titulación **"Establecimiento de Medidas de Control en contra del Fraude en Tarjetas de Crédito y Débito como una opción de Prevención de Riesgo"**, previa a la obtención del Título de**: INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA**., ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan al pie de las páginas correspondientes, cuyas fuentes se incorporan en la bibliografía. Consecuentemente este trabajo es de nuestra total autoría.

En virtud de esta declaración, nos responsabilizamos del contenido, veracidad y alcance científico del Trabajo de Titulación referido.

**Guayaquil, Octubre del 2014**

**AUTORAS**

_____
**YANNINA MADELAYNE ACOSTA VELASQUEZ.**

_____
**PATRICIA LISSETTE REYES SERRANO.**

**UNIVERSIDAD CATÓLICA**
**DE SANTIAGO DE GUAYAQUIL**

**FACULTAD DE CIENCIAS ECONÓMICAS Y ADMINISTRATIVAS**
**CONTADURÍA PÚBLICA E INGENIERÍA EN CONTABILIDAD Y AUDITORÍA CPA.**

## AUTORIZACIÓN

Nosotras, **Patricia Lissette Reyes Serrano y Yannina Madelayne Acosta Velásquez.**

Autorizamos a la Universidad Católica de Santiago de Guayaquil, la publicación en la biblioteca de la institución del Trabajo de Titulación: **"Establecimiento de Medidas de Control en contra del Fraude en Tarjetas de Crédito y Débito como una opción de Prevención de Riesgo",** cuyo contenido, ideas y criterios son de nuestra exclusiva responsabilidad y total autoría.

**Guayaquil, Octubre del 2014**

**AUTORAS**

_____
**YANNINA MADELAYNE ACOSTA VELASQUEZ.**

_____
**PATRICIA LISSETTE REYES SERRANO.**

## AGRADECIMIENTO

Agradezco a Dios por su infinito amor y por brindarme una familia especial que ha sido mi pilar fundamental para crecer profesionalmente.
A Enrique Caicedo, por su apoyo incondicional en el transcurso de mi carrera universitaria, por compartir momentos de alegría, tristeza y demostrarme que siempre podré contar con él y por sus aportes en la investigación.
Agradezco también al Tutor de ésta investigación por su valioso tiempo dedicado al desarrollo de ésta investigación y asesoramiento a la realización de la misma.

_____
**YANNINA MADELAYNE ACOSTA VELASQUEZ.**

Quiero agradecer a Dios por permitirme llegar a este momento, a mi familia por ser mi motivación día a día. También agradezco a mi tutor por brindarnos el apoyo para poder completar el proyecto.

_____
**PATRICIA LISSETTE REYES SERRANO.**

## DEDICATORIA

Dedico este trabajo principalmente a Dios, por haberme dado la vida y permitirme el haber llegado hasta este momento tan importante de mi formación profesional.

A mi papá Robert Acosta, a mi mamá Gina Velásquez y a mis hermanos Donald y Victor Acosta por sus muestras de cariño y apoyo incondicional en el transcurso de mi vida y porque nunca se escatimaron recursos para que yo finalice mi carrera universitaria, gracias por cada palabra de aliento que llenó mi vida de fuerzas y ganas de triunfar.

A mi abuela Mariela Castro, por brindarme sus consejos y por compartir mis logros académicos.

_____

**YANINA MADELAYNE ACOSTA VELASQUEZ.**

El día de hoy se incorpora la última Ingeniera de la familia Reyes Serrano y me siento inmensamente feliz y orgullosa de poder dedicárselo a ellos.

_____

**PATRICIA LISSETTE REYES SERRANO.**

**UNIVERSIDAD CATÓLICA**
**DE SANTIAGO DE GUAYAQUIL**

**FACULTAD DE CIENCIAS ECONÓMICAS Y ADMINISTRATIVAS**
**CONTADURÍA PÚBLICA E INGENIERÍA EN CONTABILIDAD Y AUDITORÍA CPA.**

**CALIFICACIÓN**

_____
**CPA. HIDALGO TACURI JHON LUIS, MSC**

# ÍNDICE GENERAL

# ÍNDICE DE TABLAS

## ÍNDICE DE GRÁFICOS

# RESUMEN

Durante este proyecto de investigación abarcaremos conceptos y definiciones básicas, descripción de los diferentes tipos de fraude, daremos un vistazo general a las tarjetas con chip inteligente, tipos penales de los delitos informáticos y concluiremos con los resultados de una encuesta realizada a los tarjetahabientes de la ciudad de Guayaquil, evidenciando el problema real que existe. En Guayas las operaciones fraudulentas en contra de los tarjetahabientes es una realidad poco investigada, según la Fiscalía General del Estado durante el año 2013 se realizaron 960 denuncias, un 38% más que el año anterior, sin embargo estos son solamente las denuncias presentadas. El propósito de esta investigación es establecer medidas de control en contra del fraude de tarjetas de crédito y débito, además de concientizar a los usuarios de las tarjetas sobre el problemática existente y el grado de exposición al fraude que se encuentra en el momento que efectúa transacciones con tarjetas. El buen uso de las tarjetas de crédito es parte de la inclusión financiera que propone el gobierno, los delitos informáticos con el uso de las mismas se intensifica y los ecuatorianos viven día a día, es por esta razón la importancia de la investigación. Los datos obtenidos durante el desarrollo de este proyecto servirán para marcar un inicio a la concientización tanto para los tarjetahabientes como a los entes de control, estos últimos con el fin de que desarrollen a profundidad estos temas de educación al usuario, sin prejuicio de las exigencias contempladas en las normativas a las Instituciones Financieras.

# INTRODUCCIÓN

Ecuador ya no es un país exento del comercio electrónico, la nueva tecnología permite realizar a los usuarios transacciones en línea para hacer uso de su “dinero plástico”, y a medida que avanzamos los delincuentes digitales o defraudadores se ponen al día con todos los cambios de sistemas informáticos y nuevas tecnología es por eso que vamos a abordar un tema al cual la mayoría de ecuatorianos está expuesto y ciertamente muchos han padecido.

Cuando hablamos de una tarjeta de crédito y/o débito se piensa en una forma muy útil de financiar ciertos gastos, pero casi nunca se piensa en cuidar ese dinero plástico el cual es mucho más vulnerable que el dinero real. Los robos o fraudes electrónicos van en aumento, dejando perdidas a miles y que las Instituciones Financieras y también los tarjetahabientes sepan cómo prevenir es importante ya que se puede disminuir el riesgo de ser víctima de fraude, que no solo pone en peligro información financiera y personal sino también los recursos monetarios.

Según el Ingeniero Alberto Andrade (2011), promotor del proyecto Red Segura el skimming es la técnica más fácil para sustraer dinero de las tarjetas crédito y/o débito, pues la banda magnética que algunas tarjetas en la actualidad tienen no es segura y el PIN con cuatro dígitos con el que cuentan es muy fácil de ser descifrado por los informáticos, el riesgo existe y se puede ser víctima de fraude si no se toman las medidas necesarias para así evitar la clonación o una filtración de información en la Administración Financiera, por este motivo ya existen en el Ecuador tarjetas de crédito y débito con un chip inteligente, la cuales limitan el ataque del fraude.

La presente investigación va a exponer los diferentes tipos de fraudes electrónicos que existen, así como las transacciones en las que se pueden dar este tipo de delitos; además de dar opciones de prevenir y no ser parte de las estadísticas. Describiremos la situación actual de las tarjetas de crédito y su evolución a través de los años y las exigencias de la

Superintendencia de Bancos y Seguros en cuanto a las seguridades que deben seguir.

Mediante la recopilación de datos impresos, electrónicos, bibliográficos y boletines, se obtuvo datos relacionados a las técnicas de fraude de tarjetas de crédito y débito en Guayaquil, indagaremos sobre la realidad que atraviesa el fraude electrónico, el perfil del defraudador; evaluaremos la información disponible sobre estos casos y las costumbres de las personas que utilizan tarjetas de crédito y débito.

Una vez obtenidos los resultados que se originaron por las encuestas realizadas se procedió a la tabulación de la información para efectuar un análisis e interpretación de los datos de la muestra aplicada.

Adicionalmente, con el fin de obtener información útil y necesaria para el desarrollo de la investigación, se solicitó a la Fiscalía General del Estado los índices de denuncias de fraude por tarjeta de crédito y débito de los últimos 3 años y a la Superintendencia de Bancos y Seguros el número actual de tarjetahabientes del país y el listado de las Emisoras de tarjetas de crédito y débito.

Toda la información previamente recolectada permitió desarrollar estrategias para la prevención de operaciones fraudulentas con tarjeta de crédito y débito para que sean aplicadas por las Instituciones Financieras y también para los tarjetahabientes para lograr minimizar el riesgo de pérdida de información y monetaria .

# CAPÍTULO I

# EL PROBLEMA

## 1.1 PLANTEAMIENTO DEL PROBLEMA

El fraude es el acto intencional de perjudicar a una persona u organización, para conseguir un beneficio ilegítimo. A lo largo del tiempo hemos conocido diferentes tipos de fraudes de estados financieros que se han realizado en grandes y pequeñas compañías, en ésta ocasión nos enfocaremos en las operaciones fraudulentas con tarjetas de crédito y débito.

Las operaciones fraudulentas con tarjeta de crédito y débito surgen a raíz del desarrollo de la tecnología, ya que éste avance ha permitido al sistema financiero brindar diferentes tipos de servicios bancarios, como por ejemplo: consultas de saldos por internet y transferencias de dinero, además los usuarios de tarjetas de crédito y débito en la actualidad poseen la facilidad de realizar transacciones comerciales vía internet, lo cual en muchas ocasiones ha resultado perjudicándolos, debido a que desafortunadamente también existen personas inmorales que hacen uso de la tecnología para cometer actos ilícitos. Por este motivo el sistema financiero y sus tarjetahabientes deben estar alerta a éste tipo de riesgo y a su vez crear controles y estrategias antifraude.

En Ecuador el tema de delitos informáticos se desarrolló en el año 2009 donde la cifra de actividades fraudulentas llego a 168, en el 2010 se reportó 2,099 casos, trece veces que el 2009, y entre los meses de enero y junio del 2011 se registraron 1,360 casos, en este mismo año la Fiscalía General del Estado estimó una pérdida cerca del millón de dólares por delitos informáticos, en el año 2012 la cifra de delitos informáticos fue 1,564 y en el 2013 de 1,623[1].

[1] El Universo. (Noviembre 2011). “Mercado negro de delito informático se expande en el país”

Mientras que el uso de tarjetas de créditos y débito sigue creciendo en el Ecuador, el ritmo de crecimiento es menor a los años anteriores, Según información de la Superintendencia de Bancos y Seguros, este tipo de fraude sigue aumentando y se vuelve un poco difícil de detectar ya que los delincuentes digitales o "hackers" utilizan técnicas muy sofisticadas, gracias a la ayuda de la tecnología y programas informáticos, perjudicando a los tarjetahabientes y a su vez ocasionando pérdidas a los bancos, porque 4 de cada 10 incidentes implica un reembolso para el cliente. (Escamilla, 2012)[2].

El Ecuador no cuenta con los controles indicados y los programas de prevención y detección de fraude son imprecisos por el alto índice de operaciones fraudulentas que se han ejecutado, para evitar este tipo de fraude se necesita observar los procesos y realizar las debidas modificaciones en los controles, de esta forma minimizar el riesgo y las pérdidas para el sistema financiero y los usuarios de tarjetas de crédito y débito.

El desarrollo de este proyecto es con la finalidad de contribuir al Sistema financiero y a cada tarjetahabiente con métodos de prevención para disminuir delitos en cajeros automáticos, además de plantear estrategias de cómo protegerse contra el fraude en línea, y como evitar la clonación de tarjetas de crédito y débito. "Hasta el mes de junio de 2013 se registraron 3,151,887 tarjetas de crédito, entre principales y adicionales y de acuerdo con el BCE el crédito otorgado por esta vía durante el año pasado sumó $260,5 millones, que corresponde al 1,29% del total entregado por el sistema financiero privado. En promedio, los tarjetahabientes deben pagar mensualmente $789.9 millones" mientras que en 2012 ese monto fue de $718,7 millones"[3], esto quiere decir que el uso de tarjeta de crédito va variando año tras año y con dicho crecimiento crediticio se van sumando

[2] CNNEXPASIÒN.(Junio 2011). Obtenido de http://www.cnnexpansion.com/mi-dinero/2012/06/20/los-5-fraudes-mas-temidos-por-los-bancos

[3] Diario el Telégrafo. (Diciembre de 2013). Obtenido de http://www.telegrafo.com.ec/economia/item/3-151-887-tarjetas-de-credito-hay-en-ecuador.html

nuevas técnicas de los delincuentes informáticos para poder realizar sus fraudes y perjudicar a los tarjetahabientes.

## 1.1.2 SITUACIÓN CONFLICTO

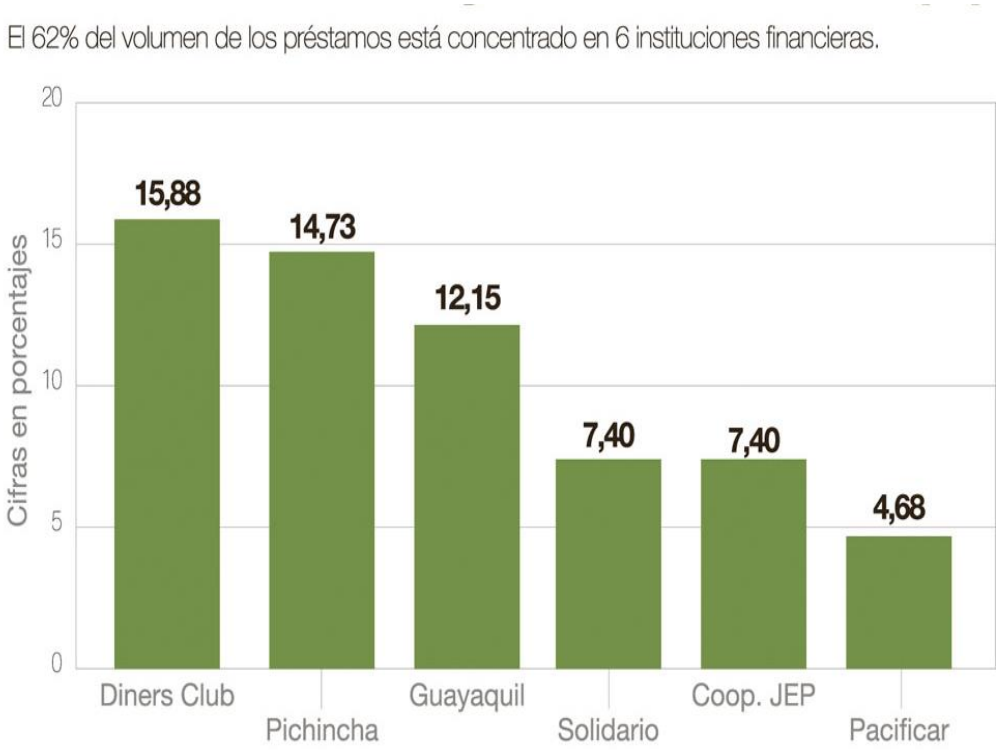
En el Ecuador no existe un control de gasto, algunos tarjetahabiente aprovechan de sus cupos de la tarjeta y realizan gastos compulsivamente, es decir no tienen auto-control y al momento de cancelar existe un retraso en el pago y los intereses comienzan a aumentar y es por este motivo en el segundo trimestre del 2012, las entidades competentes advirtieron sobre señales de sobre-endeudamiento de la población y adoptaron medidas para el adecuado control del consumo en el Ecuador. En ese entonces, Correa declaró: "En total en el sistema consideramos que 41% de las familias tiene sobreendeudamiento, estamos hablando de unas 400 mil familias. Esto puede generar graves problemas para la economía en general"[4].

Año tras año la cifra de dólares en dinero plástico aumenta, se podría decir que es por la facilidad que se tiene para adquirir una tarjeta de crédito, ya que los bancos han realizado una distribución sorprendente de crédito, inclusive si no es cliente de la institución financiera la cual está emitiendo la tarjeta igual el crédito es concedido, respaldándose en el excelente estado crediticio que puede tener dicha persona y es así como el uso de las tarjetas de crédito revela nuevos gastos de los ecuatorianos y los aumentos drásticos en los rutinas de consumo.

"El volumen de crédito de consumo con tarjetas de crédito corresponde a un 62% y se encuentra concentrado en 6 instituciones financieras Diners Club (15,88%), Banco Pichincha (14,73%), Banco de Guayaquil (12,15%), Solidario (7,40%), Cooperativa JEP (7,40%) y Pacificard (4,68%), según datos del BCE" [5] (Telegrafo).

[4-5] Diario el Telégrafo. (Diciembre de 2013). Obtenido de http://www.telegrafo.com.ec/economia /item/3-151-887-tarjetas-de-credito-hay-en-ecuador.html

**Gráfico 1: "Concentración de los Créditos de Consumo con Tarjetas de Crédito"**



Fuente: BCE, *Evolución del Crédito del Sistema Financiero Privado, diciembre 2013*. - Diseño editorial másQmenos.

Los usuarios de tarjeta de crédito ven como ventaja utilizarla porque tienen la posibilidad de diferir sus compras según su preferencia, Por ejemplo, "la gerente de Marketing de Location World, de 27 años, logró financiar su maestría virtual en España gracias a un crédito diferido en 9 cuotas. La única posibilidad de pagar sus estudios era a través de una tarjeta de crédito, explicó, del mismo modo que miles de bienes y servicios que se comercializan en Internet. El comercio electrónico impulsa el uso de tarjetas de crédito, que son la mayoría de veces la única opción de pago" [6] Las personas que usan tarjetas de crédito, en su mayoría no toman las medidas necesarias cuando hacen uso de su tarjeta y no existen medios que se encarguen de alertar a los tarjetahabientes de los diferentes tipos de fraudes de los cuales pueden ser víctimas. El decir que la responsabilidad es solo de la Institución Financiera no sería justo ya que a pesar de que no

[6] Diario el Telégrafo. (Diciembre de 2013). Obtenido de http://www.telegrafo.com.ec/economia/item/3-151-887-tarjetas-de-credito-hay-en-ecuador.html

cuentan con software para alertar un posible fraude y con estrategias eficaces para reducir los riesgos de fraude, los tarjetahabientes deben estar al día de cada técnica de fraude que aparece y aprender a protegerse de dichos fraudes que en ocasiones son en línea.

### 1.1.2 CAUSAS Y CONSECUENCIAS

Una de las principales causas de fraudes con tarjetas de crédito en Instituciones Financieras se debe a la vulnerabilidad en sus sistemas informáticos. Los recursos informáticos que las Instituciones financieras buscan proteger y mantener seguras siempre son los elementos principales de su sistema que podemos clasificar como:

1).- Hardware
2).- Software
3).- Datos.

Los tres elementos manejan una simbiosis, es decir, los DATOS se encuentran almacenados en el HARDWARE y son procesados por SOFTWARE.

En el caso del HARDWARE, encontramos la manipulación de los cajeros automáticos, esta modalidad de delito consiste en ubicar un artefacto en la ranura lectora del ATM[7], mismo que copia los datos de las tarjetas, para posteriormente ser copiadas en una tarjeta falsa, además puede existir una cámara en la parte superior, con la finalidad de que se grabe el password de las tarjetas ingresados por el mismo usuario. Una vez comprometido el hardware de esta manera se procede a extraer dinero.

En el caso de SOFTWARE, nos referimos una vez más en los cajeros automáticos (ATM), para hacer referencia a los virus que afectan el software del mismo. Podemos mencionar el troyano PLOUTUS, que si bien es cierto

[7] Automatic Transaction Machine

no es un virus que ataque directamente a los usuarios, pero si es capaz de vaciar un cajero automático. Esto nos da la certeza de que existen vulnerabilidades en el software de los cajeros automáticos.

"Kaspersky Lab será la primera compañía de seguridad en América Latina en proveer una solución especializada para proteger a los terminales de pago y cajeros automáticos de una de las más grandes cooperativas financieras y de crédito del Ecuador. La protección está dirigida a una defensa confiable contra amenazas conocidas, ataques dirigidos y la amenaza del "día cero"."[8]

### 1.1.3 DELIMITACIÓN DEL PROBLEMA

Abarcaremos los diferentes tipos de fraudes de tarjetas de crédito: Pishing, Phaming, Malware, Skimming, etc. así como el nivel de información existente para la concientización del buen uso de las tarjetas de crédito y débito y la prevención que se debe de tener para evitar caer en estas estafas.

## 1.2 FORMULACIÒN DEL PROBLEMA

¿Cómo ayudar a prevenir a las instituciones financieras y a los tarjetahabientes del Ecuador que sean víctimas de operaciones fraudulentas para evitar pérdidas?

[8] Kaspersky Lab. (Agosto 2013). Obtenido de http://latam.kaspersky.com/mx/sobre-kaspersky/centro-de-prensa/comunicados-de-prensa/kaspersky-lab-y-safensoft-proteger%C3%A1n-cajeros-

## 1.3 EVALUACIÒN DEL PROBLEMA

**CLARO:**

El uso de las tarjetas de crédito es parte de la inclusión financiera que propone el gobierno, los delitos informáticos con el uso de las mismas es un problema que se intensifica y los ecuatorianos viven día a día.

**FACTIBLE:**

La Superintendencia de Bancos y Seguros en una campaña de concientización en conjunto con las instituciones financieras pueden disminuir los casos que se denuncian.

**CONCRETO:**

Es una realidad que se vive y se debe prevenir, se llevará un lenguaje sencillo y preciso para un entendimiento y concientización real por parte del lector.

**EVIDENTE:**

Los casos sobre fraude de tarjetas de crédito y débito son denunciados y son muy comunes en el país, es un problema claro que causa pérdidas de millones al año según estadísticas.

## 1.4 OBJETIVOS

### 1.4.1 OBJETIVO GENERAL

Proporcionar una serie de medidas de prevención contra el fraude de tarjetas de crédito y débito que logren ser aplicadas por las Instituciones Financieras y tarjetahabientes, a su vez tratar de conseguir mediante

razonamientos que el tarjetahabiente cambie su idea acerca de lo que implica ser víctima de un fraude.

### 1.4.2 OBJETIVOS ESPECÍFICOS

- Entender la naturaleza y causas de fraude con tarjetas de crédito y débito, las características y perfil del defraudador;
- Identificar los diferentes tipos de fraude y que técnica prefieren aplicar los delincuentes digitales;
- Conocer el índice de crecimiento de operaciones fraudulentas con tarjeta de crédito y débito en donde los afectados han sido los tarjetahabientes de la ciudad de Guayaquil de los últimos 3 años y realizar el correspondiente análisis de los datos obtenidos, y;
- Brindar metodología de prevención y disuasión del fraude estableciendo medidas de control para las instituciones financieras y tarjetahabientes para que logren minimizar los riesgos de pérdida económica.

## 1.5 JUSTIFICACIÓN E IMPORTANCIA

En el Ecuador de acuerdo a los datos actualizados por la Superintendencia de Bancos y Seguros al mes de Junio de 2013, existe 1.9 millones de tarjetahabientes quienes registran como usuarios principales pero desde este usuario principal se desprende el 3.2 millones de tarjetas de créditos emitidas; de las cuales el 85% (es decir 2,672,880) son tarjetas principales. La diferencia (479,007 tarjetas) corresponde tarjetas adicionales.

Aquellos que tienen en su poder una tarjeta de crédito pueden ser víctimas de algún tipo de fraude, por lo que se pretende en este estudio analizar los diferentes tipos de fraudes o crímenes informáticos que podrían

existir dentro de operaciones con tarjeta de crédito y débito, para prevenir a las Instituciones Financieras y disuadir a los tarjetahabientes de dichos riesgos, ya que según informe de la Superintendencia de Bancos y Seguros la cifras de denuncias por fraudes con tarjetas de crédito y débito son las siguientes:

**Tabla 1: " Número de Denuncias por Fraudes con Tarjetas de Crédito y Débito"**

| AÑOS | DENUNCIAS EN LA SUPER DE BANCOS |
|---|---|
| **2011** | 109 |
| **2012** | 244 |
| **2013** | 697 |

**Fuente**: Superintendencia de Bancos y Seguros

Por este motivo se crea la necesidad de brindar al tarjetahabiente y a las Instituciones Financieras medidas que sean posibles de aplicar y que les permita minimizar el riesgo de fraude para evitar las grandes pérdidas económicas ya que hoy en día el defraudador sabe cómo ejecutar su actividad de la forma más sigilosa posible.

# CAPÍTULO II

# MARCO TEÓRICO

## 2.1 ANTECEDENTES DEL ESTUDIO

Las instituciones financieras del país no cuentan con óptimos programas antifraude para evitar las grandes pérdidas que pueden originarse al ser víctimas de los grandes delincuentes digitales o “hackers”, inclusive este tema debe ser de gran interés para los propietarios de las diferentes tipos de tarjetas de crédito que existen en el país, ya que deben comenzar aplicar medidas estratégicas para obstruir la participación de los defraudadores.

Ecuador no ha estado preparado tecnológicamente para combatir el fraude informático ya que los delincuentes digitales han podido tener acceso hasta las cuentas del estado y desviar fondos como ocurrió en el MAE (Ministerio de Ambiente) en donde el desvío de fondos alcanzó los 7´600.798 dólares.[9] El crecimiento del uso de las tarjetas de crédito y débito en el Ecuador, la inclusión financiera nos hace pensar que este problema se intensificará a medida que pasen los años.

Planteamos como objetivo establecer medidas de control en contra del fraude en tarjetas de crédito y débito para que sean aplicadas por las Instituciones Financieras y tarjetahabientes que constantemente son víctimas de este acto ilícito.

[9] Ministerio del Ambiente: Obtenido del “www.ambiente.gob.ec”

## 2.2 MARCO CONCEPTUAL

Durante el proyecto de investigación se mencionan los siguientes términos, los cuales consideramos pertinentes conocer en el presente trabajo de investigación:

**SAS. -** Statement on Auditing Standards.

**NIA.-** Norma Internacional de Auditoría.

**Fraude.-** "Es el acto intencional llevado a cabo por una persona o más personas de la parte gerencial u operacional de la organización" según Statement on Auditing Standards 99

El fraude puede involucrar entre otros:

- La manipulación, falsificación o alteración de registros contables o documentos.
- La malversación o distracción de activos.
- Aplicar mal intencionalmente las normas contables.

> Según NIA 240 es "un acto intencionado realizado por una o más personas de la dirección, los responsables del gobierno de la entidad, los empleados o terceros, que conlleve la utilización del engaño con el fin de conseguir una ventaja injusta o ilegal"

**Error.-** se refiere a equivocaciones no mal intencionadas, como aplicar erróneamente alguna Norma.

**Actos ilegales.-** es definido como un acto u omisión que viola una ley, norma o reglamento.

**Colusión.-** Es un convenio u contrato realizado ente dos o más personas hecho de forma fraudulenta con el objetivo de engañar y perjudicar a alguien.

**Prevención.-** Medida o disposición que se toma de forma anticipada para evitar riesgo o que suceda cualquier tipo de anomalía o problema.

**Disuasión.-** Capacidad de conseguir mediante razonamientos que alguien cambie su manera de actuar, pensar o sentir.

**Tarjetahabiente.-** es aquella persona titular o tenedor de una tarjeta de crédito y débito.

**Cuota o Pago mínimo**: Es el valor correspondiente a la tasa nominal rotativa del mercado. Este valor es calculado por el Banco con relación a la deuda que se mantenga con la institución financiera, el cual debe ser cancelado en una fecha máxima de pago. Cabe indicar que si se paga el mínimo en cada periodo el valor de los intereses se incrementará.

**Intereses:** Es el valor calculado de manera mensual sobre los consumos realizados por el tarjetahabiente hasta el corte de la tarjeta.

**Beneficios Adicionales:** Los Beneficios adicionales dependerán de la entidad financiera emisora de la tarjeta de crédito, algunas tarjetas de crédito tienen beneficios adicionales como seguros para viajes o cobertura nacional, entre otros.

**Cupo:** Es el valor autorizado por la entidad financiera para realizar consumos. Este valor dependerá del análisis de riesgo realizado por la institución emisora.

**Corte:** La fecha de corte del Estado de Cuenta dependerá de la Institución Financiera emisora. La fecha es al mes siguiente de los consumos realizados a la fecha de corte.

**Saldo:** Es el valor total adeudado del tarjetahabiente, incluido los intereses del crédito.

## 2.3 MARCO LEGAL

La Superintendencia de Bancos y Seguros bajo resoluciones norma a las instituciones financieras sobre el correcto uso de canales electrónicos. Como manifiesta PHIL WILLIAMS Profesor de Estudios de Seguridad Internacional, Universidad de Pittsburgh, ”Es necesario contar no solo con leyes e instrumentos eficaces y compatibles que permitan una cooperación idónea entre los estados para luchar contra la Delincuencia Informática, sino también con la infraestructura tanto técnica como con el recurso humano calificado para hacerle frente a este nuevo tipo de delitos transnacionales” [10] ( WILLIAMS PHIL, "Crimen Organizado y Cibernético, sinergias,endencias y respuestas").

En el Ecuador el incremento de los delincuentes digitales dio como resultado la creación de Departamento de Investigación y Análisis Forense de la Fiscalía General del Estado mediante acuerdo en el año 2008. El mantener una unidad de inteligencia especializada para los delincuentes digitales en el Ecuador es el primer escalón hacia un tratamiento real del problema, esta unidad busca asegurarles a las víctimas que sus derechos se encuentran por encima de cualquier fraude, además busca responsables que mediante juicios penales paguen condena y limpiar el espacio cubierto por los delincuentes digitales.

### 2.3.1 TIPIFICACIÓN DE DELITOS INFORMÁTICOS EN EL CÓDIGO PENAL ECUATORIANO

El 10 de agosto del 2014 entró en vigencia el nuevo Código Orgánico Integral Penal en donde en los artículos 229 y 234 se tipifican los delitos contra la seguridad de los sistemas de información[11], entre ellos tenemos:

[10] WILLIAMS PHIL, "Crimen Organizado y Cibernético, sinergias,endencias y respuestas". (s.f.). Obtenido de http://www.oas.org/juridico/spanish/cyb_ecu_plan_operativo.pdf

[11] Diario Hoy. Agosto 2014. “ Hasta 10 años por revelar información confidencial”- COIP

- **Revelación ilegal de base de datos**

En el art. 229 del nuevo Código Orgánico Integral Penal en cuanto a la revelación ilegal de base de datos indica lo siguiente:

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

- **Transferencia electrónica por activo patrimonial**

En el art. 231 del nuevo Código Orgánico Integral Penal en cuanto a la transferencia electrónica por activo patrimonial indica lo siguiente:

*(…) La persona que, con ánimo de lucro, altere, manipule o modifique el funcionamiento de programa o sistema informático o telemático o mensaje de datos, para procurarse la transferencia o apropiación no consentida de un activo patrimonial de otra persona en perjuicio de esta o de un tercero, será sancionada con pena privativa de libertad de tres a cinco años. Con igual pena, será sancionada la persona que facilite o proporcione datos de su cuenta bancaria con la intención de obtener, recibir o captar de forma ilegítima un activo patrimonial a través de una transferencia electrónica producto de este delito para sí mismo o para otra persona.*

- **Interceptación  ilegal de datos**

En el art. 230 del nuevo Código Orgánico Integral Penal en cuanto a la intercepción ilegal de datos indica lo siguiente:

*(…)Será sancionada con pena privativa de libertad de tres a cinco años:*

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

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

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

4. *La persona que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior.*

- **Ataque  a la integridad de sistemas informáticos**

En el art. 232 del nuevo Código Orgánico Integral Penal en cuanto al ataque a la integridad de sistemas informáticos indica lo siguiente:

*(…)La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años. Con igual pena será sancionada la persona que:*

1. *Diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados a causar los efectos señalados en el primer inciso de este artículo.*
2. *Destruya o altere sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general. Si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana, la pena será de cinco a siete años de privación de libertad.*

- **Los delitos contra la información pública reservada**

En el art. 233 del nuevo Código Orgánico Integral Penal en cuanto a los delitos sobre la información pública reservada indica lo siguiente:

*(…)La persona que destruya o inutilice información clasificada de conformidad con la Ley, será sancionada con pena privativa de libertad de cinco a siete años. La o el servidor público que, utilizando cualquier medio electrónico o informático, obtenga este tipo de información, será sancionado con pena privativa de libertad de tres a cinco años.*

*Cuando se trate de información reservada, cuya revelación pueda comprometer gravemente la seguridad del Estado, la o el servidor público encargado de la custodia o utilización legítima de la información que sin la autorización correspondiente revele dicha información, será sancionado con pena privativa de libertad de siete a diez años y la inhabilitación para ejercer*

*un cargo o función pública por seis meses, siempre que no se configure otra infracción de mayor gravedad.*

- **Acceso no consentido a un sistema informático**

En el art. 234 del nuevo Código Orgánico Integral Penal en cuanto a los delitos sobre la información pública reservada indica lo siguiente:

*(…)La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o re direccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años*

La nueva tipificación pretende crear un marco legal que disminuya y erradique los delitos informáticos, como observamos los artículos de delitos informáticos en el COIP se encuentran claramente detallados con sus correspondientes sanciones, es de mucha importancia y ayuda para las Instituciones Financieras y tarjetahabientes ya que los defraudadores serán sancionados por las autoridades correspondientes.

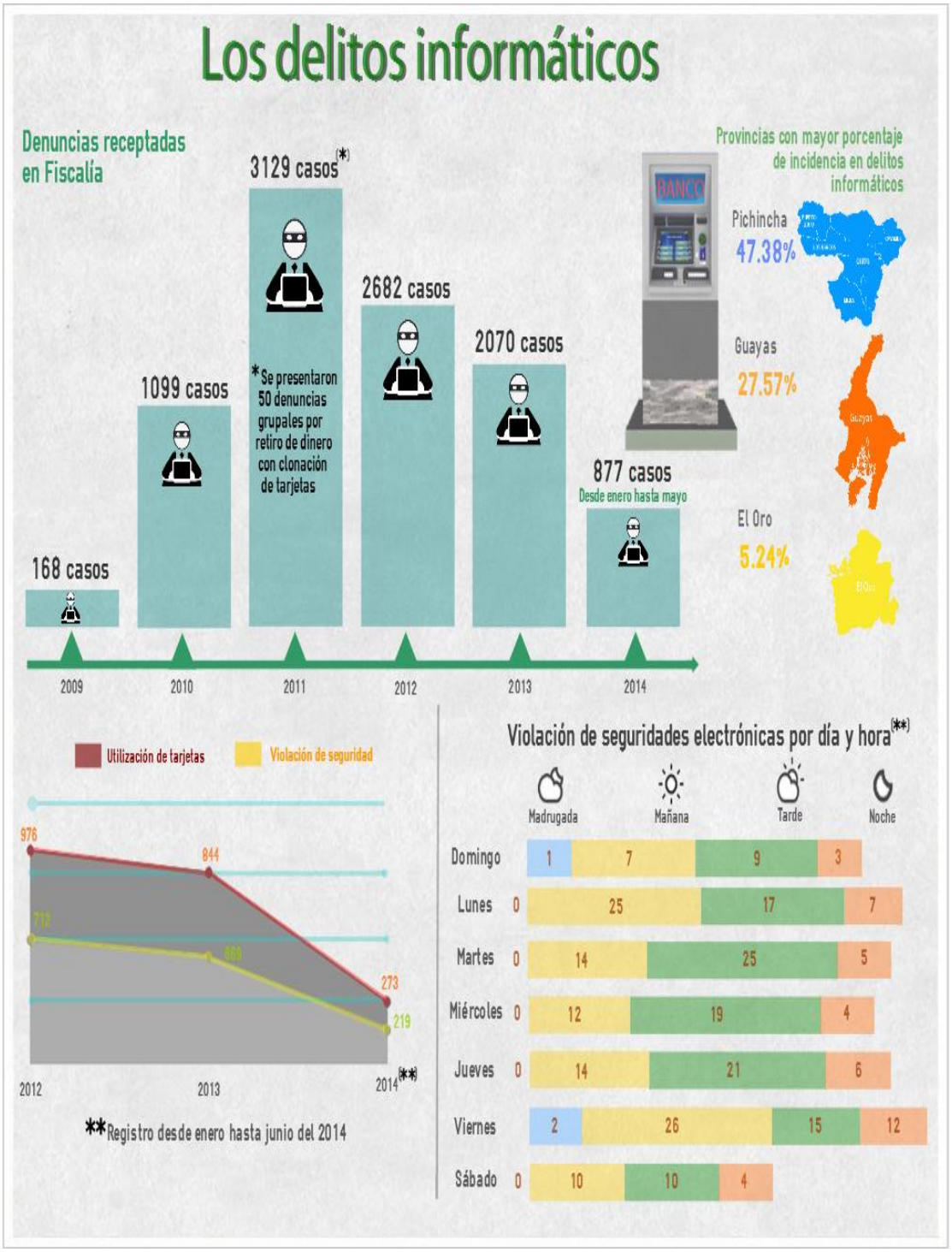
Cuando es realizada una denuncia en la Fiscalía General del Estado por uno de estos delitos informáticos en el que figura el fraude por tarjeta de crédito y débito, que es donde se orienta ésta investigación, en primer lugar se asignara y se pone en conocimiento a un fiscal, se le y se dará por comenzada la investigación de oficio, el fiscal es responsable de solicitar la información correspondiente a la Institución Financiera mediante oficio con su rúbrica, ésta deberá entregar estados de cuentas, informes de ingresos al sistema informático de su institución y, de ser necesario videos del acceso a los cajeros automáticos para determinar la identidad del presunto defraudador.

El fiscal pondrá en conocimiento a la Unidad de Delitos Informáticos para que se realicen las pericias correspondientes.

Este tipo de fraudes suelen ser ejecutados a través de transferencias electrónicas, clonación de tarjetas o claves y al momento del realizar pagos en centros comerciales. Pero no se deja de sospechar que las transferencias ilícitas se pueden realizar con la información que existe dentro de la misma institución financiera porque para los tarjetahabientes es dudoso que no se emitan alertas a correos o su teléfono como se lo realiza en el caso de transferencias licitas, por éste motivo el banco comparte la responsabilidad con el tarjetahabiente, debido a que él también debe cuidar su forma de acceder y sus claves personales.

A continuación se presenta gráfico detallado de los delitos informáticos en Ecuador:

**Gráfico 2: " Delitos Informáticos en el Ecuador"**




**Fuente:** El ciudadano – Periódico Digital del Gobierno[12]

[12] http://www.elciudadano.gob.ec/

### 2.3.2 NORMAS DE SEGURIDAD DE LA INFORMACIÓN Y GESTIÓN DE RIESGOS

La aplicación de las normas de seguridad de la información ISO 27001 es un tema que la Superintendencia de Bancos y Seguros debe exigir a las Instituciones Financieras y Compañías emisoras de tarjetas de crédito en todos sus procesos de resguardo y protección de información, ya que es obligación de éstas entidades controladas brindarle una seguridad confiable al cliente, además deberán autoevaluar su gestión sobre los riesgos de seguridad de la información es decir que también deberán aplicar ISO 27005.

Durante el examen de valoración de su gestión deberán establecer criterios básicos, tales como: evaluación, aceptación e impacto al riesgo; luego deberá establecer un plan para tratar los riesgos identificados, definir políticas y procedimientos y finalmente monitorear los controles cada cierto tiempo, verificando que se estén cumpliendo.

La ISO 27001 y la ISO 27005 son temas cíclicos es decir una vez que termina el proceso en una primera prueba deberán seguir y evaluar nuevamente los procesos.

Debemos recordar que existen diferentes tipos de vulnerabilidades en los sistemas de información que permiten a los hackers apoderarse de las bases de datos, por este motivo el departamento de prevención de Fraude de cada Institución Financiera debe estar alerta y deben ser responsables en cumplir con las Normas ISO aunque no sean constantemente supervisados, pero si existen normas de aplicación que ayuda a mitigar los posibles riesgos que se pueden presentar hay que cumplirlas porque en las instituciones financieras existe información sensible como son: usuarios, claves de cajero, números de cuenta, direcciones, etc. y se debe cuidar y evitar el robo de dicha información aplicando Normas ISO (27001 Y 207005).

### 2.3.3 APLICACIÓN DE NORMAS PCI-DSS (Payment Card Industry Data Security Standard) EN LAS INSTITUCIONES FINANCIERAS DEL ECUADOR

PCI es una norma internacional de seguridad de datos de industria de tarjetas de pago y fue creada con el objetivo principal de "proteger los datos de los tarjetahabientes en todas las operaciones que se ejecutan en la institución, para así evitar que cualquier persona tenga acceso a la información restringida, lo cual debe ser una de los principales estrategias para mitigar que los clientes sean posibles víctimas de fraudes" (Banco de Guayaquil, 2012). Fue desarrollado por las principales asociaciones expendedoras de tarjetas de crédito globales, mismas que fundaron el PCI Security Standards Council (PCI -SSC), entre otras American Express, Discover Financial Services, JCB, MasterCard Worlwide y Visa International.

El estándar PCI-DSS está compuesto por 12 criterios agrupados en seis objetivos de control general.[13]

Construir y mantener redes seguras:

- Proteger la información del tarjetahabiente;
- Establecer programas de pruebas de vulnerabilidad;
- Implementar medidas fuertes de control de acceso;
- Monitorear y probar acceso a la red regularmente;
- Mantener políticas de seguridad de la información, y;
- Niveles de cumplimiento y proceso de validación.

Por este motivo el Banco Guayaquil indica todas las Instituciones Financieras deben aplicar "buenas prácticas de seguridad de información, para así proteger los datos sensitivos de sus clientes, como por ejemplo: número de tarjeta, fecha de vencimiento, datos de la banda magnética, entre otros" (Banco de Guayaquil, 2012).

[13] Payment Card Industry Data Security. Obtenido de: https://www.pcisecuritystandards .org/documents/pci_dss_es-la_v2.pdf

El Banco Guayaquil fue el primer banco del Ecuador en obtener la certificación de la aplicación de las normas PCI-DSS para todos sus procesos como emisor, operador y adquiriente, ésta certificación le garantiza al banco que está implementando “los máximos controles de seguridad de información de las tarjetas de crédito y de débito” (Banco de Guayaquil, 2012).

Esta institución bancaria empezó el proceso de certificación en el año 2009 para lograr implementar cada requerimiento que la norma les exigía para poder completar la certificación, que iba desde una revisión por un auditor autorizado por PCI-SSC, hasta completar un cuestionario de autoevaluación, es así que logra en el año 2011 dicha certificación y consigue incrementar su seguridad al momento de realizar sus transacciones. En Latinoamérica los plazos para el cumplimiento de normas PCI así como las penalizaciones por el incumplimiento de las mismas no son plenamente vigentes, pero en otras partes del mundo dichos plazos ya vencieron; como en Estados Unidos el plazo venció en noviembre del 2007.

“En el año 2008 RSA, la División de Seguridad de EMC (NYSE: EMC), realizó una encuesta aplicada a las empresas latinoamericanas sobre seguridad de los datos de tarjetas de créditos dentro de sus organizaciones, así como los planes que tienen para poner en práctica nuevas medidas de protección de datos”[14] (EMC Corporation)

“Casi la mitad de las empresas encuestadas en Latinoamérica (47%) conocía la norma, pero un punto porcentual más (48%) no la conocía en absoluto. De entre quienes conocen las PCI DSS: – La gran mayoría (74%) respondió que se han tomado medidas para cumplir con los requisitos, pero algunos (18%) no han tomado aún medida alguna – Más de la tercera parte (35%) se encontraba por arriba de la curva y ya está en situación de cumplimiento o espera estarlo en los próximos seis meses – La cuarta parte (25%) espera cumplir en el transcurso de seis a doce meses, mientras que

[12] EMC Corporation. (Febrero 2014) Obtenido de http://spain.emc.com/about/news/press/20140226-01.htm

una cifra ligeramente menor (17%) espera hacerlo en uno a dos años. Un pequeño grupo (16%) no pudo indicar un plazo de cumplimiento concreto" [15]. (GRUPO ING - Economía fácil, s.f.)

## 2.4 RESEÑA HISTORICA DE LAS TARJETAS DE CRÉDITO

Si hablamos del origen de las tarjetas de crédito, podemos mencionar dos etapas en las que tuvieron más repunte en la historia. En el siglo XX, la empresa Western Union creó una pequeña placa de metal únicamente para sus clientes preferenciales, este objeto les permitía identificarse como usuarios y obtener un trato especial, además de líneas de crédito sin cargos.

"Hasta finales de los años 40, una gran cantidad de empresas comenzaron a emitir sus propias tarjetas de crédito, pero que solo tenían validez en sus establecimientos, como un método para atraer clientes y facilitar las compras a través del crédito. En 1924, por ejemplo, la General Petroleum Corporation emite su primer tarjeta de crédito para la compra de gasolina, y en 1929, la American Telephone & Telegraph emite la tarjeta Bell" (GRUPO ING - Economía fácil)

"Sin embargo, la primera tarjeta de crédito tal y como la conocemos hoy en día, es decir, una tarjeta con la que podemos pagar cómodamente en múltiples establecimientos sin tener que cargar con la tarjeta de cada uno de ellos, no surgió hasta 1949, fruto de una combinación de casualidades en un restaurante de Nueva York, en concreto el Major's Cabin Grill" (GRUPO ING - Economía fácil)

"Al principio la Diners' Club (literalmente, club de cenadores) tuvo poca repercusión. Sólo 14 restaurantes neoyorquinos se adhirieron, y a principios de 1950 la tarjeta únicamente la poseían unas 200 personas, la mayoría de amigos y conocidos. Sin embargo, a finales de ese mismo año, más de 20,000 personas la utilizaban y el número de establecimientos que la aceptaban crecía exponencialmente" (GRUPO ING - Economía fácil)

[15] Grupo ING (s.f.). Obtenido de. http://www.ennaranja.com/economia-facil/origen-e-historia-de-las-tarjetas-de-credito

“La Diners’ Club fue la primera tarjeta de crédito como las actuales. Su modelo de negocio se basaba en hacer de intermediario entre el establecimiento y el comprador, cobrando una comisión por transacción al primero y una comisión de mantenimiento (3 dólares anuales en 1951) al segundo, a cambio de un pago aplazado a final de mes sin intereses” (GRUPO ING - Economía fácil)

## 2.4.1 EVOLUCIÓN DE LAS TARJETAS DE CRÉDITO

“Tras el éxito de la Diners’ Club, las entidades financieras de todo el país empezaron a emitir tarjetas de crédito que se podían utilizar en múltiples establecimientos. El primero fue el Franklin National Bank de Long Island, en Nueva York, en 1951, aunque el año clave para la eclosión de las tarjetas de crédito fue 1958, año en el que se lanzaron la tarjeta American Express, de la compañía de servicios financieros homónima, que ya emitía giros y cheques de viaje, y Bank AmeriCard, la tarjeta de crédito del Bank of América, el banco más importante del estado de California” (GRUPO ING - Economía fácil)

“El éxito fue tal, que en 1965 el Bank of América llegó a acuerdos con grupos de bancos de fuera de California para que emitieran Bank Americard, desistiendo estos a sus propios sistemas. Sin embargo, otro grupo de bancos de todo el país se unieron para formar Master Charge, que luego pasaría a llamarse MasterCard, y para finales de la década, más de 1,400 bancos ofrecían una u otra tarjeta en Estados Unidos, y también había dado el salto a Europa” [16] (GRUPO ING - Economía fácil)

## 2.4.2 TARJETAS CON CHIP INTELIGENTE

Como parte de los nuevos controles a emplear por parte de las Instituciones Financieras está la incorporación de un chip en las tarjetas de crédito, según lo establecido por la Junta Bancaria y la Superintendencia de

[16] Grupo ING (s.f.). Obtenido de. http://www.ennaranja.com/economia-facil/origen-e-historia-de-las-tarjetas-de-credito

Bancos y Seguros en abril de 2012. “Este dispositivo incluirá una serie de preguntas adicionales al ingreso de la clave y un nuevo sistema informático. El objetivo es evitar la clonación y robos en los cajeros automáticos”[17]

A continuación se muestra imagen obtenida del Diario El Telégrafo, en su publicación del 12 Septiembre 2013, en el que se muestra el chip inteligente que incluirán las tarjetas de crédito y débito.

**Gráfico 3: "Tarjetas con Chip"**


**Fuente:** El Telégrafo

Las posibilidades de que tarjetas de crédito y débito sean clonadas o vulneradas se reducirán con el cambio de la banda magnética por la tecnología chip inteligente, brindará mayor seguridad a las transacciones mediante los diferentes medios de pago existente para tarjetas. (Diario el Telégrafo, 2013)

[17] Diario el Telégrafo. (s.f.). Obtenido de http://www.telegrafo.com.ec/economia/item/tarjetas-de-credito-deben-llevar-chip.html

Además se han incluido mecanismos de monitoreo y actualización de los niveles de seguridad en hardware y software; sistemas de protección contra intrusos que protejan el software de los cajeros; encriptación del envío de información confidencial mediante correo electrónico; detección de intentos de alterar códigos; emisión de alarmas para el bloqueo del canal electrónico; revisión oportuna por parte del personal técnico y otros.[18]

Sin embargo, en resolución 2358 de la Junta Bancaria de octubre del 2012 se fijó al 31 de marzo del 2013 como nuevo plazo para aplicar las normas sobre riesgos operativos. Y en su última resolución (2745), del 10 de enero pasado, se determinó que hasta diciembre de este año los cajeros automáticos deben procesar la información de las tarjetas inteligentes.

La Policía Nacional, reportó que aproximadamente 800 asaltos en cajeros automáticos durante el año 2012, es a partir de este antecedente por lo cual la Superintendencia de Bancos mediante resolución optó por agregarle seguridades a las tarjetas y exigir a las instituciones financieras que todas sus tarjetas tengan chip.

Los bancos Guayaquil, Bolivariano y Produbanco empezaron a implementar los chips en el 2012, sin embargo, es un proceso que tomará mucho tiempo, según César Robalino, director ejecutivo de la Asociación de Bancos Privados de Ecuador (ABPE) (Diario el Telégrafo, 2013).

Se ha considerado para la inclusión de las tarjetas de crédito y débito con chip el recurso humano y tecnológico que se requerirá. Es por esta razón que la Superintendencia de Bancos y Seguros en su resolución fijo los tiempos límite para el cambio de los dispositivos externos en los establecimientos, cajeros automáticos inclusive las mismas tarjetas de crédito y débito. Los entes de control mantienen total conocimiento del impacto en los procesos del sistema en los bancos.

[18] Diario El Universo. (Febrero 2014). Obtenido de: http://www.eluniverso.com/noticias /2014/02/06/ nota/2143556/hasta-2015-se-extendio-plazo-tarjetas-chip

Según la ABPE, "será necesario la actualización, pruebas y certificaciones de más de 3,250 cajeros automáticos (Atm), 33,000 dispositivos conocidos como Puntos de Venta o POS (Point of Sale), sistemas informáticos de las empresas locales operadoras de redes interbancarias, sistemas especializados de todas las entidades bancarias, fabricación y personalización de 4 millones de nuevas tarjetas con chip para reemplazar las correspondientes de banda magnética"[18]

"Mientras dure el proceso de migración a tarjetas con chip, las entidades bancarias mantendrán y fortalecerán los esquemas de seguridades en sus sistemas y sus redes de cajeros automáticos y puntos de venta para proteger a los clientes", recalcó (Robalio, 2012). En el ámbito internacional los entendidos en la materia mencionan que el nivel de seguridad para las tarjetas con tecnología chip durará aproximadamente 10 años; esto durante el tiempo que deficiencia de información y documentos en el sistema.

Cuando se ingrese la tarjeta en el cajero automático, ya no solo se deberá digitar la clave, si no que el usuario también tendrá que responder de una a tres preguntas. Por su parte el Banco deberá registrar estas respuestas en la base de datos. "De esta forma se quiere reducir las posibilidades de fraude en los cajeros, ya que actualmente la clave no es suficiente para garantizar la seguridad de los depositantes al momento de realizar un retiro, comentó Pablo Córdova, titular del Comité de Seguridad Bancaria de la ABPE. La implementación de estos chips constituye una novedad interesante en el sector financiero"[19]

Miguel Carrillo, gerente de Negocios de PacifiCard, empresa emisora de las tarjetas de crédito Visa y Mastercard, informó que en el último trimestre del año 2013 arrancarían con los cambios en el sistema y así entregar el dispositivo a su portafolio de clientes. "Actualmente usted va a un comercio pasa la banda magnética, pero no lee el chip. Ahora sí lo va a leer y dará una mayor seguridad a los clientes, dijo Carrillo. Carrillo indicó

[19] Diario el Telégrafo. (Agosto 2014). Obtenido de http://www.telegrafo.com.ec/economia /item/tarjetas-de-credito-deben-llevar-chip.html

que el mantiene en Pacificard alrededor de 450,000 clientes en crédito y el débito aproximadamente 370,000”[18]

El presidente del Banco Internacional, Enrique Beltrán, en una entrevista indicó “que su entidad que hace un 60% de sus transacciones a través de canales electrónicos, mencionó que es evidente que la industria del fraude crece y el sistema financiero está preocupado por tener los controles adecuados y proteger a los clientes”. (Diario el Telégrafo, 2013)

Un estudio presentado por GMS y Kaspersky Lab, que es una empresa especializada en productos para la seguridad informática a nivel mundial, demostró que entre 2009 y 2010 en Ecuador se incrementó a 360% el crimen cibernético.

Según el estudio presentado en 2011, el 94% de los programas de código malicioso hospedados en los servidores web del Ecuador se encuentra en la provincia de Pichincha**.**

## 2.5 ¿QUÉ ES UNA TARJETA DE DÉBITO?

Una tarjeta de débito se obtiene de forma muy sencilla su emisión empieza a partir de la apertura de una cuenta ahorros o corriente. Este tipo de tarjeta le permite al usuario realizar transacciones más sencillas, de acuerdo al monto con el que cuente en su cuenta bancaria. En la actualidad las tarjetas de débito en su mayoría ya cuentan con chip inteligente. Con la de débito únicamente se podrá sacar dinero en un cajero, o pagar un producto si se tiene efectivo en la cuenta asociada.

A continuación se presenta gráfico de una tarjeta de débito, obtenida del Interbank Perú.

**Gráfico 4: "Tarjeta de Débito"**


**Fuente:** Interbank Perú.

## 2.6 ¿QUÉ ES UNA TARJETA DE CRÉDITO?

"Una tarjeta de crédito una rectángulo de plástico numerado, que presenta una banda magnética o un microchip, y que permite realizar compras que se pagan a futuro. Para solicitar una tarjeta de este tipo, es necesario dirigirse a una institución financiera o entidad bancaria, la cual solicitará al interesado una serie de documentos y garantías para asegurarse de que se trata de una persona solvente y capaz de cumplir con sus potenciales obligaciones de pago" (Definición de: Tarjeta de Crédito)[20]

Las franquicias internacionales para los emisores de tarjeta de crédito son: Visa, MasterCard, y American Express.

En el Ecuador solo las instituciones financieras y compañías emisoras o administradores de tarjeta de crédito son los responsables de emitirla ya que la Superintendencia de Bancos y Seguro regula el sistema de tarjeta de crédito y sancionara a quienes infrinja esa disposición conforme lo que está escrito en el art. 121 d la Ley General de Instituciones del Sistema Financiero.[21]

Hace un tiempo atrás era muy común ver a las empresas con sus propias líneas de tarjeta de crédito, esto con el fin de incentivar el consumo únicamente en el establecimiento emisor.

Los datos solicitados por las entidades financieras son las siguientes:

[20] Definición de. Obtenido de. http://definicion.de/tarjeta-de-credito/
[21] Superintendencia de Bancos y Seguros. (Julio 2012). Resolución No. JB-2012-2225.

• Datos sobre las fuentes de ingreso y actividad económica;
• Referencias financieras;
• Referencias de tarjetas de crédito;
• Referencias comerciales;
• Información de personas o familiares que no vivan con el solicitante;
• Referencias patrimoniales, y;
• Información sobre la situación financiera (ingresos y egresos).

A continuación se presenta gráfico de una tarjeta de crédito:

**Gráfico 5: "Tarjeta de Crédito"**


**Fuente:** Diario 20 Minutos México.

## 2.6.1 CLASES DE TARJETAS DE CRÉDITO

Existen varias clases de tarjetas de crédito, estas tarjetas son emitidas por entidades bancarias y sirven para comprar, como para obtener dinero en efectivo.

- **Tarjeta de crédito clásica:** es la más común, las Visa, MasterCard o American Express cualquier persona la tiene. Desde el momento de la compra el crédito otorgado se le cobrará al usuario al mes vencido, es decir, todo el dinero desembolsado durante ese mes se reporta al siguiente mes.

- **Tarjetas oro y platino:** este tipo de tarjetas está dirigida a los clientes con un nivel de ingresos elevado, por esta razón el cupo que se les otorga a esta clase de tarjetas es mayor. Estas tarjetas suelen tener beneficios asociados como programas de puntos, cash back, y promociones con establecimientos.

- **Tarjetas de puntos:** se trata de tarjetas de crédito que ofrecen ventajas adicionales como programas de puntos para obtener viajes gratis, ahorrar en gasolina, descuentos en tiendas.

## 2.6.2 CLASIFICACIÓN DE LA TARJETA DE CRÉDITO SEGÚN EL TITULAR

- **Tarjetas personales**. Este tipo de tarjetas pueden ser utilizadas única y exclusivamente por la persona el titular, es decir la persona con el nombre en relieve en la tarjeta. En el momento que el adquiriente de necesite realizar una compra, además de portar su tarjeta deberá mostrar un documento de identificación que demuestre su identidad.

- **Tarjetas corporativas o empresariales**. El objetivo de las tarjetas corporativas y empresariales es mantener control de los gastos de la empresa en una sola cuenta. Estas tarjetas son pensadas para personas jurídicas; pueden ser utilizadas por la persona responsable de los gastos en la empresa sin ninguna dificultad y al mes siguiente se reportará en un estado de cuenta los gastos del mes.

  Otra de las opciones para las empresas es contar con varias tarjetas para sus empleados. Cuando ellos realicen compras con la tarjeta y el estado de cuentas pasa a la empresa y la empresa vía rol de pagos realiza las deducciones correspondientes de los consumos, en otros casos la empresa puede coordinar con el empleado el plan de pagos con la posibilidad económica del trabajador.

  Además, estas tarjetas pueden limitarse a financiar compras institucionales a distintos proveedores ya sea de servicios como de mercadería. Son tarjetas especialmente emitidas con el fin de ordenar aún más los gastos de la empresa.

### 2.6.3 CLASIFICACIÓN DE LA TARJETA DE CRÉDITO POR SU NATURALEZA Y SU OBJETIVO FINAL

Existen diferentes tipos de clasificaciones para las tarjetas de crédito en este caso las distinguiremos por su naturaleza y su objetivo final. El primer grupo de estas se dividen en locales e internacionales, las cuales dependen del alcance que posean en cuanto a su capacidad de realizar transacciones.

- **Tarjetas de Crédito Internacionales:** Las tarjetas internacionales te permiten realizar compras en cualquier parte de mundo

- **Tarjetas de Crédito Convencionales:** le permite al usuario de la tarjeta pagar los consumos realizados a través de ella, el tarjetahabiente decide el plazo a pagar según como la difiera. Si el monto adeudado es cancelado de forma completa al final del mes, no se cobran intereses, pero si queda un saldo pendiente a ser cancelado, se cobrará los intereses a una tasa anual preestablecida, la cual es establecida por la institución emisora.

- **Tarjetas Premier:** las posee un mercado reducido dentro del mercado total de tarjetahabientes**,** son iguales a las anteriores, pero con límites mayores de crédito, además de ciertos tipos de preferencia.

## 2.7 DEFINICIÓN DEL MERCADO FINANCIERO EN ECUADOR

El Mercado Financiero del Ecuador luego de la dolarización y el feriado bancario de 1999 se encuentra estable según declaraciones del Superintendente de Bancos y Seguros del Ecuador. El gobierno actual ha tomado medidas de control para las entidades financieras, además de control de lavado de activos y nuevos impuestos para este sector. En el país existían alrededor de 250 entidades financieras durante esa época, hoy en

día operan 74 entidades financieras divididas en 25 bancos privados, 2 bancos estatales, 7 sociedades financieras, 1 emisora de tarjeta de crédito, 35 cooperativas, 4 mutualistas.

Mediante Decreto 194 del año 2013, las cooperativas pasan al control de la Superintendencia de Economía Popular y Solidaria.

El Mercado Financiero Ecuatoriano está compuesto por un conjunto de principios y normas jurídicas que se basan en documentos especiales que permite canalizar el ahorro y la inversión de los diferentes sectores de la economía hacia otros que lo necesitan y esto ayuda a su crecimiento y desarrollo.

Las instituciones que conforman el mercado financiero del Ecuador son las que se encargan de intervenir de forma financiera entre el público y la entidad, para captar los recursos públicos a través del ahorro, para luego utilizar dichas captaciones en otras operaciones de crédito e inversión.

En el Ecuador se pretende crear una cultura bursátil como en los países desarrollados, es decir que las principales fuentes de financiamiento para las empresas sean por esta vía y no mediante Instituciones Financieras. En el Ecuador es el sector financiero el que cumple el rol de distribuir los fondos que reciben de los ahorradores entre las personas necesitadas de créditos. De esta manera se pretende mantener una economía saludable y generar confianza entre los ciudadanos para generar riquezas.

El mercado Financiero está formado por Bancos, Cooperativas de Ahorro y Crédito, Mutualistas, Sociedades Financieras y emisores de tarjetas de crédito, a continuación presentamos el porcentaje de participación por entidades:

**Tabla 2: "Participación Estimada del Mercado Financiero a Nivel Nacional"**

| Entidades | Porcentaje |
|---|---|
| **Bancos Privados** | 34% |
| **Estatales** | 3% |
| **Sociedades Financieras** | 9% |
| **Emisores Tarjetas de Crédito** | 1% |
| **Cooperativas** | 47% |
| **Mutualistas** | 5% |

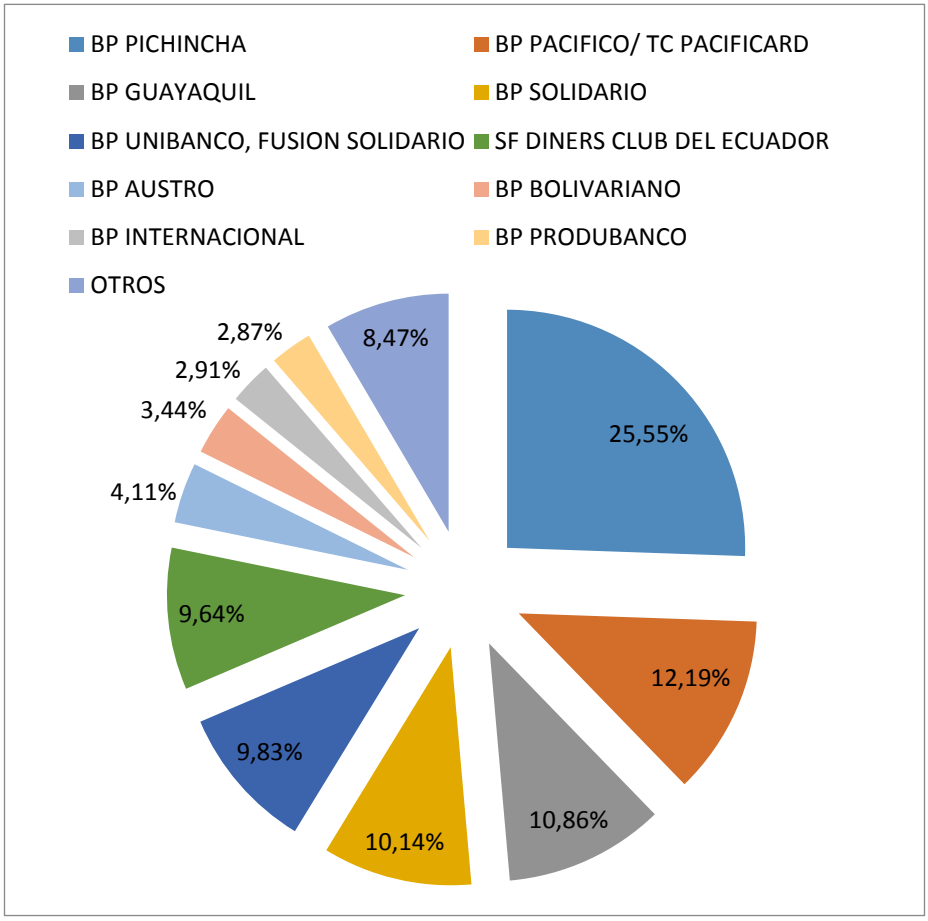
**Fuente:** Equipo editorial "Tus Finanzas"

**Elaborado por:** Autora

## 2.8 PRINCIPALES INSTITUCIONES FINANCIERAS ADMINISTRADORAS DE TARJETA DE CRÉDITO

Dentro de las principales Instituciones Financieras y compañías administradoras de tarjetas de crédito se tiene:

**Gráfico 6: "Participación de Instituciones Financieras y Emisores de Tarjetas de Crédito Autorizadas en Ecuador"**

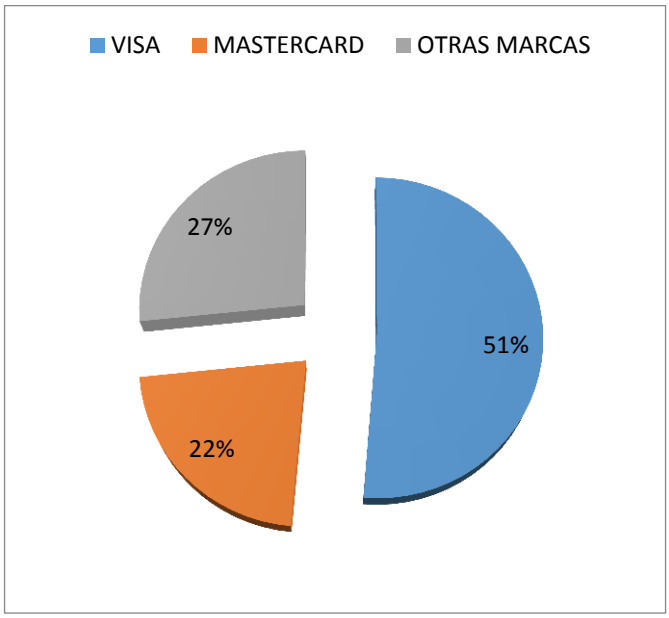



**Fuente:** Superintendencia de Bancos y Seguros
**Elaborado por:** Autoras

En este gráfico podemos observar que el Banco Pichincha es el principal emisor de tarjetas de crédito con el 25,55% de participación, seguido por Banco Pacifico/Pacificard con el 12,19%.

En cuanto a la marca de mayor circulación en el Ecuador tenemos a: Visa con el 51,37% y MasterCard con el 22,01%.

**Gráfico 7: "Marcas de Tarjetas de Crédito en el Ecuador"**

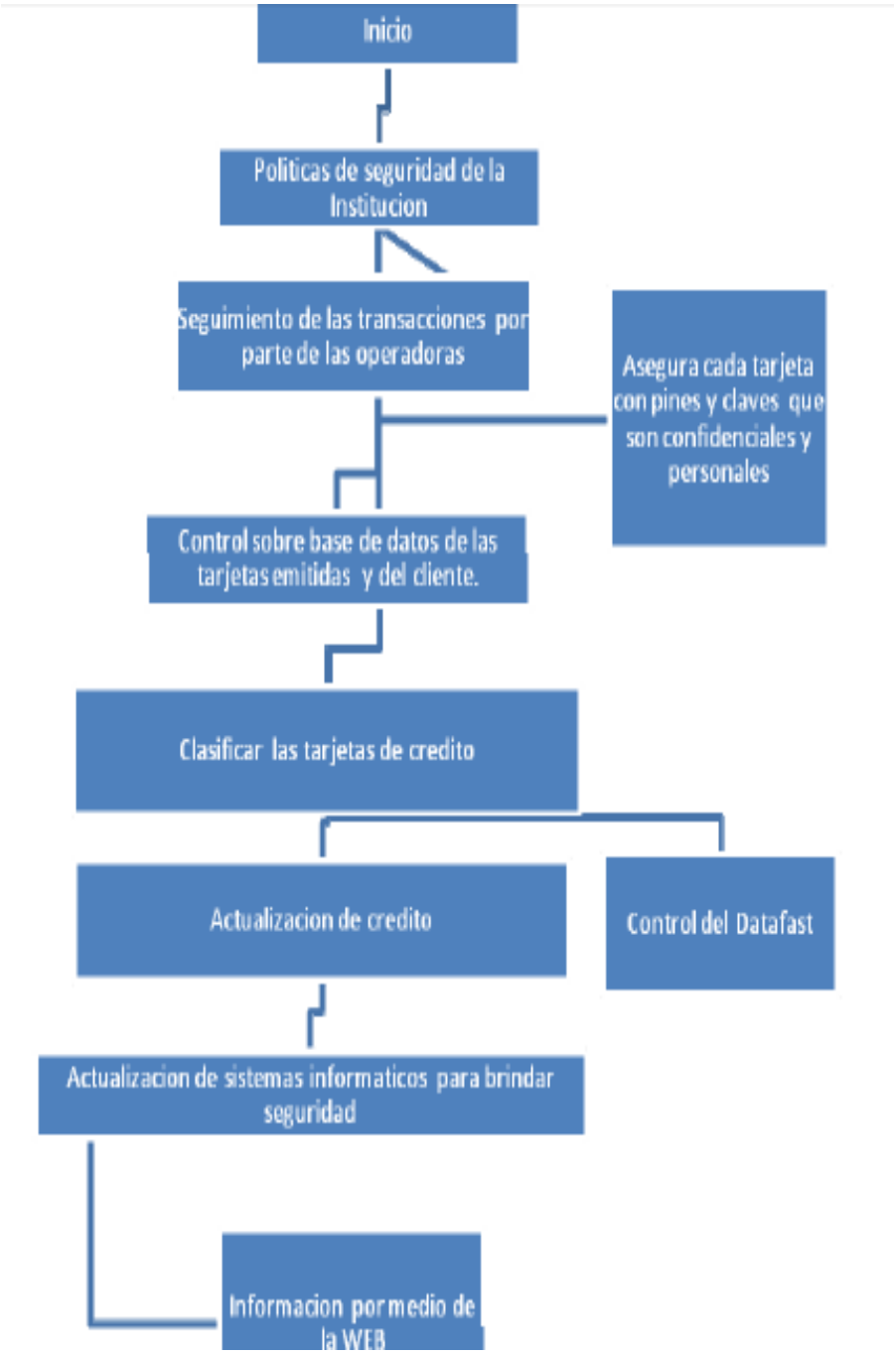



**Fuente:** Superintendencia de Bancos y Seguros
**Elaborado:** Autoras

Según resolución No. JB-2012-2151 del 26 de abril del 2012 en la que se establece los costos por servicios trimestralmente, indica: "*Que la afiliación y renovación de tarjetas de crédito no deben considerarse servicios financieros ni deben significar ingresos para los prestadores de aquellos servicios, toda vez que no constituyen el negocio financiero, el cual más bien está dado en el crédito al que se accede gracias al uso de tales tarjetas, y, por tanto la afiliación y renovación no deben cargarse al usuario financiero; además, por la afectación económica y social que aquello ha implicado en perjuicio de los usuarios*" ( Resolución No. JB-2012-2151, 2012) . Estos servicios no deben considerarse como ingresos por parte del emisor debido a que es un costo que interviene desde la primera vez que se realizó la relación comercial. Las Entidades Financiaras cobran por los costos de financiamiento de los productos que adquirimos; esto es lo único que debe de reconocerse como ingreso; además de las promociones que se establezcan con los establecimientos asociados, es por este motivo que la afiliación y renovación no deben cargarse al tarjetahabiente; inclusive el gobierno ha calificado estos costos adicionales como prejuiciosos para los ecuatorianos.

Las Instituciones y Emisoras de Tarjetas Crédito autorizadas en Ecuador tienen en aplicación los siguientes controles:

**Gráfico 8: "Flujograma de Controles Internos Existente"**



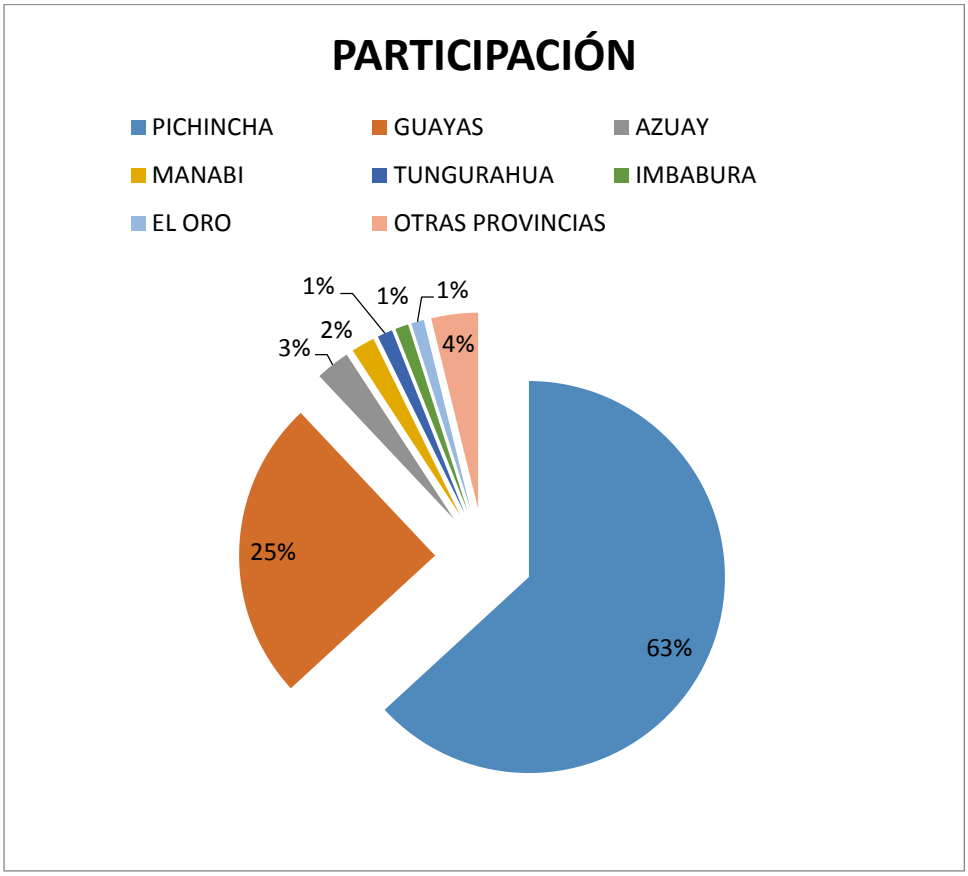

**Fuente:** Federación Latinoamericana de Bancos

## 2.9 SITUACIÓN ACTUAL DE LAS TARJETAS DE CRÉDITO EN EL ECUADOR

En el Ecuador aproximadamente hay quienes poseen seis o siete tarjetas de crédito, sin embargo la Superintendencia de Bancos y Seguros a junio del 2013 ha calculado un promedio de 1.6 tarjetas de crédito por ciudadano al Junio del 2013. Actualmente en este tipo de operaciones se concentra en un 42% del circulante en el país.

A continuación se presenta la participación por provincias de las tarjetas de crédito en el Ecuador a Diciembre del 2013.

**Gráfico 9: "Participación de las Tarjetas de Crédito por Provincia"**




**Fuente:** Superintendencia de Bancos y Seguros

**Elaborado:** Autoras

**Tabla 3: "Participación Tarjetas de Crédito por Provincia"**

| PROVINCIAS | PARTICIPACIÓN |
|---|---|
| PICHINCHA | 63,16% |
| GUAYAS | 24,81% |
| AZUAY | 2,82% |
| MANABI | 1,93% |
| TUNGURAHUA | 1,26% |
| IMBABURA | 1,10% |
| EL ORO | 1,05% |
| OTRAS PROVINCIAS | 3,85% |

**Fuente:** Superintendencia de Bancos y Seguros

**Elaborado:** Autoras

En el gráfico anterior podemos evidenciar que las dos provincias con mayor porcentaje de participación con tarjetas de crédito son: Pichincha con el 63,16% y Guayas con el 24.81%.

En el Ecuador los tarjetahabientes no toman en consideración la tasa de interés a la hora de realizar las compras con su tarjeta e inclusive no piensan en que ese valor se puede duplicar por el “pago mínimo”, esto se debe a que no existe responsabilidad por parte del tarjetahabiente al momento de hacer uso de la herramienta de crédito y a su vez porque no existe una reglamentación que regule el uso y el abuso de los emisores y así tratar de evitar inconvenientes en este sistema de pago.

El uso de tarjeta de crédito en el país se ha ido intensificándose por este motivo la Superintendencia de Compañías mediante Registro Oficial No. 640 del 23 de julio de 2009 publicó la Resolución No. DSC.Q.09.01, para regular la emisión de tarjetas de crédito de casas comerciales sujetas a control de la Superintendencia de Compañías y además La Junta Bancaria (2012), a través de la resolución JB-2012-2225, del 5 de julio del 2012 dispuso en su artículo único: “Solamente las instituciones financieras y las compañías emisoras o administradoras de tarjetas de crédito pueden actuar como emisor u operador de tarjetas de crédito. Quienes infrinjan esta disposición serán sancionadas conforme a lo previsto en el artículo 121 de la

Ley General de Instituciones del Sistema Financiero" (Resolución JB-2012-2225, 2012).

Existen cambios en las tasas de interés de los créditos diferidos, por las compras a tres, seis y doce meses. Las tasas están reguladas de acuerdo al tipo de crédito por ello el Banco Central del Ecuador regula mensualmente las tasas de interés como se muestra en el siguiente cuadro.

**Tabla 4: "Tasas de Interés Activas efectivas vigentes a Julio 2014"**

| Tasas de Interés | | | |
|---|---|---|---|
| Julio 2014 | | | |
| 1. TASAS DE INTERÉS ACTIVAS EFECTIVAS VIGENTES | | | |
| Tasas Referenciales | | Tasas Máximas | |
| Tasa Activa Efectiva Referencial para el segmento: | % anual | Tasa Activa Efectiva Máxima para el segmento: | % anual |
| Productivo Corporativo | 8.21 | Productivo Corporativo | 9.33 |
| Productivo Empresarial | 9.65 | Productivo Empresarial | 10.21 |
| Productivo PYMES | 11.26 | Productivo PYMES | 11.83 |
| Consumo | 15.98 | Consumo | 16.30 |
| Vivienda | 10.81 | Vivienda | 11.33 |
| Microcrédito Acumulación Ampliada | 22.24 | Microcrédito Acumulación Ampliada | 25.50 |
| Microcrédito Acumulación Simple | 25.08 | Microcrédito Acumulación Simple | 27.50 |
| Microcrédito Minorista | 28.53 | Microcrédito Minorista | 30.50 |
| 2. TASAS DE INTERÉS PASIVAS EFECTIVAS PROMEDIO POR INSTRUMENTO | | | |
| Tasas Referenciales | % anual | Tasas Referenciales | % anual |
| Depósitos a plazo | 4.98 | Depósitos de Ahorro | 1.18 |
| Depósitos monetarios | 0.47 | Depósitos de Tarjetahabientes | 0.57 |
| Operaciones de Reporto | 0.25 | | |
| 3. TASAS DE INTERÉS PASIVAS EFECTIVAS REFERENCIALES POR PLAZO | | | |
| Tasas Referenciales | % anual | Tasas Referenciales | % anual |
| Plazo 30-60 | 3.94 | Plazo 121-180 | 5.63 |
| Plazo 61-90 | 4.55 | Plazo 181-360 | 6.26 |
| Plazo 91-120 | 5.15 | Plazo 361 y más | 7.19 |
| 4. TASAS DE INTERÉS PASIVAS EFECTIVAS MÁXIMAS PARA LAS INVERSIONES DEL SECTOR PÚBLICO (según regulación No. 009-2010) | | | |
| 5. TASA BÁSICA DEL BANCO CENTRAL DEL ECUADOR | | | |
| 6. OTRAS TASAS REFERENCIALES | | | |
| Tasa Pasiva Referencial | 4.98 | Tasa Legal | 8.21 |
| Tasa Activa Referencial | 8.21 | Tasa Máxima Convencional | 9.33 |
| | | | |
| 7. Tasa Interbancaria | | | |
| 8. Boletín de Tasas de Interés | | | |

**Fuente:** Banco Central del Ecuador - Julio 2014

## 2.10 ¿QUÉ ES FRAUDE?

El fraude según SAS[22] 99 “Es el acto intencional que comete una persona para lucrarse perjudicando a otra”. Según la NIA[23] 240 actualizada 2013: “Es un acto intencional por parte de una o más personas de la administración o gobierno corporativo, empleados o terceros, implicando el uso del engaño para obtener una ventaja injusta e ilegal”.

En ésta investigación nos referiremos al fraude en las tarjetas de crédito y débito que es conocido como un tipo de fraude informático.

## 2.11 EVOLUCIÓN DEL FRAUDE INFORMÁTICO

En 1939, el científico húngaro Jhon Von Neumann, redactó para una revista científica la “Teoría y organización de autómatas complejos” en el que mencionaba la capacidad de desarrollar programas para la manipulación de otros, siempre y cuando tengan una estructura parecida. A partir de esta teoría en 1949, tres programadores crearon un juego que inspiró a concursos científicos importantes. Por la época estos concursos solo eran para una elite de intelectuales. Es aquí donde empieza el desarrollo de programas para la ejecutarse en los ordenadores.

Luego, “En el año 1996 se escuchó por primera vez el término pishing que apareció en los newsgroups de hackers y en la edición del Magazine 2600 de Estados Unidos. Este término tiene dos orígenes: 1) "Fishing" o pesca, refiriéndose a la pesca de credenciales o a la pesca de ingenuos para intentos de fraude, 2) Phishing - "Password Harvesting" que viene a significar cosecha de contraseñas” (Red Venezolana de Derecho Informático, 2014).

“En el 2001 aparecieron los primeros scam en Hotmail con el texto "Usted

[22] Statement on Auditing Standards
[23] Normas Internacionales de Auditoría

es uno de los 100 ganadores de Hotmail" junto con un formulario que solicitaba el usuario y la contraseña de la cuenta de la víctima. Aunque este mensaje aparecía firmado por el Staff de Hotmail, en realidad provenía de una dirección IP de Ucrania" (Red Venezolana de Derecho Informático, 2014).

"En 2002 fueron los usuarios de ICQ[24] quienes recibieron mensajes simulando la imagen de ICQ, en los que les solicitaban sus datos personales en un formulario, y mediante un script re direccionaban sus datos a una dirección de Hotmail. A finales de año Yahoo informaba que varios de sus clientes habían recibido correos donde les solicitaban los datos de sus tarjetas de crédito" (Red Venezolana de Derecho Informático, 2014).

"En 2003 les tocó el turno a los usuarios de EBAY quienes recibieron correos que simulaban alertas de Paypal solicitando sus datos bancarios y los números de sus tarjetas de crédito. Después aparecieron los primeros phishing a entidades de banca online como Barclays Bank, BBVA, en donde los phishers usaron técnicas para la ofuscación de URL. También comenzaron a registrarse nombres de dominio similares a los de las entidades bancarias. A finales de año se detectaron los primeros correos dirigidos a banca online que incluían troyanos con técnicas de ocultación. Un caso fue un ataque que introducía un troyano embebido en código HTML e incluía un script en la máquina de la víctima. Ese troyano era una variante del Spy-Tofger[25]" (Red Venezolana de Derecho Informático, 2014).

Según (Security By Default, 2010)en España, fue en este momento, cuando las técnicas para cometer fraude se enfocaron a:

- **Correos electrónicos**: masivos de spam, selectivos, acompañados por ingeniería social para captar la atención de la víctima, también podían hacer uso de webspoofing o falsas páginas web, algunas venían acompañadas de malware que redirige el nombre de dominio a otra

[24] ICQ: Es un servicio de mensajería instantánea
[25] Virus que permite capturar pulsaciones del teclado y claves guardadas

máquina (phaming). Aparece por primer vez un troyano con capacidad para capturar las pulsaciones de teclado (Keylogger[26]);

- **Sitio web**: malware que explotaba las vulnerabilidades sin parchear de los navegadores, en el sistema operativo, y una vez infectado re direccionaba a los usuarios a servidores web en donde estaban las páginas que suplantaban a las originales;

- **IRC y Mensajería Instantánea**: donde se enviaban imágenes, URL, a los usuarios con contenidos maliciosos. Se enviaba SPAM y se conectaban bots para propagar los contenidos;

- **VoIP**: simulación telefónica, uso de Bots-IVR que solicitaban las credenciales personales. Redirección a webspoofing, otros canales;

- **Buscadores**: que proporcionaban sitios maliciosos en respuesta a las búsquedas de comercio electrónico o banca online;

- **Mensajes en foros**, en **redes sociales**, tablones de anuncios, con mensajes con ingeniería social para captar a la víctima;

- **Redes P2P**, descarga de software desde páginas de descarga masiva;

- **Plataformas de juegos online**, recordamos los casos de phishing que han sufrido los jugadores del World of Warcraft;

- **Falsos antivirus y antispyware**, utilizando llamativos anuncios o pop-ups que avisos alarmantes que advierten al usuario que su sistema está infectado y debe comprar la solución que se le propone. Al usar su tarjeta para obtener este producto sus datos son capturados para su posterior uso fraudulento;

[26] Es un tipo de software o un dispositivo hardware específico que se encarga de registrar las pulsaciones que se realizan en el teclado

- **Vía teléfono móvil** (SMiShing), enviando un SMS al usuario en donde se le invita a enviar su información privada o visitar un sitio web con contenidos maliciosos, y;

- **Botnets**: que tratan de controlar un número masivo de máquinas para la captura de datos bancarios, cuentas de correo.[27]

En el Ecuador se comenzó a hablar de fraude informático en el año 2009 en donde 3,143 fraudes fueron denunciados, para el director nacional de la Unidad de Tecnologías de la Información de la Fiscalía, Jorge San Lucas el acceso a la red es el principal motivo del aumento de fraudes cibernéticos. Señaló "*como delitos más frecuentes la apropiación ilícita de montos o valores; falsificación electrónica de identidad, y daños informáticos cuando el custodio es un funcionario público*" (Diario La Hora, 2011).

Así es como se ha ido propagando a nivel mundial las diferentes técnicas para cometer fraude informático a diferentes organizaciones y personas, ayudándose del desarrollo de la tecnología y aprovechándose de la falta de información de usuarios de la red.

Enrique Mafla, experto en Seguridad Informática, sostuvo que no existen sistemas informáticos seguros. "Incluso han hackeado a la Central de Inteligencia Americana (CIA) y la Oficina Federal de Investigación (FBI, por sus siglas en inglés)". Por este motivo, recomendó que las instituciones financieras establezcan mecanismos adecuados para minimizar los riesgos tecnológicos, de acuerdo a la resolución de octubre de 2005 de la Junta Bancaria, emitida por la Superintendencia de Bancos.[28] (Diario La Hora, 2011)

[27] Securitybydefault. (Enero 2010). Obtenido de. http://www.securitybydefault.com/2010/01/origen-y-evolucion-del-efraude.html

[28] Diario La Hora. (Agosto 2011). Obtenido de http://www.lahora.com.ec/index.php/noticias/imprimir /1101191943/seccion

## 2.12 CARACTERÍSTICAS DE FRAUDE INFORMÁTICO.

Un fraude informático se lo puede definir como una manipulación de los sistemas informáticos para conseguir un beneficio económico, mediante la ejecución de un acto fraudulento para perjudicar a un tercero. A continuación se detalla ciertas características:

- Son conductas criminales ejecutadas por personas con ciertos conocimientos o técnicos en informática;
- Se aprovecha la oportunidad u ocasión que brinda un sistema, es decir facilidades de acceso y manipulación de datos;
- Pérdida económicas importantes;
- Ofrecen posibilidades de tiempo y espacio, debido a que son ejecutados a través de un ordenador sin la presencia física del criminal;
- Son muy sofisticados y relativamente frecuentes, y;
- Aprovechan vulnerabilidades o fallas en las plataformas afectadas.

## 2.13 RED FLAGS

Las banderas rojas según el informe “Red flags for fraud” (DiNapoli) son “un conjunto de circunstancias que son inusuales en la naturaleza o puede variar en la actividad. Son advertencias de que algo podría estar o está mal, es decir son posibles señales de alerta de fraude es por esta razón que los auditores, empleados y área administrativa de las Instituciones Financieras tienen que ser conscientes de

dichas señales, con el fin de monitorear dicha situación y tomar medidas correctivas cuando sea necesario.

Los empleados de las Instituciones Financieras que notan que las “banderas rojas” son ignoradas podrían erróneamente creer que está bien jugar con el sistema de información o que no va a ser descubierto, si no se toman las medidas correctivas frente a un pequeño fraude identificado, pronto se convertirá en uno mayor y será difícil de mitigarlo.

Se debe tener en cuenta los siguientes dos puntos claves en este tema:

1. No se deberá ignorar las banderas rojas: estudios de casos de fraude constantemente demuestran que las “red flags” estuvieron presentes, pero no fueron reconocidas o fueron reconocidas pero no hubo la actuación necesaria sobre estas. Cuando una “red flag” es identificada alguien debe inmediatamente tomar las acciones respectivas, investigar la situación y determinar si el fraude fue cometido.
2. Muchas veces no llega a ser fraude simplemente un error: las banderas rojas conducen a un tipo de acción inapropiada, sin embargo muchas veces esa acción suele ser un error y no precisamente un fraude. Se debe de tener la capacidad de saber reconocer la diferencia entre fraude y error y que el seguimiento de la investigación, en caso de fraude debe ser atendida por manos de una persona responsable y experta del tema.

## 2.14 OPERACIONES FRAUDULENTAS DE TARJETA DE CRÉDITO EN OTROS PAÍSES

El fraude en compras online creció un 25% en el período 2010-2012, lejos del 14% de incremento en falsificaciones de tarjetas en Estados Unidos. Aunque la tasa de fraude ha crecido, la pérdida media por delito ha descendido un 10%, debido al gran aporte y funcionamiento eficiente de las tecnologías utilizadas para solventar el fraude, como FICO Falcon Fraud Manager (que protege el 85% de las tarjetas emitidas en EEUU).

“Los fraudes electrónicos, robos digitales y daño a las computadoras hecho por delincuentes digitales o "hackers", provocaron pérdidas por 29,800 millones de pesos (mdp) a mexicanos durante el 2012, de acuerdo con el estudio "Reporte de Cybercrimen 2012", presentado por Norton by Symantec. Casi 15 millones de mexicanos han sido víctimas de algún delito digital, sobre todo a través de celulares y redes sociales. Comparando las cifras de México respecto a otros países, los "hackers" dejaron pérdidas en Estados Unidos por casi 210,000 mdp[29], mientras que en Japón apenas llegan a los 5,000 mdp” (Revista Especializada de ACFE - Capítulo México, 2012)[30]

Según los últimos datos recabados por la Organización de Consumidores y Usuarios (OCU), las reclamaciones por el uso fraudulento de las tarjetas en junio y julio fueron un 52% más bajas que en el mismo período de 2012.No obstante, la OCU ha considerado más relevante el dato referido al semestre de este año respecto al anterior, cuando el descenso de reclamaciones ha sido algo más suave si bien ha superado el 32%.

El descenso de reclamo por operaciones fraudulentas en España se debe a que ya muchos españoles no hacen uso de las tarjetas de crédito debido a la recesión económica por la que está pasando el país, la portavoz de la OCU, Ileana Izverniceanu ha recordado que, desde 2008, el número de tarjetas -tanto de débito como de crédito- ha descendido de forma continuada al pasar de 76.4 millones al inicio de la crisis a 68,8 en la actualidad.

La Asociación de Usuarios de Banco, Cajas y Seguros (ADICAE) ha apuntado que sus servicios jurídicos han percibido también la insatisfacción de los usuarios con los bancos a los que acusan de "eludir responsabilidades", según ha denunciado esta asociación, ante un fraude

[29] Millones de pesos.

[30] Revista Especializada de ACFE - Capítulo México. (Octubre de 2012). Obtenido de http://www.revistadelfraude.com/septiembre_octubre/el_peso_del_fraude.html

"son muchas las entidades que dan por hecho que el consumidor ha custodiado mal la tarjeta y, por ello, no le devuelven el dinero". [31]

## 2.15 TIPOS DE FRAUDES

El fraude puede darse de forma interna y externa.

- **Fraude interno:** es cuando una persona que forma parte de la empresa se encuentra implicada en el fraude, en el caso de operaciones fraudulentas con tarjeta de crédito podría darse que funcionaros de las instituciones financieras desvíen fondos de tarjetas de crédito de otra persona, los denominados fraudes crediticios.

- **Fraude externo:** es cuando un tercero se apropia de bienes de una forma indebida incumpliendo leyes. Ejemplos: Daños por ataques informáticos, robo de información de las tarjetas con grandes pérdidas pecuniarias.

A continuación damos a conocer los 5 principales actos ilícitos que han sido identificados por los Bancos, según Revista Especializada ACFE - México:

- **Pérdida o robo de la tarjeta**.- sucede cuando una persona toma en su poder de forma dolosa una tarjeta de crédito o simplemente se encuentra una que ha sido olvidada y la cual no le pertenece haciendo uso de ella y fingiendo ser el propietario de la misma;

- **Duplicado de tarjeta o skimming**.- consiste en duplicar la tarjeta y a su vez su codificación sin el permiso de la institución bancaria que es la emisora oficial. También consiste en la lectura no autorizada y almacenamiento de la información contenida en la banda magnética de tarjetas bancarias, mediante la utilización de dispositivos electrónicos y sin permiso del propietario;

[31] El País. Obtenido de. www.economia.elpais.com

- **Robo de datos**: esto sucede cuando es hurtada la información que contiene la tarjeta durante la transacción comercial;

- **Robo de la tarjeta antes de la entrega al titular**.-como su nombre lo indica el fraude ocurre cuando la tarjeta es robada antes de llegar a su titular. Esto ocurre cuando son enviadas por correo por la institución financiera y no cuenta con los elementos eficaces de acuses de recibo, y;

- **Cambio de identidad en tarjetas**. Existen dos tipos:

  a) **Fraude de uso**: Este delito se produce cuando un criminal roba documentos, como estados de cuenta, y los utiliza para abrir una cuenta nueva a nombre de la víctima.
  b) **Toma de posesión de la cuenta:** Con este fraude un estafador utilizará datos personales del titular para solicitar al banco que dirija pagos a otra parte.

De acuerdo con SAS (Statement on Auditing Standards) 99, los mecanismos anti lavado de dinero, deben enfocarse brindar soluciones integrales que permitan detectar más eficientemente este tipo de ilícitos, al interior de los bancos.[32]

Los bancos deben mejorar las plataformas de seguridad tecnológica que brinden mayor confianza a sus clientes.

## 2.16 PERFIL DE UN DEFRAUDADOR

Un defraudador, es una persona que comete un acto intencional con el objetivo de perjudicar a alguna persona u organización. Según SAS (Statement on Auditing Standards) 99 una persona puede cometer un fraude por tres motivos: incentivo, oportunidad y racionalización, estos tres elementos forman lo que se conoce como un triángulo de fraude que a continuación detallamos:

[32]CNN NOTICIAS. Obtenido de. www.CNNExpansion.com

**Gráfico 10: "Triangulo del Fraude"**


**Fuente:** KPMG International 2013

**INCENTIVO.-** Es cuando la persona se siente bajo presión por algún tipo de problema personal, creyendo así que tiene una razón para cometer fraude. Esto incluye:

- Inestabilidad económica
- Presiones excesivas de lograr metas financieras por parte de sus jefes o expectativas de sus familiares.
- Estilo de vida.
- Vicios.
- Problemas familiares.

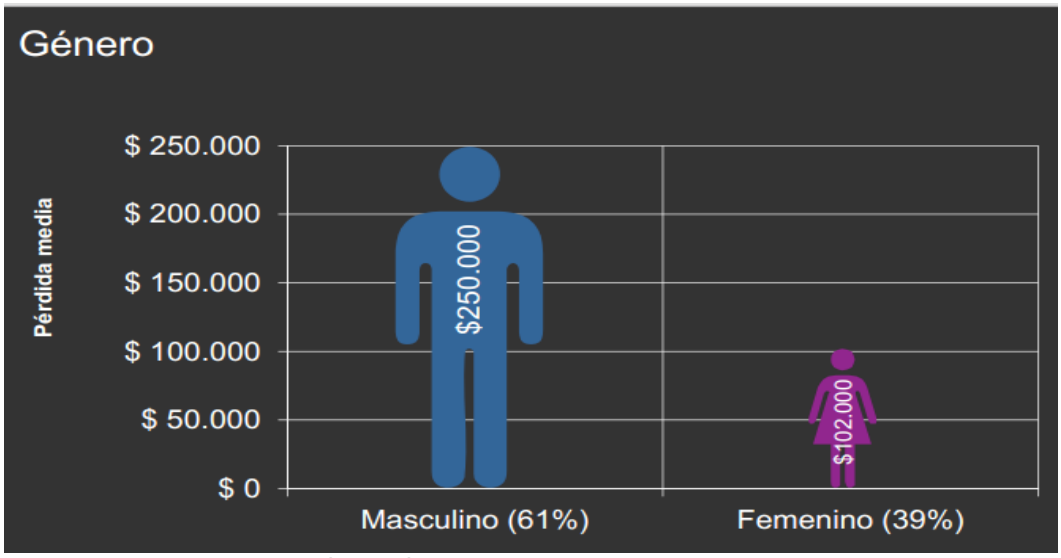
**OPORTUNIDAD.-** Es cuando no existen controles efectivos o ausencia de los mismos, y cualquier persona puede sobrepasar aquellos controles que existen, de esta forma ofrecen una oportunidad para que el fraude sea perpetuado.

**RACIONALIZACION.-** Las personas son capaces de racionalizar la forma de ejecutar un fraude, aquí también se tendrá en cuenta la actitud, carácter y los valores éticos que posea la persona, ya que muchas de ellas no ponen en práctica los valores que le han sido inculcado y se les hace fácil cometer

actos fraudulentos, pero también es posible que personas honestas, puedan ejecutar algún tipo de fraudes debido al medio en que se encuentra y que les impone mucha presión.

Cabe recalcar que el género masculino es el que comete más actos fraudulentos que el género femenino, según encuestas realizadas por la ACFE en México.

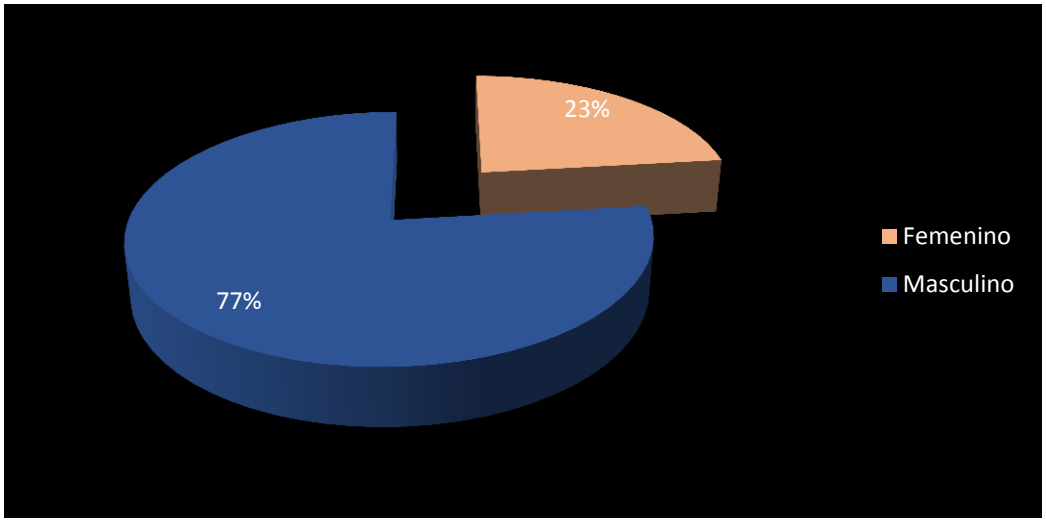
**Gráfico 11: "Perfil del Defraudador - Género"**




**Fuente**: ACFE Report To The Nation 2012

En Ecuador, en una encuesta realizada por los alumnos del noveno semestre de la carrera Ingeniería en Contabilidad y Auditoría, en donde los resultados fueron los siguientes:

**Gráfico 12: "Resultado de Encuesta realizada por alumnos de la UCSG"**




**FUENTE**: UCSG Encuesta realizada por alumnos del noveno semestre C.P.A (2013)

## 2.17 TÉCNICAS DE FRAUDE QUE APLICAN LOS DELINCUENTES DIGITALES

Las instituciones financieras y tarjetahabientes no están exentos de ser víctimas de un fraude debido a que cada vez se vuelve más sofisticadas las técnicas que aplican los delincuentes digitales y a su vez son más difíciles de detectar.

Es así como estos delincuentes digitales comienzan a crear y aplicar técnicas para alcanzar sus objetivos fraudulentos, mediante la manipulación de la información y de los programas.

Las técnicas más comunes son:

- **Introducción de datos falsos (Data Diddling).-** es el más sencillo de llevar a cabo, consiste en manipular las transacciones, es decir puedo ingresar movimientos falsos o eliminar transacciones que debieron ser ingresadas;

- **Caballo de Troya (Trojan Horse).-** consiste en darle instrucciones o rutinas no permitidas al programa para que comience a actuar de una manera distinta a la prevista en determinadas ocasiones;

- **Salami (Rounding Down).-** es cuando se manipula un gran número de pequeños importes y el fraude se comete en pequeños cortes. Ejemplo: mediante formula matemáticas se redondean los centavos de los números de una cuenta bancaria y se desvían a una cuenta controlada por el defraudador;

- **Skimming.-** En esta técnica el defraudador roba la información de tarjetas de crédito en el momento de la transacción, con la finalidad de reproducir o clonar la tarjeta de crédito o débito para su posterior uso fraudulento;

- **Puertas falsas (trap doors).-** conducta consistente en la introducción a los sistemas informáticos a través de accesos o "puertas" de entrada no previstas en las instrucciones de aplicación de los programas[33];

- **Las "Llaves Maestras" (Superzapping).-**mediante un programa denominado "superzap" se puede modificar base de datos y archivos aun si se encuentran reservados. Esto puede ser un gran riesgo para el sistema financiero porque se puede llegar tener acceso a una cuenta de un tarjetahabiente y modificar el saldo de su tarjeta, y;

- **El pinchado de líneas (Wiretapping).-**modalidad que consiste en la interferencia en líneas telefónicas o telemáticas, mediante las cuales se transmiten las informaciones procesadas.

Cualquiera de ellas puede ser empleada por el delincuente digital con el único objetivo de perjudicar a un tercero y dar por ejecutado el fraude.

[33] CNN NOTICIAS. Obtenido de. www.CNNExpansion.com

La Vicepresidenta y Analista de Gartner, Avivah Litan se pronunció acerca de los ataques de ATM de tipo salami e indicó que esta nueva técnica es una de las más utilizadas por los defraudadores de tarjeta de crédito y es muy difícil de detectar y puede resultar en pérdidas significativas aunque las cantidades que son robadas son extremadamente pequeñas pero el ataque informático va dirigido a muchos cajeros automáticos al mismo tiempo.

Esto comienza con una banda de defraudadores que comienzan a instalar dispositivos POS[34] no fiables, capaces de robar datos de tarjetas de crédito y números de identificación personal, en las tiendas que pertenecen a un minorista particular, en varios lugares de la ciudad.

Los objetos plantados dentro de estos terminales envían datos a una base de datos central, desde donde se utiliza para crear cientos de tarjetas de crédito falsas.

Las tarjetas obtienen los números PIN asociados pegados en ellas y son entregadas a una red de intermediarios para el blanqueo de dinero, para dispersarlo en todo el país. Cada intermediario recibe alrededor de cinco tarjetas falsas a la vez y recibe instrucciones para retirar cantidades muy pequeñas de cada uno de ellas. Cientos de cajeros automáticos en diferentes ciudades son atacados al mismo tiempo.

Dentro de diez minutos, los retiros simultáneos de todos estos cajeros llegan acerca de 100.000 dólares en ganancias, explica el analista de Gartner. El grupo organizacional de fraude de tarjeta de crédito repite esta operación cinco veces al mes con tarjetas diferentes y ganan 500.000 dólares.[35]

Según denuncias receptadas por la Fiscalía General del Estado las técnicas más comunes para las operaciones fraudulentas con tarjetas de crédito son: el “phishing” o robo de identidad a través de la suplantación de

[34]Point Of Sales- terminal de punto de venta lo tienen los locales comerciales.
[35]IBM – TECNOLOGIAS Lucian Constantin

correos electrónicos; el “skimming”, que clona la banda magnética de las tarjetas de crédito y de débito; y el “carding” que utiliza el número de tarjeta para hacer compras en el extranjero y la manipulación de software para engañar al usuario y la técnica conocida como “del salami”, que es difícil de identificar porque de centavo en centavo se extrae dinero de diferentes cuentas bancarias.

Juan Enrique Caicedo estudiante de sistema de información se pronunció acerca de las diferentes técnicas de fraude existentes y concluyó que: *“En la actualidad en nuestro medio (Ecuador) el índice de delitos informáticos ha crecido de una manera alarmante, pese a que el avance tecnológico no es precisamente un fuerte de nuestro país, esto se debe a que existe un buen porcentaje de nuestros estudiantes que no tienen el fácil acceso a una computadora o el internet, el mal uso o definitivamente la falta de uso de las TIC´s (TECNOLOGIAS DE LA INFORMACIÓN Y LA COMUNICACIÓN) en las aulas de clases, esto lo vemos reflejado en el campo de la seguridad informática, nosotros no tenemos expertos en seguridad informática, los informáticos que actualmente prestan sus servicios en las diferentes empresas tanto públicas como privadas, es personal extranjero; pese a no tener muchos expertos informáticos, de una manera contradictoria, los delitos informáticos están en un ascenso descomunal. Por ejemplo, uno de los delitos más cometidos a mi modo de pensar es el SKIMMING, y aquí es donde se resuelve en cierta manera esa batalla entre los niveles de conocimiento informático deficiente y el ascenso de los delitos informáticos. Analicemos un poco los conocimientos necesarios que una persona necesita para realizar skimming, pues, las habilidades informáticas que necesitan básicamente son nulas, lo que necesita el delincuente es un SKIMMER[36] y tener manos hábiles para evitar ser descubierto en el momento de pasar la tarjeta de la víctima por el scanner, además es un delito en el cual la victima entrega de manera voluntaria su tarjeta de crédito o débito. Entonces podemos deducir que cualquier persona motivada para aspectos negativos puede cometer*

[36] Es un aparato que utilizan los delincuentes informáticos para clonar las tarjetas

*SKIMMING, por lo tanto, es uno de los delitos más cometidos por su bajo porcentaje de complejidad. Al decir bajo porcentaje de complejidad solo hago referencia al delito en restaurantes, estaciones de servicio o los lugares promedio donde el tarjetahabiente utiliza su tarjeta, porque en cuanto a cajeros automáticos se refiere, el proceso ya se vuelve un poco más complejo de lo normal, lo que debería imposibilitar la alteración o la clonación de tarjetas. Por otro lado, siendo también un método que en la actualidad se está usando frecuentemente para ataques en instituciones bancarias son los TROYANOS BANCARIOS, debemos olvidar y dejar de asociar el hecho del diseño de un troyano con el típico perfil de una criatura de 17 años pegado 24/7 a su computadora programando y creando malware, ya no estamos hablando de HACKTIVISTAS que irrumpen en las seguridades para transmitir mensajes de libertad y paz, estamos hablando de que en la actualidad esto se ha vuelto un negocio muy lucrativo, grandes equipos profesionales se dedican al diseño de troyanos bancarios, estamos hablando de súper genios informáticos en todas las ramas agrupados con la única motivación que no es más que cantidades millonarias de dinero, estos grandes grupos pueden llegar a invertir hasta $100,000.00 en la elaboración de un troyano bancario. El blanco de estos cyberdelincuentes son países de américa latina con economías fuertes tales como Panamá, Chile, Colombia y países que cuentan con un bajo nivel de protección informática como Ecuador, Perú, Bolivia, Venezuela".*

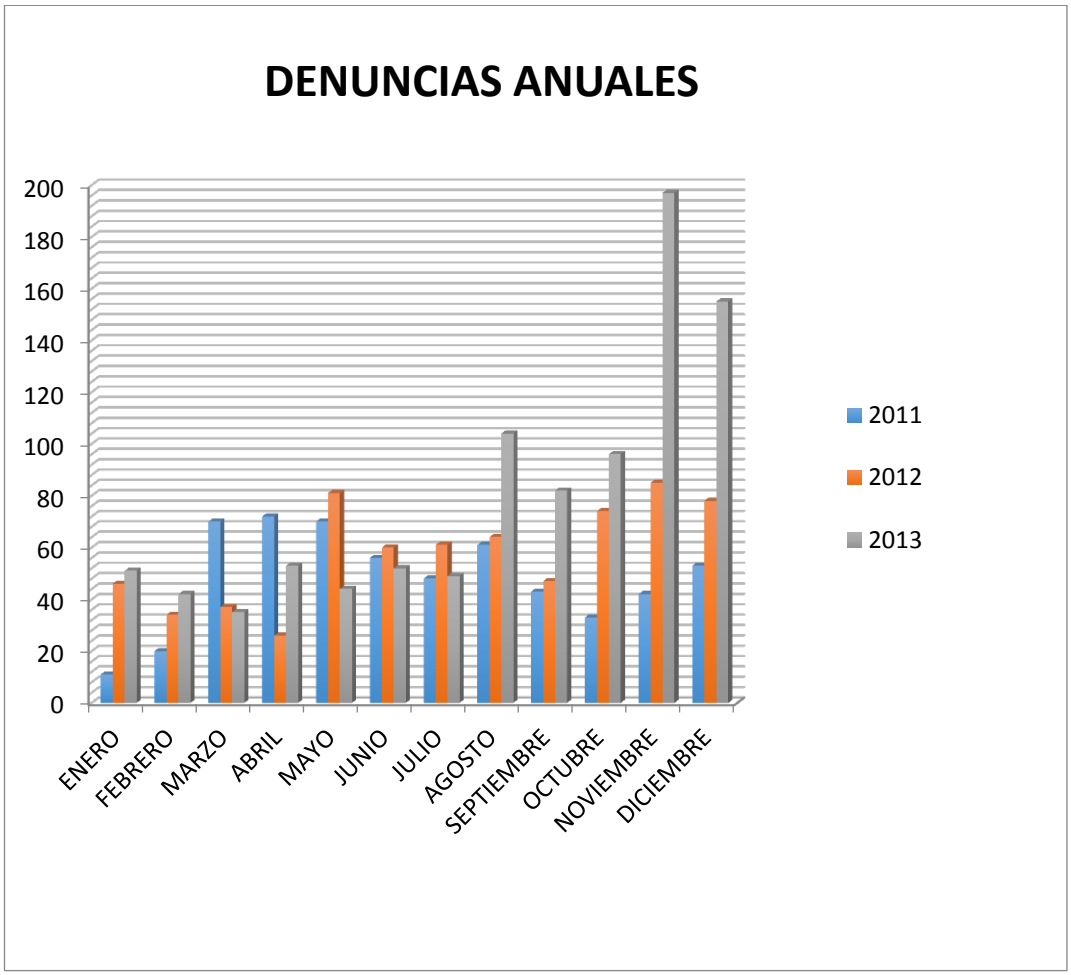
## 2.18 ÍNDICE DE CRECIMIENTO DE OPERACIONES FRAUDULENTAS CON TARJETAS DE CRÉDITO

A lo largo de los últimos 3 años Ecuador ha tenido un aumento a lo que se refiere operaciones fraudulentas con tarjeta de crédito lo cual va ligado con los diferentes fraudes informáticos, perjudicando no solo el patrimonial del Estado sino también el de centenares de clientes .Desde el 2009 la Fiscalía General de nuestro país ha registrado un aumento de denuncias de forma sorprendente, solo en ese año se reportaron 168 casos, mientras que en el 2010 con 499 quejas por "apropiación ilícita utilizando medios informáticos", como describe el delito la entidad, 579 casos en el

2011 y en el 2012 llegan a 693 y en el año 2013 960 casos de operaciones fraudulentas.

A continuación presentamos gráficos de las denuncias presentadas en la Fiscalía General del Estado – Guayas. En el primer gráfico realizamos un comparativo mensual, y en el segundo un comparativo anual.

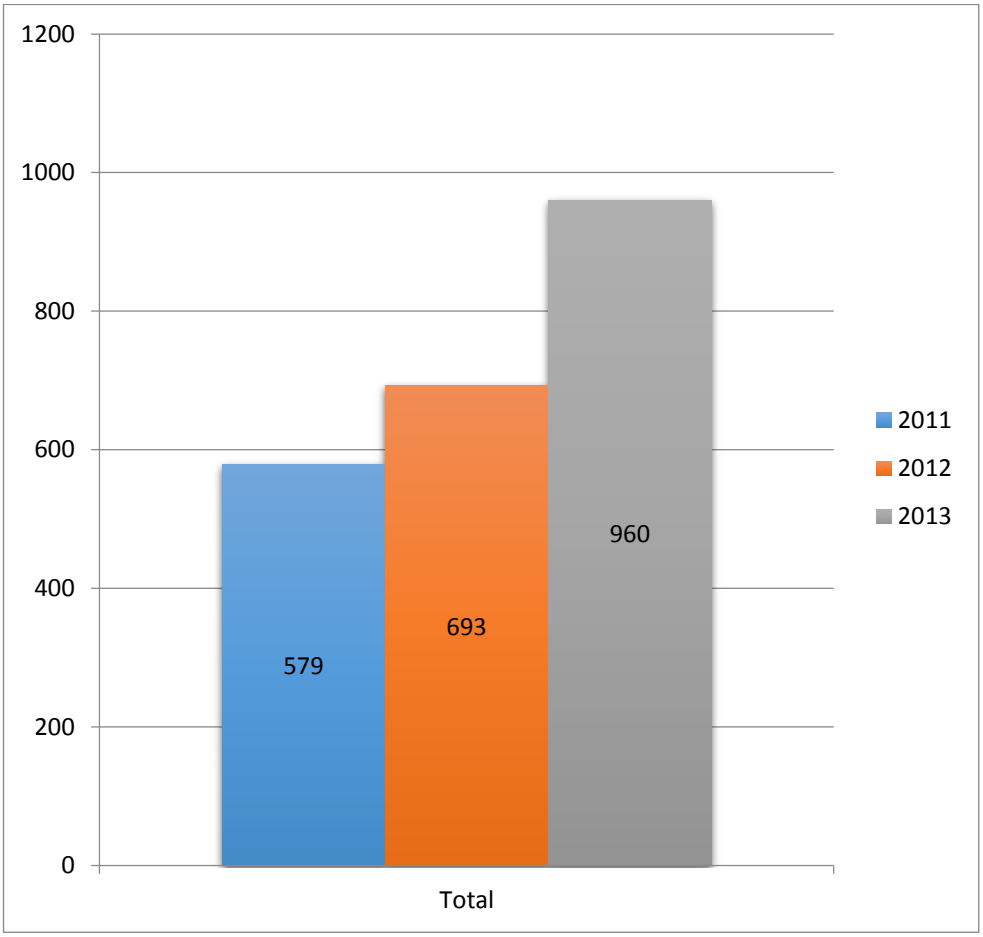
**Gráfico 13: "Denuncias receptadas por parte de la Fiscalía General del Estado"**




**Fuente:** Fiscalía General del Estado.

**Elaborado por:** Autoras.

**Gráfico 14: "Crecimiento Anual de Denuncias receptadas por parte de la Fiscalía General del Estado"**




**Fuente:** Fiscalía General del Estado.

**Elaborado por:** Autoras.

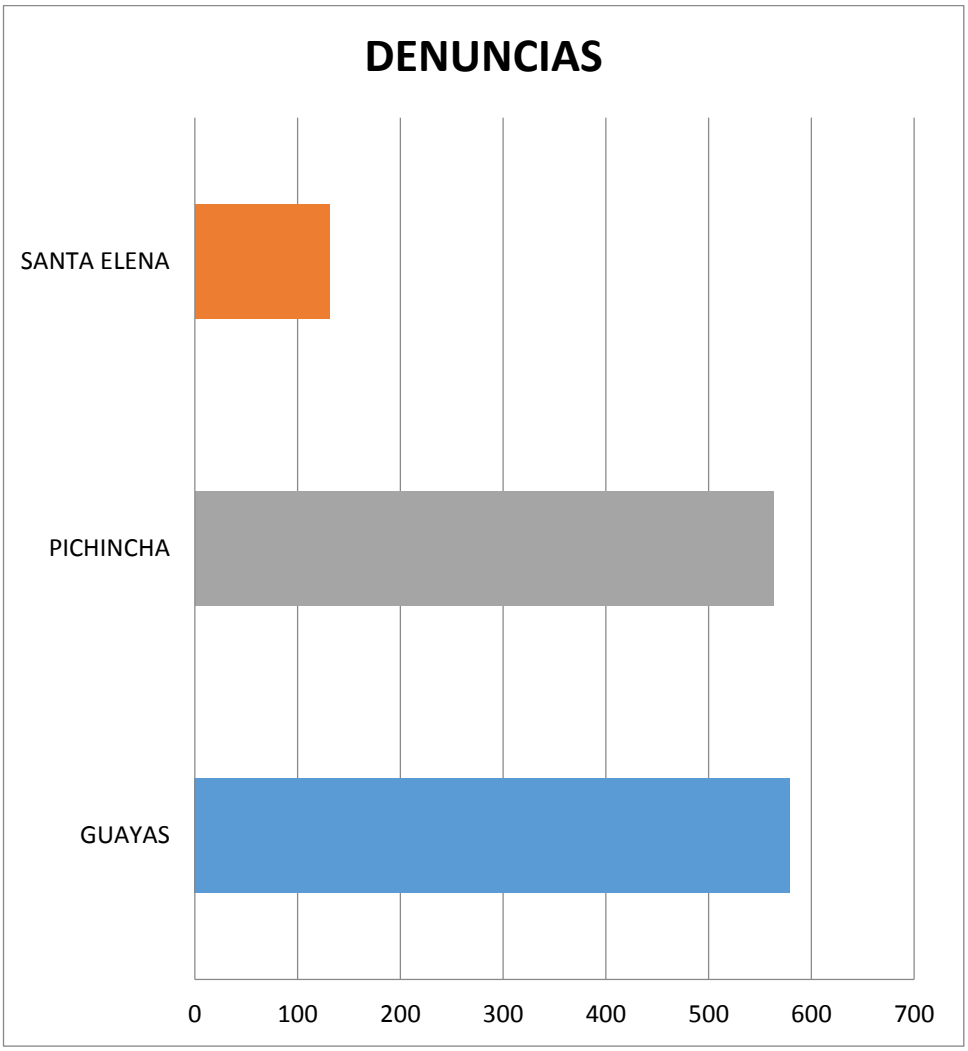
La Fiscalía General del Estado considera que los delitos informáticos son un tema de constante creciente en el Ecuador, debido al incremento de tarjetas de crédito del medio. Según estadísticas el consumo de los ecuatorianos se ha desarrollado durante los últimos años debido a la liquidez del sistema. Añaden que en muchas ocasiones los sistemas son vulnerados desde el exterior haciendo el crimen transnacional e casi imperceptible.

"Esta situación mantiene alerta a las autoridades, que incluso piensan en propuestas regionales para combatir esta nueva forma de delinquir, Ya que un estudio realizado por las empresas GMS y Kaspersky ubicó las

pérdidas económicas por delitos informáticos en el Ecuador en un millón de dólares entre 2009 y 2010" [37] (Revista de Avances Tecnológicos).

Según datos estadísticos de la Fiscalía General del Estado las provincias que más denuncias registran son: Guayas con 579, Pichincha con 563 quejas, y Santa Elena con 131.

**Gráfico 15: "Provincias con Mayores Denuncias de Operaciones Fraudulentas"**




**Fuente:** Fiscalía General Del Estado.

**Elaborado por:** Autoras.

[37] Revista de Avances Tecnológicos. (Marzo 2013) Obtenido de. http://avtecnologicvivi .blogspot. com/2013/03/delito-informatico.html

El incremento se da pese a que las Instituciones Financieras comenzaron a implementar modernos sistemas de seguridad, para intentar bloquear el ataque de los 'criminales informáticos ', de igual forma la tendencia de estos delitos comenzó a aumentar; y esto es porque atrás de estas seguridades hay gente muy especializada, con acceso a la tecnología, muy inteligentes, que siempre encuentran puertas abiertas en los sistemas para atacarlos.

La Superintendencia de Bancos y la Fiscalía aprobaron una resolución, que desde el 2011 obliga a las instituciones del sistema financiero a restituir el patrimonio de quienes han sido estafados por vía electrónica.

Según esta resolución, las instituciones deben restituir el 100% del robo cuando los valores van de US$1 a USD 2,000, cuando van de US$ 2,001 a USD 10,000 mil es reconocido el 80 % y si el fraude sobrepasa los USD 10,000 debe ser reconocido el 60%.[38]

La Junta Bancaria debido a los diferentes fraudes con tarjeta crédito solicitó al sistema financiero que sus sistemas informáticos sean blindados, por esta razón algunos bancos realizaron cambios en sus páginas de internet , por ejemplo el Banco Pichincha tiene una tarjeta llamada "ekey" para las transacciones que sus clientes quieran realizar, la tarjeta que se le es entregada contiene número que son coordenadas y cuyos números son solicitados de forma aleatoria en cada transacción en línea que sea realizada por el cliente.

El Banco Pichincha recalcó que: *"Ninguna transacción puede concretarse sin que el cliente no tenga físicamente, ante sí las coordenadas (tarjeta ekey) impresos en la tarjeta. Es importante indicar, que ninguna tarjeta se repite y que tanto la generación de las tarjetas eKey, como su distribución a los clientes, se lo hace con tecnología de última generación y*

[38]El Diario Noticias Manabí - Ecuador

*siguiendo los más estrictos estándares de seguridad. Jamás, ninguna información queda almacenada en ninguno de los sistemas, ni bajo conocimiento de funcionario alguno. También se incorporó un mecanismo de autenticación biométrico. Aquí los clientes requieren de una clave un poco más larga y que es validada por el sistema, en cada ingreso a la banca en línea. "Cada vez que el cliente ingrese a su cuenta, el sistema irá 'aprendiendo' la forma en la que el cliente escribe su clave, en el teclado de su computador. De ahí que se trata de un sistema biométrico, ya que ninguna persona 'escribe' igual a otra. De esta manera, el sistema puede detectar si la clave está siendo escrita por la persona correcta, o por alguien distinto a él, que por cualquier razón, tuvo acceso a su clave".*

El Banco Guayaquil, también tomo en consideración lo ordenado por la Junta Bancaria de blindar sus sistemas informáticos y para brindarle un servicio más seguro a sus clientes, Angelo Caputti, presidente ejecutivo de la entidad indicó que optaron por el uso de un sistema biométrico para acceder a los servicios en la página web. En este sistema el usuario debe escoger una fotografía la cual debe reconocer cada vez que se acceda al portal. Además, se hace un registro del computador en el que está operando el cliente y con eso se ha podido reducir el índice de delitos.

En cambio el Banco del Pacifico, instaló en los cajeros automáticos dispositivos de seguridad para las transacciones, y en la banca transaccional en línea también existen controles para asegurar la identidad del usuario.

Otras de las empresas que comenzó a implementar seguridades para las compras a través de tarjetas de crédito es American Express, al momento de hacer compras en la página web se piden claves adicionales a los clientes, esto hace un poco más largo el proceso de compra, pero ellos comprenden que a la larga es por seguridad.

Y en el Banco del Pacifico, los cajeros automáticos tienen instalados dispositivos de seguridad para las transacciones, y en la banca transaccional en línea también existen controles para asegurar la identidad del usuario. Es

así como cada Institución Financiera ha ido implementando nuevos sistemas para disminuir el riesgo de fraude con tarjeta de crédito y para así brindarles a sus clientes se seguridad y evitar el crecimiento de perdida monetaria que afecta tanto a la Institución Financiera y al tarjetahabiente.

## 2.19 METODOLOGÍA DE PREVENCIÓN Y DISUASIÓN DEL FRAUDE

"Aquellos que se encargan de evaluar el fraude han utilizado el triángulo del fraude como método estándar desde la década de 1950 para entender las motivaciones de los defraudadores. Sin embargo, el triángulo del fraude no resulta suficiente para disuadir, prevenir y detectar el fraude debido a que la presión y la racionalización no son factores que puedan ser observados" (Fraud Magazine de la ACFE, 2011)

La disuasión del fraude se refiere a la creación de un entorno en el que las personas no se animen a cometer fraudes, aun cuando sea posible. Debido a que la oportunidad involucra tanto el acceso para cometer el fraude y la percepción de que el estafador pueda salirse con la suya, uno de los aspectos más importantes de la disuasión es el temor de ser atrapado. En "Robo por Empleados" (Simon & Schuster, 1983), Richard C. Hollinger y John P. Clark encontraron que la certeza percibida de detección está inversamente relacionada con el robo de empleados - es decir, mientras que los empleados piensen que existen más probabilidades de ser detectados, menos probabilidades de que en realidad lo harán.

El segundo aspecto de la disuasión es el miedo al castigo. En 2005, el Federal Sentencing Guidelines Manual define a la disuasión como un mensaje claro enviado a la sociedad de que entre más se repita una conducta criminal, más severa será el castigo.

Además, Sutherland[39] sugiere que los empleados, en particular aquellos de los altos cargos, establezcan el tono ético para la organización. Cuando los líderes muestran conductas cuestionables, poco éticas o fraudulentas, los empleados normalmente honestos serán más propensos a racionalizar el fraude. Por el contrario, la teoría de Sutherland, también sugiere que los empleados con altos valores éticos pueden influir en aquellos que tienen tendencia a cometer fraudes

Como resultado de estos conceptos, la disuasión se logra generalmente a través de una variedad de esfuerzos asociados con los controles y programas que crean un lugar de trabajo con integridad y alientan a los empleados a denunciar actividades ilegales potenciales. Estas acciones aumentan la probabilidad percibida de que un acto de fraude será detectado y reportado.

La disuasión del fraude también se puede lograr mediante el uso de una continua vigilancia y software de auditoría[40] (Fraud Magazine de la ACFE, 2011). Las técnicas y controles contra el fraude incluyen:

- Un tono ético del alto mando;
- Un código de conducta;
- Una comunicación abierta con los empleados, vendedores, proveedores y clientes;
- Monitoreo de empleados;
- Líneas de denuncia;
- Protección de los denunciantes;
- Un protocolo para castigar a perpetradores;
- El monitoreo de contratistas, y
- Auditoría de fraude proactiva.

Además la revista de Fraude ACFE[41] nos indica lo siguiente con respecto a la disuasión:

[39] Edwin H. Sutherland fue un sociólogo estadounidense. Está considerado como uno de los criminólogos más influyentes del siglo XX
[40] Fraud Magazine ACFE (s.f.). Obtenido de http://prismamx.net/pdfs/mas_alla.pdf

*"La disuasión incluye a todos los profesionales entornos corporativos, incluyendo la junta directiva, el comité de auditoría, la alta dirección y los auditores externos e internos. La idea de la disuasión tiende a abordar dos aspectos del triángulo del fraude: oportunidad y racionalización. Cuando los controles y programas de lucha contra el fraude se presentan como elemento de disuasión, el defraudador percibe que las oportunidades de cometer y ocultar el fraude se han reducido o eliminado. La racionalización del defraudador puede ser disuadida o reducida a través de programas de entrenamiento y una fuerte cultura corporativa que establezca un alto estándar ético. Es importante destacar que, para los profesionales, los esfuerzos de disuasión son observables y se pueden utilizar para evaluar la probabilidad de ocurrencia de fraude*".

En las instituciones Financieras es importante que se realicen constantes vigilancias por parte de autoridades reguladoras y gubernamentales, principalmente por su naturaleza y por las posibilidades de ser víctimas de fraude y de sufrir grandes pérdidas monetarias.

Los elementos que deben ser considerados para regular las instituciones financieras y prevenir el Fraude son:

[41] Association of Certified Fraud Examiners

**Gráfico 16: "Regulación Financiera"**


**Fuente:** Superintendencia de Bancos y Seguros.
**Elaboración:** Autoras.

Una pobre administración de riesgos, una mala dirección de controles internos inadecuados y una supervisión inadecuada de los riesgos operativos han sido algunos de los factores que han contribuido para que los delincuentes informáticos se aprovechen de las vulnerabilidades encontradas en ciertas Instituciones Financieras, logrando ejecutar sus fraudes, que en la mayoría de las ocasiones son de alrededor de US$500,000 dólares.

Las Instituciones Financieras están obligadas a brindarles a sus clientes (tarjetahabientes), seguridad para que los mismos sigan confiando en el servicio que ellos les brindan para el uso de sus tarjetas de crédito.

En la actualidad muchos tarjetahabientes han sido víctimas de algunos de los tipos de fraude que hemos mencionado en el desarrollo de la investigación, en donde sus tarjetas han sido clonadas, saldos descontados sin que los propietarios de las tarjetas hayan realizado alguna compra

comercial, entre otros actos ilícitos que los delincuentes informáticos realizan sin que nadie contrarreste sus malas acciones, puesto que los tarjetahabientes depositan la totalidad de su confianza en la Institución Financiera que les provee la tarjeta de crédito y no creen en la necesidad de tomar medidas preventivas para evitar fraudes en sus tarjetas crédito, sino más bien se desligan de la responsabilidad que también deberían tener y la trasladan 100% al proveedor de las tarjetas de créditos que poseen.

Pero a pesar de haber salido la resolución No. JB-2012-2148 por la Junta Bancaria Ecuatoriana en donde se establecía los montos a devolver si algún tarjetahabiente sufría algún robo de saldos de su tarjetas, la cual obligaba de cierta forma a tomar mayores y mejores medidas de seguridad para minimizar el riesgo pero algunas de las Instituciones Financieras no cumplían con la misma y en muchos casos se resistían a devolverle al afectado la cifra correspondiente.

El fraude no puede erradicarse pero puede prevenirse o inhibirse implementado los controles internos adecuados que cada Institución Financiera debe poseer y en el caso de los tarjetahabientes aplicando estrategias para evitar ser víctimas de fraude.

## 2.20 PRÁCTICAS DE PREVENCIÓN Y DETECCCIÓN DE FRAUDE PARA LAS INSTITUCIONES FINANCIERAS

La cultura antifraude se debe determinar e implementar desde la alta Dirección y debe contener los valores, la cultura, y principios de integridad además no se debe tolerar ninguna conducta inapropiada por muy leve que se considere.

Las Instituciones Financieras deben contar con las herramientas necesarias para implementar las mejores prácticas de disuasión de fraude

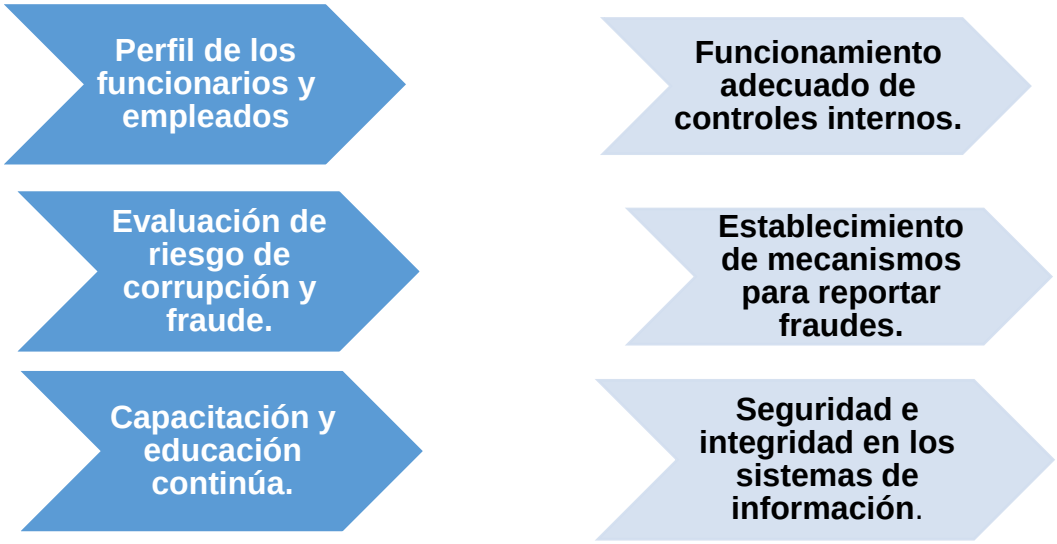
que ayudarán a prevenir, detectar y reducir de manera significativa el índice de fraudes de tarjeta de crédito y débito.

La implantación de las mejores prácticas en las Instituciones Financieras, implica el establecimiento de una política integral que brinde seguridad a los empleados y a los tarjetahabientes, se tendrá que examinar las causas y consecuencias de todo fraude que sea detectado y se diseñará estrategias factibles que reduzcan su incidencias y efecto. Entonces, ¿Qué deben hacer las Instituciones Financieras para blindarse contra posibles Fraudes de tarjeta de crédito y débito? Simplemente, adoptar las mejores prácticas que ayuden a reducir los índices del fraude y la corrupción.[42]

La Asociación de Examinadores de Fraude Certificados-ACFE (domiciliado en México), considera que se pueden implementar 11 prácticas dentro de las organizaciones para la prevención, detección y disuasión de fraudes. Para propósito de ésta investigación consideramos la implementación de solo 6 de estas prácticas de prevención de fraude citadas por el ACFE, a continuación las mencionamos:

[42]http://www.revistadelfraude.com/Ediciones_anteriores/julio_agosto/Las%20mejores%20practicas%20para%20prevencion%20y%20deteccion%20del%20fraude%20.html 2014 ACFE-México

**Gráfico 17: "Prácticas para la Prevención, Detección y Disuasión de Fraudes"**




**Fuente:** http://www.revistadelfraude.com/; Edición: Agosto 2014
**Elaborado por:** Autoras

- **Perfil de los funcionarios y empleados**

La selección debe estar dirigida en relación a las funciones del puesto, debe existir independencia, objetividad, honestidad e imparcialidad. Los cargos deben estar al mando de profesionales totalmente preparados y honestos y que ya hayan tenido experiencia.

- **Funcionamiento adecuado de controles internos.**

La administración debe garantizar la gestión y el desempeño eficaz de la Institución Financiera y su apropiada rendición de cuentas. Debe existir un fortalecimiento del control interno en los procesos de la parte operativa de

las tarjetas de créditos y de forma continua deben revisarse para inhibir o detectar alguna posibilidad de fraude.

- **Evaluación de riesgo de corrupción y fraude.**

  - ✓ Cumplir y asegurar el cumplimiento de las políticas, metodologías y procedimientos definidos por la administración encargada de la evaluación de riesgos o por la unidad antifraude si existiese.
  - ✓ Controlar las mediciones de riesgos realizadas por las aéreas responsables.
  - ✓ Realizar las acciones pertinentes de acuerdo con los resultados de los análisis.

- **Establecimiento de mecanismos para reportar fraudes.**

  - ✓ Línea Ética de Denuncias: Se le otorga confianza a terceros para recibir reportes de fuentes internas y externas, prevalece el anonimato y la confidencialidad. Aquellas denuncias anónimas a su vez deben ser investigadas de manera eficaz y oportuna. Procedimientos para la atención de quejas o reclamaciones y aceptar toda la información proporcionada de manera anónima.

- **Capacitación y educación continúa**
  - ✓ Educación continua a los empleados en temas vinculados con su cargo y sus respectivas funciones, es esencial ya que ayuda a prevenir y detectar el fraude, ya que ciertos empleados a través del uso indebido de los recursos de la organización o en ayuda con otro empleado de la misma u otra aérea se ponen de acuerdo para cometer algún fraude, esto es lo que se conoce como colusión.

- ✓ Por la falta de capacitación a los empleados comienzan a surgir una serie de problemáticas ya que el personal de la Institución Financiera comienza a incumplir las políticas y procedimientos y los controles previamente establecidos.
- ✓ Evitar el conflicto de intereses y propiciar blindaje mediante la concientización.
- ✓ Capacitar en temas éticos a los miembros de la entidad.

- **Seguridad e integridad en los sistemas de información**

  Las Instituciones Financieras deben implementar controles que invaliden el acceso de personas no autorizadas a los sistemas, ya que el delincuente informático puede ser uso de las técnicas conocidas como: Puertas falsas (trap doors) o Las "Llaves Maestras" (Superzapping), y puede consultar o modificar cualquier tipo de información o también pueden llegar a tener acceso a la propia base de datos y archivos aunque se encuentren reservados, siendo este un gran riesgo porque se puede llegar tener acceso a una cuenta de un tarjetahabiente y modificar el saldo de su tarjeta y trasladar cualquier cifra a un número de cuenta desconocido.

  Una de las formas para disminuir el Riesgo en el sistema financiero es el blindaje de seguridad que consiste en limitar los controles de seguridad y las claves de acceso a los sistemas de las aéreas relacionadas con la intermediación de cuentas bancarias, valores y divisas, para evitar que recaigan en una sola persona, el cumplimiento de cada control y sus procedimientos para reducir el Riesgo operativo.

  Se sugiere que las Instituciones Financieras deban tener un Plan de Recuperación de Desastres (DRP), debido a que diversos esquemas fraudulentos involucran la manipulación de datos de entrada o de registros de salida en los diferentes sistemas.

  A continuación se presenta técnicas para los sistemas de información seguros:

- **Gráfico 18: "Integración de Sistemas de Información"**


**Fuente:** http://www.revistadelfraude.com/; **Edición:** Agosto 2014
**Elaborado por:** Autoras

Es responsabilidad de los altos directivos de las Instituciones Financieras asegurar la implementación de cada control que se haya creado para minimizar el riesgo de posibles ataques de fraude por parte delincuentes informáticos externos o internos, sobre todo como líderes de las Instituciones Financieras deben comenzar a crear una cultura basada en el profesionalismo e integridad.

# CAPÍTULO III

# DISEÑO Y MODALIDAD DE LA INVESTIGACIÓN

De acuerdo a lo expuesto por BUENDÍA, COLÁS Y HERNÁNDEZ (1997), El marco metodológico es donde se expone la manera de cómo se va a realizar la investigación, los pasos para realizarlo y el método investigativo que se utilizará.

En el desarrollo de esta investigación se empleó el método de investigación descriptiva que es una forma de estudio para saber quién, donde, cuando, cómo y porqué del sujeto del estudio.[43] Mediante el desarrollo de ésta investigación se pretende conocer de forma detallada las diferentes técnicas de fraude que utilizan los delincuentes digitales o defraudadores para perjudicar a los usuarios de tarjetas de crédito y/o débito para posteriormente determinar cuál es la técnica más utilizada en la ciudad de Guayaquil y cuanto es el promedio de victimas por fraude en los últimos 3 años para de ésta forma poder proporcionar una serie de medidas de prevención contra el fraude de tarjetas de créditos y/o débitos que logren ser aplicadas por las Instituciones Financieras y también para los tarjetahabientes, a su vez hacerles conocer a los tarjetahabientes los riesgos que pueden tener al no usar correctamente sus respectivas tarjetas y todo lo que implicaría ser víctima de un fraude.

Además describiremos el perfil del defraudador para que los tarjetahabientes al momento de realizar alguna transacción con sus respectivas tarjetas, tengan en consideración tales características y las correspondientes precauciones para así evitar ser víctimas de un posible fraude

El enfoque que se utilizó es mixto ya que responden a una metodología fundamentada en la técnica cuantitativo-cualitativa, en donde se utiliza la recolección y el análisis de datos para contestar preguntas de

[43] Namakforoosh(2005). Metodología de Invetsigación. Mexico: Limusa

investigación y probar hipótesis establecidas previamente, y se confía los resultados en la medición numérica, el conteo y el uso de la estadística,[44] a fin de identificar las posibles causas y vulnerabilidades con que se originan los fraudes en las tarjetas de crédito y /o débito, así como describir las nuevas implementaciones de seguridad que están empleando las Instituciones Financieras como es el caso de cambio de tarjetas con banda magnética por una tarjeta con chip inteligente.

La técnica que se utilizó para organizar nuestra investigación es la de campo[45] que nos permite la observación en contacto directo con el objeto de la investigación, las páginas web relacionadas con el fraude de tarjetas de crédito y débito fueron de gran ayuda para ampliar nuestros conocimientos acerca de cada técnica de fraude que son empleadas por los defraudadores, también se optó por realizar encuestas a tarjetahabientes con la finalidad de identificar que técnica de fraude es la más utilizada en Guayaquil, se solicitó la información estadística actualizada a la Fiscalía General del Estado mediante una carta dirigida al Dr. Paul Ponce Quiroz(Fiscal Provincial Del Guayas), con el propósito de determinar el porcentaje de denuncias receptadas.

## 3.1 TIPO Y DISEÑO DE INVESTIGACIÓN

La investigación realizada puede entrar dentro de los parámetros de la modalidad de investigación documental ya que el desarrollo de ésta investigación hace referencia a la prevención y disuasión de operaciones fraudulentas con tarjeta de crédito y/o Débito con el propósito de ampliar y profundizar el conocimiento de su naturaleza, con apoyo, principalmente, en trabajos previos, información y datos divulgados por medios impresos, audiovisuales o electrónicos.

[44] Marcelo M. Gómez. Argentina. (2006) Introducción a la Metodología de la Investigación Científica el enfoque cuantitativo

[45] Balcells I Jungyent, J. Mexico. (1994). La investigación social: introducción a los métodos y técnicas. Barcelona: Escuela Superior de Relaciones Públicas, PPU.

Vélez S. (2001), afirma que este tipo de investigación tiene como objetivo “el desarrollo de las capacidades reflexivas y críticas a través del análisis, interpretación y confrontación de la información”.

Entre los propósitos de este tipo de investigación se encuentran: describir, mostrar, probar, persuadir o recomendar.

La investigación debe llevar a resultados originales y de interés para el grupo social de la investigación, por este motivo tomamos en cuenta toda y cada una de las características del problema, el tipo de investigación elegido y de acuerdo a los objetivos previamente planteados concluimos que ésta investigación cuenta con los propósitos de describir, probar y recomendar.

Describir, pues se detalla el perfil y la naturaleza de los defraudadores, como proceden en el momento del delito, y detalles vitales para tener una visión totalmente despejada de lo que el delito se trata.

Probar mediante datos reales, los fraudes cometidos en la ciudad de Guayaquil, la técnica que se empleó y si existen las difusiones correspondientes por partes de las autoridades para prevenir los fraudes con tarjeta de crédito y/ o débito.

Recomendar el planteamiento de una metodología de prevención para los tarjetahabientes y las Instituciones Financieras para disminuir el riesgo de fraude y evitar las pérdidas monetarias que afecta económicamente y emocionalmente a las víctimas.

## 3.2 POBLACIÓN Y MUESTRA

### 3.2.1 POBLACIÓN

También llamada universo o colectivo, es el conjunto sobre el que estamos interesados en obtener conclusiones (hacer inferencia). Normalmente es demasiado grande para poder abarcarlo.

En este caso al referirnos a la población, estaremos hablando del total de tarjetahabientes que según información al mes de junio de 2013 por parte de la Superintendencia de Bancos y Seguros (SBS), hay un número estimado de 1.9 millones de tarjetahabientes, el cual el 25% corresponden a la ciudad de Guayaquil.

## 3.2.2 MUESTRA

La muestra es un subconjunto de la población, por esto el número que compone la muestra es menor que el de la población, pero suficiente para que la estimación de los parámetros determinados tenga un nivel de confianza adecuado. Para que el tamaño de la muestra se idóneo es preciso recurrir a su cálculo.[46]

En base a esto se determinó que 1.016 sería el total de nuestra muestra, llegando así a lo que se detalla a continuación:

**Tabla 5: Determinación de la Muestra**

| | |
|---|---|
| Total de Tarjetahabientes en Ecuador | **1.900.000** |
| Total en Guayaquil (25%) | 475.000 |
| Total Encuestados | 1.016 |
| Muestra Cubierta | 0,21% |

Para el desarrollo de la presente investigación se realizaron encuesta a un total de 1,016 tarjetahabientes y para la tabulación de los resultados se hizo uso de los gráficos estadísticos con su respectivo análisis e interpretación y por razones de ubicación para realizar la encuesta se eligió como zona geográfica la ciudad de Guayaquil, hombres y mujeres del sector

[46] http://www.smo.edu.mx/colegiados/apoyos/muestreo

Norte y Sur de Guayaquil mayores de 18 años de edad que indispensablemente tenían que ser usuarios de tarjetas de crédito y/o débito.

## 3.3 DOCUMENTOS

La documentación utilizada para esta investigación fue tomada de denuncias que fueron realizadas por las víctimas de fraude en la Fiscalía General del Estado, boletines electrónicos publicados por las mismas instituciones financieras emisoras de las tarjetas.

A efectos de obtener la información que sirvió de base para alcanzar los resultados del presente estudio, se realizaron encuestas a usuarios de tarjetas de crédito y/o débito, dicha encuesta fue realizada a los alrededores de los diferentes centros comerciales que existen en la ciudad de Guayaquil como son: Mall del Sol, Mall del sur, San Marino, City Mall, Riocentro Norte. Riocentro Ceibos y Riocentro Sur.

Como limitación al trabajo de investigación, hacemos mención a la prohibición que la administración de los centros comerciales establecen no realizar encuestas dentro de los mismos, es por aquello que se optó por realizarlo a los alrededores; así como otra dificultad fue el encontrarse personas dispuestas a proporcionar información a las encuestas realizadas ya que es un tema delicado y las personas en Guayaquil no acceden con facilidad a responder encuestas en las calles debido a la inseguridad que existe.

## 3.4 ENCUESTAS

Se encuestaron a usuarios de tarjetas de crédito y/o débito para analizar las diferentes técnicas de fraude de las que se puede ser objeto por no tener las correspondientes precauciones al hacer uso de las tarjetas, así como para conocer qué porcentaje ha sido víctima de algún tipo de fraude y si sus reclamos han sido atendidos y resueltos por las correspondiente autoridades ya sea por la Superintendencia de Bancos o por el Banco Emisor de la Tarjeta, se procedió a tabular los resultados obtenidos en las

1,016 encuestas elaboradas a continuación se detalla la información obtenida:

## Formato De Encuesta Realizada Para El Proyecto Investigativo:

**ENCUESTA**

1. ¿Ha sufrido alguna vez fraude por tarjetas de crédito/débito?
   __Si
   __No

2. Si la respuesta fue afirmativa indicar fraude:
   __Fishing(Los delincuentes obtienen información confidencial a través de un correo electrónico)
   __Skimming (el delincuente la pasa por un aparato llamado skimmer que graba la información de la banda magnética)
   __Phaming (re-direcciona al usuario y lo manda a una página que se ve como la original de su banco)
   __Malware (aquellos diseñados para captar y grabar las teclas que el usuario digita

3. ¿Realizó reclamo?
   __Si
   __No

4. ¿Si usted realizó el reclamo indicar frente a cual entidad de estas lo realizó?
   __Superintendencia de Bancos
   __Emisor de la tarjeta.

5. ¿El reclamo fue favorable?
   __Si
   __No

6. ¿Considera usted que existe información suficiente sobre prevención de fraudes con tarjetas de crédito/débito?
   __Si
   __No

7. ¿Considera conveniente se realice difusión sobre la prevención de fraudes con tarjeta de crédito/debito?
   __Si
   __No

8. ¿Cuál de estas alternativas considera conveniente para prevenir los fraudes con tarjetas de crédito/débito?

   __Clave adicional por compras/débitos mayores a un valor determinado.
   __Convenios de fortalecimiento de confianza entre establecimientos[47].
   __ Seguros contra fraude electrónico.
   __ Claves adicionales con códigos QR[48].
   __ Prohibir venta de bases de datos.
   __ Mensajes frecuentes para educar sobre Seguridad de la Información
   __Otros (especificar)

[47] Convenios entre empresas para la adecuada administración de la información de los clientes.
[48] Sistema que permite almacenar información en una especie de código de barras de última generación.

## 1. ¿Ha sufrido alguna vez fraude por tarjetas de crédito/débito?

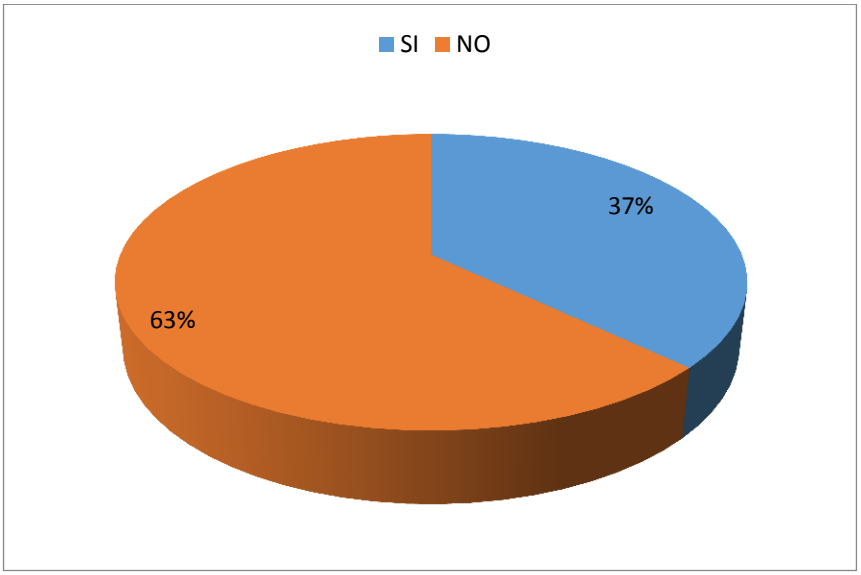
**Tabla 6**

| Detalle | Datos | % |
|---|---|---|
| **SI** | 377 | 37.11% |
| **NO** | 639 | 62.89% |
| **TOTAL** | 1016 | 100.00% |

**Fuente:** Investigación del mercado

**Elaborado por:** Autoras

**Gráfico 19**




**Fuente:** Investigación del mercado

**Elaborado por:** Autoras

### Análisis e Interpretación

Se realizó la encuesta a un total de 1016 tarjetahabientes de los cuales un 63% nos mencionó que no habían sido víctima de fraude por tarjeta de crédito y/o débito mientras que un 37% si han sido perjudicados por algún tipo de fraude, esto a pesar de que el índice de fraude con tarjeta de crédito y/o débito ha ido incrementando en el año 2012 y 2013.

**2. Si la respuesta fue afirmativa indicar fraude:**

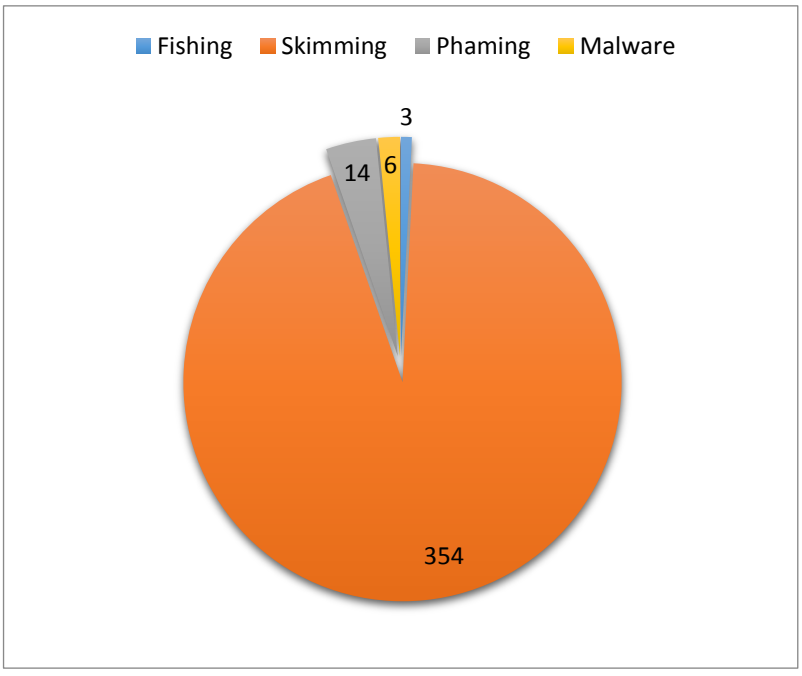
**Tabla 7**

| Detalle | Datos | % |
|---|---|---|
| **FISHING** | 3 | 0.80% |
| **SKIMMING** | 354 | 93.90% |
| **PHAMING** | 14 | 3.71% |
| **MALWARE** | 6 | 1.59% |
| **TOTAL** | 377 | 100.00% |

**Fuente:** Investigación del mercado

**Elaborado por:** Autoras

**Gráfico 20**




**Fuente:** Investigación del mercado

**Elaborado por:** Autoras

**Análisis e Interpretación**

Los encuestados nos hicieron conocer por cual técnica de fraude han sido víctimas, se detallaron 4 técnicas de fraude más comunes que son realizadas por el defraudador y se obtuvo que el 1% de los encuestado ha sido víctima de fraude por Fishing, que consiste en que los delincuentes obtienen información confidencial a través de un correo electrónico, el 94% encuestado ha sido víctima de fraude por skimming en esta técnica el delincuente la pasa por un aparato llamado skimmer la tarjeta y graba la información de la banda magnética, el 4% ha sido víctima con la técnica phaming que es la que re-direcciona al usuario y lo manda a una página que se ve como la original de su banco, mientras que el 2% ha sido víctima con la técnica llamada malware que es aquella que es diseñada para captar y grabar las teclas que el usuario digita.

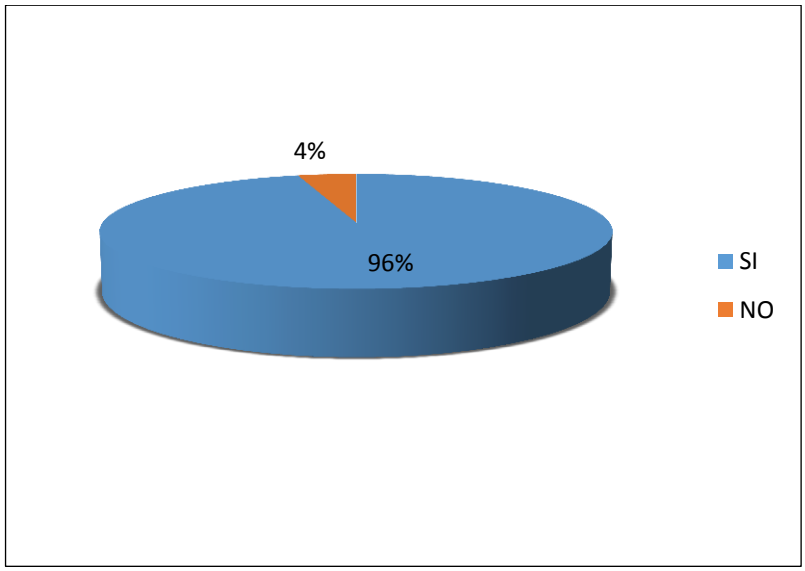
## 3. ¿Realizó el reclamo?

**Tabla 8**

| Detalle | Datos | % |
|---|---|---|
| **SI** | 361 | 95.76% |
| **NO** | 16 | 4.24% |
| **TOTAL** | 377 | 100.00% |

**Fuente:** Resultados de Encuestas
**Elaborado por:** Autoras

**Gráfico 21**




**Fuente:** Resultados de Encuestas
**Elaborado por:** Autoras

### Análisis e Interpretación

De los encuestados que si han sido víctimas de fraude, el 96% indicó que si ha realizado el reclamo correspondiente mientras que el 4% ha optado por no realizar ningún reclamo, algunos de ellos nos indicaban que era porque el fraude era de un valor no tan alto, más o menos era un promedio de $25.

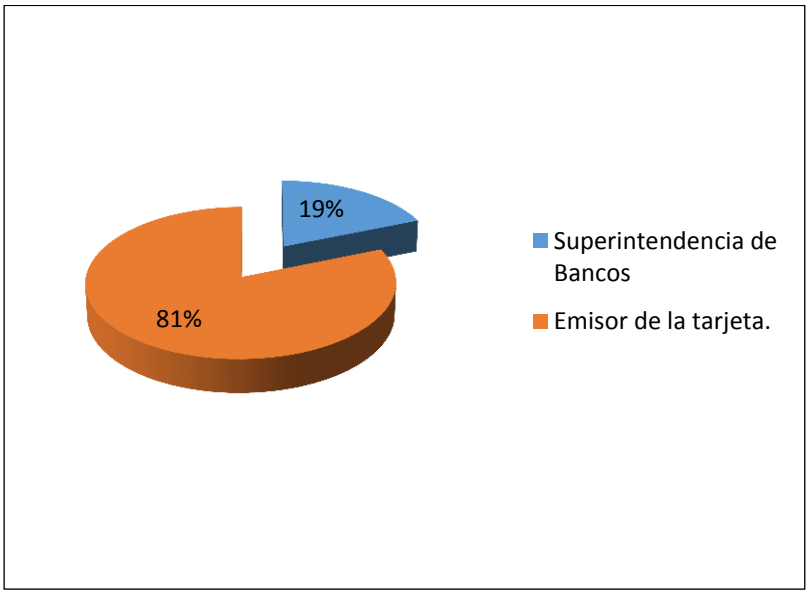
**4. ¿Si usted realizó el reclamo indicar frente a cual entidad de estas lo realizó?**

**Tabla 9**

| Detalle | Datos | % |
|---|---|---|
| SUPERINTENDENCIA DE BANCOS | 71 | 18.83% |
| EMISOR DE LA TARJETA. | 306 | 81.17% |
| TOTAL | 377 | 100.00% |

**Fuente:** Resultados de Encuestas
**Elaborado por:** Autoras

**Gráfico 22**




**Fuente:** Resultados de Encuestas
**Elaborado por:** Autoras

**Análisis e Interpretación**

El 81% de la población encuestada decidió poner el reclamo frente al emisor de la respectiva tarjeta que poseen, mientras que el 19% o realizo en la Superintendencia de Bancos, cabe recalcar que algunos encuestados nos indicaban que no tenían conocimiento que en la Superintendencia de Bancos también se podía poner el reclamo por el fraude.

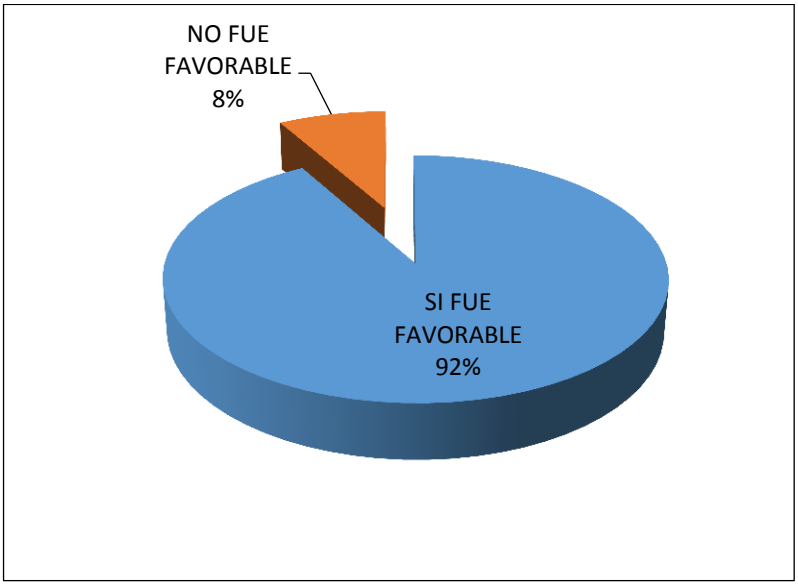
## 5. ¿El reclamo fue favorable?

**Tabla 10**

| Detalle | Datos | % |
|---|---|---|
| **SI FUE FAVORABLE** | 346 | 91.78% |
| **NO FUE FAVORABLE** | 31 | 8.22% |
| **TOTAL** | 377 | 100.00% |

**Fuente:** Resultados de Encuestas
**Elaborado por:** Autoras

**Gráfico 23**




**Fuente:** Resultados de Encuestas
**Elaborado por:** Autoras

### Análisis e Interpretación

Para el 92% de los encuestados fue favorable el reclamo que realizaron es decir las cantidades fueron reembolsadas en su totalidad pero el 8% que es un porcentaje considerablemente bajo no obtuvo reembolso de la cantidad que fue sustraída de su tarjeta mediante el fraude ya que no pudieron probar el faltante de dinero de la tarjeta.

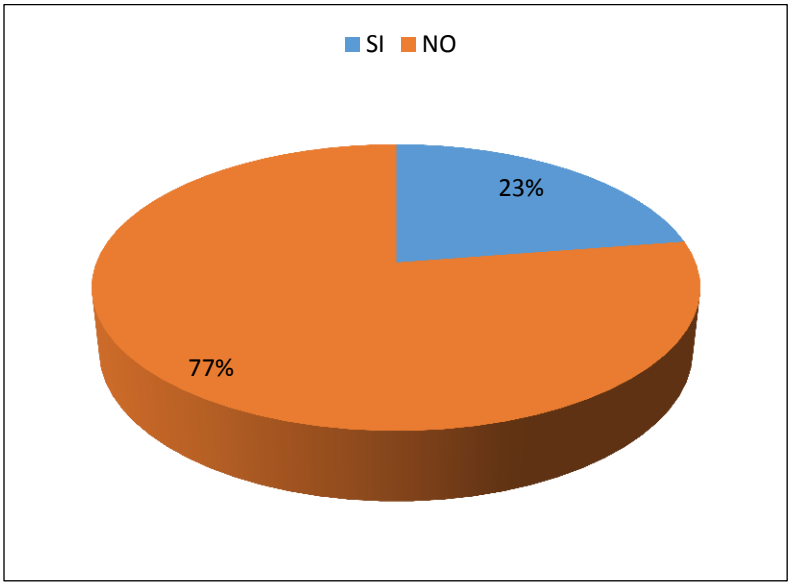
**6. ¿Considera usted que existe información suficiente sobre prevención de fraudes con tarjetas de crédito/débito?**

**Tabla 11**

| Detalle | Datos | % |
|---|---|---|
| **SI** | 229 | 22.54% |
| **NO** | 787 | 77.46% |
| **TOTAL** | 1016 | 100.00% |

**Fuente:** Resultados de Encuestas
**Elaborado por:** Autoras

**Gráfico 24**




**Fuente:** Resultados de Encuestas
**Elaborado por:** Autoras

**Análisis e Interpretación**

Para el 77% de los encuestados no existe información suficiente sobre prevención de fraudes con tarjetas de crédito/débito, la mayoría de ellos solo tenían conocimiento sobre la clonación de las tarjetas por las noticias de los diferentes canales televiso que hacen referencia de la desarticulación de bandas de clonadores de tarjeta y/o débito pero no porque las Entidades pertinentes han tomado las medidas necesarias, mientras que tan solo un 23% considera que si existe información sobre prevención de fraudes con tarjetas de crédito/débito.

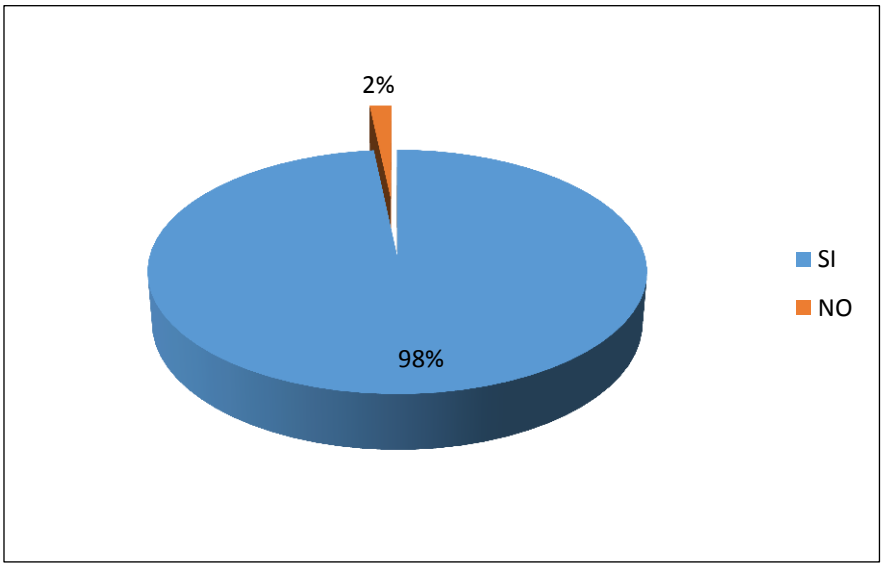
**7. ¿Considera conveniente se realice difusión sobre la prevención de fraudes con tarjeta de crédito/debito?**

**Tabla 12**

| Detalle | Datos | % |
|---|---|---|
| **SI** | 999 | 98.33% |
| **NO** | 17 | 1.67% |
| **TOTAL** | 1016 | 100.00% |

**Fuente:** Resultados de Encuestas
**Elaborado por:** Autoras

**Gráfico 25**




**Fuente:** Resultados de Encuestas
**Elaborado por:** Autoras

**Análisis e Interpretación**

Con un total de 98% la población encuestada consideró la importancia de la difusión de medidas preventivas para los tarjetahabientes para que así las Instituciones Financieras, emisoras de tarjetas blinden sus seguridades y constantemente estén controlando las posibles vulnerabilidades de sus sistemas informáticos y de sus cajeros automáticos y así lograr disminuir el riesgo, mientras que un mínimo de encuestados que corresponde al 2% no considera conveniente que se le informe a la ciudadanía sobre las medidas de seguridad que deben emplear para evitar fraudes con sus tarjetas.

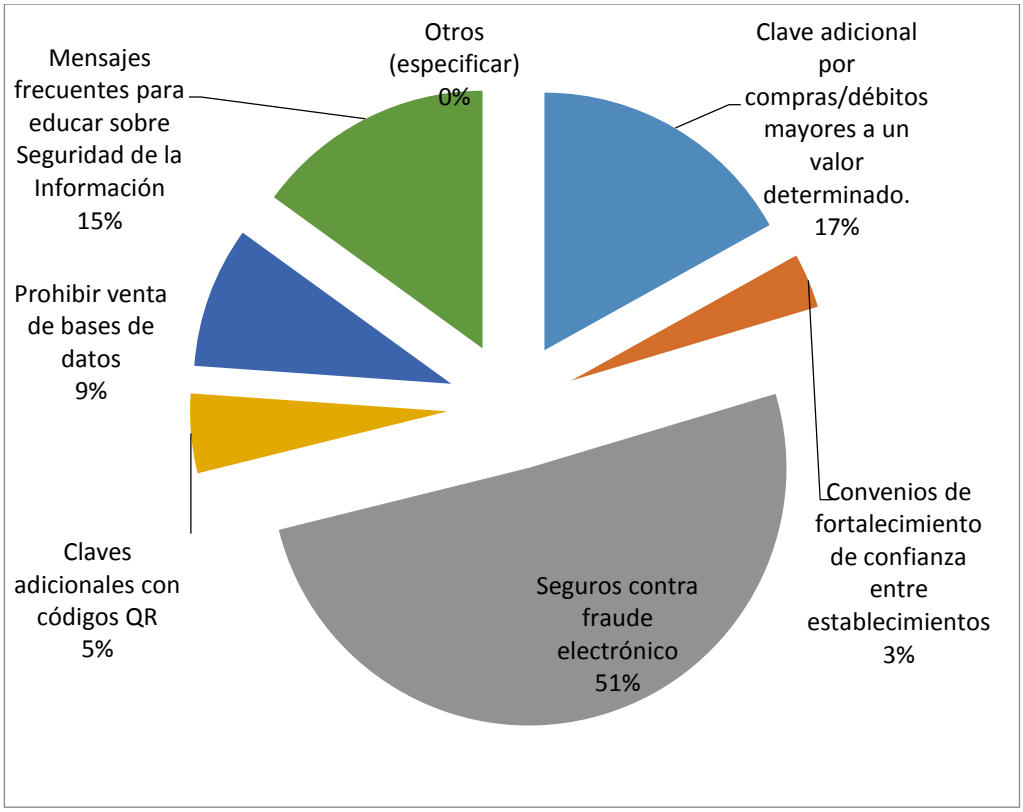
**8. ¿Cuál de estas alternativas considera conveniente para prevenir los fraudes con tarjetas de crédito/débito?**

**Tabla 13**

| Detalle | Datos | % |
|---|---|---|
| **Clave adicional por compras/débitos mayores a un valor determinado.** | 187 | 16.92% |
| **Convenios de fortalecimiento de confianza entre establecimientos** | 38 | 3.44% |
| **Seguros contra fraude electrónico** | 561 | 50.77% |
| **Claves adicionales con códigos QR**[49] | 55 | 4.98% |
| **Prohibir venta de bases de datos** | 98 | 8.87% |
| **Mensajes frecuentes para educar sobre Seguridad de la Información** | 166 | 15.02% |
| **Otros (especificar)** | | |
| TOTAL | 1105 | 100.00% |

**Fuente:** Resultados de Encuestas
**Elaborado por:** Autoras

**Gráfico 26**




**Fuente:** Resultados de Encuestas

**Elaborado por:** Autoras

[49] Sistema que permite almacenar información en una especie de código de barras de última generación.

**Análisis e Interpretación**

A los encuestados se les dio ciertas alternativas para que respondan cuales les consideraban conveniente para prevenir los fraudes con tarjetas de crédito/débito, el 51% dijo que lo mejor alternativa era un seguro contra fraude electrónico, cabe recalcar que éste seguro no debe por qué tener un costo adicional para el usuario dela tarjeta ya que las Instituciones Financieras están obligadas mediante ley a reponerle al tarjetahabiente el total de la cifra que haya sido sustraída siempre y cuando sea demostrado que el fraude fue porque el defraudador pudo vulnerar las seguridades de dicha entidad, el 17% estuvo de acuerdo que el proporcionar una “Clave adicional” por compras/débitos mayores a un valor determinado era la mejor alternativa para ir en una constante disminución del riesgo de fraude, el 15% optó por mensajes frecuentes para educar sobre Seguridad de la Información a cada tarjetahabientes ya que una gran mayoría no son consiente del buen uso que deben darle a sus respectivas tarjetas, el 9% dice que se deberá prohibir venta de bases de datos el 5% Claves adicionales con códigos QR que se refiere a un Sistema que permite almacenar información en una especie de código de barras de última generación que será de gran ayuda para las compras online, mientras que un 3% optó por Convenios de fortalecimiento de confianza entre establecimientos para la adecuada administración de la información de los clientes. Aunque en las opciones se les daba la oportunidad para que los encuestados de forma abierta pongan una alternativa, nuestras alternativas expuestas les fue suficiente y ninguno de los 1.016 encuestados decidió dar alguna alternativa diferente a las indicadas.

# CAPÍTULO IV

# CONCLUSIONES Y RECOMENDACIONES

La finalidad de ésta investigación sobre las técnicas de fraudes más usados con tarjeta de crédito y débito es poder brindarles a las Instituciones Financieras y a los tarjetahabientes medidas de control para que puedan ser aplicadas para prevenir el riesgo.

## 4.1 MEDIDAS DE PREVENCIÓN PARA LAS INSTITUCIONES FINANCIERAS CONTRA EL FRAUDE EN TARJETAS DE CRÉDITO Y DÉBITO

### 4.1.1 POLÍTICAS GENERALES COMO UNA OPCIÓN DE PREVENCIÓN DE FRAUDE

Las Instituciones Financieras podrán aplicar en el interior de su organización las siguientes políticas:

- Debe existir un comité de ética dentro de la Institución Financiera con la finalidad de controlar el cumplimiento de las políticas de prevención de fraude que hayan sido establecidas en el código de ética elaborado previamente;

- Actualizar la información básica de todos los clientes y analizar los tipos de operaciones y con qué frecuencias las realizan;

- Los empleados de las Instituciones Financieras deben estar capacitados sobre los servicios nuevos que se vayan a brindar a los clientes y previamente al lanzamiento, la unidad de cumplimento debe verificar y analizar cuáles son las transacciones que se derivan de dicho servicio, si existen vulnerabilidades y si se necesita reportar a los Órganos de Control;

- Los jefes de cada área deberán supervisar a su personal y hacer cumplir las políticas de prevención y control de fraude;

- La información que se posea sobre algún fraude que haya sido detectado debe ser confidencial;

- La unidad de cumplimiento en conjunto con las aéreas administrativas deberán absolver las consultas de los clientes;

- Realizar como control una verificación automática en el sistema de lavado de activo previo a la vinculación del cliente;

- Verificar en el Buró de Crédito el historial crediticio del cliente, y;

- Controlar el funcionamiento del sistema de información para detectar cual anomalía de forma oportuna y constatar que se esté cumpliendo con todos los límites establecidos.

Estas políticas propuestas ayudarán a las Instituciones Financieras a la prevención, monitoreo y al análisis para comprobar posible fraude:

**Prevención:** estudia el posible riesgo al que estaría expuesta la organización según sus actividades y procedimientos, en este paso se proceden a implementar los controles que existan o a crear los que sean necesarios para disminuir el riesgo de que se cometa el fraude.

**Monitoreo:** se realizará los análisis de datos obtenidos y se utilizaran los parámetros necesarios para observar si no hay desvío de información y si cada funcionario está cumpliendo con sus respectivas funciones y así comprobar la adecuada segregación de funciones.

**Análisis para comprobar posible fraude**: si se sospecha de algún posible fraude hay que observar dicha aérea poner a prueba a los funcionarios que la conforman y si se llegase a comprobar que se ha cometido fraude dentro

de la organización o que se llevara a cabo se debe tomar las correctas medidas y verificar los controles diseñados para ver si necesitan ser modificados o si no han estado siendo aplicados de forma correcta.

### 4.1.2 IMPORTANCIA DE LA APLICACIÓN DE MARCO COSO ENTERPRISE RISK MANAGEMENT (ERM)

Según COSO (Committee of Sponsoring Organizations of the Treadway) "*el Control Interno es un proceso llevado a cabo por la dirección y el resto del personal de una entidad, diseñado con el objeto de proporcionar un grado de seguridad razonable*", es por este motivo que sugerimos a las Instituciones financieras aplicar controles tomando como base de referencia todos o algunos de los componentes que sustenta la práctica del COSO ERM ya que ayudará a la eficacia y eficiencia de las operaciones que desarrollen y los usuarios se sentirán confiados al momento de realizar sus transacciones.

También recomendamos implementar el "COSO ERM" con el objetivo de que se diseñen o evalúen los controles ya existentes dentro de las Instituciones Financieras para reconocer si se han diseñado o si se están llevando a cabo de la manera correcta; los controles son efectivos cuando:

- Previenen;
- Detectan, y;
- Dan una respuesta inmediata frente a posibles irregularidades o riesgos de fraude en las que se vería afectada la entidad.

El "COSO ERM" ayudará a las Instituciones Financieras mediante la gestión de posibles riesgos de fraude que pudieran presentarse, poniendo en ejecución los siguientes 8 componentes con el que se encuentra estructurado[50]:

[50] http://www.aec.es/web/guest/centro-conocimiento/coso Committee of Sponsoring Organizations of the Treadway)

- **Ambiente de control:** son los valores y filosofía de la organización, influye en la visión de los trabajadores ante los riesgos y las actividades de control de los mismos;
- **Establecimiento de objetivos:** estratégicos, operativos, de información y de cumplimientos;
- **Identificación de eventos:** que pueden tener impacto en el cumplimiento de objetivos;
- **Evaluación de Riesgos:** identificación y análisis de los riesgos relevantes para la consecución de los objetivos;
- **Respuesta a los riesgos:** determinación de acciones frente a los riesgos;
- **Actividades de control:** Políticas y procedimientos que aseguran que se llevan a cabo acciones contra los riesgos;
- **Información y comunicación:** eficaz en contenido y tiempo, para permitir a los trabajadores cumplir con sus responsabilidades, y;
- **Supervisión:** para realizar el seguimiento de las actividades.

**Gráfico 27: "Marco Coso ERM"**


Fuente: http://www.aec.es/web/guest/centro-conocimiento/coso

## 4.1.3 INDICADORES DE GESTIÓN

Por lo anteriormente sugerido, es de mucha importancia que la Instituciones Financieras hagan uso de indicadores de gestión, éstos son realizados por los líderes de la organización y se refieren a una unidad de medida gerencial que como su nombre lo indica permitirá a la organización evaluar su gestión o desempeño frente a sus metas y objetivos planteados.

Los indicadores de gestión deben cumplir con una serie de características para comprobar que sea útil y efectivo:

- **RELEVANTE:** Que esté relacionado con los objetivos y metas planteadas por la organización;
- **CLARAMENTE DEFINIDO:** Que dicho indicador me ayude a obtener resultados acerca del tema a investigar y que haya una correcta recopilación y comparación de datos;
- **COMPARABLE:** Que se pueda comparar dentro y fuera de la organización para realizar el estudio correspondiente, también debe ser fácil de usar y comprender, y;
- **COSTO-EFECTIVO:** Que la organización no necesite incurrir en elevados costos para poder aplicar los indicadores.[51]

De acuerdo a la Federación Latinoamericana de Bancos hemos considerado 7 indicadores de Gestión para que el departamento de Prevención de Fraude de las Instituciones Financieras pueda controlar, mejorar y comprobar los procesos ya existentes y Mediante los resultados que se obtengan al emplear los indicadores puedan cubrir las falencias existentes como por ejemplo la capacitación del personal, y detectar el número de transacciones inusuales por parte de los tarjetahabientes en periodos determinados y el cumplimiento de las políticas y procedimientos.

[51] http://www.degerencia.com/tema/indicadores_de_gestion

A continuación detallamos los Indicadores de Gestión a aplicar:

| INDICADORES DE GESTION PARA LAS INSTITUCIONES FINANCIERAS | | | | |
|---|---|---|---|---|
| **OBJETIVOS** | **METAS** | **ACTIVIDADES** | **INDICADORES** | **CUMPLIMIENTO** |
| **1. CAPACITACIÓN** | | | | |
| a) Tener al personal capacitado<br>b) cumplir con el plan de capacitación | Capacitar al 100% del personal | a) Diseño del material de difusión.<br>b) Programar la capacitación.<br>c) Evaluar las capacitaciones.<br>d) Elaborar informes de los resultados obtenidos | Número de colaboradores<br>vs<br>N total del personal de la empresa. | El calendario de capacitación se elaborará con RRHH |
| **2.CONTROLES** | | | | |
| a) Controlar que a nivel nacional se cumplan con las políticas, normas y reglamentos.<br>b) Cumplir plan anual de controles | Disminuir el riesgo, aplicando las políticas, normas y reglamentos. | a) Preparar las hojas de trabajo por áreas.<br>b) Verificar la documentación.<br>c) Controlar que las transacciones sean con tarjetas válidas.<br>d) Monitoreo diario de cuentas.<br>f) Realizar el seguimiento respectivo. | Transacciones Fraudulentas<br>Vs<br>Porcentaje<br>Numero diario de transacciones monitoreadas | Revisión de Fraudes detectados |
| **3.CLIENTE EXTERNO** | | | | |
| a) Conocer a su cliente, por su nicho de mercado y su actividad económica.<br>b) Informar oportunamente clientes con transacciones inusuales al Comité de ética para su análisis. | Que el personal de negocios aplique la política clara y precisa<br>“ conozca bien a su cliente” | a) Solicitar carpetas de créditos.<br>b) Visitar a los establecimientos<br>c) Elaborar los informes de novedades<br>d) Capacitar a los establecimientos.<br>e) Efectuar seguimientos a las transacciones inusuales para saber qué comercio<br>está involucrado. | Capacitar a los establecimientos<br>vs<br>Visitas a los establecimientos | Cronograma de Capacitación |
| **4.CLIENTE INTERNO** | | | | |
| a) Tener clientes internos con valores morales positivos.<br>b) Realizar las dos visitas al año para verificar el cumplimiento de sus políticas. | Que los Jefes inmediatos conozcan a sus empleados y tengan una información actualizada y adecuada.<br>Que el personal que ingresa sea idóneo mediante el conocimiento de sus antecedentes | a) Verificar al muestreo si la carpeta del personal nuevo tiene la documentación en regla.<br>b) Controlar que anualmente se actualice la información de los empleados antiguos.<br>c) Determinar si existen situaciones inusuales en el personal | Número de carpetas con novedades<br>vs<br>Muestra realizada. | Última semana del mes de julio |

| OBJETIVOS | METAS | ACTIVIDADES | INDICADORES | CUMPLIMIENTO |
|---|---|---|---|---|
| **5. ENVIO DE INFORMACION** | | | | |
| a) Enviar oportunamente a las entidades de control y con información confiable.<br>b) No ser amonestados ni multados por los organismos de control. | Que la información remitida sea y enviada dentro del tiempo establecido, de acuerdo a sus características informáticas | a) Registrar en un archivo de Excel los fraudes detectados<br>b) Revisar las novedades del archivo.<br>c) Corregir los errores encontrados.<br>d) Verificar la veracidad de la información.<br>e) Estructurar el archivo en el formato especial.<br>d) Enviar con los oficios respectivos. | Numero de fraudes detectados vs número de fraudes registrados | Hasta el 01 de cada mes |
| **6.TRANSACCIONES INUSUALES** | | | | |
| a) Detectar a clientes que realicen transacciones inusuales.<br>b) Informes mensuales de clientes que tengan transacciones inusuales al Comité de ética. | Identificar a tiempo a clientes con transacciones inusuales y minimizar el riesgo de un posible lavado de activos. | a) Subir archivos.<br>b) Procesar con las herramientas disponibles.<br>c) Obtener resultados de los procesos.<br>d) Analizar cada uno de los casos.<br>e) Determinar si existen insuavidades.<br>f) Entregar a los oficiales de negocios la información de los clientes.<br>g) Pedir a los oficiales que determinen mediante visitas a los establecimientos si son transacciones inusuales.<br>h) En caso de ser inusuales tomar una definición en el comité de Ética. | No de clientes con transacciones inusuales vs. Número de la muestra | Hasta 5 de cada mes |
| **7) CREACION DE SERVICIOS** | | | | |
| a) Participar activamente en la creación de nuevos servicios.<br>b) Que todos los servicios nuevos tengan controles para minimizar el riesgo. | Conocer los nuevos servicios, para crear los controles y disminuya el riesgo del mismo. | a) Asistir a las reuniones de creación de nuevos servicios.<br>b) Conocer los procesos del servicio.<br>c) Emitir criterios del servicio con relación al riesgo de fraude.<br>d) Diseñar una hoja de control.<br>e) Realizar seguimiento al servicio creado. | Clientes ubicados vs. La muestra | Cuando exista la creación de nuevos servicios |

**Fuente:** Federación Latinoamericana de Bancos
**Elaborado por:** Autoras

### 4.1.4 MÉTODOS DE PREVENCIÓN PARA DELITOS EN CAJEROS AUTOMÁTICOS EN LAS INSTITUCIONES FINANCIERAS

Actualmente el sector financiero en nuestro país está sujeto a constantes ataques por parte de delincuentes digitales o hackers, de manera que cada vez los tarjetahabientes se sienten menos seguros al realizar sus transacciones o retiros en los cajeros automáticos, se utilizan métodos cada vez más avanzados para el robo de identidad o clonación de tarjetas ésta situación nos genera la necesidad imperiosa de proponer medidas de seguridad muy actuales, modernas y sofisticadas, para de esta manera las Instituciones Financieras disminuyan el riesgo de fraude y evitar pérdidas millonarias.

Como una propuesta para la seguridad de las instituciones financieras en cajeros automáticos podemos mencionar lo siguiente:

- Evaluar el nivel de seguridad de la plataforma y la red IP del cajero automático, para poder detectar las diferentes vulnerabilidades e implementar una política de seguridad para corregir dichas falencias en la seguridad;
- Evaluación técnica constante en los cajeros automáticos, para de esta manera tener la certeza de que no ha sido vulnerado ningún componente, brindando así seguridad y confiabilidad;
- Mantener una política de confidencialidad en las comunicaciones que circulan en la red de los cajeros automáticos, de esta manera se reduce algún intento de intersección de las comunicaciones;
- Migrar totalmente de tarjetas de crédito y débito con banda magnética a chip, de ésta manera se busca disminuir el porcentaje de vulnerabilidad en las operaciones con tarjetas de crédito y débito, evitando así skimming o delitos similares, y;
- Disminuir la posibilidad de que el delito sea cometido desde dentro de la misma institución financiera, mediante la implementación de un sistema de usuarios privilegiados en los sistemas, analizando las

posibilidades de acceso por parte de cada uno de los usuarios de la entidad, encontrando las posibles vías de acceso que puede tener el posible defraudador interno. Se recomienda realizar una simulación de un ataque desde adentro de la institución financiera, de manera que las vulnerabilidades saltan a la luz y así brindaran la posibilidad de tener un sistema óptimo.

## 4.2 MEDIDAS DE PREVENCIÓN PARA LOS TARJETAHABIENTES CONTRA EL FRAUDE EN TARJETAS DE CRÉDITO Y DÉBITO

El jefe de Investigación Global y Equipo de Análisis de América Latina de Kaspersky, sugiere el mantenerse actualizado sobre cómo están operando los criminales de la informática ya que el estar protegido por antivirus no es suficiente.

### 4.2.1 FRAUDE EN LÍNEA

- Nunca se debe responder a los mensajes que suelen llegar al correo electrónico ya que el 100% de los mensajes solicitan información personal, que por seguridad se recomienda no brindar la información solicitada;
- Existen muchos vínculos que no son de confianza por este motivo es mejor que no se haga clic en ningún vínculo que aparezca en un mensaje sospechoso. En su lugar, visite los sitios Web escribiendo su dirección URL en el explorador o usando el vínculo Favoritos;
- Utilice contraseñas seguras y cámbielas con frecuencia combine letras en mayúsculas y minúsculas, números y símbolos de esta forma dificulta que otras personas puedan adivinarlas. No use palabras reales. Use una contraseña distinta para cada una de las cuentas;
- Mantener relaciones comerciales sólo con empresas que conozca y en las que confíe, póngase en contacto sólo con empresas conocidas que tengan en su sitio Web comercial una declaración de privacidad que afirme

específicamente que la empresa no cederá su nombre ni su información a terceros;

- La dirección Web debe ir precedida por **https://** en lugar del habitual **http://** en la barra de direcciones del explorador. Además, haga doble clic en el icono de candado  de la barra de estado del explorador para mostrar el certificado digital del sitio. El nombre que sigue a **Emitido para** del certificado debe coincidir con el sitio en el que piensa que está. Si sospecha que un sitio Web no es lo que debe ser, abandónelo inmediatamente e informe de ello. No siga ninguna de las instrucciones que contenga;
- Es importante que utilice un firewall, que mantenga el equipo actualizado y que utilice software antivirus, especialmente si se conecta a Internet mediante un módem por cable o un módem de línea de suscriptor digital (DSL);
- También se recomienda que considere el uso de software antispyware se puede descargar este software de Microsoft o utilizar un producto de otros fabricantes que esté disponible en el sitio de descargas y versiones de prueba de software de seguridad;
- Revise las confirmaciones de pedidos y los extractos de sus tarjetas de crédito y sus cuentas bancarias en cuanto los reciba, para verificar de que sólo se le están cargando las transacciones realizadas;
- Informe inmediatamente de cualquier irregularidad en sus cuentas marcando el número que se muestra en el extracto bancario, y;
- Es preferible la tarjeta de crédito que tenga el menor límite de crédito, porque así se limita la cantidad de dinero que el ladrón puede robar si obtiene los datos de la tarjeta, ahora varios de los principales emisores de tarjetas de crédito ofrecen a los clientes la opción de comprar en línea con números de tarjeta de crédito virtuales, de un solo uso, que caducan al cabo de uno o dos meses.

### 4.2.1 METODOS DE PREVENCIÓN PARA LOS TARJETAHABIENTES AL MOMENTO DE USAR UN CAJERO AUTOMÁTICO.

Los defraudadores o hackers harán todo lo posible para obtener su información personal o los datos de su tarjeta, sus fraudes llegan a ser un poco ingeniosas, pero si se toman las medidas de prevención correspondiente se podrá evitarlos.

Hoy en día los tarjetahabientes son muy propensos a que sean víctimas de fraude como la clonación de tarjetas de crédito y de débito, esto como ya sabemos se conoce como skimming y consiste en realizar una duplicación de manera ilegal de una tarjeta, existen muchas herramientas las cuales hacen posible este tipo de delitos en muchos casos los tarjetahabientes no se percatan de ser víctimas de estos delitos sino hasta que realizan una compra y se encuentran con la sorpresa que la tarjeta se encuentra al límite o con la llegada del estado de cuenta. Para evitar ser víctimas pueden en poner en prácticas los siguientes métodos de prevención

- Cuando el tarjetahabiente vaya a retirar dinero de algún cajero automático, asegurarse de que este no cuente con ningún dispositivo extraño instalado en la ranura donde se introduce la tarjeta de crédito o de débito;
- En el momento que proceda a ingresar el password o PIN (PERSONAL IDENTIFICATION NUMBER), intente cubrir con la otra mano, ya que suelen instalar pequeñas cámaras para grabar el password;
- Consultar con la entidad emisora de la tarjeta de crédito o débito si cuenta con la opción de alerta por medio de SMS (SHORT MESSAGE SERVICE), de esta manera el tarjetahabiente sabrá el momento exacto en que se realiza o se ejecuta una transacción,y;

- Tratar en lo posible de ubicar cajeros automáticos donde exista iluminación suficiente y que los cajeros automáticos luzcan en buen estado.

### 4.2.2 METODOS DE PREVENCIÓN PARA LOS TARJETAHABIENTES AL MOMENTO DE USAR UNA COMPUTADORA PARA REALIZAR UNA TRANSACCION

- Trate siempre de utilizar una computadora de confianza, porque en otros computadores nos podemos encontrar con sorpresas como KEYLOGER.
- En la actualidad encontramos conexiones wifi en muchas zonas públicas, si vas a conectarte desde tu computadora de una de estas redes públicas, evita en la medida de lo posible realizar transacciones en línea.
- Mantén actualizado el software de protección de tu computadora para evitar virus que nos puedan causar problemas.
- Crear contraseñas seguras y que no tengan nada que ver con la vida personal, ya que muchos defraudadores son muy astutos en cuanto a ingeniería social se trata.
- Considerar de extrema alerta correos en donde se solicite información personal o datos vitales de su tarjeta de crédito.
- Denunciar correos solicitando información personal a la institución emisora de su tarjeta de crédito.
- Exigir al establecimiento solicitar el POS electrónico para procesar las transacciones, ya que es el medio más rápido y seguro para realizar una transacción.

Además en la página web de la Superintendencia de Bancos del Ecuador se dan más prácticas para que los tarjetahabientes tomen en consideración en el momento de utilizar su tarjeta de crédito.

- Tenga en cuenta que los bancos y entidades financieras no piden claves secretas de tarjetas, ni los nombres de sus familiares más cercanos por teléfono o correo electrónico. Esto podría ser un phishing.

- Apenas reciba su tarjeta, firme en la parte de atrás con tinta negra y recuerde que nadie podrá hacer compras fraudulentas con su tarjeta si comprueban su firma con la firma de su cédula.

- Nunca lleve con usted todas sus tarjetas Si sale de viaje, comuníquelo a su entidad financiera Si se cambia de dirección, igualmente notifíquelo.

- Nunca dé su clave o PIN a NADIE.

- Si va a realizar compras fuera de sus hábitos, comuníqueselo a la entidad financiera.

- Lleve siempre el número de contacto de la tarjeta de crédito para reportar robos

Todas las Instituciones Financieras tienen la obligación de recibir su reclamo escrito, cuando usted se acerque a entregarlo recuerde que antes puede llamar para comunicar el fraude y luego de 48 horas presentarlo por escrito. Pregunte siempre quien le atendió y el código de la notificación.

La Superintendencia de Bancos y Seguros tiene un departamento de Servicio al Cliente (SAC) para recibir sus quejas y reclamos, y defender sus derechos frente a las instituciones controladas.

Con lo anterior expuesto podemos concluir que desde el año 2002, la cantidad de tarjetas de crédito en el Ecuador se ha incrementado considerablemente, al pasar de 593,035 a 3,151.887 tarjetas de crédito al finalizar el año 2013, en 20 entidades financieras operadoras y administradores de tarjetas de crédito . De este total el 85% de este total son

tarjetas principales y el 15% restante son adicionales. Durante esta investigación hemos evidenciado un crecimiento tanto en el número de tarjetahabientes como a nivel de denuncias en la fiscalía las cuales aumentaron en el 2012, 19.7% y en el 2013, 38.5%, sin embargo debemos mencionar que esto no refleja la verdadera problemática que existe con respecto al fraude con tarjetas de crédito y débito.

Según informe de Center for Strategic and International Studies y la empresa de seguridad McAfee los delitos informáticos son una industria creciente, el mismo informe menciona que "el costo anual de la ciberdelincuencia en la economía global supera los 445 000 millones de dólares, cifra que incluye tanto las ganancias de los delincuentes como los costos que suponen a las empresas la recuperación y la defensa"[52] (McAfee, Inc.) Sin embargo mencionan que esta cifra es conservadora debido a que no se logró obtener información de ciertos países. En el 2013, se estima que a más de 800 millones de personas su información personal fue robada.

México y Estados Unidos son los países con más alto índice de fraude con tarjetas de crédito en el mundo, según estudio realizado por las firmas de investigación Aite Group y de servicios de pagos electrónicos ACI Worldwide en 17 países. En el Ecuador en el año 2012, al menos $2,4 millones devolvieron las entidades financieras por el crecimiento de los delitos informáticos. La Superintendencia de Bancos y Seguros registró en este mismo año 244 delitos de phising.

Para que los bancos puedan realizar la devolución de los valores reclamados, se deben analizar pistar de auditoría, videos, manipulación de datos internos etc. y así determinar si el reclamo es válido; pero en el caso de ser descuido del cliente, se procede a informar que no se cancelará indicando los motivos. Según Cesar Robalino, representante de la Asociación de Banco Privados, desde junio a octubre del 2013 los bancos reportaron 2000 casos.

[52] McAfee, Inc. (s.f.). Obtenido de http://www.mcafee.com/mx/resources/reports/rp-economic-impact-cybercrime2-summary.pdf

Es importante mencionar en nuestras conclusiones que mediante Resolución JB-2012-2090 del 12 de Enero del 2012, la Junta Bancaria resolvió que todas las entidades financieras del sistema privado "contratarán anualmente con las compañías de seguro privado, coberturas que aseguren a la entidad contra fraudes generados a través de su tecnología de la información, sistemas telemáticos, electrónicos o similares"[53], sin embargo esta resolución no es garantía de la devolución de los valores por parte de las IFIS.

En nuestra investigación hemos consultado sobre la incidencia y las pérdidas operativas por la utilización de tarjetas de crédito y débito en cierto Banco de Guayaquil y nos indicaron que desde Agosto 2013 a Mayo 2014 se han registrado 1.507 fraudes externos, con pérdidas US $71,868. Es en este momento donde dejamos en evidencia el nivel de pérdidas y el grado de incidencia que existe en apenas 10 meses.

Debido a la incidencia de los delitos informáticos en los que se incluyen los fraudes con tarjeta de débito y crédito, se han incluido en el código penal nuevos tipos penales tales como: Transferencia electrónica por activo patrimonial, intercepción ilegal de datos, ataque a la integridad de los sistemas informáticos. La persona que cometa lo ya tipificado será sancionada con pena privativa de libertad hasta 10 años.

Una de las formas en las que la Junta Bancaria y la Superintendencia de Bancos han intervenido es mediante la Resolución JB-2014-2903 del 24 de Abril del 2014, en la que establece la obligatoriedad del establecimiento comercial de verificar firma y rúbrica del tarjetahabiente en el reverso de la tarjeta, además de exigir la presentación del documento de identificación para la verificación correspondiente y anotarlo en el comprobante. Cuando antes de la reforme solo se solicitaba en casos de dudas.

---

[53] Superintendencia de Bancos y Seguros. (s.f.). Obtenido de http://www.sbs.gob.ec/medios/PORTALDOCS/downloads/normativa/2012/resol_JB-2012-2090.pdf

La migración de las tarjetas de crédito y débito de banda magnética a chip, según el Julio Dobronsky, Director Ejecutivo de la Asociación de Instituciones Financieras del Ecuador es una gran inversión tanto a nivel económico como a nivel de recurso humano, inclusive menciona que las instituciones financieras pequeñas están sacrificando su rentabilidad. Es totalmente acertada esta migración ya que se están ofreciendo más seguridades al momento de transaccionar con estas tarjetas. El nuevo plazo para que las instituciones financieras emitan tarjetas de crédito y débito con chip inteligente, es el 19 de Junio del 2015, además deben adoptar estándares internacionales de seguridad en estos dispositivos.

La Superintendencia de Bancos y Seguros mantiene en la web un portal del usuario en el que se ofrece a la ciudadanía varias opciones sobre cultura financiera. En este espacio difunden información sobre el buen uso de los productos y servicios que ofrece el sistema financiero, incluyendo las tarjetas de crédito, además de información general sobre los delitos informáticos, un espacio llamado “evite fraudes electrónicos”.



Además observamos el canal de YouTube de la Superintendencia de Bancos y Seguros, que el 11 de Mayo del 2014 y 24 de Julio del 2014, publicaron un video llamado “Los Fraudes Electrónicos”, el cual intenta alertar al usuario sobre los fraudes electrónicos. Es conveniente indicar que hasta Agosto del 2014 solo han tenido 100 visitas en total. Es importante recomendar que la Superintendencia de Bancos y Seguros realice una difusión real de este y demás videos sobre fraudes.

# BIBLIOGRAFÍA


Antiguo codigo penal del ecuador. (s.f.).

WILLIAMS PHIL, "Crimen Organizado y Cibernético, sinergias,endencias y respuestas". (s.f.). Obtenido de http://www.oas.org/juridico/spanish/cyb_ecu_plan_operativo.pdf

Banco de Guayaquil. (Febrero de 2012). Obtenido de http://saladeprensabg.com/boletin/banco-de-guayaquil-primer-banco-en-recibir-certificacion-pci-dss/

Definición de: Tarjeta de Crédito. (s.f.). Obtenido de http://definicion.de/tarjeta-de-credito/

Deloitte. 2012. Obtenido de http://www.deloitte.com/mx

Diario el Telégrafo. (Septiembre de 2012). Obtenido de http://www.telegrafo.co m.ec/justicia/item/fraude-informatico-se-multiplica-en-tres-anos.html

Diario el Telégrafo. (Diciembre de 2013). Obtenido de http://www.telegrafo.com. ec/economia/item/3-151-887-tarjetas-de-credito -hay-en-ecuador.html

Diario el Telégrafo. (Septiembre de 2013). Obtenido de http://www.telegrafo.co m.ec/economia/item/tarjetas-de-credito-deben-llevar-chip.html

Diario El Universo. (Noviembre de 2011). Obtenido de http://www.eluniverso.com/2011/11/13/1/1422/mercado-negro-delitos-informaticos-expande-pais.html

Diario Hoy. (Septiembre de 2013). Obtenido de http://www.hoy.com.ec/noticias-ecuador/las-tarjetas-de-credito-tendran-chip-en-2015-590918.html

Diario Hoy. (Enero de 2014). Obtenido de http://www.hoy.com.ec/noticias-ecuador/hasta-10-anos-por-revelar-informacion-confidencial-598327.html

Diario La Hora. (Agosto de 2011). Obtenido de http://www.lahora.com.ec/index .php/noticias/imprimir/1101191943/seccion

DiNapoli, T. P. (s.f.). Red Flags for Fraud. New York, Estados Unidos.

EMC Corporation. (s.f.). Obtenido de http://spain.emc.com/about/news/press/20 140226-01.htm

En Naranja. (s.f.). Obtenido de http://www.ennaranja.com/economia-facil/origen- e-historia-de-las-tarjetas-de-credito/

Escamilla, V. M. (12 de JUNIO de 2012). Los 5 fraudes mas temido por los bancos. *CNNEXPASIÒN*, pág. 1.

Fraud Magazine de la ACFE. (Septiembre de 2011). Obtenido de http://prisma mx.net/pdfs/mas_alla.pdf

Kaspersky Lab. (Agosto de 2013). Obtenido de http://latam.kaspersky.com/mx /sobre-kaspersky/centro-de-prensa/comunicados-de-prensa/kaspersky-lab-y-safensoft-proteger%C3%A1n-cajeros-

McAfee, Inc. (s.f.). Obtenido de http://www.mcafee.com/mx/resources/reports/rp-economic-impact-cybercrime2-summary.pdf

Red Venezolana de Derecho Informático. (Enero de 2014). Obtenido de http://revederin.blogspot.com/2014_01_01_archive.html

Revista de Avances Tecnológicos. (s.f.). Obtenido de http://avtecnologicvivi.blogspot.com/2013/03/delito-informatico.html

Revista Especializada de ACFE - Capítulo México. (Octubre de 2012). Obtenido de http://www.revistadelfraude.com/septiembre_octubre/el_peso_del_fraude.html

Robalio, C. (2012). tarjeta de credito deben llevar chip. *Diario Expreso*.

Superintendencia de Bancos y Seguros. (s.f.). Obtenido de http://www.sbs.gob.ec/medios/PORTALDOCS/downloads/normativa/2012/resol_JB-2012-2090.pdf

Telegrafo. (3 de marzo de 2014). *Así está el crédito en el Ecuador*.

www.leyes.com. (2004).

Superintendencia de Bancos y Seguros del Ecuador (s.f.). Obtenido de http://www.sb s.gob.ec/practg/p_index

Banco Central del Ecuador (s.f.). Obtenido de http://www.bce.fin.ec/

Namakforoosh (2005). Metodología de Invetsigación. Mexico:Limusa

Marcelo M. Gómez en su libro Introducción a la Metodología de la Investigación Científica el enfoque cuantitativo

BALCELLS I JUNGYENT, J. (1994). La investigación social: introducción a los métodos y técnicas. Barcelona: Escuela Superior de Relaciones Públicas, PPU.

# GLOSARIO

- **PCI DSS:** Payment Card Industry Data Security Standard, significa Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago.

- **POS: Terminal** de Punto de Venta.

- **Dirección IP: E**s un acrónimo para “Internet Protocol” son un número único e irrepetible con el cual se identifica una computadora conectada a una red que corre el protocolo IP.

- **IFIs: Instituciones** Financieras.

- **SBS:** Superintendencia de Bancos y Seguros

- **Simbiosis:** Cualquier asociación en la que sus miembros se benefician unos de otros.

- **ATM:** Automated Teller Machine Máquina de Cajero Automático.

- **Keylogger:** es un tipo de software o un dispositivo hardware específico que se encarga de registrar las pulsaciones que se realizan en el teclado

# ANEXOS

**DR. PAUL PONCE QUIROZ**
**FISCAL PROVINCIAL DEL GUAYAS**

Ciudad.-

De Mis consideraciones.-

Reciba un cordial y afectuoso saludo de parte de quien suscribe la presente petición, soy egresada de la Facultad de Economía de la Universidad Católica de Santiago de Guayaquil, estoy preparando mi tesis para recibirme de Ingeniera en Contabilidad y Auditoría, siendo el tema de la misma "Operaciones Fraudulentas con Tarjetas de Crédito ", entre los temas que he considerado para ser investigados dentro de mi tesis , se encuentran la parte estadística de los delitos que se han cometido mediante la modalidad de tarjetas de crédito , por tal razón solicito muy comedidamente amparada en los dispuesto en el Art. 66, numeral 23 de nuestra Constitución , se sirva autorizar al departamento de estadística de la Fiscalía Provincial del Guayas, se proporcione por escrito con firma de responsabilidad y vía email la siguiente información:

1.- Cuantos fraudes por tarjetas de crédito y debido se han denunciado en la Fiscalía del Guayas desde el año 2008 al 2013.

2.-Cuanto es el monto en dólares al cual asciende, el perjuicio cometido por medio de los fraudes por tarjetas de crédito y débito, desde el año 2008 al 2013.

La información solicitada podrá ser enviada al correo electrónico **yannina_acosta@hotmail.com.**

Por la atención favorable a la presente, extiendo de antemano mi sincero agradecimiento, deseándole éxitos y su tan importante cargo.

Muy atentamente.-

**YANNINA ACOSTA VELASQUEZ**
**C.C. 0924348857**

David Gonzalez/SuperIntendencia de Bancos (dgonzalez@sbs.gob.ec) Agregar a contactos 15/08/2014 Acciones

Para: yannina_acosta@hotmail.com

Estimada Yannina, he analizado su requerimiento los puntos 1, 2, 5 y 6 le enviaré en el transcurso de la próxima semana, ya que es una información que requiere ser procesada, lo cual toma tiempo.

Los puntos 3 y 4 he solicitado a la unidad que se encarga de tramitar los reclamos de los clientes y estoy a la espera de la respuesta.

EL punto 7 lo puede investigar en nuestro sitio web en el apartado de normativa, ahí encontrará las resoluciones emitidas por la Superintendencia de Bancos y Seguros y la Junta Bancaria.

En el punto 6 tengo una duda, necesita todo el crédito de consumo consolidado con el de tarjetas de crédito o necesita separado por operaciones de crédito de consumo y operaciones con tarjeta de crédito.

Saludos,

David González Z.
SUBDIRECCIÓN DE ESTADÍSTICAS
SUPERINTENDENCIA DE BANCOS Y SEGUROS

URG. Requerimiento de información para el desarrollo de tesis

David Gonzalez/SuperIntendencia de Bancos (dgonzalez@sbs.gob.ec) Agregar a contactos 20/08/2014 Documentos Acciones

Para: yannina madelayne acosta velasquez

De: **David Gonzalez/SuperIntendencia de Bancos** (dgonzalez@sbs.gob.ec)
Enviado: miércoles, 20 de agosto de 2014 18:30:45
Para: yannina madelayne acosta velasquez (yannina_acosta@hotmail.com)

1 dato adjunto (466,2 kB) Outlook.com Vista activa


Descargar como zip

Estimada Yannina, adjunto le envío la serie de tarjetahabientes por entidad emisora, marca y clase de tarjeta, provincia y cantón de emisión.

Saludos,

David González Z.
SUBDIRECCIÓN DE ESTADÍSTICAS
SUPERINTENDENCIA DE BANCOS Y SEGUROS

Telfs: 299-7600 y 299-6100 Ext. 1923

## Rnv: delitos de medios informaticos

Enviado de Samsung Mobile

-------- Mensaje original --------
De: Francisco Castillo Aguirre <castillof@fiscalia.gob.ec>
Fecha: 29/07/2014 10:04 (GMT-05:00)
Para: yannina_acosta@hotmail.com
Asunto: delitos de medios informaticos

Buenos días, adjunto información desde el 2011 hasta el 2013, la información de los año 2008 hasta el 2010 está pendiente dado a que el sistema lleva colapsado varios días, en cuanto se habilite le paso la información pendiente, en cuanto al punto 2 de su solicitud, como le indique a su papá, esa información deberán recabarla en las fiscalías especializadas que ven ese delito, para más información o cualquier consulta, mis números y correos se encuentran en la firma al final de este mensaje

Ing. Francisco Castillo Aguirre
Asistente Administrativo
Gestion de la Informacion y Estudios - Estadisticas
FISCALÍA PROVINCIAL DEL GUAYAS
04-2-596700 ext. 395153 celular 0997874117
email castillof@fiscalia.gob.ec
Edificio La Merced, 10° piso
Gral. Córdova 811 y Víctor Manuel Rendón

FGE
Fiscalía General del Estado
ECUADOR

## RESOLUCIÓN JB-2012-2090

### LA JUNTA BANCARIA

### CONSIDERANDO:

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

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

Que el artículo 1, del capítulo I "De la gestión integral y control de riesgos", del título X "De la gestión y administración de riesgos", del libro I "Normas generales para la aplicación de la Ley General de Instituciones del Sistema Financiero" de la Codificación de Resoluciones de la Superintendencia de Bancos y Seguros y de la Junta Bancaria, dispone que las instituciones del sistema financiero, deberán establecer esquemas eficientes y efectivos de administración y control de todos los riesgos a los que se encuentran expuestas en el desarrollo del negocio, conforme su objeto social, sin perjuicio del cumplimiento de las obligaciones que sobre la materia establezcan otras normas especiales y/o particulares; y, que la administración integral de riesgos es parte de la estrategia institucional y del proceso de toma de decisiones;

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

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

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

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

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

## RESUELVE:

En el libro I "Normas generales para la aplicación de la Ley General de Instituciones del Sistema Financiero" de la Codificación de Resoluciones de la Superintendencia de Bancos y Seguros y de la Junta Bancaria, efectuar el siguiente cambio:

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

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

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

   **41.1** Alteraciones de bases de datos;

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

   **41.3** Falsedad informática;

   **41.4** Estafa informática;

   **41.5** Daño informático; y,

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

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

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

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

Ab. Pedro Solines Chacón
**PRESIDENTE DE LA JUNTA BANCARIA**

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

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

## RESOLUCIÓN JB-2012-2148

### LA JUNTA BANCARIA

### CONSIDERANDO:

Que en el título II "De la organización de las instituciones del sistema financiero privado", del libro I "Normas generales para la aplicación de la Ley General de Instituciones del Sistema Financiero" de la Codificación de Resoluciones de la Superintendencia de Bancos y Seguros y de la Junta Bancaria, consta el capítulo I "Apertura y cierre de oficinas en el país y en el exterior de las instituciones financieras privadas y públicas sometidas al control de la Superintendencia de Bancos y Seguros";

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

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

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

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

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

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

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

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

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

**RESUELVE:**

En el libro I "Normas generales para la aplicación de la Ley General de Instituciones del Sistema Financiero" de la Codificación de Resoluciones de la Superintendencia de Bancos y Seguros y de la Junta Bancaria, efectuar los siguientes cambios:

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

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

   1.1 Sustituir el numeral 39.2, por el siguiente:

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

   1.2 Sustituir el numeral 39.6, por el siguiente:

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

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

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

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

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

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

2. Incluir como tercera disposición transitoria, la siguiente:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

**4.3.8 Medidas de seguridad en canales electrónicos.-** Con el objeto de garantizar que las transacciones realizadas a través de canales electrónicos cuenten con los controles, medidas y elementos de seguridad para evitar el cometimiento de eventos fraudulentos y garantizar la seguridad y calidad de la información de los usuarios así como los bienes de los clientes a cargo de las instituciones controladas, éstas deberán cumplir como mínimo con lo siguiente:

**4.3.8.1** Las instituciones del sistema financiero deberán adoptar e implementar los estándares y buenas prácticas internacionales de seguridad vigentes a nivel mundial para el uso y manejo de canales electrónicos y consumos con tarjetas, los cuales deben ser permanentemente monitoreados para asegurar su cumplimiento;

**4.3.8.2** Establecer procedimientos y mecanismos para monitorear de manera periódica la efectividad de los niveles de seguridad implementados en hardware, software, redes y comunicaciones, así como en cualquier otro elemento electrónico o tecnológico utilizado en los canales electrónicos, de tal manera que se garantice permanentemente la seguridad y calidad de la información;

**4.3.8.3** El envío de información confidencial de sus clientes y la relacionada con tarjetas, debe ser realizado bajo condiciones de seguridad de la información, considerando que cuando dicha información se envíe mediante correo electrónico o utilizando algún otro medio vía Internet, ésta deberá estar sometida a técnicas de encriptación acordes con los estándares internacionales vigentes;

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

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

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

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

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

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

Para el caso de consumos con tarjetas, se deberán personalizar los cupos máximos, principalmente para los siguientes servicios: consumos nacionales, consumos en el exterior, compras por internet, entre otros;

**4.3.8.9** Incorporar en los procedimientos de administración de seguridad de la información la renovación de por lo menos una vez (1) al año de las claves de acceso a cajeros automáticos; dicha clave deberá ser diferente de aquella por la cual se accede a otros canales electrónicos;

**4.3.8.10** Las instituciones deberán establecer procedimientos de control y mecanismos que permitan registrar el perfil de cada cliente sobre sus costumbres transaccionales en el uso de canales electrónicos y

tarjetas y definir procedimientos para monitorear en línea y permitir o rechazar de manera oportuna la ejecución de transacciones que no correspondan a sus hábitos, lo cual deberá ser inmediatamente notificado al cliente mediante mensajería móvil, correo electrónico, u otro mecanismo;

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

**4.3.8.12** Asegurar que exista una adecuada segregación de funciones entre el personal que administra, opera, mantiene y en general accede a los dispositivos y sistemas usados en los diferentes canales electrónicos y tarjetas;

**4.3.8.13** Las entidades deberán establecer procedimientos y controles para la administración, transporte, instalación y mantenimiento de los elementos y dispositivos que permiten el uso de los canales electrónicos y de tarjetas;

**4.3.8.14** Las instituciones del sistema financiero deben mantener sincronizados todos los relojes de sus sistemas de información que estén involucrados con el uso de canales electrónicos;

**4.3.8.15** Mantener como mínimo durante doce (12) meses el registro histórico de todas las operaciones que se realicen a través de los canales electrónicos, el cual deberá contener como mínimo: fecha, hora, monto, números de cuenta (origen y destino en caso de aplicarse), código de la institución del sistema financiero de origen y de destino, número de transacción, código del dispositivo: para operaciones por cajero automático: código del ATM, para transacciones por internet: la dirección IP, para transacciones a través de sistemas de audio respuesta - IVR y para operaciones de banca electrónica mediante dispositivos móviles: el número de teléfono con el que se hizo la conexión. En caso de presentarse reclamos, la información deberá conservarse hasta que se agoten las instancias legales. Si dicha información constituye respaldo contable se aplicará lo previsto en el tercer inciso del artículo 80 de la Ley General de Instituciones del Sistema Financiero;

**4.3.8.16** Incorporar en los procedimientos de administración de la seguridad de la información, controles para impedir que funcionarios de la entidad que no estén debidamente autorizados tengan acceso a consultar información confidencial de los clientes en ambiente de producción. En el caso de información contenida en ambientes de desarrollo y pruebas, ésta deberá ser enmascarada o codificada.

Todos estos procedimientos deberán estar debidamente documentados en los manuales respectivos.

Además, la entidad deberá mantener y monitorear un log de auditoria sobre las consultas realizadas por los funcionarios a la información confidencial de los clientes, la cual debe contener como mínimo: identificación del funcionario, sistema utilizado, identificación del equipo (IP), fecha, hora, e información consultada. Esta información deberá conservarse por lo menos por doce (12) meses;

**4.3.8.17** Las instituciones del sistema financiero deberán poner a disposición de sus clientes un acceso directo como parte de su centro de atención telefónica (call center) para el reporte de emergencias bancarias, el cual deberá funcionar las veinticuatro (24) horas al día, los siete (7) días de la semana;

**4.3.8.18** Mantener por lo menos durante seis (6) meses la grabación de las llamadas telefónicas realizadas por los clientes a los centros de atención telefónica (call center), específicamente cuando se consulten saldos, consumos o cupos disponibles; se realicen reclamos; se reporten emergencias bancarias; o, cuando se actualice su información. De presentarse reclamos, esa información deberá conservarse hasta que se agoten las instancias legales;

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

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

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

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

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

**4.3.8.24** Es función de auditoría interna verificar oportunamente la efectividad de las medidas de seguridad que las instituciones del sistema financiero deben implementar en sus canales electrónicos; así también deberán informar sobre las medidas correctivas establecidas en los casos de reclamos de los usuarios financieros que involucren debilidades o violación de los niveles de seguridad;

**4.3.8.25** Implementar técnicas de seguridad de la información en los procesos de desarrollo de las aplicaciones que soportan los canales electrónicos, con base en directrices de codificación segura a fin de que en estos procesos se contemple la prevención de vulnerabilidades;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Ab. Pedro Solines Chacón
**PRESIDENTE DE LA JUNTA BANCARIA**

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

Lcdo. Pablo Cobo Luna
**SECRETARIO DE LA JUNTA BANCARIA**

## RESOLUCION JB-2012-2151

**LA JUNTA BANCARIA**

**CONSIDERANDO:**

Que el primer inciso del artículo 52 de la Constitución de la República del Ecuador, publicada en el Registro Oficial No. 449 de 20 de octubre del 2008, establece que las personas tienen derecho a disponer de bienes y servicios de óptima calidad y a elegirlos con libertad, así como a una información precisa y no engañosa sobre su contenido y características;

Que los numerales 2, 4 y 5 del artículo 4 de la Ley Orgánica de Defensa del Consumidor, publicada en el suplemento del Registro Oficial No. 116 de 10 de julio del 2000, señalan como derechos fundamentales del consumidor que proveedores públicos y privados oferten bienes y servicios competitivos de óptima calidad y a elegirlos con libertad; a la información adecuada, veraz, clara, oportuna y completa sobre los bienes y servicios ofrecidos en el mercado, así como sus precios, características, calidad, condiciones de contratación y demás aspectos relevantes de los mismos, incluyendo los riesgos que pudieren presentar; y, a un trato transparente, equitativo y no discriminatorio o abusivo por parte de los proveedores de bienes o servicios, especialmente en lo referido a las condiciones óptimas de calidad, cantidad, precio, peso y medida;

Que el primero y segundo incisos del artículo 201 de la Ley General de Instituciones del Sistema Financiero, reformado con el artículo 11 de la Ley de Creación de la Red de Seguridad Financiera, publicada en el tercer suplemento del Registro Oficial No. 498 de 31 de diciembre del 2008, disponen que los servicios activos, pasivos o de cualquier otra naturaleza que presten las instituciones financieras deberán sujetarse a las tarifas máximas que serán segmentadas por la naturaleza de cada institución financiera y determinadas trimestralmente por la Junta Bancaria y publicadas en las páginas web y oficinas de la Superintendencia de Bancos y Seguros y de las instituciones financieras conforme a la normativa expedida para el efecto por la Junta Bancaria; que la Superintendencia de Bancos y Seguros autorizará previamente los servicios a ser libremente aceptados y recibidos por los clientes y usuarios y determinará las actividades propias del giro del negocio que no constituyen servicios; que las actividades bancarias propias del giro del negocio que implican transacciones básicas que realizan los clientes e información esencial respecto del manejo de sus cuentas, serán gratuitas;

Que con resolución No. JB-2009-1315 de 12 de junio del 2009, la Junta Bancaria aprobó las normas contenidas en el capítulo I "De las tarifas por servicios financieros", del título XIV "De la transparencia de la información", del libro I "Normas generales para la aplicación de la Ley General de Instituciones del Sistema Financiero" de la Codificación de Resoluciones de la Superintendencia de Bancos y Seguros y de la Junta Bancaria;

Que el artículo 4 del citado capítulo I dispone que la Junta Bancaria determinará trimestralmente tanto el listado de las transacciones básicas que por su naturaleza son gratuitas cuanto de los servicios financieros sujetos a las tarifas máximas establecidas, las que regirán a partir del primer día de los meses de enero, abril, julio y octubre, y se publicarán antes del inicio del respectivo trimestre;

Que con fundamento en las consideraciones precedentes, la Junta Bancaria, a través de resolución No. JB-2012-2138 de 27 de marzo de 2012, aprobó las tarifas máximas para el periodo trimestral que comprende los meses de abril, mayo y junio del 2012;

Que el estado de cuenta constituye información esencial cuyo acceso debe garantizarse a sus titulares para el manejo de cualquier producto bancario y, consecuentemente su emisión y entrega, por cualquier medio, deben ser gratuitos;

Que la afiliación y renovación de tarjetas de crédito no deben considerarse servicios financieros ni deben significar ingresos para los prestadores de aquellos servicios, toda vez que no constituyen el negocio financiero, el cual más bien está dado en el crédito al que se accede gracias al uso de tales tarjetas, y, por tanto la afiliación y renovación no deben cargarse al usuario financiero; además, por la afectación económica y social que aquello ha implicado en perjuicio de los usuarios;

Que la disposición transitoria única contenida en la resolución No. JB-2012-2138, determinó que "*Durante la vigencia de esta resolución la Junta Bancaria podrá modificar sus disposiciones, en cualquier tiempo, para reformar las tarifas máximas, así como para incorporar nuevos servicios sujetos a tarifa, o para agregar transacciones básicas que por su naturaleza deben ser gratuitas.*"; y,

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

**RESUELVE:**

**ARTÍCULO 1.-** Reformar las tarifas máximas para el período trimestral que comprende los meses de abril, mayo y junio del 2012, aprobadas mediante resolución JB-2012-2138 de 27 de marzo de 2012, dentro de las cuales las instituciones del sistema financiero podrán efectuar cobros por la prestación efectiva de los servicios financieros que constan en los siguientes cuadros, eliminándose las correspondientes a servicio de entrega de estados de cuenta; y, servicios de afiliación y renovación de tarjetas de crédito:

**SERVICIOS CON TARIFAS MÁXIMAS**

| No. | SERVICIO GENÉRICO | NOMBRE DEL SERVICIO | EN DÓLARES |
|---|---|---|---|
| 1 | Servicios con cuentas corrientes | Costo por un cheque | 0,30 |
| 2 | | Cheque devuelto nacional | 2,79 |
| 3 | | Cheque devuelto del exterior | 3,24 |
| 4 | | Cheque certificado | 2,00 |
| 5 | | Cheque de gerencia | 2,50 |
| 6 | | Cheque consideración cámara de compensación | 3,00 |
| 7 | | Oposición al pago de cheques | 3,00 |
| 8 | | Abstención de pago de cheques | 3,00 |
| 9 | | Revocatoria de cheques | 3,00 |
| 10 | Servicios de retiros | Retiro cajero automático clientes de la propia entidad en cajero de otra entidad | 0,50 |
| 11 | | Retiro cajero automático clientes de otra entidad en cajero de la entidad | 0,50 |
| 12 | | Retiro de efectivo en corresponsales no bancarios de la propia entidad | 0,35 |
| 13 | Servicios de consultas | Impresión Consulta por cajero automático | 0,35 |
| 14 | Servicios de referencias | Referencias bancarias | 2,65 |
| 15 | | Corte de estado de cuenta | 1,83 |
| 16 | Servicios de copias | Tarjeta de crédito y tarjeta de pago, copia de voucher / vale local | 2,00 |
| 17 | | Tarjeta de crédito y tarjeta de pago, copia de voucher / vale del exterior | 10,00 |
| 18 | | Tarjeta de crédito, copia de estado de cuenta | 0,50 |

Continua en la siguiente página

| No. | SERVICIO GENÉRICO | NOMBRE DEL SERVICIO | EN DÓLARES |
|---|---|---|---|
| 19 | Servicios de transferencias | Transferencias interbancarias SPI recibidas | 0,30 |
| 20 | | Transferencias interbancarias SPI enviadas, internet | 0,50 |
| 21 | | Transferencias interbancarias SPI enviadas, oficina | 2,15 |
| 22 | | Transferencias interbancarias SCI recibidas | 0,30 |
| 23 | | Transferencias interbancarias SCI enviadas, internet | 0,28 |
| 24 | | Transferencias interbancarias SCI enviadas, oficina | 1,93 |
| 25 | | Transferencias al exterior en oficina | 55,49 |
| 26 | | Transferencias recibidas desde el exterior | 10,00 |
| 27 | | Transferencias nacionales otras entidades oficina | 2,00 |
| 28 | Servicios de consumos nacionales | Tarjeta de crédito y tarjeta de pago, consumo en gasolineras | 0,26 |
| 29 | Servicios de reposición | Reposición de libreta/cartola/estado de cuenta por pérdida, robo o deterioro | 1,00 |
| 30 | | Tarjeta de débito, reposición | 4,94 |
| 31 | Servicios de emisión | Tarjeta de débito, emisión | 5,15 |
| 32 | Servicios de renovación | Tarjeta de débito, renovación | 1,85 |

**SERVICIO CON TARIFA MÁXIMA - CUENTA BÁSICA**

| No. | SERVICIO GENÉRICO | NOMBRE DEL SERVICIO | EN DÓLARES |
|---|---|---|---|
| 1 | Servicios de cuenta básica | Emisión del paquete de apertura de cuenta básica* | 6,00 |

* El paquete de cuenta básica contiene como mínimo: la tarjeta electrónica, la clave de seguridad de acceso a los diferentes canales de atención que apliquen, el instructivo ilustrado de uso de cuenta y la copia del contrato de apertura de cuenta.

**TARIFAS PORCENTUALES DE AFILIACIÓN A ESTABLECIMIENTOS COMERCIALES**

| No. | SERVICIO | EN PORCENTAJE |
|---|---|---|
| 1 | Tarifas de afiliación a establecimientos comerciales, crédito corriente (%) | 4,50 |
| 2 | Tarifas de afiliación a establecimientos comerciales, crédito corriente, Salud y Afines (%) | 4,50 |
| 3 | Tarifas de afiliación a establecimientos comerciales, crédito corriente, Educación (%) | 4,50 |

**ARTÍCULO 2.-** Incluir cómo transacciones básicas, y por su naturaleza gratuitas, a la emisión y entrega, por cualquier medio, de estados de cuenta; y, los servicios de afiliación y renovación de tarjeta de crédito, para cuyo efecto se reforma la lista de transacciones básicas de acuerdo al siguiente cuadro:

| No. | SERVICIOS | APLICA PARA | EN DÓLARES |
|---|---|---|---|
| 1 | Apertura de cuentas | Cuenta de ahorros | 0,00 |
| | | Cuenta corriente | 0,00 |
| | | Cuenta básica | 0,00 |
| | | Cuenta de integración de capital | 0,00 |
| | | Depósitos a plazos | 0,00 |
| | | Inversiones | 0,00 |
| | | Información crediticia básica | 0,00 |
| 2 | Depósitos a cuentas | Cuenta de ahorros | 0,00 |
| | | Cuenta corriente | 0,00 |
| | | Cuenta básica | 0,00 |
| | | Depósitos a plazos | 0,00 |
| | | Inversiones | 0,00 |
| 3 | Administración, mantenimiento, mantención y manejo de cuentas | Cuenta de ahorros | 0,00 |
| | | Cuenta corriente | 0,00 |
| | | Cuenta básica | 0,00 |
| | | Depósitos a plazos | 0,00 |
| | | Inversiones | 0,00 |

Continua en la siguiente página

| No. | SERVICIOS | APLICA PARA | EN DÓLARES |
|---|---|---|---|
| 4 | Consulta de cuentas | Consulta, Oficina | 0,00 |
| | | Consulta visual, Cajero automático | 0,00 |
| | | Consulta, Internet | 0,00 |
| | | Consulta, Banca Telefónica | 0,00 |
| | | Consulta, Banca Celular | 0,00 |
| 5 | Retiros de dinero | Retiro de dinero por ventanilla de la propia entidad | 0,00 |
| | | Retiro de dinero por cajero automático clientes propia entidad | 0,00 |
| 6 | Transferencia dentro de la misma entidad | Transferencias, medios físicos (ventanilla) | 0,00 |
| | | Transferencias, medios electrónicos (cajero automático, internet, teléfono, celular y otros) | 0,00 |
| 7 | Cancelación o cierre de cuentas | Cuenta de ahorros | 0,00 |
| | | Cuenta corriente | 0,00 |
| | | Cuenta básica | 0,00 |
| 8 | Activación de cuentas | Activación de Cuenta de ahorros | 0,00 |
| | | Activación de Cuenta corriente | 0,00 |
| | | Activación de Cuenta básica | 0,00 |
| | | Activación de Tarjeta de Crédito | 0,00 |
| | | Activación de Tarjeta de Debito y/o Pago | 0,00 |
| 9 | Mantenimiento de Tarjeta de Crédito | Mantenimiento de Tarjeta de Crédito | 0,00 |
| | | Mantenimiento pago mínimo de Tarjeta de Crédito | 0,00 |
| | | Mantenimiento pago total de Tarjeta de Crédito | 0,00 |
| 10 | Pagos a Tarjetas de Crédito | Pagos a Tarjetas de Crédito, por los diferentes canales | 0,00 |
| 11 | Bloqueo, anulación o cancelación | Bloqueo, anulación o cancelación de Tarjeta de Débito y/o Pago | 0,00 |
| | | Bloqueo, anulación o cancelación de Tarjeta electrónica de Cuenta Básica | 0,00 |
| | | Bloqueo, anulación o cancelación de Tarjeta de Crédito | 0,00 |
| 12 | Emisión de Tabla de Amortización | Emisión de Tabla de Amortización, primera impresión | 0,00 |
| 13 | Transacciones fallidas en cajeros automáticos | Transacciones fallidas en cajeros automáticos, todos los casos | 0,00 |
| 14 | Reclamos de clientes | Reclamos justificados | 0,00 |
| | | Reclamos injustificados | 0,00 |
| 15 | Frecuencia de transacciones | Cuenta de ahorros | 0,00 |
| | | Cuenta corriente | 0,00 |
| | | Cuenta básica | 0,00 |
| | | Tarjeta de crédito | 0,00 |
| 16 | Reposición libreta/ cartola/ estado de cuenta por actualización | Reposición libreta/ cartola/ estado de cuenta por actualización | 0,00 |
| 17 | Emisión y entrega de estado de cuenta | Tarjeta de crédito y todo tipo de cuenta y por cualquier medio, vía o canal de entrega | 0,00 |

**AFILIACIÓN Y RENOVACIÓN DE TARJETAS DE CRÉDITO**

| CLASIFICACIÓN DE TARJETAS DE CRÉDITO | SEGMENTO DE TARJETA | TARJETAS PRINCIPALES | | TARJETAS ADICIONALES | |
|---|---|---|---|---|---|
| | | Afiliación (en dólares) | Renovación (en dólares) | Afiliación (en dólares) | Renovación (en dólares) |
| Persona natural | Todos los segmentos | 0 | 0 | 0 | 0 |
| Empresarial | | 0 | 0 | 0 | 0 |
| Marca compartida | | 0 | 0 | 0 | 0 |
| Sistema cerrado | | 0 | 0 | 0 | 0 |
| Tarjeta básica | | 0 | 0 | 0 | 0 |

**ARTÍCULO 3.-** La Superintendencia de Bancos y Seguros controlará la observancia de las tarifas máximas establecidas en esta resolución, y aplicará, de ser el caso, las sanciones que correspondan, sin perjuicio de exigir la restitución de los valores indebidamente cobrados.

**ARTÍCULO 4.-** La presente norma entrará en vigencia a partir de su publicación en el Registro Oficial, fecha desde la cual las instituciones del sistema financiero se abstendrán de cobrar al usuario valor alguno por afiliación y renovación de tarjetas de crédito, así como por emisión y entrega de estados de cuenta.

**DISPOSICIÓN TRANSITORIA ÚNICA.-** Durante la vigencia de esta resolución la Junta Bancaria podrá modificar sus disposiciones, en cualquier tiempo, para reformar las tarifas máximas, así como para incorporar nuevos servicios sujetos a tarifa, o para agregar transacciones básicas que por su naturaleza deben ser gratuitas.

**DEROGATORIA.-** Quedan derogadas todas las resoluciones dirigidas a una o más instituciones bancarias o financieras, a través de las cuales se haya aprobado o establecido el costo de tarifas relacionadas con los servicios que mediante esta resolución se establecen como gratuitos, tarifa cero.

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

Ab. Pedro Solines Chacón
**PRESIDENTE DE LA JUNTA BANCARIA**

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

Lcdo. Pablo Cobo Luna
**SECRETARIO DE LA JUNTA BANCARIA**

## RESOLUCION No. JB-2012-2225

### LA JUNTA BANCARIA

### CONSIDERANDO:

Que el primer inciso del artículo 121 de la Ley General de Instituciones del Sistema Financiero establece que las personas naturales o jurídicas que no forman parte del sistema financiero y no cuentan con el respectivo certificado expedido por la Superintendencia de Bancos y Seguros, quedan expresamente prohibidas de realizar operaciones reservadas para las instituciones que integran dicho sistema, especialmente la captación de recursos del público, exceptuando la emisión de obligaciones cuando ésta proceda al amparo de la Ley de Mercado de Valores; que tampoco podrán hacer propaganda o uso de avisos, carteles, recibos, membretes, títulos o cualquier otro medio que sugiera que el negocio de dicha persona es de giro financiero o de seguros:

Que la letra p) del artículo 51, en concordancia con el artículo 2 de la citada ley, establece que las instituciones financieras pueden actuar como emisor u operador de tarjetas de crédito, de débito o tarjetas de pago;

Que el tercer inciso del artículo 1 de la referida ley señala que las compañías emisoras o administradoras de tarjetas de crédito son instituciones de servicios financieros, que deberán tener como objeto social exclusivo la realización de esa actividad, y que quedarán sometidas a la aplicación de normas de solvencia y prudencia financiera y al control que realizará la Superintendencia dentro del marco legal que regula a dichas instituciones, en base a las normas que expida para el efecto;

Que en el título I "De la constitución", del libro I "Normas generales para la aplicación de la Ley General de Instituciones del Sistema Financiero" de la de la Codificación de Resoluciones de la Superintendencia de Bancos y Seguros y de la Junta Bancaria, consta el capítulo V "Constitución, funcionamiento y las operaciones de las compañías emisoras o administradoras de tarjetas de crédito y los departamentos de tarjetas de crédito de las instituciones financieras";

Que es necesario reformar dicha norma con el propósito de establecer con claridad que sólo las instituciones financieras y las compañías emisoras o administradoras de tarjetas de crédito pueden actuar como emisor u operador de tarjetas de crédito;

Que la Junta Bancaria, en sesiones celebradas el 22 de junio y el 5 de julio del 2012, analizó el texto de la presente resolución; y,

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

### RESUELVE:

En el libro I "Normas generales para la aplicación de la Ley General de Instituciones del Sistema Financiero" de la Codificación de Resoluciones de la Superintendencia de Bancos y Seguros y de la Junta Bancaria, efectuar el siguiente cambio:

**ARTÍCULO ÚNICO.-** En el capítulo V "Constitución, funcionamiento y las operaciones de las compañías emisoras o administradoras de tarjetas de crédito y los departamentos de

tarjetas de crédito de las instituciones financieras"; del título I "De la constitución", efectuar las siguientes reformas:

1. En el artículo 1, realizar los siguientes cambios:

   1.1 Incluir como primer inciso, el siguiente:

   **"ARTÍCULO 1.-** Solamente las instituciones financieras y las compañías emisoras o administradoras de tarjetas de crédito pueden actuar como emisor u operador de tarjetas de crédito. Quienes infrinjan esta disposición serán sancionadas conforme a lo previsto en el artículo 121 de la Ley General de Instituciones del Sistema Financiero."

   1.2 Eliminar el sexto inciso.

2. En el segundo inciso del artículo 5, eliminar la frase "... , en tanto que las tarjetas de crédito de circulación restringida podrán ser emitidas por establecimientos comerciales."

3. Cambiar la denominación de la sección VIII "Disposición transitoria" por "Disposiciones transitorias", e incluir como segunda a la siguiente:

   "**SEGUNDA.-** A partir de la vigencia de la presente reforma, no se podrá autorizar la emisión de tarjetas de crédito de circulación restringida.

   Se exceptúan las tarjetas de crédito de circulación restringida emitidas por compañías que son originadoras de procesos de titularización de cartera que, a la presente fecha, mantengan valores en circulación en el mercado ."

   La Superintendencia de Compañías regulará y establecerá el cronograma para la eliminación de las tarjetas de crédito de circulación restringida emitidas por compañías que son originadoras de procesos de titularización de cartera."

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

Ab. Pedro Solines Chacón
**PRESIDENTE DE LA JUNTA BANCARIA**

**LO CERTIFICO**: Quito, Distrito Metropolitano, el cinco de julio del dos mil doce.

Lcdo. Pablo Cobo Luna
**SECRETARIO DE LA JUNTA BANCARIA**

## RESOLUCIÓN JB-2014-2903

## LA JUNTA BANCARIA

## CONSIDERANDO:

Que en el título I "De la constitución", del libro I "Normas generales para la aplicación de la Ley General de Instituciones del Sistema Financiero" de la Codificación de Resoluciones de la Superintendencia de Bancos y Seguros y de la Junta Bancaria, consta el capítulo V "Constitución, funcionamiento y las operaciones de las compañías emisoras administradoras de tarjetas de crédito y los departamentos de tarjetas de crédito de las instituciones financieras";

Que el numeral 15.2 del artículo 15, del citado capítulo V, establece que en los contratos celebrados con los establecimientos afiliados, es obligación del establecimiento el emitir la nota de cargo y de verificar que la firma y rúbrica que consigne el tarjetahabiente sea la misma que conste en el reverso de la tarjeta; y, que en caso de duda, el establecimiento exigirá el documento de identificación y anotará en el comprobante el número de la cédula de identidad o del pasaporte;

Que es necesario reformar dicha norma con el propósito de establecer como una medida de seguridad, la obligatoriedad del establecimiento de siempre requerir el documento de identificación del tarjetahabiente; y,

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

## RESUELVE:

En el libro I "Normas generales para la aplicación de la Ley General de Instituciones del Sistema Financiero" de la Codificación de Resoluciones de la Superintendencia de Bancos y Seguros y de la Junta Bancaria, efectuar la siguiente reforma:

**ARTÍCULO ÚNICO.-** Sustituir el numeral 15.2 del artículo 15, del capítulo V "Constitución, funcionamiento y las operaciones de las compañías emisoras administradoras de tarjetas de crédito y los departamentos de tarjetas de crédito de las instituciones financieras", del título I "De la constitución", por el siguiente:

**"15.2** Obligatoriedad del establecimiento de emitir la nota de cargo y de verificar que la firma y rúbrica que consigne el tarjetahabiente sea la misma que conste en el reverso de la tarjeta y en el documento de identificación, para lo cual el

establecimiento exigirá la presentación del documento de identificación y anotará en el comprobante el número de la cédula de ciudadanía, identidad o pasaporte;"

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

Dr. Xavier Villavicencio Córdova
**PRESIDENTE DE LA JUNTA BANCARIA (S)**

**LO CERTIFICO**.- Quito, Distrito Metropolitano, el veinticuatro de abril del dos mil catorce.

Lcdo. Pablo Cobo Luna
**SECRETARIO DE LA JUNTA BANCARIA**