UNIVERSIDAD CATÓLICA

DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRÍA EN ADMINISTRACIÓN DE EMPRESAS

TEMA:

MIGRACIÓN DE BANDA MAGNÉTICA A CHIP PARA EVITAR FRAUDES DE CLONACIÓN DE TARJETAS DE CRÉDITO O DÉBITO. ¿LOS BANCOS ECUATORIANOS ESTÁN PREPARADOS PARA ESTE CAMBIO?

AUTORES:

Mariela Jaramillo Acevedo

María José Zambrano

MAGÍSTER EN ADMINISTRACIÓN DE EMPRESAS

TUTOR:

Intriago López Ricardo Javier

Guayaquil, Ecuador

2013

UNIVERSIDAD CATÓLICA

DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRÍA EN ADMINISTRACIÓN DE EMPRESAS

CERTIFICACIÓN

Certificamos que el presente trabajo fue realizado en su totalidad por la licenciada en contabilidad y auditoría **Mariela Patricia Jaramillo Acevedo** y la ingeniera **María José Zambrano Alvarado**, como requerimiento parcial para la obtención del Grado Académico de **MAGÍSTER EN ADMINISTRACIÓN DE EMPRESAS.**

DIRECTOR DE TESIS

_____

(nombres, apellidos)

REVISOR(ES)

_____

(nombres, apellidos)

_____

(nombres, apellidos)

DIRECTOR DEL PROGRAMA/CARRERA

_____

Econ. María del Carmen Lappo

Guayaquil, a los 14 días del mes de Marzo del año 2014

UNIVERSIDAD CATÓLICA

DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRÍA EN ADMINISTRACIÓN DE EMPRESAS

DECLARACIÓN DE RESPONSABILIDAD

Nosotros, Mariela Patricia Jaramillo Acevedo y

María José Zambrano Alvarado

DECLARAMOS QUE:

La Tesis "***MIGRACIÓN DE BANDA MAGNÉTICA A CHIP PARA EVITAR FRAUDES DE CLONACIÓN DE TARJETAS DE CRÉDITO O DÉBITO. ¿LOS BANCOS ECUATORIANOS ESTÁN PREPARADOS PARA ESTE CAMBIO?"*** previa a la obtención del **Grado Académico de MAGÍSTER EN ADMINISTRACIÓN DE EMPRESAS,** ha sido desarrollada en base a una investigación exhaustiva, 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 de la tesis del Grado Académico en mención.

Guayaquil, a los 14 días del mes de Marzo del año 2014

AUTORES

_____ _____

Mariela Patricia Jaramillo Acevedo **María José Zambrano Alvarado**

UNIVERSIDAD CATÓLICA

DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRÍA EN ADMINISTRACIÓN DE EMPRESAS

AUTORIZACIÓN

Nosotros, **Mariela Patricia Jaramillo Acevedo**

María José Zambrano Alvarado

Autorizo a la Universidad Católica de Santiago de Guayaquil, la **publicación** en la biblioteca de la institución de la **Tesis de MAGÍSTER EN ADMINISTRACIÓN DE EMPRESAS** titulada: ***MIGRACIÓN DE BANDA MAGNÉTICA A CHIP PARA EVITAR FRAUDES DE CLONACIÓN DE TARJETAS DE CRÉDITO O DÉBITO. ¿LOS BANCOS ECUATORIANOS ESTÁN PREPARADOS PARA ESTE CAMBIO?"***, cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y total autoría.

Guayaquil, a los 14 días del mes de Marzo del año 2014

AUTORES:

_____ _____

Mariela Patricia Jaramillo Acevedo **María José Zambrano Alvarado**

AGRADECIMIENTO

Queremos agradecer de manera especial a la Universidad Católica Santiago de Guayaquil que nos ha brindado la oportunidad de culminar nuestros estudios de postgrado en esta prestigiosa institución. A los profesores quienes han transmitido sus conocimientos con mucho profesionalismo y dedicación. Y de manera muy especial queremos reconocer la labor realizada por nuestra Directora de la Maestría Econ. María del Carmen Lappo quien nos ha guiado durante este arduo proceso para poder culminar con éxito este tan anhelado deseo.

Mariela Jaramillo Acevedo

María José Zambrano Alvarado

DEDICATORIA

La presente tesis está dedicada principalmente
a Dios, a mis padres, hermanos, sobrinos, amigos
y a todos los que de una u otra forma han contribuido
a convertir este gran sueño en realidad.

Mariela

Dedico este trabajo principalmente a Dios por haberme dado fuerzas y valor para culminar con éxito esta etapa tan importante en mi vida, a mi hijo quien permaneció conmigo los nueve meses mientras asistía a clases, a mi esposo, hermanos y padres quienes con su apoyo y consejos han sabido guiarme a culminar mi meta profesional.

María José

INDICE GENERAL

INDICE DE TABLAS

INDICE DE FIGURAS

Introducción

Hoy en día, el avance tecnológico ha permitido que el sistema financiero ofrezca a sus clientes servicios bancarios con tecnología de punta como es el uso del plástico o la denominada tarjeta de crédito y la Banca en Línea, que brinda al usuario la posibilidad de realizar transacciones y consultas a través de la Internet.

Desafortunadamente, también la delincuencia se desarrolla y se encarga de crear tecnología para fines inmorales, como lo son el robo y la estafa. Es por esto que es importante que tanto las instituciones financieras como sus clientes estén alerta a este tipo de riesgos, que no solo ponen en peligro información financiera y personal sino también sus recursos.

Uno de los fraudes más conocidos no solo en nuestro país sino en otros países del mundo como Venezuela, Brasil y México son los fraudes con tarjetas de crédito y débito por clonación.

De acuerdo a información proporcionada por el Grupo Multisistemas de Seguridad Industrial, la mayoría de operaciones de fraudes con tarjetas de crédito clonadas en países como México, están dirigidas por bandas de argentinos y venezolanos cuyo monto asciende a unos 70 millones de dólares anuales. En el 2009 en México se reportaron 720 casos de tarjetas de crédito clonadas, según datos de la Condusef 2010 (Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros).

En Ecuador de acuerdo a datos proporcionados por la Fiscalía General del Estado, los casos de fraude electrónico se han incrementado de 119 que se registraron en el 2009 a 1308 registradas a marzo del 2011 lo que representa entre y $ 1 y $ 2 millones de dólares de perjuicio (Diario El Universo, 2011). Los métodos más utilizados son el phishing es decir la suplantación de la identidad de un sitio web por otro para extraer información de modo fraudulento y el skimming a través del cual el delincuente copia o escanea la información financiera y personal de su tarjeta de crédito o débito y luego la regraba en una tarjeta falsa, creando así una réplica que tiene los mismos alcances y limitaciones que la tarjeta personal original, más conocido como clonación.

Según el ingeniero Alberto Andrade (2011), socio estratégico de la empresa ecuatoriana Red Segura, hoy en día, es fácil falsificar y/o clonar las tarjetas, pues la banda magnética que tienen no es segura, y el PIN con cuatro dígitos con el que cuentan es muy fácil de descifrar por informáticos, él asegura que el riesgo más grande en estos dos dispositivos es la clonación o una filtración de información en la administración financiera. Por ello, propone como única solución la eliminación de la banda magnética y la implementación de tecnologías seguras en una tarjeta inteligente, ya que la complejidad técnica al elaborar los PICC es alta y limita el ataque.

El experto señaló que uno de los mayores riesgos en las tarjetas actuales no es que la dupliquen, sino que esta no cambia su clave de

encriptación nunca, "El riesgo está dado porque cualquier persona puede grabar una banda magnética".

Actualmente en Ecuador, las tarjetas de crédito operan con una banda magnética y un microprocesador integrado en los plásticos; sin embargo, las tarjetas de débito sólo tienen una banda magnética, lo que las deja más vulnerables a una clonación, según lo manifestado por Dimas Gómez, director de Marketing para Latinoamérica y vocero de GEMALTO.

El presente trabajo de tesis está orientado a hacer una investigación que determine si la migración de tarjetas de crédito o débito de banda magnética a chip en el Ecuador reducirá los fraudes por falsificación (clonación) y por consiguiente el perjuicio económico que esto genera no solo a las empresas emisoras de tarjetas de crédito o débito sino también a sus clientes, considerando la inversión que el banco tiene que efectuar para implementar este proceso.

Mediante la recopilación bibliográfica de libros, folletos, revistas e internet, se obtuvo datos relacionados con el tema de fraudes por falsificación de tarjetas de crédito y/o débito en el Ecuador, así como información que permitió conocer en qué consiste el proceso de migración de banda magnética a chip en tarjetas de crédito para evitar este tipo de delitos, la necesidad de que se migre el portafolio a tecnología chip, tomando como ejemplo casos de éxito en otros países en la aplicación de este proceso, así como los beneficios que este cambio generaría tanto para las Instituciones Financieras como para los usuarios de tarjetas de crédito.

Para el desarrollo del estudio de investigación se utilizaron los siguientes métodos:

Primero que todo se parte de la percepción del servicio de tarjetas de crédito y/o débito en el Ecuador por parte de los usuarios, así como conocer si los tarjetahabientes están siendo afectados por fraudes de falsificación de sus tarjetas, para mediante una serie de estudios obtener información que permita conocer si la aplicación de un proceso de migración del portafolio a tarjetas con chip beneficiará tanto a las instituciones financieras como a los usuarios, utilizando para el efecto el método exploratorio y descriptivo.

Luego se plantean los objetivos, tanto el general como los específicos, los cuales pudieron alcanzarse utilizando una serie de estudios que permitieron obtener información necesaria para el efecto.

Seguidamente se procedió a la recolección de la información apoyándonos en herramientas como la encuesta, entrevista y la observación directa.

Una vez obtenidos los resultados se procedió a tabular la información para efectuar un análisis e interpretación de los datos de la muestra aplicada, que presenta y discute los resultados.

El estudio de mercado se lo realizó tomando como base los resultados, obtenidos en la encuesta, demostrando el grado de confianza que presentan los usuarios al efectuar sus transacciones con tarjetas de crédito, se estableció el porcentaje de víctimas de fraude por falsificación y el

grado de conocimiento de mecanismos de prevención y detección de fraudes por falsificación de tarjetas. Es así, que a un 60.97% de la población le inspira poca confianza efectuar sus transacciones con tarjetas de crédito, pese a que el 22% de la población ha sido víctima de algún tipo de fraudes de los cuales el mayor porcentaje corresponde a robo de tarjeta de crédito mientras el 16% corresponde a falsificación (clonación) de tarjetas de crédito.

La segmentación del mercado fue realizada en base a la población de la ciudad de Guayaquil, (INEC, 2010) que son usuarios de tarjetas de crédito y/o débito, información obtenida de la Superintendencia de Bancos y Seguros (2013).

Adicionalmente, con el fin de obtener información útil y necesaria para el desarrollo del trabajo de investigación, se efectuó entrevistas a especialistas en temas de control y prevención de fraudes que laboran en entidades financieras, quienes coincidieron en que la tecnología chip reducirá la incidencia de fraudes por clonación al hacer más difícil la falsificación de tarjetas de crédito y/o débito, disminuyendo de esta forma las pérdidas que por este delito puedan generarse tanto para las Instituciones Financieras como en el usuario.

En el capítulo V se detalla el proceso de implementación de tarjetas con chip y su implicación tecnológica, nos indica la necesidad de migrar a tarjetas inteligentes en el Ecuador, detalla en qué consiste el proceso de migración, los métodos de autenticación, sistemas operativos,

certificaciones, capacitación del personal de la banca, el tiempo estimado que duraría la aplicación del mismo, etc. adicionalmente se determinan los posibles impactos que conllevaría la migración en cuanto a la emisión de las tarjetas de crédito y/o débito, culminando en la contestación de la interrogante que se presenta en el tema de tesis, en cuanto a si los Bancos de Ecuador estarían listos para salir al mercado con tarjetas EMV Chip.

Toda la información previamente mencionada permite llegar a la conclusión de que la implementación de la tecnología chip es un proceso en boga, que a pesar de que su costo podría resultar relativamente alto para las entidades financieras y emisoras de tarjetas de crédito es una inversión a largo plazo, que brindará mayor seguridad al usuario al momento de efectuar sus transacciones, disminuyendo fraudes cuyo origen es la falsificación de las tarjeta, ya que es muy probable que los estafadores migren sus actividades de falsificación de tarjetas de banda magnética a regiones que todavía no han implementado esta tecnología, por lo que es importante estar protegidos. Por otro lado significará también un avance tecnológico de utilidad para el usuario, generando mayor confianza y estandarizando procesos vinculados a la banca a nivel mundial.

CAPÍTULO I: MARCO REFERENCIAL

1.1 Antecedentes

A lo largo de la historia han ocurrido fraudes que han ocasionado grandes catástrofes en el ámbito económico teniendo una implicación grande a nivel mundial.

La rapidez con que evoluciona la humanidad no ha sido extraña al mundo financiero, que recibe el impacto del enorme desarrollo tecnológico, acelerando los procesos, creando nuevos productos inimaginables hace cien años, acercando a los clientes a las operaciones bancarias y relacionando a los bancos entre sí.

Luego de todo este avance tecnológico se ha determinado que se pueden realizar fraudes, desfalcos y demás delitos que son temidos por las empresas a nivel mundial, pero en donde más repercute es en los países desarrollados, ya que el fraude se lo vincula con otros delitos como el terrorismo, el secuestro, el sabotaje y el hurto.

La modernización y globalización de las operaciones financieras han sido positivas para los usuarios o consumidores de los servicios financieros, sin embargo la tecnología no sólo ha sido utilizada para las buenas prácticas, sino también por estafadores, incrementando el riesgo de las entidades financieras, lo que ha tenido que ser contrarrestado con los

propios avances tecnológicos y con supervisión interna y externa más rigurosa.

Una de las reclamaciones más frecuentes según La Asociación de Usuarios de Banca AUSBANC y Servired, que es la empresa que lleva el sistema de pagos de VISA España, está relacionada con el uso de tarjetas robadas y de tarjetas copiadas o duplicadas.

Este tipo de delito, también llamado cloning o skimming, consiste en la duplicación de tarjetas de crédito sin que éstas sean sustraídas del titular, razón por la cual el dueño de la tarjeta no hace la denuncia hasta que revisa su estado de cuenta a fin de mes, lo que da tiempo a los estafadores para hacer elevadas compras con el duplicado y/o efectuar retiros a través de cajeros automáticos.

A un nivel global, el reporte Nilson estimó que las pérdidas por fraude de tarjetas alcanzaron los $6.89 mil millones en $14.6 billones de compras de bienes y servicios y disposiciones de efectivo en 2009.4 De acuerdo al reporte Nilson, mientras que la tendencia de fraude global se ha mantenido constante, las cantidades perdidas por fraude están aumentando y con las tasas actuales de crecimiento se estima llegar a los $10 mil millones de dólares para 2015.5 Mercator Advisory Group reporta que las pérdidas por fraude se encuentre probablemente dramáticamente reportadas por debajo de la cantidad real y que podrían ser en realidad tan altas como $16 mil millones de dólares, especialmente cuando se consideran todos los costos asociados como las investigaciones forenses para los compromisos de

información, demandas, fraude no detectado y pérdidas mal clasificadas por los emisores.6 (Smart Card Alliance América Latina y el Caribe, 2011, página 5).

El valor real del fraude, sin embargo, excede la cantidad actual de pérdidas en dólares. Las compañías de servicios financieros incurren en daños a su reputación, mayores costos de operación por la necesidad de mantenerse vigilantes (incluyendo el monitoreo de transacciones), reducción en la productividad, y mayores gastos de personal; también corren con los costos de la reemisión de tarjetas después de que se produce un incidente de fraude. Un costo que con frecuencia no se observa y no se entiende bien es el impacto que el fraude tiene en el uso de tarjetas y pérdidas de ingresos, con emisores observando menores tasas de activación en las tarjetas re-emitidas y disminución en los volúmenes de transacciones. (Smart Card Alliance América Latina y el Caribe, 2011, página 6).

Es por esto que en América Latina y algunos países de occidente con el fin de mitigar los fraudes de falsificación de tarjetas han implementado la tecnología de tarjetas con chips, teniendo una mejora en los sistemas de seguridad y una reducción significativa en el número de fraudes por clonación de tarjetas de crédito (Visa America Latina y el Caribe, 2012).

De acuerdo a un informe emitido en junio del 2012 por Credibanco Co, estructurador y gestor de negocios en la cadena de valor de instrumentos de pago y operador de los sistemas Visa en Colombia, manifiesta que no se reporta ningún caso de falsificación o clonación de tarjetas con la tecnología

EMV, específicamente desde el año 2010 cuando comenzó en el país la migración de tarjetas con banda magnética a tecnología Chip EMV, dispositivo que genera tranquilidad en la banca que ha adaptado este novedoso mecanismo.

Como un ejemplo del impacto de EMV, la Asociación de Tarjetas del Reino Unido (UK Cards Association) reporta una reducción dramática en el fraude desde la introducción de las tarjetas EMV. El fraude de tarjetas robadas y extraviadas se encuentra en el punto más bajo de las últimas dos décadas, y el fraude por falsificación de tarjetas también se ha reducido significativamente y se encuentra en el punto más bajo desde 1999. La pérdidas en comercios del Reino Unido se han reducido 67 por ciento desde el 2004, el fraude por tarjetas robadas o extraviadas se ha reducido en 58 por ciento entre 2004 y 2009; y el fraude por tarjetas no recibidas por correo se ha reducido en 91 por ciento desde el 2004. (Smart Card Alliance América Latina y el Caribe, 2011, página 6)

De acuerdo con información de la empresa GEMALTO, dedicada a la fabricación de los plásticos bancarios en el país, Ecuador tiene un retraso en la migración de tarjetas de débito bancarios con chip frente a países latinoamericanos como Venezuela, Colombia y Brasil los cuales en un par de años tendrán el 100% de su portafolio remplazado.

Ante esta situación, y la creciente utilización de mecanismos fraudulentos que intentan hacer cada vez más vulnerable la información de las tarjetas de débito o crédito con banda magnética, los emisores han

comenzado a migrar hacia otras tecnologías que reduzcan esa posibilidad, es por eso que en Ecuador, los bancos están comenzando a desarrollar las estrategias para cambiar sus tarjetas de banda a chip de acuerdo con la disposición emitida por la Superintendencia de Bancos y Seguros con resolución JB-2012-2148 de 26 de abril del 2012.

Un punto importante que debe tenerse en cuenta es que los estafadores son conocidos por explotar siempre el punto más débil de la cadena, moviéndose de lugares donde se presentan mecanismos más fuertes de autenticación y trasladándose a aquellos lugares donde no los hay, o cambiándose de las instituciones financieras y comercios que cuentan con mecanismos más sofisticados de detección del fraude hacia aquellos que cuentan con mecanismos menos sofisticados. Con más de mil millones de tarjetas EMV emitidas globalmente y proyecciones que indican un crecimiento constante en la emisión de tarjetas EMV, es muy probable que los criminales migren sus actividades de falsificación de tarjetas de banda magnética a regiones que todavía no han implementado EMV, lo que conlleva a un incremento de fraude internacional (cross-border) adquirido en esos países. Individualmente, la industria de pagos de cada uno de los países de la región de América Latina deberá determinar si se encuentra preparada para el potencial incremento significativo del fraude con tarjetas, si el fraude migra de países que ya se encuentran habilitados para EMV a mercados que aún no lo están en la región. (Smart Card Alliance América Latina y el Caribe, 2011, página 6).

1.2 Planteamiento del problema

Mediante este estudio se pretende demostrar la percepción del servicio de tarjetas de crédito y de débito en el país y su nivel de confianza respecto a estos para posteriormente describir y proponer la implementación de un proceso de migración a tarjetas con chip en la que el sistema de seguridad tenga menores posibilidades de vulnerabilidad, así como la facilitación de uso.

Hasta el 2010 la Policía Judicial recibía 5 denuncias por día sobre fraudes electrónicos y robo de tarjetas bancarias por medio de internet. De esa fecha hasta hoy no existen datos concretos, sin embargo del 2010 al 2013 esta cifra se ha incrementado, por lo que la Superintendencia de Bancos y Seguros, Órgano de Control de las Entidades Financieras y de Seguros, ha dispuesto un cronograma con plazos para implementar medidas que puedan mitigar este tipo de delitos.

Durante los últimos años los sistemas de la banca han evolucionado, sin embargo su crecimiento en comparación con otros países de América Latina no ha sido tan acelerado, lo que podría evidenciar una lenta adaptación de nuevas tecnologías.

En la actualidad, la red de servicios financieros permite a los usuarios efectuar transferencias, giros o pagos en línea, a través del uso de canales como: la banca móvil y la banca internet. En América Latina el 25% de operaciones totales efectuadas fueron realizadas a través de banca internet,

lo cual deja ver su alta importancia y crecimiento en la región (Comscore S.A.). En Ecuador desde el 2001, el total de usuarios de internet respecto a la población total, medida como densidad o penetración del servicio, pasó de 2% al 48,1% a junio de 2012. (Secretaria Nacional de Telecomunicaciones [Senatel], 2012)

Estos porcentajes son similares a los registrados en cuanto al uso de tarjetas inteligentes en la región. En América Latina, El Caribe y Canadá se han emitido 182,4 millones de tarjetas inteligentes, lo que representa el 26,4% del total de tarjetas que circulan. (Smart Card Alliance América Latina y el Caribe, 2011, página 8)

En la legislación ecuatoriana no existe una norma sobre la responsabilidad del usuario de tarjetas de crédito, no obstante hay que fijarse en las cláusulas estipuladas en el contrato que suscriben los clientes al momento de recibir una tarjeta de crédito. Sin embargo, el titular no asumirá ninguna responsabilidad por los pagos fraudulentos que se produzcan con la tarjeta después del aviso a la entidad de su pérdida o robo, salvo que el titular haya incurrido en fraude o negligencia grave.

Si bien no existe una norma que indique el plazo mínimo para realizar una notificación a la entidad acerca del robo o extravió de una tarjeta de crédito se recomienda que está se haga a la brevedad posible. (Superintendencia de Bancos y Seguros, 2012).

1.3 Objetivos

1. 3.1 Objetivos Generales

Establecer el costo beneficio que implica la migración de tarjetas con banda magnética a chip en el Ecuador, considerando la inversión que tienen que efectuar los Bancos Emisores de tarjetas para la implementación de este proceso.

1.3.2 Objetivos Específicos

- Describir en qué consiste el proceso de migración de las tarjetas de crédito de banda magnética a tarjetas inteligentes o chip.
- Identificar las causas y debilidades que originan fraudes de clonación en las tarjetas de crédito y débito con banda magnética.
- Determinar las mejores prácticas de seguridad para los usuarios con la implementación de tarjetas con chip.
- Proponer los mecanismos y estrategias para evitar fraudes en las tarjetas de crédito, desde el punto de vista del consumidor, de la emisora de la tarjeta.

CAPÍTULO 2 . MARCO TEORICO

BANCA Y TARJETAS DE CRÉDITO

Para analizar el proceso de cambio a tarjetas con chip es importante delimitar primero los tipos de tarjetas de crédito existente y la función de estas.

Se podría decir que existe una tarjeta de crédito para cada tipo de usuario. A partir de esto se definen las debilidades de los sistemas que estas usan.

A este tipo de tarjetas las tarjetas con chip llegan para ofrecer un cambio al manejo y a las seguridades del sistema hasta ahora usado en países como Ecuador.

2.1 Definiciones de Tarjetas de Crédito

Las tarjetas de crédito son medios de pago que se utilizan principalmente a través de una Terminal Punto de Venta (TPV) o a través de cajeros automáticos para la extracción de dinero en efectivo. Su estructura es principalmente de plástico de dimensiones establecidas y que guardan una gran cantidad datos en una banda magnética o chip, así como en su soporte físico. Si bien estas tarjetas tienen medidas de seguridad, estas pueden variar de institución a institución.

Una tarjeta de crédito es una tarjeta de plástico con una banda magnética, y un número en relieve que sirve para hacer compras y pagar el

préstamo en fechas posteriores. Entre las más conocidas del mercado Nacional están: Visa, American Express, MasterCard y Diners Club, Pacificard, entre otras (Las Tarjetas de Crédito, 2013).

Las grandes tiendas y almacenes del mundo también emiten tarjetas de crédito para sus clientes.

2.1 La Tarjeta de Crédito

Es una tarjeta de plástico con una banda magnética, a veces un microchip, y un número en relieve que sirve para hacer compras. Por su capacidad de realizar pagos se las llama también dinero plástico.

La mayor ventaja es la flexibilidad que le da al usuario, quien puede pagar sus saldos por completo cada mes o puede pagar en parte.

2.1.2 La Tarjeta de Débito

Es una tarjeta bancaria de plástico con una banda magnética, usada para extraer dinero de un cajero automático y también para pagar compras en comercios que tengan un terminal lector de tarjetas bancarias.

Se diferencia de la tarjeta de crédito en que el dinero que se usa nunca se toma a crédito sino del que se disponga en la cuenta bancaria (*débito*).

2. 2 Clasificación de las tarjetas de crédito

Las tarjetas de crédito se han convertido en la forma de transacción más sencilla para el hombre. El hecho de evitar tener dinero en efectivo en

una operación de negocios y tener el respaldo de una institución, ofrece seguridad para las partes.

Dentro de las tarjetas existentes en el mercado mundial, existe la siguiente clasificación:

- Según el emisor
    - Bancarias
    - No bancarias
- Según el público
    - Personales
    - De empresas
- Por su duración
    - Limitadas e Ilimitadas

2.2.1 Clasificación de las tarjetas de crédito según el emisor

Tarjetas Bancarias: Son las emitidas por una Entidad Financiera

Dentro de la clasificación Tarjetas Bancarias y con sus mismas características generales, hay un tipo de tarjetas denominado Tarjetas de Marca Compartida. Estas tarjetas están emitidas por una Entidad Financiera en colaboración con un socio comercial. Existen dos modalidades de Tarjetas de Marca Compartida: Cobranded y Affinity o de Afinidad.

La diferencia entre ambas viene dada por la existencia o no de ánimo de lucro en el socio comercial. Un ejemplo de Tarjeta de Marca Compartida de modalidad Cobranded es la Tarjeta Visa Repsol BBVA y de modalidad Affinity la Tarjeta Visa Cruz Roja BBVA. En el mercado existen diferentes marcas de Tarjetas Bancarias: Visa, Mastercard, Diners, Pacificard, American Express etc.

Tarjetas No Bancarias: Son las emitidas por un emisor privado no bancario.

Dentro de las Tarjetas no Bancarias podemos encontrar dos grandes grupos: Tarjetas T&E: Destinadas en general al pago de actividades relacionadas con viajes y entretenimiento. Algunos ejemplos son American Express, Diners o JCB. Tarjetas Privadas: Destinadas de forma exclusiva al pago en los establecimientos propios del emisor de la Tarjeta.

2.2.2 Clasificación de las tarjetas de crédito según el público

Las Tarjetas Bancarias según el público objetivo al que vayan destinadas pueden ser:

Tarjetas Personales: Son aquellas que están diseñadas para cubrir las necesidades de los pagos derivados de la compra de bienes y servicios del consumo privado. Las tarjetas personales pueden ser en función de la forma de pago de Crédito, de Débito o Pre-pago (monedero o virtuales). O bien, pueden admitir varias de estas formas de pago en un mismo plástico.

Tarjetas de Empresa: Son aquellas destinadas a cubrir los gastos de aprovisionamiento, viajes y representación de las empresas. Las Tarjetas de empresa pueden ser, también en función de la forma de pago, de Crédito o Débito, aunque la modalidad más habitual es la de crédito.

2.2.3 Clasificación por el crédito concedido y la modalidad de pago

- Las Tarjetas de Crédito de pago inmediato, que son aquellas que tienen una determinada fecha de pago previamente establecida.
- Revolting Credit que son aquellas que permiten hacer uso de un monto total de crédito previamente abonado este en su totalidad o en determinado porcentaje previamente acordado.
- Las mixtas, que combinan e incorporan elementos propios de los dos tipos antes mencionados.

2.3 Compañías emisoras de tarjetas de crédito

Son compañías emisoras o administradoras de tarjetas de crédito las sociedades anónimas que prestan servicios de carácter financiero, mediante la emisión, administración, financiamiento o mercadeo de tarjetas de crédito de pago y de afinidad de circulación general, en moneda nacional o extranjera; así como tarjetas de crédito o de pago de circulación restringida en moneda nacional, previa autorización de la Superintendencia de Bancos y Seguros.

Son emisoras de tarjetas de crédito las sociedades autorizadas que realizan, por propia emisión o por concesión de marca, las siguientes actividades (Superintendencia de Bancos y Seguros, 2012):

1. Emitir y promover la tarjeta;
2. Calificar y aprobar las solicitudes de los tarjetahabientes y de afiliación de establecimientos;
3. Conceder líneas de crédito, ya por utilización de la tarjeta de crédito en establecimientos comerciales o por entrega de dinero en efectivo;
4. Efectuar cobros a los tarjetahabientes y pagos a los establecimientos;
5. Recibir fondos de sus tarjetahabientes con la finalidad de efectuar cargos a sus futuros consumos.
6. Otras actividades estrictamente relacionadas con el objeto de las compañías emisoras o administradoras de tarjetas de crédito, las que deberán ser reportadas a la Superintendencia de Bancos y Seguros, quien informará a la Junta Bancaria.

Los emisores de las tarjetas de crédito podrán operar por sí mismos dichas tarjetas o contratar su administración y operación total o parcial con una entidad autorizada por la Ley General de Instituciones del Sistema Financiero.

Son administradores u operadores de las tarjetas de crédito, las sociedades autorizadas a operar como tales, que convienen con una entidad

emisora en realizar cualquiera de las actividades detalladas, excepto la emisión.

2.4 El Crédito Corriente y diferido

El buen uso de las tarjetas de crédito permite un mejor manejo de los ingresos familiares, ya que no hay que esperar a fin de mes para hacer ciertas compras, principalmente cuando se utiliza crédito corriente, ya que este debe ser pagado a finales del mes y no representa una carga financiera.

No obstante, siempre hay la tentación, o la necesidad, de diferir el pago más allá del crédito corriente, y si bien la transacción es exactamente la misma desde el punto de vista práctico, los costos del crédito corriente vs el diferido o el rotativo son diferentes.

Estos costos adicionales, son manejables para los usuarios siempre que el financiamiento no exceda su capacidad de pago mensual. En otras palabras son pequeño porcentaje de diferido y rotativo es bueno, pero el problema se da cuando se van acumulando saldos atrasados y los costos financieros suben (ahí se entra en un círculo vicioso: se pagan solo los mínimos, se acumula el saldo, sube el interés y cada vez es más difícil pagar la deuda).

Como es lógico, con más tarjetas en el mercado el volumen de crédito ha subido. Eso es perfectamente comprensible en una economía que viene recuperándose de la crisis económica, y que tiende a gastar más a medida

que sube el ingreso real (porque ha caído la inflación). Pero una lectura más cercana a la estructura del endeudamiento puede decirnos algo más.

El crédito corriente representaba en el año 2004 el 32% del total y en lo que va del año ha bajado al 21%. Los ecuatorianos están recurriendo en forma creciente al crédito diferido y rotativo. El saldo total (es decir, lo que falta por pagar) registrado hasta el primer trimestre del 2012 era de 1600 millones de dólares, y todos meses el saldo total va creciendo, lo que significa que se está contratando nueva deuda pero que no se está pagando la totalidad de la misma. (http://investiga.ide.edu.ec/).

En los actuales momentos, los tarjetahabientes están cancelando sus deudas con intereses altos, acogiéndose a la opción del diferido, no obstante la morosidad no ha subido en forma anormal. Se mantiene en niveles del 5% promedio, lo cual es una muestra de que las cuentas se están pagando por parte de los consumidores, con un poco de retraso pero se están pagando.

Tabla 1. Tasas de interés América Latina

	Brasil	México	Chile	Perú	Colombia
2013	**%**	**%**	**%**	**%**	**%**
Abr	7,50	4,00	5,00	4,25	3,25
Mar	7,25	4,00	5,00	4,25	3,25
Feb	****	****	5,00	4,25	3,75
Ene	7,25	4,50	5,00	4,25	4,00
2012	**%**	**%**	**%**	**%**	**%**
Dic	7,25	4,50	5,00	4,25	4,25
Nov	7,25	4,50	5,00	4,25	4,50
Oct	7,25	4,50	5,00	4,25	4,75
Sep	****	4,50	5,00	4,25	4,75
Ago	7,50	****	5,00	4,25	4,75
Jul	8,00	4,50	5,00	4,25	5,00
Jun	****	4,50	5,00	4,25	5,25
May	8,50	****	5,00	4,25	5,25
Abr	9,00	4,50	5,00	4,25	5,25

Mar	9,75	4,50	5,00	4,25	5,25
Feb	****	****	5,00	4,25	5,25
Ene	10,50	4,50	5,00	4,25	5,00

Fuente: (Thomson Reuters, 2013)

2.5 Ventajas y desventajas en el uso de la tarjeta de crédito

En la vida cotidiana el uso de la tarjeta de crédito tiene ventajas y desventajas claramente identificadas y el conocimiento de éstas, permite el correcto uso y la toma de acciones preventivas para evitar contratiempos.

2.5.1 Ventajas

Las ventajas importantes que se conocen sobre el uso de la tarjeta de crédito se describen a continuación:

- Aceptación en el ámbito mundial en cualquier comercio que exhiba la marca a que pertenezca.
- Se puede utilizar en compras o retiros de efectivo.
- Mayor conveniencia de servicios.
- Crédito inmediato.
- Menor riesgo de ser víctima de robo de efectivo o cheques.
- Uso del financiamiento por los consumos durante el mes.
- Financiamiento gratuito en caso de pago de contado.
- Acceso a los cajeros automáticos, los 365 días del año, las 24 horas.
- Seguro de viajes.

- Seguro de autos rentados.
- Seguro contra robo.
- Seguro contra fraude.
- Reemplazo del plástico en caso de emergencia, en cualquier parte del mundo.
- Transacciones a través del Internet.
- Referencias crediticias para el buen usuario.
- Reducción de costos administrativos para los establecimientos.
- Reducción de riesgo de manejo de efectivo para el comercio.
- Garantía de pago y evita gestión de cobro al comercio.
- Aumento de volumen de ventas para el comercio.
- Descuentos y promociones especiales por ser poseedor de una tarjeta de crédito en particular si es buen usuario de la misma.

2.5.2 Desventajas

Las desventajas de la tarjeta de crédito con relación a las ventajas que ofrece, son pocas y al igual que las ventajas van tanto para el tarjeta-habiente como para el comercio:

- Alta tasa de interés por el financiamiento, 1.63 % mensual. http://investiga.ide.edu.ec

- Las tasas de interés en el caso de las tarjetas de consumo está en el 16% anual. http://investiga.ide.edu.ec
- Comisiones por transacciones; (retiros de efectivo, por cheque rechazado, por pago retrasado).
- Riesgo de robo y fraude.
- Riesgo de extravió y fraude.
- Descontrol en gastos del usuario o tarjeta habiente.
- Por uso del financiamiento, el costo del bien adquirido sube.
- Riesgo de caer en mora por los altos pagos que pueda generar.
- Riesgo de caer en cobro jurídico por mora.
- Riesgo de malas referencias crediticias.
- Pérdida por transacciones fraudulentas para el establecimiento.
- El comercio cae en riesgo de cancelación de la afiliación, por liquidar transacciones fraudulentas.

2.6 Definición de Fraude

El vocablo Fraude se refiere a: Engaño que se hace a uno para procurarse una ventaja en detrimento de él, de los actos del deudor que dejan al acreedor sin medios de obrar lo que se debe (Comisión Federal de Comercio, 2008).

El término fraude se refiere a un acto intencional por parte de uno o más individuos de la administración, empleados o terceras personas, que da como resultado una representación errónea de los estados financieros.

El fraude puede implicar:

- Manipulación, falsificación o alteración de registros o documentos.
- Malversación de activos.
- Supresión u omisión de los efectos de transacciones en los registros o documentos.
- Registro de transacciones sin sustancia.
- Mala aplicación de políticas contables.

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

Las entidades financieras por administrar activos que por su naturaleza inherente son de fácil conversión o por el tipo de actividad que desempeñan, están expuestas a ser víctima de actividades fraudulentas en forma más rápida que el resto de empresas.

Los tipos más frecuentes de actividades de fraude, que usualmente ocurren podrían incluir pero no limitarse a:

- Utilizar plásticos destruidos parcialmente
- Lavado de dinero con tarjeta crédito
- Robo de estados de cuenta.

- Consumo y retiros de efectivo usando una tarjeta de crédito no entregada o robada o clonada.
- Robo de base de datos de clientes.
- Operaciones de créditos y pagos a cuentas fraudulentas.
- Activación de tarjetas inactivas y retiro de fondos de éstas.

2.7 Tipos de fraudes más comunes

Los fraudes más conocidos son los siguientes:

- Fraudes relacionados con las claves de banca electrónica de los usuarios. Con estas claves, los delincuentes realizan transferencias de cuentas de clientes hacia otras personas y luego realizan retiros en efectivo.
- Ofertas en página web de productos o servicios que no existen
- Suplantación de identidad, es decir que los delincuentes abren cuentas o realizan transacciones a nombre de las personas a las que les han robado su cédula o pasaporte.

2.8 Formas como los delincuentes obtienen las claves

Las personas inescrupulosas tienen diferentes formas de engañar a los usuarios para obtener claves, algunas de estas formas son: (Superintendencia de Bancos y Seguros, 2011):

Phishing.- Obtienen información confidencial a través de un correo electrónico en el que engañan al usuario haciéndole creer que debe enviar sus claves o datos para confirmación o actualización de datos.

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

Phaming.- Similar al anterior, pero en esta modalidad el delincuente re-direcciona al usuario, es decir, lo manda a una página que se ve como la original de su banco y que recogerá las claves confidenciales cuando el usuario las digite.

Malware.- El malware bancario, los troyanos y keyloggers son todos programas utilizados para fines delictivos, como por ejemplo aquellos diseñados para captar y grabar las teclas que el usuario digita cuando ingresa su clave en una página web.

Skimming.- Al momento en que una persona entrega su tarjeta de crédito en un local comercial, el delincuente la pasa por un aparato llamado skimmer que graba la información de la banda magnética de la tarjeta y luego la graba en una tarjeta falsa.

Estafa Piramidal.- La estafa piramidal, la carta nigeriana se distribuyen por correo electrónico y tratan de convencer al usuario de que entregando una suma de dinero o sus claves electrónicas, luego obtendrá grandes ganancias a través de una red social en la que aportan muchas personas.

Figura 1. Ciberdelitos en el mundo

Fuente: Norton

2.9 Situación actual de las tarjetas de créditos

En el Ecuador, la principal tendencia apunta a conformar una especie de democratización del acceso al uso de la tarjeta. El tradicional mercado de las tarjetas, el de los sectores alto y medio alto, está copado. Se describe que, de los ciudadanos urbanos, cada uno de ellos tiene un promedio de por lo menos dos tarjetas. Significa que si alguien desea lanzar una nueva tarjeta debe competir con las dos ya existentes en la billetera. Del consumo final de hogares en el país, que es de aproximadamente $30,000 millones, $6,700 millones salen de este sector y $2,200 millones se hacen con tarjetas. (Asociación de Bancos Privados, 2012)

En una economía emergente como la ecuatoriana, el uso de la tarjeta de crédito permite acceder a bienes y servicios sin necesidad de contar con el efectivo al momento de comprar; además concede un plazo de tiempo para realizar el pago por medio de cuotas “aparentemente convenientes”; no obstante, un manejo irresponsable de esta herramienta de crédito, por parte de los usuarios, así como una insuficiente reglamentación que regule el uso y el abuso de emisores e intermediarios del negocio, pueden ocasionar inconvenientes a todos los participantes de este sistema de pago.

Actualmente se ha tomado conciencia que la legislación ecuatoriana ha sido durante décadas un tanto flexible en el establecimiento de tasas de interés, comisiones y costos de las Tarjetas de Crédito, intensificándose el problema a partir del último lustro, con la aparición masiva de nuevas Tarjetas dirigidas a consumidores menos solventes y con costos mucho más elevados.

El Registro Oficial No. 640 del 23 de julio de 2009 publica la Resolución de la Superintendencia de Compañías No. DSC.Q.09.01, por la cual se regula la emisión de tarjetas de consumo, descuento, crédito de casas comerciales y otras similares de circulación restringida para adquisición de bienes o servicios en casas comerciales sujetas a control de la Superintendencia de Compañías.

No obstante, La Junta Bancaria (2012), a través de la resolución JB-2012-2225, del 5 de julio del 2012 dispuso que los establecimientos comerciales no podrán emitir tarjetas de crédito o también llamadas de

circulación restringida, señalando que solamente las instituciones financieras y las compañías emisoras o administradoras de tarjetas de crédito pueden actuar como emisor y operador del plástico.

Esto significaría que las utilizadas por empresas como De Prati, Etafashion, Créditos Económicos o Pycca tendrán que salir de circulación. La única excepción para esta norma son las tarjetas de crédito "emitidas por compañías que son originarias de procesos de titularización de cartera", es decir, que han realizado operaciones en la Bolsa de Valores que comprometen sus ganancias.

Tabla 2. Tasas de interés activas efectivas vigentes a Mayo 2013

Tasas Referenciales		Tasas Máximas	
Tasa Activa Efectiva Referencial para el segmento:	% anual	Tasa Activa Efectiva Máxima para el segmento:	% anual
Productivo Corporativo	8.17	Productivo Corporativo	9.33
Productivo Empresarial	9.53	Productivo Empresarial	10.21
Productivo PYMES	11.20	Productivo PYMES	11.83
Consumo	15.91	Consumo	16.30
Vivienda	10.64	Vivienda	11.33
Microcrédito Acumulación Ampliada	22.44	Microcrédito Acumulación Ampliada	25.50
Microcrédito Acumulación Simple	25.20	Microcrédito Acumulación Simple	27.50
Microcrédito Minorista	28.82	Microcrédito Minorista	30.50
2. TASAS DE INTERÉS PASIVAS EFECTIVAS PROMEDIO POR INSTRUMENTO			
Tasas Referenciales	% anual	Tasas Referenciales	% anual
Depósitos a plazo	4.53	Depósitos de Ahorro	1.41
Depósitos monetarios	0.60	Depósitos de Tarjetahabientes	0.63
Operaciones de Reporto	0.24		
3. TASAS DE INTERÉS PASIVAS EFECTIVAS REFERENCIALES POR PLAZO			
Tasas Referenciales	% anual	Tasas Referenciales	% anual
Plazo 30-60	3.89	Plazo 121-180	5.11
Plazo 61-90	3.67	Plazo 181-360	5.65
Plazo 91-120	4.93	Plazo 361 y más	5.35

Fuente: (Banco Central del Ecuador, 2013)

En este gráfico se puede observar las tasas referenciales y máximas de acuerdo al tipo de crédito.

En el actual gobierno, las Instituciones Financieras emisoras de tarjetas de crédito ya no están percibiendo ingresos por concepto de afiliación y renovación, en virtud de que mediante resolución No. JB-2012-2151 del 26 de abril del 2012, la Junta Bancaria (2012) resolvió que las entidades financieras no cobrarán por ciertos servicios a partir de abril del 2012, entre los cuales se encuentra la afiliación y renovación de tarjetas de crédito manifestando que 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.

Además de los costos de renovación, también ha existido cambio en las tasas de interés de los créditos diferidos, es así que en las compras a tres, seis y doce meses, antes había diferenciación de los intereses. Mientras más corto era el plazo, se le daba al cliente una tasa más baja, sin embargo ahora las tasas están reguladas de acuerdo al tipo de crédito, según el cuadro expuesto anteriormente.

Como conclusión se puede mencionar que la cultura consumista del ecuatoriano, este sector ha estado en crecimiento en los últimos años. De

ahí que la meta esté en llegar a otros espacios de la pirámide de ingresos, algo en lo que trabajan esmeradamente las Instituciones Financieras.

Es importante mencionar que bajo las nuevas leyes impuestas a las tarjetas de crédito las instituciones financieras buscan medidas a tomar, bajo el supuesto de no suspender el servicio o cerrar las tarjetas de gente que no tiene mucho volumen de operaciones, por lo tanto, los bancos buscan compensaciones en las medidas ya mencionadas.

2.10 Tarjetas de crédito autorizadas en Ecuador

Las tarjetas de crédito autorizadas por la Superintendencia de Bancos y Seguros del Ecuador son:

Tabla 3. Tarjetas de crédito autorizadas en Ecuador

INSTITUCIÓN	TARJETA
BANCO DE GUAYAQUIL	AMERICAN EXPRESS
SOCIEDAD FINANCIERA DINERS CLUB	DINERS
BANCO AUSTRO S.A.	MASTERCARD
BANCO BOLIVARIANO C.A.	MASTERCARD
BANCO DE GUAYAQUIL	MASTERCARD
BANCO DEL PACIFICO S.A.	MASTERCARD
BANCO PRODUBANCO	MASTERCARD
BANCO INTERNACIONAL S.A.	MASTERCARD
BANCO PICHINCHA C.A.	MASTERCARD
PACIFICARD S.A.	MASTERCARD
PACIFICARD S.A.	VISA
BANCO AMAZONAS S.A.	VISA
BANCO AUSTRO S.A.	VISA
BANCO BOLIVARIANO C.A.	VISA
BANCO COMERCIAL DE MANABI S.A.	VISA
BANCO DE GUAYAQUIL S.A.	VISA
BANCO PRODUBANCO	VISA
BANCO DEL PICHINCHA	VISA
BANCO DE LOJA S.A.	VISA
BANCO DE MACHALA S.A.	VISA
BANCO GENERAL RUMIÑAHUI S.A.	VISA
BANCO INTERNACIONAL S.A.	VISA
BANCO PROMERICA S.A.	VISA
BANCO TERRITORIAL S.A.	VISA
BANCO UNIBANCO S.A.	VISA
INTERDIN	VISA
MUTUALISTA AZUAY	VISA
MUTUALISTA PICHINCHA	VISA
BANCO SOLIDARIO S.A.	MI SOCIA - BCO. SOLIDARIO
BANCO TERRITORIAL S.A.	CREDITO SI-BCO. TERRITORIAL
BANCO UNIBANCO S.A.	CUOTA FACIL - UNIBANCO
BANCO INTERNACIONAL S.A.	ROSE - BANCO INTERNACIONAL

Fuente: Estructuras integradas de datos / Sistema Operativos de Activos /Dirección Nacional de Estudios y Estadísticas/ Dirección de Estadísticas/DLS

CAPÍTULO 2: FRAUDES Y SU REPERCUSIÓN SOCIAL

Con la implementación de nuevas tecnologías para la gestión de transacciones bancarias se han originado una serie de fraudes capaces de atentar a la sociedad y su seguridad.

2.1 Fraude con Tarjeta de Crédito

Transacción en la cual el tarjeta habiente no participó, ni autorizó un consumo o retiro de fondos con su plástico (GFI Software, 2013).

Para ampliar el concepto de fraude con tarjeta de crédito (Iron Port, 2013), se puede decir que: son todas aquellas transacciones realizadas con un plástico válido o inválido, con el fin premeditado de obtener bienes y servicios, los cuales serán cargados al estado de cuenta del titular del mismo, como transacciones legítimas, que obviamente el tarjeta habiente no reconocerá, lo cual representa pérdida para el banco emisor de la tarjeta; esto dependerá del tipo de fraude para determinar si los valores son recuperables o no.

2.2 Causas y Efectos de un Fraude

Es indudable que los fraudes se cometen por causas que en la mayoría de los casos, la persona que los realiza, justifica este hecho para sentirse bien de haber cometido el delito.

Se puede indicar que una de las principales causas internas por las que se comete un fraude está originada por la necesidad de dinero que el empleado o la persona tenga y generalmente se argumenta que la empresa tiene mucho dinero y que por tanto, tomar una pequeña cantidad de dinero no causará ningún daño. En algunas ocasiones el empleado lo toma con la intención de devolverlo.

Una segunda causa interna por la que se comete un fraude es porque una persona se siente mal remunerada o en condiciones de desventaja en relación con otros funcionarios o empleados en el orden económico

Una tercera causa de fraude es por controles y procedimientos deficientes en el manejo de las actividades y operaciones de la empresa.

Como cuarta causa aunque esta no es interna podría influir en la acción de cometer fraude la situación económica del país, la tasa de desempleo y la violencia, entre otros.

En lo que se refiere a causas que podrían influir directamente a cometer fraudes con tarjeta de crédito a continuación se enumeran las siguientes:

2.2.1 Causas Internas

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

2.2.2 Causas Externas

Situación económica del país: En diciembre de 2012 las operaciones de consumo de crédito cerraron en 552,706 cifra superior a las del 2011 durante el mismo período que era 545,394. El volumen del crédito de consumo llegó a $384,4 millones en diciembre de 2012, frente a los $389,4 millones del mismo mes del año anterior. (Banco Central del Ecuador, 2013)

Robo de tarjeta o clonación de plásticos: Los asaltos y la tecnología hacen que para los delincuentes el negocio de la tarjeta de crédito represente una fuente magnífica para obtener beneficio económico.

2.2.3 Efectos

Los efectos de un fraude con tarjeta de crédito solo se podrán medir cuantitativamente. Con cifras se demuestra la cantidad con que ha sido desfalcado un banco emisor de tarjeta de crédito. Estos efectos repercuten negativamente en los siguientes aspectos:

- Índices negativos de cartera en mora.
- Pérdida de credibilidad.
- Deterioro la imagen.
- Disminución de total de clientes: Debido a que hay clientes que prefieren cancelar su tarjeta después de que han sido objeto de fraude.

2.3 Fraudes mediante clonación de tarjetas de crédito

Hoy en día es muy frecuente escuchar hablar sobre la clonación de tarjetas de crédito y débito, por lo que se hace importante conocer a qué nos referimos cuando hablamos de clonación.

La clonación es un término usado en nuestros tiempos para indicar que es una copia exacta de alguna cosa y en el caso de las tarjetas de crédito, se utiliza el mismo término.

La clonación de tarjetas de crédito o débito, también conocido como skimming, consiste en la duplicación de tarjetas de crédito o débito sin el consentimiento del dueño de la tarjeta. En otras palabras es una vulneración directa a reglas de seguridad de las entidades financieras y una afectación clara al deber de idoneida de los emisores de tarjetas de crédito.

Quienes poseen una tarjeta de crédito pueden ver que éstas presentan una banda magnética en la parte posterior, la misma que hoy en día es muy fácil de copiar su contenido en otro plástico con un dispositivo electrónico, a este proceso se le llama clonación de tarjetas de crédito.

2.4 Causas de la clonación de tarjetas de crédito

Además de los cajeros automáticos, se pueden clonar las tarjetas en gasolineras, restaurantes y otros negocios donde se entregan las mismas para efectuar los pagos, una de las principales causas por las que se puede presentar la clonación de las tarjetas de crédito o débito es porque el dueño no está presente o cerca en el momento en que operan la tarjeta, por lo que no se dan cuenta del fraude hasta que les llega el estado de cuenta o cuando van a comprar en una tienda o por internet con su tarjeta y le dicen que la misma está al límite o se la rechazan.

Cualquier persona puede ser una víctima con solo facilitar su tarjeta en una tienda o restaurante y no estar atentos a ella o por introducir la tarjeta en un cajero ATM especialmente manipulado.

Según datos proporcionados por la Policía Judicial de Pichincha existen bandas de clonadores de tarjetas de crédito que operan dentro y fuera del país los cuales reclutan personal de discotecas, restaurantes y gasolineras, para que suministren datos de tarjeta-habientes nacionales y extranjeros.

En nuestro país, los restaurantes y gasolineras serian algunos de los sitios donde los delincuentes consiguen cómplices que se encargan de clonar las tarjetas, es por eso que no es muy recomendable pagar con tarjetas en este tipo de negocios, ya que normalmente las personas que hacen el trabajo de clonar para los delincuentes reciben una baja gratificación.

2.5 Formas cómo se puede clonar una tarjeta de crédito

Existe una amplia gama de actividades delictivas que se pueden efectuar a través de una tarjeta de crédito, sin embargo, nos referiremos a los que se realizan exclusivamente por la clonación de la misma. A continuación mencionaremos las formas de clonación más comunes:

a) Clonación para compras
b) Clonación para retiros de cajeros

La primera de estas formas: consiste en copiar la información contenida en la banda magnética de una tarjeta de crédito, para luego transferir la misma a otro plástico y por medio de ese segundo elemento,

realizar compras con el saldo o el crédito que el tarjeta habiente pudiera tener disponible en la misma.

La segunda, si bien comienza con la copia de la información contenida, además requiere de la obtención del numero confidencial del cliente para la realización de retiros, ya que como sabemos sin ese número (Nip o número de identificación personal o Pin por sus siglas en inglés) no es posible realizar extracciones en los cajeros automáticos que es a lo que se apunta con esta conducta en particular.

2.6. Fases en la clonación de tarjetas al efectuar compras

Para la clonación de una tarjeta de crédito, las personas inescrupulosas realizan su actividad en tres etapas claramente identificadas, estas son:

1. **Primera etapa:**

La víctima que realiza un pago, en un almacén, restaurantes o gasolineras, pierde contacto visual con su tarjeta de crédito.

La persona que recibe el pago, pasa la banda de la tarjeta en un dispositivo conocido como skimmer. Este skimmer es un lector de tarjetas de crédito, que se puede comprar por US$1,200 dólares aproximadamente, en sitios como Mercado Libre o de Remate.com. Recuperado (http://eleconomista.com.mx/finanzas-personales/2011/09/25/proteja-sus-tarjetas-contra-skimmer)

Este dispositivo que tiene el tamaño de una cajetilla de cigarrillos, contiene un chip capaz de leer y almacenar el código de la banda magnética de las tarjetas para su posterior descarga.

Tiene la capacidad de almacenarla información de 500 tarjetas de crédito y cuando es usada lícitamente, la máquina permite verificar los datos del cliente para aprobar una compra por parte del emisor de la tarjeta. Recuperado de (http://eleconomista.com.mx/finanzas Personales/2011/09/25/proteja-sus-tarjetas-contra-skimmer).

Esta operación puede ser realizada por el mesero, por el cajero o por cualquier otro empleado que tome contacto con el plástico.

2. **Segunda etapa:**

El que obtiene la información se la entrega a una segunda persona, que es la que descarga la misma en una computadora y desde allí la graba a otros plásticos en blanco, a los cuales también se les agregarán logotipos institucionales y se le imprime la apariencia de una verdadera tarjeta.

3. **Tercera etapa:**

Se entrega ese plástico ya terminado a una persona que es la que sale a realizar las compras a los diferentes comercios, preferiblemente de productos que sean de fácil venta como por ejemplo electrónica de punta y de alto valor de mercado. Una vez obtenida de manera ilegítima la mercadería, se comercializa en el mercado negro (adonde también van los

productos robados) para de esta manera hacer efectivas las ganancias de todos los que intervienen en el proceso.

1.5.4 La clonación de tarjetas en cajeros automáticos

En el caso de los cajeros automáticos, la mecánica delictiva varía de la anterior. Debido a la necesidad de la obtención del número confidencial, no es tan simple como el primer proceso sino que se desarrolla a través de la colocación de dispositivos de lectura en los mismos equipos de retiro de dinero, lo cual puede consistir en la colocación de un skimmer a un lado de los lectores reales.

De esta manera se obtienen los datos de la banda magnética y para la obtención del número de identificación personal se colocan cámaras ocultas que graban en video la digitación que realiza el tarjeta-habiente o en su caso se colocan equipos de computación en lugar de las pantallas de los cajeros para que al digitar los números estos queden grabados en el equipo que colocó el sujeto activo y de esa manera completar la información necesaria.

Una vez obtenida la información, se hace llegar la misma al sujeto que la grabará a una tarjeta en blanco, pero en este caso no se requiere la impresión de logotipos ya que nadie llegara a ver la misma y el cajero automático no puede leer los datos impresos, sino solo los que se encuentran en la banda magnética o bien en el chip en algunos casos. La entrega de esta información puede variar, según la tecnología que se aplique al proceso, en algunos casos existen mecanismos de transmisión

automática por los cuales el clonador puede recibir esta información por vía inalámbrica o frecuencias de radio. Una vez colocados los datos y obtenido el número de identificación personal, un tercer sujeto se apersona en los cajeros y con la tarjeta clonada hace retiros de efectivo haciéndose pasar por el titular ante los sistemas automatizados de entrega de dinero.

Existen en los dos casos al menos tres sujetos (aunque en casos muy aislados pueden ser dos o incluso uno, no obstante por cuestiones de tiempo físico esto es muy improbable), uno que obtiene la información, uno que duplica la misma y produce o reproduce las tarjetas de originales y el tercero que posee las mismas y con ellas realiza las compras o retiros de efectivo según el caso.

2.7 Problemática actual en el uso de tarjetas de crédito en el Ecuador: Pérdidas por clonación

En Ecuador la clonación de tarjetas de crédito desde cajeros automáticos ha causado enormes pérdidas de dinero tanto a sus propietarios como a las entidades bancarias. Según datos de la Fiscalía el total de robos electrónicos podría llegar al millón de dólares en el primer semestre del 2011, manifestando que en el 2009 se reportaron 168 casos de este tipo de fraudes, en el 2010 los casos ascendieron a 1099 y en el primer semestre (enero a junio) se reportaron 1360 denuncias, lo que nos demuestra que esta modalidad de fraudes va en aumento (Noticias en Línea, 2011).

Las pérdidas reales son mucho mayores. Se manejan estadísticas que el estándar de pérdidas es el 0.4% del total de las compras con tarjetas, por lo que sin ningún problema el año pasado los bancos en su conjunto perdieron cerca de $20 millones.

2.8 Medidas de Seguridad en Canales Electrónicos para prevenir clonación de tarjetas

Como consecuencia de diversos reclamos y denuncias de consumidores de servicios financieros y con el fin de proteger los intereses del público y 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 como la clonación de tarjetas de débito o de crédito, la Junta Bancaria recientemente promulgó la Resolución No. JB-2012-2148 de fecha 26 de abril del 2012, en la que dispuso que las Instituciones financieras y emisoras de tarjetas de crédito implementen suficientes medidas de seguridad para mitigar el riesgo de fraude mediante el uso de información y comunicaciones (Superintendencia de Bancos y Seguros, 2012).

La resolución reforma varios artículos contenidos en las “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.

En esta normativa se dispuso que las instituciones financieras deberán implementar 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.

De acuerdo a la resolución tendrán que disponer de un programa o sistema de protección contra intrusos (Antimalware) que proteja el software instalado en el cajero automático y que detecte oportunamente cualquier alteración en su código, configuración o funcionalidad.

Asimismo, dispone que deberán instalar mecanismos 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, además de un mantenimiento preventivo y correctivo de los cajeros automáticos cuyas claves de acceso tipo “administrador” deben ser únicas y reemplazadas periódicamente.

Adicionalmente, deben disponer de cerraduras de alta tecnología y seguridades que garanticen el acceso controlado al interior de los mismos.

Dentro de la misma resolución No.JB-2012-2148 la Junta Bancaria reformó el capítulo V “De La Gestión de riesgo operativo”, en el que se incluyó cambios que garanticen la efectividad, eficiencia y confiabilidad de la información a través de canales electrónicos.

La norma dispone que para el uso y manejo de canales electrónicos y consumos de tarjetas, las entidades financieras deberán adoptar e implementar los estándares y buenas prácticas de seguridad vigentes a nivel mundial.

Estableciendo procedimientos de monitoreo para controlar la efectividad de los niveles de seguridad implementados en hardware, software, redes y comunicaciones, así como cualquier otro elemento utilizado.

En cuanto a la emisión de tarjetas, la normativa dispone a las instituciones del sistema financiero emitir tarjetas inteligentes, es decir que deben contar con microprocesador o chip; debiendo adoptar estándares internacionales de seguridad y las mejores prácticas vigentes sobre su uso y manejo.

La Junta Bancaria señala que el envío de información vía internet a los clientes y la relacionada con tarjetas, debe estar sometida a técnicas de encriptación evaluando la efectividad y vigencia del mecanismo de encriptación utilizado.

Las instituciones controladas ofrecerán 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 establece cada entidad.

De igual manera, deben incorporar en los procedimientos administrativos de seguridad de la información la renovación de por lo menos una vez al año de las claves de acceso a cajeros automáticos, la misma que debe ser diferente de aquella por la cual se accede a otros canales electrónicos.

Los plazos para la implementación de esta norma serán de 9, 18 y 36 meses conforme a la primera disposición transitoria de la resolución, debiendo sujetarse al cronograma de implementación que a continuación se detalla:

Tabla 4. Cronograma de implementación tarjetas inteligentes

FASES PARA LA MIGRACIÓN DE TARJETAS DE BANDA MAGNÉTICA A TARJETAS INTELIGENTES		
FASE	**DESCRIPCIÓN**	**TIEMPO (MESES)**
0	Diagnostico inicial de la entidad para implementar Tarjetas con Chip	6
1	Implementar adecuaciones para operar con tarjetas inteligentes, en:	12
	Cajeros Automáticos	
	Adquirencias	
	Tarjetas de Crédito	
	Tarjetas de Débito	
2	Entrega de Tarjetas con Chip	18
		36

Fuente: Superintendencia de Bancos y Seguros

Elaboración: Autoras

2.9 Repercusiones sociales

Los ecuatorianos se sorprenden cada día más con la capacidad que tienen los delincuentes para sustraer su dinero en un abrir y cerrar de ojos sin necesidad de utilizar fuerza. Al tradicional atraco a mano armada, o bolsiqueo en el transporte público, los delincuentes ya le han sumado prácticas más sofisticadas: ahora tienen la posibilidad de robar sin que la víctima se dé cuenta y sin ejercer violencia.

Figura 2. Estadísticas de las victimas que han sufrido fraudes

Fuente: Norton

A diario se escuchan denuncias, como la de un usuario a quien le aparecieron dos consumos con su tarjeta de crédito, uno en un

hipermercado al que nunca ha ido y otro en un almacén de zapatos que no conoce. El problema le costó dos mil dólares. Aunque el seguro de su tarjeta cubrió el desfalco, el cliente no tiene ni idea de cómo los ladrones lograron hacer esas compras, pues manifiesta nunca haber perdido de vista su tarjeta.

Hace un par de semanas, varios usuarios de diferentes bancos reportaron haber sufrido la clonación de sus tarjetas: una de las afectadas perdió 4 mil dólares en pocos minutos. Lo mismo sucedió a varios clientes del Banco de Guayaquil, quienes también sufrieron clonaciones de sus plásticos.

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

Esto no quiere decir que no haya un problema, pues Colombia tiene registros más altos que Brasil y México, que son países más grandes y con problemáticas delincuenciales similares. Solo en lo que va del año, la Dirección de Investigación Criminal o Interpol de Colombia (Dijín) ha detectado cinco operaciones por clonación de tarjetas débito y crédito y ha capturado a 28 personas. De otra parte, por delitos asociados a hurto electrónico, transferencias no consentidas de activos, violación de datos o

uso de software malicioso, han sido capturadas 87 personas en los últimos dos años.

Muchas de estas bandas son internacionales y la razón de que lo sean es que la logística de estas bandas es tecnológica: los delincuentes no solo importan fácilmente nuevas prácticas de defraudación sino que pueden traficar bases de datos sobre eventuales víctimas.

La naturaleza del delito también ha cambiado. Estas bandas no están concentradas solo en robar dinero, que resulta ser la etapa más fácil del delito. De hecho, lo primero que roban este tipo de bandas es información valiosa sobre los clientes bancarios. Y para ello utilizan técnicas muy diversas, mucho más complejas que la simple clonación. Hacen llamadas por celular, envían correos electrónicos con virus, logran acceso a redes sociales como Facebook y Twitter, entre otras. Por esta vía, acceden a datos muy importantes como direcciones de email, nombres de bancos donde tiene la cuenta la víctima, números celulares y hasta analizan las rutinas de las personas. A esto se le ha denominado 'ingeniería social', que es reconstruir el perfil de alguien para saber por donde se puede sacar información clave para hacer el robo.

Adicionalmente este tipo de delincuentes hacen inteligencia, adquieren mejores tecnologías, conocen del tema. Antes, la clonación de tarjetas se daba de una manera rústica y hasta burda, con aparatos y cámaras de video instaladas superficialmente en los mismos cajeros. Pero ahora los dispositivos de clonación se han vuelto más pequeños y hasta utilizan

tecnología celular, así no tienen que ir a retirar sus dispositivos para poder disponer de la información, sino que la puede recibir como mensaje de texto en su propio celular y empezar a cometer sus fraudes y hurtos.

La pregunta que muchas personas se hacen es a quién se responsabiliza. Lo problemático es que este tipo de delitos termina enfrentando a las dos víctimas del hecho: los usuarios y los bancos.

Figura 3. Informe de Norton sobre los Ciberdelitos

Fuente: Norton

Cualquier estrategia que se aplique debe implicar que autoridades, usuarios y bancos trabajen en conjunto. Por un lado, los usuarios tienen que estar más atentos para impedir que los delincuentes obtengan sus datos.

Por otro lado las instituciones financieras deben seguir fortaleciendo sus sistemas para reducir así el margen de maniobra a los ladrones.

Actualmente el fraude virtual se está convirtiendo en un problema reiterado para muchos usuarios y bancos, quienes sin darse cuenta están perdiendo parte de su patrimonio en cuestión de minutos.

Este problema afecta a los usuarios no solamente en forma económica, sino también en forma laboral y emocional, ya que en muchos casos el dinero destinado por ellos (que podría ser cualquiera de nosotros o algún familiar) para cubrir sus necesidades básicas, gastos médicos y/o cumplir con sus obligaciones desaparece de sus cuentas en cuestión de minutos, a esto se suma que en ocasiones los delincuentes efectúan consumos sin su autorización, ocasionando contrariedad, estrés, angustia y hasta problemas laborales y crediticios.

CAPÍTULO III: TARJETAS CON BANDA MAGNÉTICA Y TARJETAS CON CHIP

En el plano de las ventajas y las desventajas de las tarjetas con chip y las magnéticas se introducen algunas variables. Estas van desde el concepto hasta a la operación que define su uso.

Según lo que ofrecen las tarjetas con chip la tecnología y la seguridad de su uso podría ser superior a las tarjetas con banda magnética.

Cabe entonces desarrollar una explicación sobre los distintos factores que intervienen en este proceso.

3.1 Tarjetas con banda magnética

Tarjeta magnética o electrónica es aquella que cuenta con una banda magnética que puede ser leída por un dispositivo electrónico. En dicha banda, aparece la información del usuario. Las tarjetas de crédito y débito se enmarcan dentro de este tipo de tarjetas, al igual que aquellas que, al ser pasadas por cierto lector, posibilitan el acceso a determinados lugares.

Las tarjetas de crédito o las tarjetas de débito con banda magnética, permiten el acceso a los cajeros automáticos, donde es posible obtener dinero en efectivo y completar distintas operaciones, adicionalmente realizar compras sin efectivo, en el caso de las tarjetas de débito el dinero para pagar la adquisición se descuenta inmediatamente de la cuenta bancaria del usuario.

Forrest Perry, ingeniero de IBM, inventó en 1960 la tarjeta de banda magnética bajo el auspicio del gobierno de los Estados Unidos. Esta tarjeta tenía como mecanismo de seguridad una “firma” embebida (MagnaPrint, MagnePrint o BluPrint) en la tarjeta que le permitía al dispositivo lector validar la identidad de la tarjeta junto con otro factor de autenticación para validar al usuario el cual es desde luego una clave personal.

Las primeras tarjetas con banda magnética fueron usadas desde principios de los sesenta en el transporte público, London Transit Authority instaló un sistema de tarjeta con banda magnética en el sistema de tren London Underground, en Londres.

A nivel de entidades financieras se empezaron a usar en 1951, a finales de los sesentas implementaron la tarjeta plástica con banda magnética.

En 1970 cuando se establecieron los estándares internacionales (ISO 7811) el uso de la banda magnética se masificó y se extendió su uso a nivel mundial.

En 1971 The American Banking Association en Estados Unidos aprobó el uso de la banda magnética a nivel bancario.

El 16 de Enero de 1973 Robert E. Lawhend y William E. Steele patentaron una impresora para tarjetas con banda magnética, que fue asignada a Internacional Business Machines Corp. (IBM) con la patente No. 3711359 en Estados Unidos.

3.2 Problemas o debilidades que presentan las tarjetas con bandas magnéticas

La tecnología que está más extendida en la actualidad es la basada en banda magnética, prácticamente todo el mundo dispone de alguna tarjeta, normalmente de uso financiero, que por su parte posterior incorpora una banda de color marrón oscuro.

Esta banda magnética es similar a un pedazo de cinta magnética de una cassette musical. Su misión es almacenar cierta información, como el nombre del titular, el número de su cuenta, el tipo de tarjeta y el PIN.

Básicamente se puede decir que identifica al usuario con la máquina con la que se pone en contacto (ATM, TPV.), y está máquina o dispositivo, sola en ciertas operaciones, o conectándose on-line con otros dispositivos en otras, gestiona una serie de operaciones y guarda cierta información de cada transacción.

Hasta el punto mencionado la tecnología chip aporta prácticamente lo mismo que la banda magnética. Sin embargo hay al menos tres campos en los que la potencialidad implícita en el chip da a esta última tecnología una clara ventaja de cara al futuro, por lo que podemos pronosticar, sin mucho miedo a errar, que el chip sustituirá muy próximamente a la banda magnética:

1. **Coste transacciones:** La tarjeta de banda magnética es un elemento fundamentalmente de carácter pasivo en las transacciones, a partir

del momento de la identificación, la banda magnética precisa de ponerse en contacto con un host o una red de hosts para realizar la operatoria, de modo que son estos los que realmente operan.

Esto implica la necesidad de conexiones on-line, bien sea en el mismo momento de la operación, o, en algunas ocasiones perfectamente predeterminadas, posteriormente. Este último tipo de operaciones, las operaciones denominadas off-line, son claramente la excepción. Ello acarrea un coste muy importante de comunicaciones.

2. **Seguridad:** El contenido de la banda magnética, por la tecnología que implica, puede ser leído y, aunque no es sencillo, puede ser manipulado por personas con conocimiento y medios adecuados.
3. **Capacidad de almacenamiento de información:** la cantidad de información incorporable a una banda magnética es pequeña y, fundamentalmente, estática, por lo que la relación entre el usuario de la tarjeta y el emisor es muy unidimensional, únicamente se actualiza cuando se interactúa a través de hardware sofisticado (ATMs).

Los principales motivos que causan desperfecto en la banda magnética, ordenados de mayor a menor impacto, son los siguientes:

4. **Causados por campos magnéticos:** Éstos pueden ser producidos por teléfonos móviles; cierres de imán de bolsos, monederos, agendas, cartera, etc.; aparatos electrónicos como altavoces, microondas, televisores, aparatos de video, etc., y finalmente imanes y electroimanes.

La distancia a que se encuentra la banda magnética de la tarjeta del campo magnético es determinante a la hora de que se produzca daño en la misma, cuanto más cerca estén, mayor será el daño. Dependiendo del deterioro producido puede inutilizar totalmente la tarjeta, incluso hasta el punto de que no se pueda introducir en el lector de tarjetas del cajero automático, o sólo afectarle su uso en cajeros o en tpv's (datafonos).

5. **Causados por electricidad estática:** La tarjeta es un material plástico que en determinadas condiciones, por ejemplo frotación con lana, puede almacenar electricidad estática. Esta electricidad estática se descarga de forma violenta, en forma de chispa eléctrica por lo general inapreciable, cuando el plástico es puesto en contacto con un material conductor conectado a una toma de tierra. Ocasionalmente esta chispa puede producirse directamente en la banda magnética provocando el borrado de una zona de la misma.

6. **Causados por el lógico deterioro debido al uso**: Cualquier objeto se va deteriorando con su uso y las bandas magnéticas no están exentas de este deterioro. Este deterioro está directamente relacionado con la intensidad de uso: a medida que más se usa una tarjeta más probable es que se deteriore. En el caso de las tarjetas, y debido al enorme número de operaciones que realizan, se ven afectadas por el deterioro debido al uso continuado.

3.3 Tarjetas con Chip

El término Tarjeta con Chip ha sido utilizado para referirnos a dispositivos del tamaño de una tarjeta de crédito, que tienen integrado un microchip para almacenar información del usuario y realizar transacciones una vez que es insertada en un lector especial.

Lo que hace inteligente a estas tarjetas es el chip que tiene empotrado. Este chip puede contener memoria para almacenamiento de datos con cierto nivel de seguridad o puede contener además un microprocesador controlado por un sistema operativo con la capacidad de procesar datos y ejecutar programas de manera local en la tarjeta. En este contexto la palabra “inteligente” se relaciona a la capacidad que tiene la tarjeta para procesar datos.

Además de almacenar casi 200 veces más información que las tarjetas convencionales, es decir, aquéllas que cuentan con banda magnética, las tarjetas inteligentes poseen inteligencia electrónica, tal como lo hace un ordenador y son capaces de realizar transacciones en la misma tarjeta.

A la tarjeta se le incorpora un microcircuito que posee un microprocesador y una memoria (variable) en la que se pueden almacenar aplicaciones y datos, lo cual la hace comparable a una pequeña computadora.

Entre algunas definiciones de tarjeta inteligente podemos mencionar las siguientes:

Una tarjeta con Chip es un tipo de tarjeta de plástico con una computadora de circuito integrado (Chip) empotrado que almacena y realiza transacciones de datos entre usuarios.

Sistema portador de información electrónico que usa tarjetas de plástico del tamaño de una tarjeta de crédito con un circuito integrado incrustado que guarda información de los procesos.

Según MasterCard, esta nueva tecnología es aplicada en las soluciones de pago de esa empresa en varios países de América Latina (incluyendo Brasil, México, Colombia, Chile y Ecuador), y ya ha llegado a 393 millones de plásticos en todo el mundo.

3.4 Beneficios que ofrece la tarjeta con Chip

Tabla 5. Diferencia entre tipos de tarjetas

DIFERENCIAS ENTRE LAS TARJETAS	
TARJETAS CON CHIP	**TARJETAS BANDA MAGNÉTICA**
Guardan información del cliente en el chip	Guardan una identificación del cliente para conectarse a una base de datos
Dificultad de falsificar el chip en poco tiempo	Fácil de falsificar la información de la banda
El chip tiene mayor durabilidad	La Banda Magnética soporta poca resistencia al uso frecuente

Fuente: Superintendencia de Bancos y Seguros

Elaboración: Autoras

Las ventajas más importantes que ofrece la tarjeta con Chip en relación a la tarjeta de Banda Magnética son:

- Cantidad de información que se puede grabar en el chip
- Dificultad para falsificar el chip
- Durabilidad en uso frecuente del chip

Otro punto importante de la tarjeta inteligente con chip, es el tiempo de la transacción ya que el chip guarda la información del cliente y cuando se desea hacer un pago la información del cliente está disponible, contrario a la tarjeta de banda magnética que solo guarda una identificación del cliente para acceder a una base de datos que necesita conexión en línea. En este tiempo, se depende de la velocidad de la conexión para que verifique los datos del cliente.

Gracias a su gran capacidad de memoria y habilidad para procesar información, la tarjeta inteligente ofrece varios usos comparada con la Tarjeta con Banda Magnética. Por ejemplo:

Se pueden pagar parquímetros y tarifas de transporte público sin tener que cargar billetes o monedas.

Permiten que el titular combine varias tarjetas en una sola. Es decir, algunas pueden servir como tarjeta de crédito, tarjeta de débito, tarjeta de tienda e incluso tarjeta de seguro.

- Ofrecen mejores programas de lealtad para los consumidores.
- Permiten su uso como monedero electrónico, entre otras.

Sin embargo no todos los servicios pueden llegar a implementarse en los distintos países.

Mayor seguridad: Las tarjetas inteligentes ofrecen el más alto grado de protección contra fraude o falsificación, toda vez que por cada transacción que usted realice con ella, se realiza una verificación de uso y validez de la misma. La tecnología Chip es altamente sofisticada, lo cual hace que la falsificación de una tarjeta sea costosa y difícil. Para prevenir la introducción de información no garantizada en los chips de las tarjetas inteligentes, normalmente se dividen en secciones, haciéndolas más privadas y seguras.

Conveniencia: Las tarjetas inteligentes pueden almacenar información acerca de sus más recientes transacciones, incluyendo la fecha, el nombre del comercio y la cantidad total de la transacción. También pueden tomar el valor real electrónico transferido de su cuenta bancaria y almacenarlo en una aplicación dentro del microchip; de este modo, usted podrá pagar los productos y servicios que desee, sin necesidad de cargar efectivo.

3.5 Funcionamiento de las Tarjetas con Chip

Las Tarjetas con chip se caracterizan por tener insertado en el plástico un microcircuito fuertemente protegido por sistemas de encriptación lo cual garantiza un mayor nivel de seguridad para los usuarios.

Las Tarjetas con chip se insertan en un terminal y permanecen allí durante toda la transacción, el chip tiene almacenadas las reglas del emisor

y la forma en que debe comportarse al momento de autorizador una transacción.

EMV es acrónimo de Europa y Mastercard Visa, las tres compañías que inicialmente colaboraron en el desarrollo del estándar de este sistema operativo.

Esta tecnología brinda para su tarjeta:

- Un mayor nivel de seguridad ya que implica una reducción del fraude.
- Una protección extra en el uso de su tarjeta.
- La posibilidad de controlar de forma más detallada la aprobación de transacciones con su tarjeta sin conexión (offline).
- La inversión de responsabilidades en su uso en comercios, ya que los comerciantes son responsables de todo fraude resultante de una transacción realizada sin EMV en sus sistemas.
- Cada tarjeta lleva incorporados los siguientes elementos:

Con Chip

Cada tarjeta lleva un microchip fuertemente protegido por encriptación, lo cual hace que resulte difícil defraudar con este tipo de tarjeta.

Con PIN

Personal Identity Number: un número de cuatro dígitos que sólo conoce el usuario de la tarjeta. Se introduce en el momento del pago con la tarjeta en un comercio o en extracciones de efectivo en los cajeros.

3.6 Funcionamiento en comercios y cajeros

Cuando se ha realizado una compra en un comercio, pueden ocurrir dos cosas:

- Que el comercio disponga de un terminal apto para tarjetas con Chip
- Que el comercio disponga de un terminal que solo lea tarjetas con banda magnética

Si el comercio dispone de un terminal apto para Tarjetas con Chip, una vez introducida la tarjeta le solicitarán que teclee su número PIN (puede darse el caso de que algunas tarjetas no exijan el poner el pin, si lo tuviere es importante cuidar siempre que nadie lo observe, ni pueda copiar su número) y a continuación finalizará la operación y se emitirá recibo de compra que no es necesario firmar.

En caso de que por cualquier circunstancia no funcionase correctamente el terminal, su tarjeta también puede funcionar con el sistema de banda magnética en cuyo caso sí será necesario firmar el comprobante de la operación.

En caso de que el PIN tecleado sea incorrecto, el terminal lo solicitará de nuevo hasta 3 veces y si no se introduce el correcto no se autorizará la operación y se desactivará automáticamente la tarjeta.

Durante todo el tiempo que dure la operación de pago la tarjeta permanecerá insertada en el terminal TPV.

Si el comercio no dispone de un terminal apto para tarjetas con Chip, su tarjeta se encuentra igualmente preparada para funcionar con el sistema de banda magnética. En este caso se le solicitará la firma en el comprobante de la operación.

Cuando se realiza cualquier consulta o extracción de efectivo en un cajero automático, el funcionamiento es similar tanto si la tarjeta funciona con el sistema de Chip como con banda magnética, ya que siempre será solicitado teclear el número PIN para validar la operación.

3.7 Evolución y expansión de las Tarjetas con Chip

A escala global, aproximadamente una de cada cinco tarjetas de la marca MasterCard llevan ahora un chip y aproximadamente la cuarta parte de todos los dispositivos de POS (terminales de puntos de venta) han sido actualizados para aceptar estas tarjetas.

Sin embargo, su implementación no significa la abolición de la tarjeta de banda magnética. Éstas continuarán siendo aceptadas en todos los comercios afiliados MasterCard. Su uso es el más difundido en el mundo y por esa razón permanecerá en las tarjetas con el objetivo de que éstas continúen siendo aceptadas en los comercios.

En la expansión de la tecnología, la región de América Latina ha experimentado un aumento significativo en los últimos dos años: el número de tarjetas con chip se ha más que duplicado y, en mercados como Brasil,

se ha logrado la aceptación en la gran mayoría de los terminales de puntos de venta.

Según un estudio publicado con el título "El mercado mundial de tarjetas bancarias, edición 2011" por IMS Research en el 2011 (proveedor de investigaciones de mercados para la industria electrónica) se expresa que en Brasil las tarjetas inteligentes podrían llegar a 450 millones de unidades al finalizar el 2016. Este es un número muy interesante y demuestra la tendencia de la migración a este tipo de tarjetas en el país más grande de América del sur.

Este crecimiento considerable puede ser atribuido al número de bancos en Brasil y en países como México, Chile, Ecuador y Colombia en poco tiempo comenzará la tendencia hacia la emisión de tarjetas con chip. Los bancos en Venezuela, Costa Rica, Panamá y el Caribe ya se encuentran en varias fases de ejecución para la migración a esta nueva tecnología.

En Ecuador el volumen de tarjetas inteligentes emitidas es mínimo, de hecho hasta enero del 2011 Pacificard era el único emisor de tarjetas de crédito ecuatoriano certificado para ofrecer tarjetas con chip tanto Mastercard como Visa, por lo que actualmente se encuentran trabajando en el tema de migración del portafolio, buscando certificaciones y organizando sus proyectos de migración, de tal forma que se ajusten a los plazos establecidos en la resolución No.JB-2012-2148 del 26 de abril del 2012, emitida por la Junta Bancaria, para su implementación.

Estos casos marcan un hito en el cuestionamiento de uso de las tarjetas con banda magnética, existiendo posibilidades de mejora.

Dentro de una población determinada se evaluaron los aspectos que ponen en riesgo el uso de tarjetas con banda magnética.

CAPÍTULO IV: METODOLOGIA DE LA INVESTIGACION

Mediante este estudio se pretende demostrar la percepción del servicio de tarjetas de crédito y de débito en el país y su nivel de confianza respecto a estos para posteriormente describir y proponer la implementación de un proceso de migración a tarjetas con chip en la que el sistema de seguridad tenga menores posibilidades de vulnerabilidad, así como la facilitación de uso.

Los casos de falsificación (clonación) de tarjetas son frecuentes en ciudades urbanas como Guayaquil y la frecuencia con que ocurren y se denuncian estos casos marcan un hito en el cuestionamiento de uso de las tarjetas con banda magnética, existiendo posibilidades de mejora.

Dentro de una población determinada se evaluaron los aspectos que ponen en riesgo el uso de tarjetas con banda magnética.

Posteriormente se llega a distintas conclusiones vinculadas al proceso de cambio de tecnología.

4.1 Enfoque

Los resultados del trabajo de investigación tendrán un enfoque mixto, ya que responden a una metodología fundamentada en las técnicas cualitativa y cuantitativa, a fin de identificar las posibles causas y debilidades que originan fraudes de falsificación (clonación) en las tarjetas de crédito y

débito, así como describir en qué consiste el proceso de migración de banda magnética a tarjetas con chip.

Adicionalmente se busca poder determinar mediante la identificación de los procesos y el contexto de las tarjetas de crédito y/o débito con chip sus costos aproximados y beneficios de aplicación en el Ecuador.

A partir del contexto se pretende analizar si la forma de migración propuesta es la adecuada para el mercado ecuatoriano.

4.2. Tipo de Investigación

El tipo de investigación utilizado en el presente estudio se basó en la investigación exploratoria y descriptiva.

La investigación exploratoria según Sellriz (1980) es aquella que se efectúa sobre un tema u objeto desconocido o poco estudiado, por lo que sus resultados constituyen una visión aproximada de dicho objeto, es decir, un nivel superficial de conocimiento.

Según el Manual de técnica de la investigación educacional de Deobold B. Van Dalen y William J. Meyer, la investigación descriptiva consiste en llegar a conocer las situaciones, costumbres y actitudes predominantes a través de la descripción exacta de las actividades, objetos, procesos y personas, esta investigación no solo recoge los datos sobre la base de una teoría sino que exponen y resumen la información de manera cuidadosa y luego analizan minuciosamente los resultados, a fin de extraer generalizaciones significativas que contribuyan al conocimiento.

En la exploración de los tarjetahabientes ecuatorianos se encontró algunas de los temores que presentan en el uso de esta tecnología, como consecuencia del número de casos de robos y fraudes por falsificación de tarjetas de crédito y débito que se registran en el país y que son de conocimiento público entre los usuarios.

4.3 Herramientas de la Investigación

Las herramientas que se utilizaron para obtener información en el presente proyecto de investigación fueron encuestas y entrevistas.

Se entrevistó a expertos en el mercado financiero para mostrar desde su percepción los beneficios de la migración de tarjetas con banda magnética a tarjetas con chip.

De la misma manera se encuestaron a usuarios de tarjetas de crédito para analizar su percepción y conocimiento del uso y los beneficios de las mismas al momento de efectuar sus transacciones, así como consultar si habían sido víctima de algún tipo de fraude por falsificación.

4.4 Segmentación del Mercado

Para el desarrollo del presente estudio se ha utilizado como metodología el muestreo estadístico. Por razones de ubicación y costos se determinó como zona de cobertura geográfica a la ciudad de Guayaquil, como marco de muestra se ha tomado personas hombres y mujeres de

diferentes sectores de la ciudad mayores de 18 años de edad que sean usuarios de tarjetas de crédito.

Según datos del censo de población y vivienda del 2012 la población del cantón Guayaquil está bordeando los 2’35 millones de personas (Instituto Nacional de Estadísticas y Censos [Inec], 2010), correspondiendo un 25% del total tarjetahabientes bancarios (1´9 millones) a la ciudad de Guayaquil lo que representa 475,000 personas aproximadamente (Superintendencia de Bancos y Seguros, 2013)

4.5 Determinación de la población y muestra

Según datos publicados por el Instituto Nacional de Estadísticas y Censos, INEC (2010), la población del cantón Guayaquil es de 2,350,915 habitantes.

Según información estadística publicada por la Superintendencia de Bancos y Seguros (SBS), al mes de junio de 2013 se registra un número estimado de 1,9 millones de tarjetahabientes (entre tarjetahabientes principales y con tarjeta adicional), lo que representa un total de 3 millones de tarjeta de crédito (3.151.877), de las cuales el 85% (es decir 2´672.880) son tarjetas principales y la diferencia (479.007) corresponde a tarjetas adicionales.

Del total del tarjetahabientes aproximadamente el 25% corresponden a la ciudad de Guayaquil, es decir 475,000 personas en la ciudad tienen al menos una tarjeta de crédito.

Por lo expuesto en virtud de que el tamaño de la muestra supera las 100,000 personas, lo que sería demasiado extenso, la población de estudio se determinará a través de la fórmula de población infinita.

Para el efecto se aplicará la siguiente fórmula para determinar la muestra aleatoria.

Tabla 6. Determinación de la muestra

Confianza	99,0%	97,0%	95,0%	90,0%
Valor de Z	**2,58**	**2,17**	**1,96**	**1,64**
1,0%	16.641	11.772	9.604	6.724
1,5%	7.396	5.232	4.268	2.988
2,0%	4.160	2.943	2.401	1.681
2,5%	2.663	1.884	1.537	1.076
3,0%	1.849	1.308	1.067	747
3,5%	1.358	961	784	549
4,0%	1.040	736	600	420
4,5%	822	581	474	332
5,0%	666	471	384	**269**

Fórmula Empleada	$n=\frac{z^2 p^*(1-p)}{e^2}$

Para este caso se tiene que:

Se espera que p=50% corresponde a la proporción de habitantes de Guayaquil que tiene una tarjeta de crédito y q (1-p) es la proporción que no tiene tarjetas de crédito.

Con un nivel del confianza del 90% se obtiene un valor de variable Z de +-1,64 que representa el valor dentro de la distribución normal y un valor esperado E = 5% que constituye el margen de error.

Esto da un tamaño de la muestra de 269 personas que deben ser encuestadas.

Por otro lado, según información publicada por la Superintendencia de Bancos y Seguros en el país existen 20 entidades financieras Operadoras y Administradoras de tarjetas de crédito que se encuentran bajo control de la Superintendencia de Bancos y Seguros, para efectos de realizar las entrevistas no se utilizó muestra sino que se seleccionó a 3 especialistas en temas de control de fraudes bancarios en representación de las instituciones financieras y un representante de las empresas procesadoras de tarjetas de débito y crédito en el país.

4.6 Levantamiento de información

A efectos de obtener la información que sirvió de base para alcanzar los resultados del presente estudio, se efectuaron entrevistas a especialistas en temas de control de fraudes bancarios y encuestas a tarjetahabientes de la banca.

4.6.1 Entrevistas

Se entrevistaron a tres especialistas de instituciones financieras que laboran en temas de control de fraudes bancarios y un especialista de empresas procesadoras de tarjetas de débito y crédito, las mismas que a continuación se incluyen.

Como limitación al presente trabajo de investigación se puede mencionar, la dificultad de conseguir las entrevistas con expertos de la banca, como consecuencia de que las Instituciones Financieras son muy celosas con los datos que proporcionan, manteniendo en reserva cierta información por política interna o por temor a incurrir en daños de su reputación, razón por la cual no pudo presentarse el número de entrevistas sugerido por uno de los revisores.

4.6.1.1 Entrevista 1

ENTREVISTA: Ing. Jorge A. Armanza - Jefe de Control y Prevención de Fraudes Pacificard

FECHA: Viernes, 3 de mayo del 2013

1. **¿Actualmente, considera que la clonación de tarjetas afecta a un gran porcentaje de tarjetahabientes en el país?**

Sí, el costo hundido del negocio o rubro por falsificación de banda magnética podría decirse que del 100% del total de fraudes presentados es el 90% aproximadamente.

El rango normal o razonable en montos por este rubro se encuentra entre el 0.3% y 0.7% del total de facturación anual, el monto no debería exceder el 1%, si pasa de ese porcentaje ya es considerado alarmante.

La métrica para medir los fraudes es:

$$\frac{\text{Fraudes}}{\text{Facturación}} = \%\ \text{nivel de fraudes sobre facturación}$$

Sin embargo, podría considerarse que el fraude por falsificación de banda magnética se encuentra controlado en nuestro país en comparación con Latinoamérica.

2. **¿Si no existiera la resolución que obliga a las entidades bancarias a cambiar el tipo de tarjetas que se emiten actualmente por otras con chip, cuál sería el riesgo a mediano plazo?**

Si no existiera la resolución, Mastercard y Visa Internacional te obligan a cambiar el tipo de tarjetas de todas formas, de hecho tenían un cronograma de migración progresivo que iba hasta el 2015 aproximadamente.

El riesgo a mediano plazo sería que el fraude de banda magnética migre es decir que el fraude existente en otros países migre hacia el nuestro y que la institución responda financieramente por esas estafas.

Adicionalmente, el riesgo comercial de que no te acepten las tarjetas en otros países.

3. **¿De acuerdo a su experiencia, cuáles son los problemas más importantes que podrían surgir en el proceso de implementación de estas nuevas tarjetas inteligentes?**

De orden tecnológico: Interoperabilidad, porque es una tecnología nueva que implica aprendizaje, por poner un ejemplo, antes al deslizar la tarjeta por el POS éste leía los datos de la banda rápidamente, con la nueva tecnología podría decirse que el chip conversa con el POS y se toma su tiempo para reconocer los datos que en él se encuentran.

En resumen uno de los problemas surgiría por el cambio de tecnología, la curva de aprendizaje está en la parte más baja.

Tema de fraude: Que la persona que conozca de fraudes se interese por otro tipo de fraudes, es decir que evolucione a temas de internet y fraudes internos.

4. **¿Cuáles podrían ser los proveedores de las máquinas o software necesarios para la implementación?**

Por parte del emisor nuestro proveedor autorizado es Gemalto. Los Pos también deben migrar. Los dueños de Datafast son: Banco Guayaquil, Pacificard y Banco del Pichincha.

Por el momento las tarjetas con banda magnética y chip trabajarán conjuntamente en este proceso, pero poco a poco se irá eliminando las tarjetas con banda magnética.

5. **Cuáles son los beneficios para el banco y para la sociedad, por la emisión de tarjetas inteligentes?**

    1. Confianza y seguridad de cara al cliente, que se sienta seguro siempre que haga una transacción.
    2. Para el Banco disminución de pérdidas y falsificación de banda magnética.

4.6.1.2 Entrevista 2

ENTREVISTA: Ing. Carlos Aguirre - Credimatic

FECHA: Miércoles, 24 de julio del 2013

1. ¿Actualmente, considera que la clonación de tarjetas afecta a un gran porcentaje de tarjetahabientes en el país?

Estuvimos involucrados en un tema de skimming el año pasado y pudimos constatar lo siguiente:

El porcentaje de afectación no lo conocemos con exactitud ya que antes de la resolución ley que obliga a los bancos a responder ante los casos de fraude no había un verdadero esfuerzo de parte de estos para evitarlo. Actualmente los bancos están luchando contra este fenómeno y según dicen el monto del fraude es bastante significativo.

2. ¿Si no existiera la resolución que obliga a las entidades bancarias a cambiar el tipo de tarjetas que se emiten actualmente por otras con chip, cuál sería el riesgo a mediano plazo?

Si no existieran las resoluciones sobre el tema de fraude y actualmente las que obligan a los emisores de tarjetas a mejorar la tecnología y seguridad, estaríamos en la situación en la cual el usuario del servicio termina pagando en primera instancia, pero a mediano plazo se restringiría el uso de medios de pago y afectaría la credibilidad del sistema.

3. ¿De acuerdo a su experiencia, cuáles son los problemas más importantes que podrían surgir en el proceso de implementación de estas nuevas tarjetas inteligentes?

Como en todo proceso de migración al principio se presentan muchas dificultades asociadas a temas técnicos, cambios de infraestructura, nuevos desarrollos, etc, pero lo que observamos es que aunque EMVco estandariza las tarjetas chip financieras cada marca está en la posibilidad de establecer sus propias condiciones, a esto hay que sumar que existen diferentes tipos de hardware (chip) para la implementación y se necesita adaptarse a lo que ofrece el fabricante.

Esto indica que tendremos que manejar un ecosistema muy variado de tecnologías conviviendo en el mismo ambiente.

4.¿Cuáles podrían ser los proveedores de las máquinas o software necesarios para la implementación?

Datacard provee el hardware o integra hardware de terceros. Por ejemplo la 280 tiene un grabador de chip marca Gemplus. También provee el software ya sea desarrollado por la empresa o producto de la adquisición de otras empresas que se dedican al desarrollo de este tipo de soluciones. Gemalto conocemos que provee mucho del hardware para chip y también tiene sus propios sistema para la administración de la personalización. Como proveedores de plásticos con chip tenemos: Gemalto, Oberthur, Morpho.

5. ¿Cuáles son los beneficios para el banco y para la sociedad, por la emisión de tarjetas inteligentes?

Para el banco, a futuro tendrá una disminución en la demanda de transacciones en línea cuando empiece a implementarse la tecnología DDA y transacciones offline. Para la sociedad la posibilidad de aumento en la seguridad de sus transacciones aumentará la confianza en el uso de medios de pago y que vendrá acompañado de nuevas aplicaciones que pueden integrarse en el futuro en un mismo chip.

4.6.1.3 Entrevista 3

ENTREVISTA: Especialista que prefiere mantener su nombre e institución en reserva

FECHA: Miércoles, 24 de julio del 2013

1. ¿Actualmente, considera que la clonación de tarjetas afecta a un gran porcentaje de tarjetahabientes en el país?

Afecta a la población pero no tendría un porcentaje sobre los clientes afectados con este tipo de problemas.

2. ¿Si no existiera la resolución que obliga a las entidades bancarias a cambiar el tipo de tarjetas que se emiten actualmente por otras con chip, cuál sería el riesgo a mediano plazo?

El riesgo a mediano plazo estaría primero en que no podríamos realizar transacciones en el exterior en los países de Europa ya que ellos manejan sus transacciones solo con POS que aceptan tarjetas con CHIP, otro de los inconvenientes que tendríamos es al mantener una tarjeta con banda el acceso a la información es más fácil para realizar clonaciones o fraudes.

3. ¿De acuerdo a su experiencia, cuáles son los problemas más importantes que podrían surgir en el proceso de implementación de estas nuevas tarjetas inteligentes?

- Costos por la inversión que tendrían que realizar las Instituciones Financieras (adquisición de plásticos, programas para configuración del Chip y equipos).
- Cambios en el manejo de la seguridad física de las instalaciones y los programas, así también dentro del manejo de la información.
- Tiempo de la migración de la información de los tarjetahabientes.
- Implementación y capacitación del personal.
- Inducción del cliente sobre el nuevo manejo de las tarjetas con chip, protección de datos y claves asignadas para transacciones.

4. ¿Cuáles podrían ser los proveedores de las máquinas o software necesarios para la implementación?

- Vidortec/Datacard (www.vidortec.com.ec)
- Gemalto (www.gemalto.com)
- Medianet
- Datafast

5. ¿Cuáles son los beneficios para el banco y para la sociedad, por la emisión de tarjetas inteligentes?

- Protección de la información (mayor seguridad en las transacciones)
- Reconocimiento de tarjetas a nivel mundial para poder realizar transacciones dentro y fuera del país.

4.6.1.4 Entrevista 4

ENTREVISTA: Especialista Banco Guayaquil que prefiere mantener su nombre en reserva

FECHA: Lunes, 27 de enero del 2014

1.¿Actualmente, considera que la clonación de tarjetas afecta a un gran porcentaje de tarjetahabientes en el país?

SI, efectivamente, existe algunas bandas de clonadores que están operando en el país, recientemente hubo una falla de seguridad en uno de los bancos del país, mismo que ocasionó que se vean comprometidas muchas tarjetas**.**

2 ¿Si no existiera la resolución que obliga a las entidades bancarias a cambiar el tipo de tarjetas que se emiten actualmente por otras con chip, cuál sería el riesgo a mediano plazo?

El riesgo ya está presente, y se comprometería en mayor proporción, debido a que las mafias de clonadores estarían operando sin ningún tipo de obstáculos

3. ¿De acuerdo a su experiencia, cuáles son los problemas más importantes que podrían surgir en el proceso de implementación de estas nuevas tarjetas inteligentes?

Los costos, el tiempo de implementación, obtener el personal idóneo, la priorización de este tipo de proyectos, sobre otros que mantenga el banco.

4.¿Cuáles podrían ser los proveedores de las máquinas o software necesarios para la implementación?

Los proveedores que tienen certificación de cumplimiento con las franquicias, tanto para la generación de tarjetas, como para la venta de software de personalización, entre otros.

5. ¿Cuáles son los beneficios para el banco y para la sociedad, por la emisión de tarjetas inteligentes?

La seguridad de que no clonen la tarjeta, no solo a nivel país, sino al resto del mundo; las personas ya no serían víctimas de la clonación, y el banco dejaría de perder dinero por devolver al cliente lo que se han robado.

4.6.1.5 Análisis de las entrevistas

De las entrevistas efectuadas a expertos de diferentes entidades bancarias, podemos indicar que coinciden en que la tecnología de chip reducirá la incidencia de fraudes al hacer más difícil la falsificación de tarjetas, ayudando a disminuir el uso indebido de una tarjeta robada o extraviada.

Manifiestan que esta nueva tecnología apunta a reducir el fraude por falsificación de tarjetas, así como ofrece una gama de oportunidades comerciales para los bancos y usuarios finales.

Adicionalmente, afirman que de no existir la resolución de Junta Bancaria que los obliga a cambiar su portafolio a tarjetas con chip el riesgo a mediano plazo sería que el fraude existente en otros países migre al Ecuador y que los Bancos respondan financieramente a sus clientes por esas estafas, lo que afectaría la credibilidad del sistema reduciendo el consumo de los clientes a través de este medio, adicionalmente existe el riesgo de que no acepten las tarjetas en otros países, ya que en algunos lugares en el exterior, manejan sus transacciones únicamente con POS que aceptan tarjetas con CHIP, lo que dificultaría a los usuarios efectuar sus transacciones con tarjetas con banda magnética en caso de que viajen fuera del país.

Dentro de los problemas más importantes que los expertos indican que podrían surgir se encuentran la interoperabilidad ya que es una tecnología

nueva que implica aprendizaje, que los fraudes evolucionen a temas de internet o fraudes internos, dificultades asociadas a temas técnicos, cambios de infraestructura, nuevos desarrollos, costos por la inversión que tendrían que realizar las Instituciones Financieras para adquisición de plásticos, programas para configuración del chip y equipos, tiempo de migración de la información de los tarjetahabientes, capacitación del personal, inducción del cliente sobre el nuevo manejo de las tarjetas con chip, entre otros.

Por último, coinciden todos los entrevistados en que la emisión de tarjetas con chip generará confianza y seguridad a los clientes, ya que ellos se sentirán más seguros al momento de efectuar sus transacciones y para las Instituciones Financieras significará disminución de pérdidas por falsificación de tarjetas de crédito.

Por lo expuesto y del análisis de las entrevistas efectuadas se puede concluir que la implementación de la tecnología chip es un proceso en boga, que a pesar de que su costo podría resultar relativamente alto para las entidades financieras y emisoras de tarjetas de crédito es una inversión a largo plazo, que brindará mayor seguridad al usuario al momento de efectuar sus transacciones, disminuyendo fraudes cuyo origen es la falsificación de las tarjeta, ya que lo más probable es que los estafadores migren sus actividades de falsificación de tarjetas de banda magnética a regiones que todavía no han implementado esta tecnología, por lo que es importante estar protegidos.

Por otro lado significará también un avance tecnológico de utilidad tantos para las entidades financieras como para el usuario, generando mayor confianza y estandarizando procesos vinculados a la banca a nivel mundial.

4.6.2 Encuestas

Se encuestaron a usuarios de tarjetas de crédito y/o débito para analizar su percepción y conocimiento del uso y los beneficios de las tarjetas con chip, así como para conocer si han sufrido algún tipo de fraude por clonación y se procedió a tabular los resultados, los mismos que a continuación se incluyen:

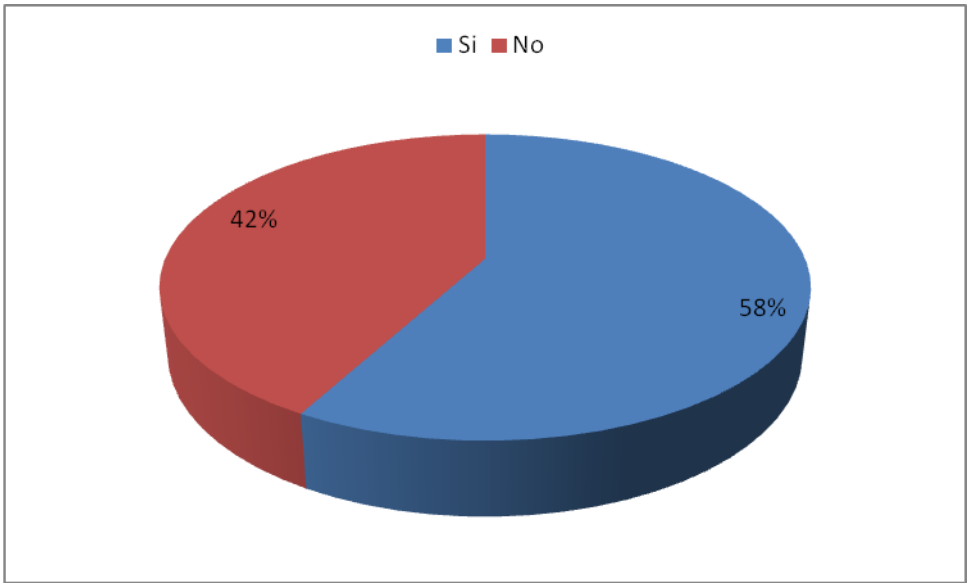
1. **¿Posee usted alguna de las siguientes tarjetas de crédito: Visa, Mastercard, Diners, American Express, otra?**

Tabla 1 Encuesta: Pregunta 1

TABLA DE FRECUENCIA		
DETALLE	**DATOS**	**PORCENTAJE**
Si	156	57,99%
No	113	42,01%
TOTAL	**269**	**100%**

Fuente: Investigación del mercado
Elaborado por: Las autoras

Gráfico 1 Encuesta: Pregunta 1



Fuente: Investigación del mercado
Elaborado por: Las autoras

Análisis e Interpretación

El 58% de los encuestados posee una de las tarjetas de crédito mencionadas, mientras que un 42% no posee ninguna.

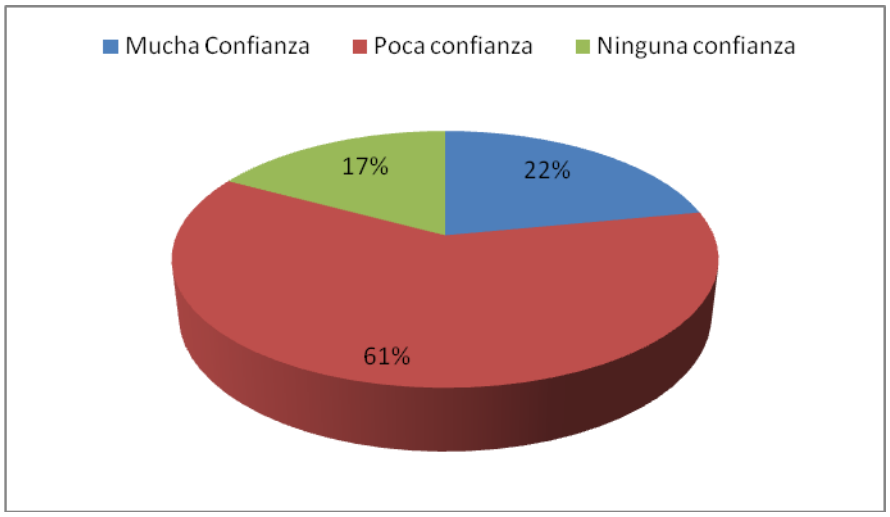
2. **¿Cuánta seguridad y/o confianza le inspira efectuar actualmente sus transacciones con tarjetas de crédito?**

Tabla 2 Encuesta: Pregunta 2

TABLA DE FRECUENCIA		
DETALLE	**DATOS**	**PORCENTAJE**
Mucha Confianza	59	21,93%
Poca confianza	164	60,97%
Ninguna confianza	46	17,10%
TOTAL	**269**	**100%**

Fuente: Investigación del mercado
Elaborado por: Las autoras

Gráfico 2 Encuesta: Pregunta 2



Fuente: Investigación del mercado
Elaborado por: Las autoras

Análisis e Interpretación

De los encuestados el 60,97% indicó que le inspira poca confianza efectuar sus transacciones con tarjetas de crédito, mientras el 21,93% manifestó que le inspira mucha confianza y el 17,10% indicó que no le inspira ninguna confianza.

3. **¿Ha sido usted víctima de algún tipo de fraude de tarjeta de crédito o débito?**

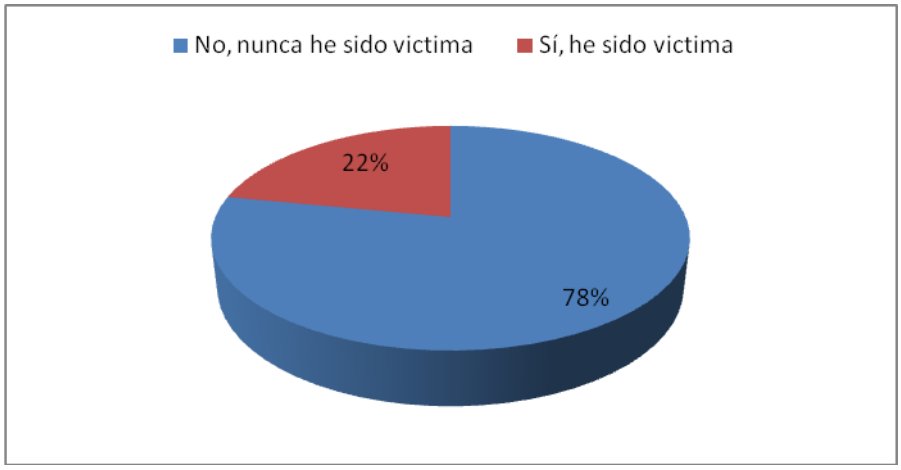
Tabla 3 Encuesta: Pregunta 3

TABLA DE FRECUENCIA		
DETALLE	**DATOS**	**PORCENTAJE**
No, nunca he sido victima	210	78,07%
Sí, he sido victima	59	21,93%
TOTAL	**269**	**100%**

Fuente: Investigación del mercado

Elaborado por: Las autoras

Gráfico 3 Encuesta: Pregunta 3



Fuente: Investigación del mercado

Elaborado por: Las autoras

Análisis e Interpretación

De la población encuestada solo el 22% ha sido víctima de algún tipo de fraude de tarjeta de crédito o débito, mientras que un 78% nunca ha sido víctima de fraude de este tipo. Esto, a pesar de que como se evidencia en la pregunta anterior el 60,97% de los encuestados muestra poca confianza a realizar transacciones con tarjetas de crédito.

4. De los siguientes tipos de fraude ¿En cuales usted ha sido víctima?

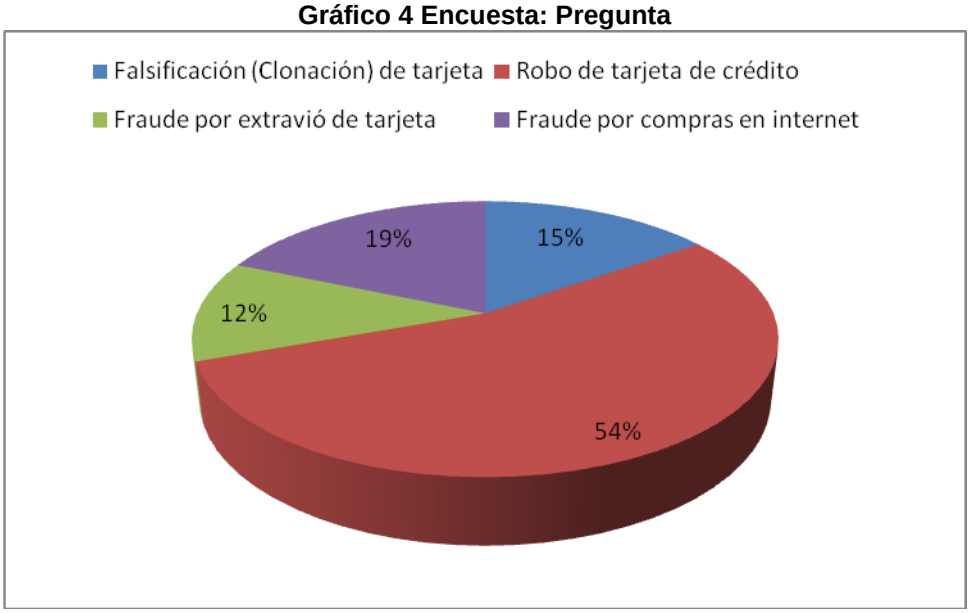
Tabla 4 Encuesta Pregunta 4

TABLA DE FRECUENCIA		
DETALLE	**DATOS**	**PORCENTAJE**
Falsificación (Clonación) de tarjeta	9	15,25%
Robo de tarjeta de crédito	32	54,24%
Fraude por extravió de tarjeta	7	11,86%
Fraude por compras en internet	11	18,64%
TOTAL	**59**	**100%**

Fuente: Investigación del mercado

Elaborado por: Las autoras

Gráfico 4 Encuesta: Pregunta



Fuente: Investigación del mercado

Elaborado por: Las autoras

Análisis e Interpretación

De la población que respondió haber sido víctima de fraude el 54% sufrió robo de su tarjeta de crédito, mientras que sólo un 15% atravesó un caso de falsificación o clonación.

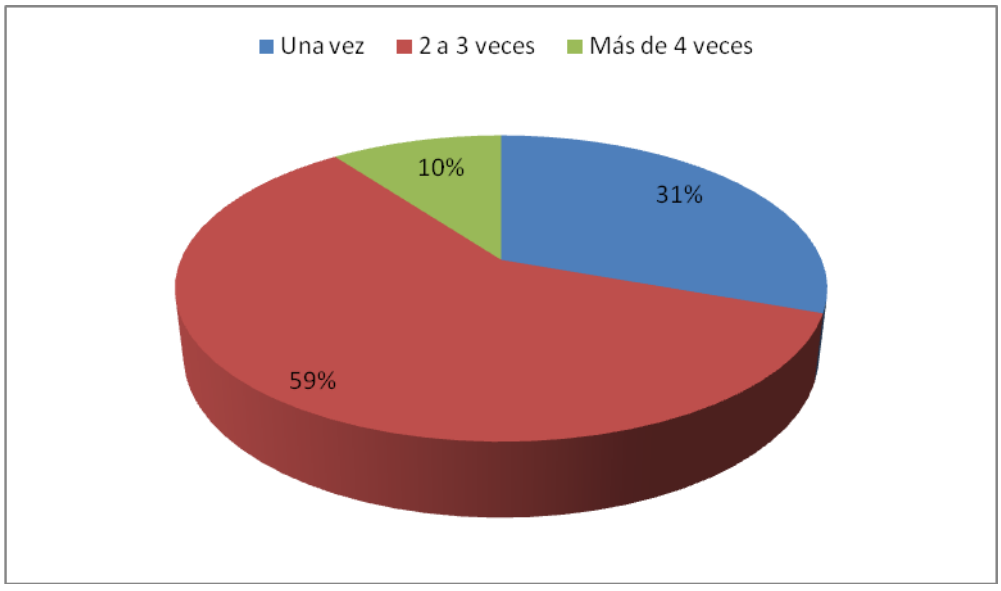
5. **¿Cuántas veces ha sido víctima de fraude con tarjetas de crédito o débito?**

Tabla 5 Encuesta: Pregunta 6

TABLA DE FRECUENCIA		
DETALLE	**DATOS**	**PORCENTAJE**
Una vez	18	30,51%
2 a 3 veces	35	59,32%
Más de 4 veces	6	10,17%
TOTAL	**59**	**100%**

Fuente: Investigación del mercado
Elaborado por: Las autoras

Gráfico 5 Encuesta: Pregunta



Fuente: Investigación del mercado
Elaborado por: Las autoras

Análisis e Interpretación

El 59% de la población fue víctima de fraude con tarjetas de crédito o débito presentó de 2 a 3 fraudes, mientras que el 31% fue víctima una sola vez y sólo el 10% más de 4 veces.

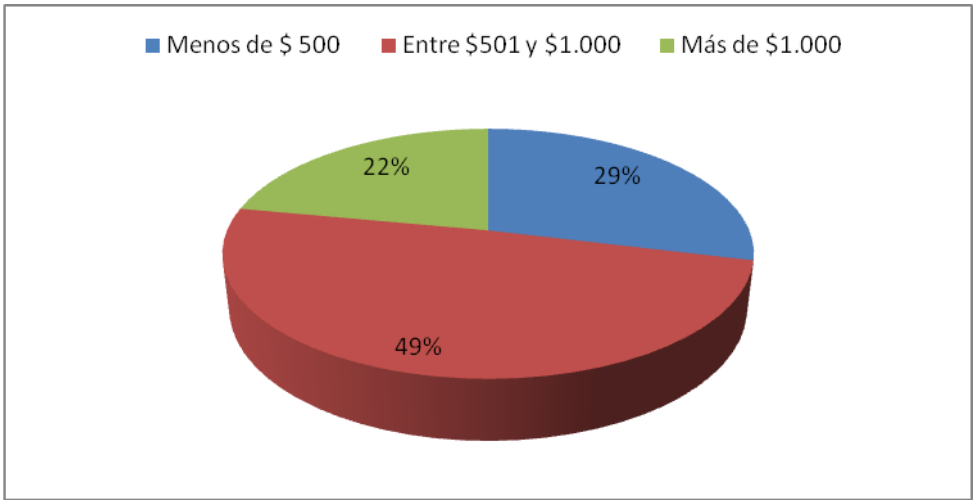
6. En promedio ¿A cuánto asciende el monto sustraído en el fraude?

Tabla 6 Encuesta: Pregunta 6

TABLA DE FRECUENCIA		
DETALLE	**DATOS**	**PORCENTAJE**
Menos de $ 500	17	28,81%
Entre $501 y $1.000	29	49,15%
Más de $1.000	13	22,03%
TOTAL	**59**	**100%**

Fuente: Investigación del mercado
Elaborado por: Las autoras

Gráfico 6 Encuesta: Pregunta 6



Fuente: Investigación del mercado
Elaborado por: Las autoras

Análisis e Interpretación

Al 49% de la población víctima de fraudes le fueron sustraídos entre US$501 y US$1,000, al 29% menos de $500 y al 22% más de $1,000. En esta pregunta se podría evidenciar el pre-conocimiento de los actores del fraude sobre el perfil de sus víctimas.

7. ¿Ha recuperado parcial o totalmente el dinero robado?

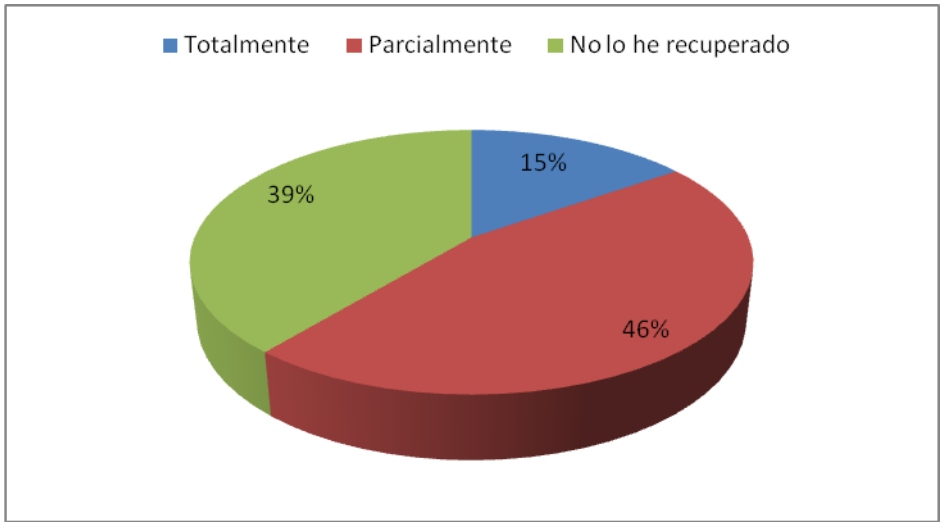
Tabla 7 Encuesta: Pregunta 6

TABLA DE FRECUENCIA		
DETALLE	**DATOS**	**PORCENTAJE**
Totalmente	9	15,25%
Parcialmente	27	45,76%
No lo he recuperado	23	38,98%
TOTAL	**59**	**100%**

Fuente: Investigación del mercado

Elaborado por: Las autoras

Gráfico 7 Encuesta: Pregunta 6



Fuente: Investigación del mercado

Elaborado por: Las autoras

Análisis e Interpretación

Sólo un 15% de las víctimas de fraude recuperó totalmente el dinero sustraído mientras que el 46% lo recuperó de manera parcial y el 39% no lo recuperó. Esto podría evidenciar las políticas de cobertura de seguro de las entidades financieras para este tipo de fraudes para las personas que lo poseen y para las que no lo tienen falta de denuncia a entidades e instancias correspondientes.

8. Cuál fue el daño principal que sufrió producto del fraude?

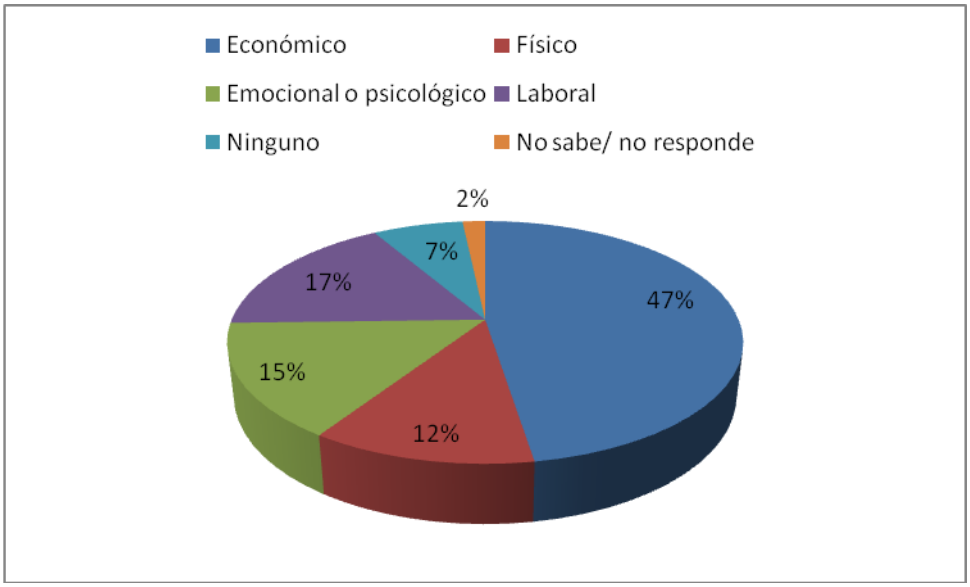
Tabla 8 Encuesta: Pregunta 8

TABLA DE FRECUENCIA		
DETALLE	**DATOS**	**PORCENTAJE**
Económico	28	47,31%
Físico	7	11,83%
Emocional o psicológico	9	15,21%
Laboral	10	16,90%
Ninguno	4	6,76%
No sabe/ no responde	1	1,99%
TOTAL	**59**	**100%**

Fuente: Investigación del mercado

Elaborado por: Las autoras

Gráfico 8 Encuesta: Pregunta 8



Fuente: Investigación del mercado

Elaborado por: Las autoras

Análisis e Interpretación

Las afectaciones de las víctimas de fraude son principalmente económicas, siendo el porcentaje de estas un 47%, 17% laborales, un 15% tiene efectos emocionales y un 12% consecuencias físicas.

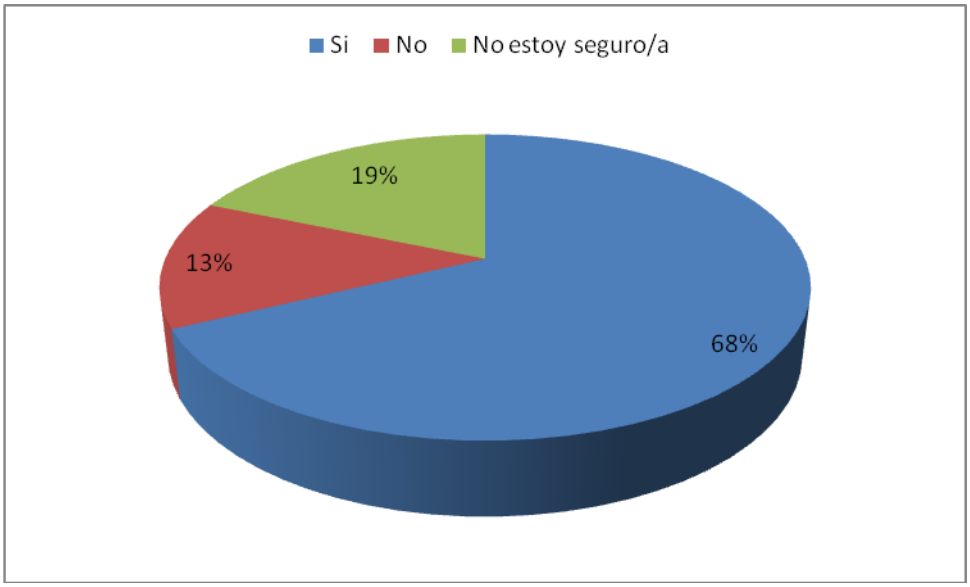
9. ¿Estaría dispuesto/a a contratar algún seguro contra fraudes de tarjeta de crédito?

Tabla 9 Encuesta: Pregunta 9

TABLA DE FRECUENCIA		
DETALLE	**DATOS**	**PORCENTAJE**
Si	40	67,80%
No	8	13,56%
No estoy seguro/a	11	18,64%
TOTAL	**59**	**100%**

Fuente: Investigación del mercado
Elaborado por: Las autoras

Gráfico 9 Encuesta: Pregunta 9



Fuente: Investigación del mercado
Elaborado por: Las autoras

Análisis e Interpretación

La mayor parte de las víctimas de fraude estaría dispuesta a contratar un seguro, representando esta población el 68%, mientras que un 13% no estaría dispuesto y un 19% se muestra inseguro al respecto.

4.7 Conclusiones

Los resultados que se obtuvieron producto de las encuestas efectuadas tienen múltiples interpretaciones, ya que del total de personas encuestadas la mayor parte posee al menos una tarjeta de crédito, no obstante que a la mayoría le inspira poca confianza efectuar sus transacciones con tarjetas de crédito, pese a que solo el 22% ha sido víctima de algún tipo de fraude en este sentido.

De la población que respondió haber sido víctima de fraude el 54% sufrió robo de su tarjeta de crédito, mientras que sólo un 15% atravesó un caso de falsificación o clonación. La mayoría de las víctimas de fraude con tarjetas de crédito (59%) presentó de 2 a 3 estafas, mientras que el 31% fue víctima una sola vez. Los rangos de pérdida por clonación ascienden en su mayor parte entre US$501 y US$1000 dólares, posiblemente por el cupo diario máximo permitido para el retiro en cajeros automáticos en el mismo Banco o en algún Banco de la red, que depende básicamente de la política de cada Entidad.

Este tipo de fraudes al que la ciudadanía en general está expuesta, afecta a las víctimas principalmente en forma económica, laboral, ya que las preocupaciones por no poder cubrir sus obligaciones o el destino al que estaba dirigido el dinero interfiere en el normal desarrollo de sus actividades laborales y un 15% indica haber tenido efectos emocionales como depresión, impotencia, ira, etc.

Por lo expuesto, haciendo un análisis de las encuestas practicadas se puede concluir que se evidencia la falta de confianza de los tarjetahabientes al momento de efectuar sus transacciones como producto de la vulnerabilidad de las tarjetas de crédito con banda magnética, las mismas que son fácilmente falsificadas. Llama significativamente la atención que sólo una proporción muy pequeña de los usuarios conocen los mecanismos de prevención y detección de fraudes, no obstante que el mismo es un ilícito latente que perturba a la población y que si no se toman medidas, podría ir en incremento e incluso migrar de otros países al nuestro, pese a que aparentemente aún no afecta a un gran porcentaje de los habitantes.

CAPÍTULO V: IMPLEMENTACION DE LA SOLUCION EMV Y SU IMPLICACION TECNOLOGICA

La principal razón para definir la necesidad de migrar a tarjetas inteligentes en nuestro país se la puede encontrar en el tema de la seguridad, debido al alto nivel de riesgo asociado a las tecnologías de tarjetas con banda magnética (facilidad de falsificación, copia, etc.), las franquicias que apoyan el negocio con tarjeta, y los mismos bancos, que son los que sufren con este tipo de delito, se ven en la necesidad de realizar alianzas dirigidas a desarrollar una tecnología que, en palabras sencillas, les haga más difícil a los delincuentes tecnológicos poder falsificar y autenticarse como dueño de una tarjeta de crédito que no le pertenezca, como todo lo más importante es ser primero, ya que la curva de aprendizaje del delincuente es muy rápida y podría suceder que cuando las instituciones implanten una versión X de esta tecnología, la misma no sea tan efectiva, como se dice generalmente la facilidad de delinquir se migra inicialmente de lado del que es más débil.

En el Ecuador el porcentaje de víctimas de fraude por clonación de tarjeta de crédito o débito no es muy elevado con relación al resto de países que han sufrido con este tipo de delitos como Colombia, México, Venezuela, etc. este ilícito va en incremento, cuyo perjuicio económico afecta no solo a la ciudadanía, sino también a las instituciones financieras en general.

Desde la perspectiva del hábito de uso de los comercios, la curva de adopción ha sido bastante exitosa. Para los bancos, los elementos de seguridad de la tecnología CHIP, han venido motivando el remplazo sistemático de los plásticos de banda magnética por tarjetas con CHIP. Algunas de estas mismas entidades han avanzado a la fase de explotación de la tecnología, generando proyectos de multiaplicación (más de un producto sobre el CHIP) y de CHIP con interfaz dual (con contacto y sin contacto).

Según Leaño (2012) La migración a tecnología EMV garantiza la disminución del fraude cuando hay presencia de la tarjeta, especialmente con el fraude cuyo origen es el copiado de información, Skimming con lectores de la banda magnética, pues si el Banco emisor solo permite hacer las transacciones con Chip para aquellas tarjetas que tengan esta tecnología, y no permite utilizar la banda magnética, entonces se sabe que quien realiza la transacción es el cliente con la tarjeta original y en caso de haber copiado la banda no se podrá aprobar la transacción Leaño. (página 15)

En la actualidad, la aceptación y evolución de las tarjetas con banda magnética a los dispositivos Visa con Chip va en aumento en toda la región. Países como Brasil, México Colombia y Venezuela son los países que tienen mayor porcentaje de migración nacional a EMV.

En Brasil, la penetración en la transaccionalidad con tarjetas Chip fue del 63% en un período mayor a tres años, mientras que en Colombia en

menos de dos años se ha logrado una transaccionalidad del 42,72% con Chip y se espera terminar el año 2012 con el 60%. (Credibanco,2012)

En Brasil se estima para el 2015 un aumento de cerca de 4 millones de terminales que tendrán la tecnología EMV y en México se proyecta para el mismo periodo con 582.000 POS certificados y actualizados para recibir tarjetas con Chip.

Figura 5. Tarjetas con chip

Fuente: Banco de Bolivia

5.1 Identificación del proceso

La migración de tarjetas de bandas magnéticas a tarjetas con chip es un proceso en boga en gran parte del mundo que se plantea por razones de seguridad y para implementar un avance tecnológico que sea de más utilidad para los usuarios. Con éste también se estandarizan los procesos vinculados a la banca a nivel mundial. En el Ecuador la entidad encargada de ejecutar este proceso es la Asociación de Bancos Privados del Ecuador (ABPE).

Los bancos tienen la obligación de terminar el proceso de migración para diciembre del 2015, todo esto implica una serie de procesos vinculados a toda la plataforma que conforma el sector.

César Robalino, director ejecutivo de la Asociación de Bancos Privados ABPE asegura que la migración tardaría ese período por cuanto el impacto tecnológico que conlleva en la infraestructura de la banca nacional (El Comercio, 2012).

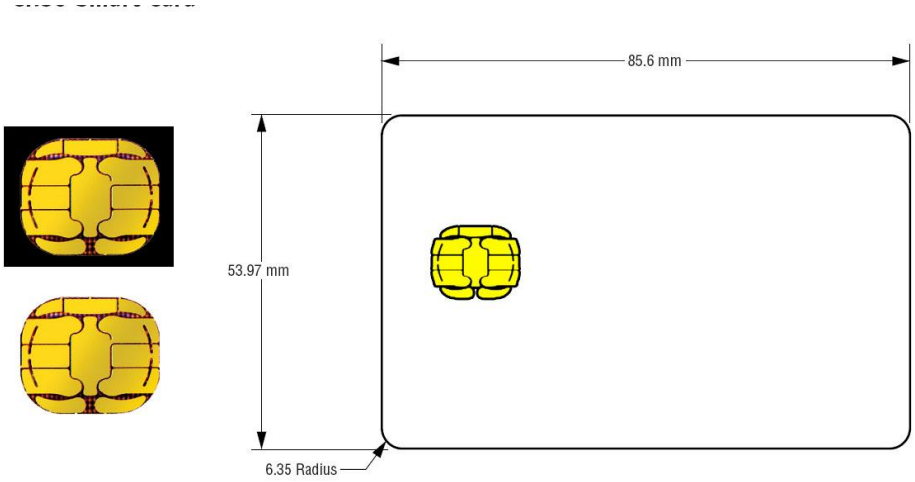
La tecnología con chips funciona de manera que el inserta la tarjeta con chip en un lector de tarjetas y la deja en la terminal hasta que se completa la transacción. El lector de tarjetas identifica si una tarjeta está activada con el número de identificación personal (NIP). De ser así, se indicará al cliente que ingrese su NIP, en lugar de firmar un recibo. Las transacciones con chip serán similares a las transacciones de banda magnética en la mayoría de sus características (Mastercard, 2011)

Comprender el proceso y su necesidad es uno de los primeros pasos para que existan las posibilidades de implementar esta tecnología.

5.2 Preparación de emisión de las tarjetas

En la preparación para la emisión de tarjetas EMV, los emisores necesitan considerar las implicaciones de hardware, software y del proceso de emisión. Con la finalidad de mantener el orden y control sobre las definiciones de negocio y parámetros de riesgo que luego son trasladados a la tarjeta mediante el proceso de personalización y especialmente cuando se tienen varios productos es importante mantener una plantilla sobre las características de cada de cada una de las tarjetas.

Figura 6. Diseño de la emisión de tarjetas con Chip



Fuente: Banred

Los emisores que emiten tarjetas con chip bajo la tecnología EMV deben certificar sus tarjetas ya sea a través de las franquicias ó por medio de una empresa certificadora. Para el caso de las franquicias ellas le indican

al emisor las opciones de empresas certificadoras que dan este tipo de servicio.

5.3 Tecnología en las tarjetas inteligentes

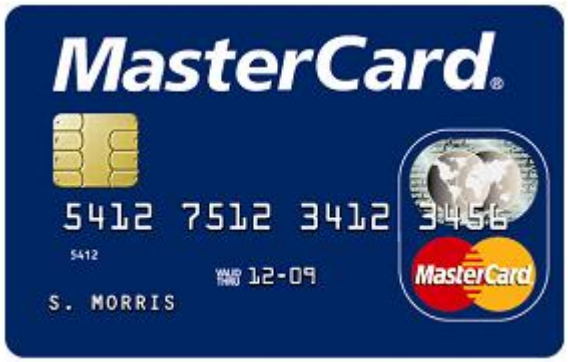
La tecnología de tarjetas inteligentes toma un microprocesador de circuito integrado seguro y lo incorpora dentro de una forma de pago (form factor). El microcircuito generalmente se alimenta de la energía del dispositivo lector por lo que requiere del mismo para poder funcionar.

La interface con el lector puede ser de contacto o sin contacto. Las tarjetas de interface doble (Dual-interface cards) incorporan las dos interfaces y dependiendo de las opciones disponibles en el punto de aceptación, se pueden comunicar ya sea utilizando la interface de contacto o sin contacto.

Las tarjetas de contacto se comunican con el lector mediante una placa de contactos. La palca debe entrar en contacto con el terminal, generalmente mediante un lector de inserción donde se introduce la tarjeta. Los cajeros automáticos (ATMs) generalmente utilizan lectores motorizados que llevan la tarjeta dentro del ATM para prevenir su retiro mientras se ejecuta la transacción.

Las tarjetas sin contacto contienen una antena y se comunican con el lector mediante radio frecuencia (RF). Las tarjetas de interface doble combinan ambas tecnologías.

Figura 7. Diseño frontal tarjeta inteligente



Fuente: Mastercard

5.4 EMV y la Seguridad en las tarjetas

EMV es un grupo de especificaciones de estándar Abierto para tarjetas inteligentes de pagos y dispositivos de aceptación. EMVCo, controlado por American Expresss, JBC, Mastercard y Visa, administra y mantiene y mejora las especificaciones de EMV para garantizar la interoperabilidad global de las tarjetas de pagos basadas en microcircuitos, incluyendo puntos de ventas y cajeros automáticos ATM.

El propósito primario se EMV es asegurar que los estándares para las tarjetas inteligentes de pago sean interoperables globalmente. Estos estándares se encontraban limitados a la tarjeta de contacto , sin embargo ahora ya se incluyen algunos estándares a las tarjetas sin contactos.

Las tarjetas de contacto se comunican con el lector mediante una placa de contactos, la placa debe de entrar en contacto con el terminal, generalmente mediante un lector de inserción donde se introduce la tarjeta. Los cajeros automáticos ATM generalmente utilizan lectores motorizados

que llevan dentro de la tarjeta ATM para prevenir su retiro mientras se ejecuta la transacción.

Las tarjetas sin contactos contienen una antena y se comunican con el lector mediante Radiofrecuencia.

En consecuencia, el almacenamiento e información de pago de manera segura dentro de un microcircuito en lugar de la banda magnética, la utilización de EMV mejora la seguridad de las transacciones de pago al agregar funcionalidad en tres áreas:

1. Autenticación de la tarjeta, protegiendo contra tarjetas falsificadas.
2. Verificación del cliente, autenticando al portador de la tarjeta protegiéndolo contra tarjetas robadas y extraviadas.
3. Autorización de la transacción, utilizando reglas definidas por el emisor para autorizar transacciones.

.

5.4.1 Métodos de Autenticación de la tarjeta

La autenticación de la tarjeta protege a los medios de pagos contra el uso de las tarjetas falsificadas. Lo métodos de autenticación de la tarjeta se encuentran definidos en las especificaciones EMV y en las especificaciones de pagos de las principales compañías de pago con tarjeta.

Los métodos de autenticación de datos más comúnmente usados por las tarjetas con chip al momento de procesar una transacción son: Static Data Authentication (SDA) y Dynamic Data Authentication (DDA).

SDA.- Este método es el más simple y más barato, el proceso de autenticación es realizado por el terminal haciendo uso de un esquema de

firma digital basado en la técnica de claves públicas para confirmar la legitimidad de los datos críticos residentes en a tarjeta y que previamente fueron introducidos en la misma durante el proceso de personalización.

La palabra estática es usada para indicar que siempre se usará la misma firma digital para todas las transacciones que se realicen con la tarjeta, por lo tanto para que el chip realice esto no se requiere de un procesador criptográfico

DDA.- Este método es el más sofisticado y seguro de realizar la autenticación de la tarjeta y requiere que las tarjetas con chip posean un procesador criptográfico y por lo tanto el costo de las mismas es más alto, de igual forma que la modalidad SDA este método procede a validar los datos contenidos en la tarjeta pero con la característica de que pueden detectar si los datos de la tarjeta han sido copiados o falsificados dado que se genera un criptograma por cada transacción.

5. 4.2 Métodos de Verificación del Cliente

La verificación del cliente autentica al portador de la tarjeta. El uso de un número de identificación personal es un método común de verificación del cliente que autentica al cliente y evita que el uso de la tarjeta robada o extraviada.EMV soporta cuatro tipos de CVM:

- Pin fuera de línea (Pin Offline)
- Pin en línea (Pin Online)
- Verificación de Firma

- No VCM

El pin fuera de línea es el único método de verificación del cliente soportado por EMV que no está disponible por las tarjetas con banda magnética. El pin fuera de línea es almacenado de manera segura en la tarjeta, cuando el cliente introduce su pin durante la transacción el terminal POS envía el PIN a la tarjeta EMV para su verificación, la tarjeta compara el PIN introducido con el PIN almacenado dentro del microcircuito y envía el resultado de vuelta al terminal POS, que puede entonces aprobar la transacción fuera de línea y enviar la transacción y el resultado de la verificación del PIN al sistema central (host) del emisor para su autorización.

El PIN en línea no es almacenado en la tarjeta porque el PIN es enviado en línea para que sea validado por el emisor. El PIN en línea es soportado actualmente por las tarjetas de banda magnéticas y ampliamente soportales en terminales POS y cajeros automáticos en América Latina.

El cliente introduce el PIN en el terminal POS, el mismo es encriptado y enviado en línea al sistema central (host) del emisor para su validación. La seguridad de validación del PIN en línea se encuentra basada en los estándares de Triple encripción de datos.

La verificación de la firma requiere que se proceda a firmar en papel en el POS, tal como sucede actualmente para las transacciones con tarjeta de banda magnética. La validación se realice cuando la firma en el recibo es comparada y coincida con la parte trasera de la tarjeta.

EMV también soporta transacciones que no requieren de ningún CVM (no CVM). La opción de No CVM es utilizada típicamente para transacciones de bajo valor o para transacciones realizadas en lugares con terminales POS no atendidos.

5. 4.3 Autorización de la Transacción

Las transacciones EMV pueden ser autorizadas ya sean en línea o fuera de línea. Las transacciones en línea, procede tal como ocurre hoy en día en América Latina para las tarjetas con banda magnética. La información de la transacción es enviada al emisor junto con un criptograma especifico para esa transacción y el emisor puede aprobar o declinar dicha transacción.

En una transacción fuera de línea, la tarjeta y la terminal se comunican y utilizan una serie de parámetros de riesgos definidos por el emisor que se encuentran almacenados en la tarjeta para determinar si la transacción puede ser aprobada.

Las transacciones fuera de línea son utilizadas cuando las terminales no tienen conectividad en línea (por ejemplo un Kiosko para la venta de boletos), en países donde el costo de las telecomunicaciones son altos o durante horarios picos para aumentar la velocidad de las transacciones.

5.5 Certificaciones EMV

La certificación los esquemas de evaluación EMV utilizan un enfoque de estandarizado de la industria y un enfoque de capas es aplicado de forma escalonada a los circuitos integrados y luego a los sistemas operativos y a la

aplicación. Cada pieza de la cadena de valor puede reutilizar la certificación del paso previo para alcanzar su propia verificación.

EMVCo evalúa todas las tarjetas inteligentes basadas en chips EMV y las implementaciones de la solicitud de pago comunes de EMVC0 (Common Payment Application) para garantizar que se ajusten a las directrices de seguridad de EMVCo, incluyendo actualizaciones de firmware y software necesarias para acceder a las funciones de seguridad de chip.

CPA (Common payment Application) trata de las especificaciones que deben cumplir los emisores que desean emitir sus propias tarjetas con chip bajo la tecnología y estándar EMV sin tener que estar afiliados a una franquicia. Este tipo de tarjetas generalmente son emitidas para ser usados en ámbitos privados, domésticos ó nacionales y por lo tanto para garantizar la interoperabilidad de las mismas debe existir una fuerte coordinación entre los emisores y las redes e instituciones adquirientes.

Todas las instituciones debidamente autorizadas y que actualmente están trabajando con tarjetas de banda magnética pueden emitir tarjetas con chip EMV.

Las marcas de pago individual : American Express, Discover, MasterCard y Visa, evalúan la seguridad de sus aplicaciones de pago. Estas evaluaciones, que son realizadas por reconocidos laboratorios externos de seguridad proporcionan un alto nivel de seguridad para que puedan manejar métodos de ataques más conocidos.

5.6 Tamaño de la memoria

El tamaño de la memoria de una tarjeta con chip, también conocida con el nombre de EEPROM (Electrically Erasable Programmable Read Only Memory) determina la complejidad y el número de aplicaciones que pueden ser usadas en una misma tarjeta. En general entre más complejo es el set de aplicaciones a poner en la tarjeta, mayor cantidad de memoria se requiere, también dependiendo de cuan avanzado y complejo sea el método de autenticación de la tarjeta el consumo de memoria es mayor.

Se podría decir que una tarjeta con chip que reúna al menos las mínimas características requiere como mínimo 4K de memoria EEPROM para poder trabajar con una sola aplicación de pagos, aunque la flexibilidad y escalabilidad a futuro se verá severamente restringida.

Tabla 7. Certificaciones del software de Chip EMV

Arquitectura con Chip EMV	Evaluaciones y Certificaciones
Nivel de datos • Datos de Personalización • Parámetros de Administración de Riesgo • Información del Cliente • Certificados y llaves criptográficas	• Las marcas de pago validan la personalización de la tarjeta, previo a la emisión en producción.

Nivel de Aplicación EMV • American Express • Discovery • MAstercard Mchip, PayPass Mchip • Visa VSDC, payWare	• Las marcas de pago certifican las aplicaciones
• **Nivel de Plataforma y Sistemas** Operativos • Advantis • Tarjeta Java GlobalPlatform • Multos • Otros sistemas operativos nativos	• EMVC0 certifica los sistemas operativos abiertos de chip • Las marcas de pago certifican implementaciones de sistema operativo EMV nativo. • Multos tiene su propio sistema operativo.
Chip Hardware EEPROM ROM Motor Criptografico (DES, PKI) Logica de protección de Memoria	

Fuente : Datacard Group, Smart Card Alliance

Antes de realizar la selección del sistema operativo o plataforma, es importante entender que tipo de beneficios, estándares y soporte que recibe cada aplicación.

5.7 Sistemas operativos

La búsqueda de sistema operativo con el que trabajará la tarjeta cae en dos categorías, elegir un sistema operativo propietario ó un sistema operativo abierto.

Los sistemas operativos propietarios corresponden a desarrollos realizados por cierto tipo de empresas en particular en base a prácticas ó definiciones propias que solo son conocidos por ellos, una de las ventaja es su costo, las desventajas son que aquellas tarjetas no permiten cambiar su funcionalidad ó soportar otro tipo de aplicaciones a menos que sean desarrollados por el mismo proveedor, lo cual se traduce en tiempo y costos elevados y además al ser sistemas propietarios para un tipo de fabricante, al momento de cambiar de proveedor esto impacta el proceso de personalización de la tarjetas.

La selección de una plataforma abierta ofrece una mayor cantidad de proveedores y aplicaciones para la tarjeta, estos sistemas permiten cargar y ejecutar aplicaciones de manera estándar sobre las tarjetas con chip de muchos proveedores lo cual implica a futuro evitar complicaciones y preocupaciones relacionadas con la interoperabilidad y escalabilidad.

Es importante anotar que existen proveedores que ya incluyen las aplicaciones pre-cargadas de acuerdo a las especificaciones EMV adoptadas por las principales franquicias tales como Visa (VSDC) ó Mastercard (M/chip).

Tabla 8. Descripción de Plataforma EMV

Plataforma	Descripción	Beneficio
Advantis	Especificación de personalización	Fácil implementación y personalización
GlobalPlatform	Estándar abierto para administración de aplicaciones	Facilidad para agregar aplicaciones
Multos	Especificaciones Técnica	Simple especificación técnica
Nativa	No es estándar, ni propietaria	Sistema operativo cerrado y difícil

Fuente: Smart Card Alliance Latino America - Scala

5.8 Personalización de la Tarjeta con Chip

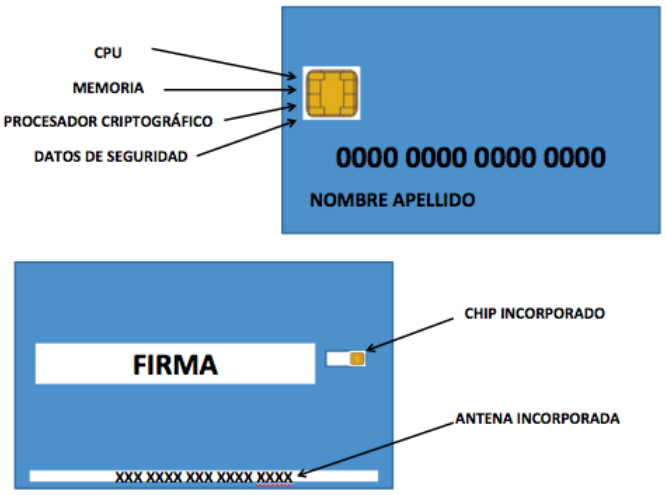
La personalización de la tarjeta es uno de los pasos finales de la migración. En este se incluyen los nombres, perfiles y números de cuenta del destinatario final pues a partir de este proceso el uso de la tarjeta podrá realizarse únicamente por su propietario. Éste proceso se realiza normalmente de manera gráfica, ya sea por medio de estampado o troqueleando los datos.

EMV trabaja con tipos de perfiles en los que se fijan el valor de los parámetros de la tarjeta de forma que quede establecido el comportamiento de ésta. Estos perfiles se asignan en función de las siguientes consideraciones:

- Tipo de producto (crédito o débito) al que pertenece la tarjeta
- Gestión de Riesgo a llevar a cabo por parte de la tarjeta
- Métodos de Verificación de Usuario que soporte la tarjeta
- Autenticación de Emisor/Tarjeta soportada o no por la tarjeta

Los gestores de esta información tienen la opción de no utilizar los perfiles recomendados por el sistema internacional y emitir los propios.

Figura 8. Diseño de tarjeta



Fuente: Mastercard

5.9 Implementación de la tecnología en POS

Para que el sistema de tarjetas inteligentes pueda ser procesado se requiere cambiar el hardware y software de todos los puntos en los que se requiere el uso de las tarjetas de débito y de crédito. A nivel nacional existen más de 10 millones de cuentas de ahorro y 850.000 corrientes, cuyos titulares utilizan cajeros automáticos (Superintendencia de Bancos y Compañías).

Los cajeros automáticos han sido sinónimos y cómodo acceso al dinero en efectivo. La simplicidad de estos dispositivos también los hace un objetivo primordial para los defraudadores, las características clave de la

tarjeta EMV es la inclusión de un chip de seguridad, el soporte de las tarjetas EMV en cajeros automáticos requiere de un cambio generalizado.

Como resultado del esfuerzo en los países que implementaron EMV, el fraude en cajeros automáticos esta migrando desde países que ya implementaron EMV hacia aquellas aéreas que aun no han activado la funcionalidad de EMV.

Figura 9. Diseño de Transacción

Fuente: Mastercard

EL uso de tarjetas con PIN y CHIP EMV ayudaron a reducir el fraude en cajeros automáticos en un 36% en Europa en 2009 en comparación con

2008, de acuerdo con el consejo Europeo de Pagos (European Payments Council Report), Abril 2010.

Por lo tanto al momento de examinar los cajeros automáticos deberán tomar en cuenta las siguientes capacidades:

- Capacidades de Hardware
- Capacidades de Software EMV
- Certificaciones de las marcas
- Capacidad de actualización del software del Terminal y Planes

5.9.1 Hardware en cajero automático

El hardware requerido en el cajero automático incluye varios componentes. Un cajero automático necesita un CID de contacto EMV para leer las tarjetas de contacto EMV. Un lector de chip aprobado es esencial. Algunos cajeros automáticos pueden haber sido vendidos como EMV listos; Sin embargo, es esencial asegurarse que el dispositivo instalado ha sido certificado y que la última versión de la especificación está instalada o puede actualizarse.

El cajero automático deberá equiparse con un PIN pad de encripción aprobado.

5.9.2 Software del cajero automático

El software del cajero automático debe incluir un software para activar todas las funciones de hardware necesarias. Éste debe incluir un firmware o software específico para habilitar las aplicaciones específicas sin contacto apoyadas por las tarjetas o dispositivos NFC usados en el cajero automático.

Esta es una consideración importante al evaluar los terminales, y es útil para comprender los requisitos de software y de certificación de los terminales.

Los cajeros automáticos deben tener un kernel EMV aprobado y certificado y deben apoyar todas las extensiones requeridas para el protocolo de mensajería.

*5.*9.3 Certificaciones de las Marcas

Las terminales de contacto y sin contacto EMV requieren de múltiples certificaciones:

- EMVCo Nivel 1: Certificación de la funcionalidad de la interfaz entre tarjeta y lector.
- EMVCo Nivel 2: Certificación de la funcionalidad de la aplicación de software del terminal.
- Certificación de las marcas de pago.

Figura 10. Requerimiento de certificación de cajeros automáticos.

Fuente: EMV

Para lograr las certificaciones de nivel 1 y nivel 2, los terminales deberán someterse a pruebas de laboratorio para verificar el cumplimiento de las características electromecánica, interfaz lógica y requisitos del protocolo de transmisión (nivel 1) y los requerimientos de aplicaciones de debito y crédito (nivel 2) definidos e3n las especificaciones EMV.

La certificación EMV garantiza que el terminal cumple con los requisitos de la especificación básica EMV. EMVC0 proporciona solo certificaciones de nivel 1 y 2.

EMV admite tantas opciones de implementación, se pueden necesitar varias implementación de EMV en un mismo terminal. Cada marca de pago puede aplicar las normas de EMV en una forma diferente y cada marca requiere de programación específica en el terminal para la aplicación de esa

marca. Los terminales de ATM, deben pasar por un conjunto de pruebas definidas por cada marca de pago para la recibir la certificación a nivel de marca.

La certificación de las aplicaciones del terminal puede ser un proceso largo para el proveedor de la aplicación del terminal. Mientras que muchos de los proveedores de terminales ya tienen terminales que han sido certificados por las principales marcas de pago, la certificación es transferible silo si la aplicación se mantiene sin cambio a través de implementaciones. Si hay cambios para una aplicación especifica, un nuevo proceso de aprobación será requerido para la aplicación. Cuando se adquiere un terminal ATM, asegúrese de que tiene un Kernel de software y que se han implementado las extensiones necesarias para el protocolo de mensajería.

5.9.4 Capacidad de actualización del terminal y planes

Los cajeros automáticos instalados en América Latina soportan en la actualidad chip de contacto EMV y tarjetas de banda magnética. Todos los proveedores de ATMs informan haber ofrecido cajeros EMV durante los últimos 5 años. Los cajeros automáticos mas nuevos están equipados para aceptar tarjetas EMV y la mayoría de las implementaciones de América Latina ya cuentan con lectores de chip habilitados. El costo de un lector de chip es casi lo mismo que el costo de un lector no chip, porque los

proveedores de ATMs atienden países donde los lectores de chip ya son estándar.

Los cajeros automáticos han evolucionado en los últimos 10 años de sistemas propietarios cerrados a los equipos que ejecutan los sistemas operativos estándar. El software de los cajeros automáticos modernos puede actualizarse fácilmente. Para proteger contra la incertidumbre de qué tipo de instrumento de pago se debe apoyar, los propietarios de los ATMs están aprovechando esta capacidad de aplicación futura para instalar terminales con el hardware que soporta transacciones EMV de contacto o sin contacto.. Estos terminales están diseñados para facilitar las actualizaciones y descargas de aplicaciones remotas y han recibido certificaciones de nivel de marca con aplicaciones de EMV que pueden ser descargadas en el futuro.

5.10 Cambio de tarjetas

Se debe realizar una comunicación masiva a los usuarios de tarjetas de crédito y de débito para que realicen el cambio de tarjetas.

Una de las medidas que se puede adoptar para que el cambio sea progresivo y los usuarios a los que no lleguen las comunicaciones debidas sobre la migración no tengan inconvenientes es el método aplicado en Bolivia.

En el país andino se implementó un sistema que permitía leer tarjetas de banda magnética y a la vez tarjetas con chip. Sin embargo para los propósitos de esta migración se requiere que los usuarios hagan el cambio.

En el caso de Colombia la implementación del sistema de tarjetas con chip se hizo según el requerimiento de los usuarios. Si uno de éstos perdía su tarjeta la que se entregue sería con chip.

5.11 Capacitación a personal de la banca

La migración a tecnología EMV representa un gran desafío para las instituciones financieras, no solamente las tarjetas y los terminales cambian drásticamente sino que también son afectados todos los otros componentes que son parte integral del proceso.

Esto incluye el proceso de emisión y personalización de las tarjetas, los sistemas de criptografía, los sistemas autorizadores, hardware y software de los terminales, del sistema de administración de terminales, el manejo de los parámetros de riesgo, procesos de certificación, educación y entrenamiento a clientes y usuarios de esta nueva tecnología.

Todos estos cambios deben ser cuidadosamente identificados, planeados y correctamente manejados. Para ayudar a las instituciones financieras a lograr un proceso de migración exitoso Banred ofrece los siguientes servicios ya sea en forma de consultoría y/o acompañamiento:

- Capacitación EMV tanto para las áreas técnicas como de negocio.
- Gerencia y acompañamiento en los proyectos de migración.
- Análisis del impacto operacional.
- Elaboración de planes de migración.

- Pruebas y certificaciones funcionales.

5.12 Costo

Para la implementación de esta tecnología no se manejan cifras exactas ya que mucho depende del tamaño de la institución, el volumen de tarjetas que se emitan, la disponibilidad y los rubros destinados dentro del presupuesto para este fin, sin embargo de las entrevistas realizadas a funcionarios de emisoras de tarjetas de crédito y entidades financieras se ha podido establecer costos aproximados que incluirían hardware, software, servicios profesionales, capacitación, costos internos, etc. los mismos que a continuación se detallan:

Tabla 9. Costo de la Tarjeta con Chip

Costo de Tarjeta con chip		**$ 1,70**
Más (Impuestos)	(+)	$ 0,30
Total costo de tarjetas		$ 2,00
Número aproximado de tarjetas a emitirse	(X)	400.000,00
Total costo emisión de plástico		$ 800.000,00
	(+)	
Adquisición de software y hardware		$ 1.700.000,00
Costo total aproximado		**$ 2.500.000,00**

Fuente: Pacificard (Valores aproximados)
Elaborado por: Las autoras

5.13 Ventajas o beneficio de la aplicación del proceso de Migración a tarjetas con Chip

Mejora la seguridad de infraestructura de transacciones de pago, eliminando al Ecuador como un destino para los criminales que se dedican al fraude global con tarjetas de banda magnética.

Incrementa la satisfacción de clientes internacionales cuando utilizan sus tarjetas EMV en comercios y cajeros automáticos (ATMs) en América Latina.

Mantiene la relación con el resto del mundo a medida que se migra a EMV.

El proceso de migración a tarjetas con chip o tarjetas inteligentes requiere de un determinado tiempo y la correcta capacitación para su migración y uso. Sin embargo el factor de mayor jerarquía en su implementación es pensarlo como un dispositivo que tiene la capacidad de autenticarse y actualizarse en función de la seguridad que se requiera de este.

La implementación de este sistema es un valor agregado para los proveedores de servicios bancarios, así como una manera de integrarse a estándares internacionales.

A pesar de que el costo de adquirir este servicio podría resultar alto es una inversión que a largo plazo permitirá que los usuarios de tarjetas de

débito y de crédito puedan acceder a más servicios y cuenten con una serie de aplicaciones que les facilite sus transacciones comerciales, así como la compatibilidad de este sistema con otros a escala mundial.

5.14 Puntos a considerar y posibles impactos en el proceso de migración en cuanto a la emisión de las tarjetas de crédito con chip.

Existen varios puntos a considerar y posibles impactos en el proceso de migración a tarjetas de crédito con chip, los mismos que a continuación se exponen:

Financiero: Definitivamente esta es una tecnología más costosa, al no estar globalizada, es más difícil para los proveedores de este tipo de tarjetas disminuir los precios, aun cuando las franquicias han hecho un gran esfuerzo para apoyar la disminución de los mismos, lo que afecta financieramente a los bancos y administradoras de tarjetas de crédito.

Estratégicos: Esta nueva tecnología hace que los bancos tengan que definir procesos de migración y generación de plásticos que posiblemente no tenían planificados, en general la estructura organizativa de los bancos deben cambiar para apoyar una nueva forma de hacer negocios y definir productos, y definitivamente la parte de seguridad exige la redefinición de nuevos procesos internos y externos para el mantenimiento del esquema de seguridad que esta tecnología exige.

Operativos: Los bancos deben adaptar sus tecnologías para poder emitir plásticos con estas características, comprar equipos nuevos, tomar decisiones como si los emiten ellos o los emiten fuera, y en este último caso, es esto seguro?, otra de las interrogantes que se hacen las entidades es en qué tipo de plástico invertir para que su esquema de inventario sea duradero?, no hay que olvidar que mientras más se involucran en tecnología más fácil es que la misma quede obsoleta, por lo que esta pregunta es muy importante en los primeros pasos del proceso.

5.15. ¿Los Bancos de Ecuador estarían listos para salir al mercado con tarjetas EMV Chip?

De las entrevistas efectuadas a expertos en temas control y prevención de fraudes podría decirse que existen dos visiones en cuanto a si los Bancos ecuatorianos estarían listos para salir al mercado con tarjetas inteligentes.

Por una parte si hablamos de si están tecnológicamente preparados para salir al mercado con EMV CHIP, podría decirse que dado que en abril del 2012 se emitió la resolución JB-2012-2148 por parte de la Superintendencia de Bancos y Seguros que obliga a las entidades a migrar su portafolio de tarjetas de crédito a tecnología chip, en los últimos meses los bancos nacionales han realizado un gran esfuerzo para prepararse para esta salida. Algunos en la dualidad emisor-adquirente, otros en una de las dos, además de que existen procesos de apoyo a los bancos que han ideado las franquicias que ayudan a aquellos que no cuentan con el tema

financiero y logístico para salir con esta tecnología, sin embargo como en todo proceso de migración al principio se presentarán muchas dificultades asociadas a temas técnicos, cambios de infraestructura, nuevos desarrollos, curva de aprendizaje etc, no obstante lo que se observa es que aunque EMVco estandariza las tarjetas chip financieras cada marca está en la posibilidad de establecer sus propias condiciones, a esto hay que sumar que existen diferentes tipos de hardware (chip) para la implementación y se necesita adaptarse a lo que ofrece el fabricante.

Por otro lado si se refiere al negocio externo de los bancos, podría decirse que el mercado ecuatoriano no está tan preparado como otros países que ya han implementado algún tipo de esquema de negocio basado en EMV, como es el caso de México o Venezuela.

Para que esta experiencia de implantación haciendo negocio sea exitosa, es necesario un plan muy fuerte de educación tanto a nivel de los comercios como de los Tarjeta Habientes, además de que los bancos tienen que pensar su nueva forma de hacer negocios basado en esta tecnología.

Conclusiones

Las tarjetas inteligentes son un vínculo vital en la cadena de confianza de un sistema de identificación seguro. Ellos actúan como el agente de confianza del emisor y brindan la capacidad única de asegurar y verificar con precisión la identidad de los portadores de tarjetas, autenticar la credencial del documento de identidad y presentar la credencial al sistema de Identificación.

Las tarjetas inteligentes brindan una plataforma tecnológica óptima para sistemas de identificación seguros que pueden responder a las necesidades de las empresas y negocios para una verificación segura y exacta de la identificación.

Muchos fraudes se podrían evitar con la planeación y sistemas de control adecuados. El diseño e implementación de políticas claras de prevención, detección e información dentro de la misma compañía.

En forma global la estrategia principal para el tarjetahabiente, es dar un amplio conocimiento al cliente de los parámetros de utilización de las tarjetas de crédito y conocimiento de los posibles fraudes que se pueden dar, tener actualizado al cliente con el debido uso de claves y pines que tienen las mismas.

Para afrontar tales vulnerabilidades e implementar un sistema de identificación seguro, las organizaciones deben definir una cadena de confianza que abarque todos los procesos y componentes de un sistema de identificación seguro. La cadena de confianza empieza con la definición del

modelo, las políticas de seguridad, los acuerdos de negocio entre las organizaciones envueltas en los sistemas de Identificación seguro e incluye todos los componentes del sistema de Identificación desde los procesos y documentos que son utilizados para la verificación inicial y el registro del mismo.

La eficiencia, consolidación de programas y las características de seguridad brindadas a través del uso de tarjetas de identificación inteligentes, permiten a instituciones y negocios aumentar la seguridad mientras mejoran los servicios y reducen los costos operativos.

Finalmente, se debe informar a los clientes que deben destruir toda tarjeta caducada, que tenga banda magnética, para de esta manera evitar se realice una clonación de la misma.

Recomendaciones

El proceso de migración debe estar sujeto a cada uno de los estándares internacionales planteados de manera que en el futuro este sistema pueda ser usado de forma global.

Este sistema debe tener las correctas regulaciones de forma que se establezcan mecanismos claros y transparentes que permitan establecer responsabilidades ante la ocurrencia de un hecho de fraude en un entorno CHIP y PIN.

La banca debe asumir tanto los costos de la implementación como las formas de regulación. Se registra que en varios países debido al costo que implica esta migración se han desestimado los gastos de seguridad de manera que en su incurrencia se asume como culpable al tarjetahabiente.

La correcta capacitación tanto a los usuarios como a los proveedores es vital para que el sistema pueda funcionar desde el principio y para que los usuarios se familiaricen de forma inmediata con este, dado que si no lo comprenden desde un inicio puede complicar tanto su uso como su efectividad haciendo que las transacciones se alarguen.

Con esto se descarta la posibilidad de que el staff o personal del banco pueda estar vinculado con algún tipo de fraude.

Bibliografía

Andrade, A. (2011 -11-Octubre). Clonar tarjetas llega a su fin, la tecnología lo evita. Diario Hoy.

Friedman, Jerome. (2009). Aprendizaje Automatico, Boston, Ma Pearson.

Kevin D. Mitnick y William L. Simón (2007). EL Arte de la Intrusión, Madrid, Alfaomega Grupo Editor.

2010, Contactless Payment Specification For Payment Systems, 160-189. Recuperado de http:// www.emvco.com

2008. EMV Integrated Circuit Card Specifications for Payment Systems, version 4.2, 78-80. Recuperado de http:// www.emvco.com

FÍGOLI PACHECO, (1998). El Acceso No Autorizado a Sistemas Informáticos, 67-98. Recuperado de http://www.derecho.org.

Abadi, M., Burrows, M., Kaufman, C. and Lampson, B.(2009), Authentication and delegation with smart-cards, Science of Computer Programming, pp. 93-113,

Steve Rogers. (2002). Smart Cards and Biometrics in Privacy-Sensitive Secure Personal Identification Systems," first published by the Smart Card Alliance, 93-113. Recuperado de http:// http://www.openauthentication.org/

Jonathan Zittrain, (2008). Consumer Fraud and Identity Theft Complaint http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2008. California, PR: Edition

Yurcan Bryan, (2014) VNUnet, "EMC Purchases Verid, a Specialist in Knowledge-Based Authentication." http://www.vnunet.fr/news/groupe-emc-rach-te-verid-sp-2018533. California, PR: Edition

Superintendencia de Bancos y Seguros, 2011. http://www.sbs.gob.ec/practg/sbs_index?vp_art_id=531&vp_tip=2

Superintendencia de Bancos y Seguros, 2012. SBS. From http://www.sbs.gob.ec/

Thomson Reuters. (2013, 26 Abril). Reuters México. From http://mx.reuters.com/article/businessNews/idMXL2N0DD1VV20130426

"Logical Access Security: The Role of Smart Cards in Strong Authentication," Smart Card Alliance report, Octubre 2004

Randy Vanderhoof, (2009) Privacy and Secure Identification Systems: The Role of Smart Cards as a Privacy-Enabling Technology, Smart Card Alliance white paper. Recuperado de http://www.smartcardalliance.org/

(2011). Smart Card Case Studies and Implementation Profiles," Smart Card Alliance report. Recuperado de http://www.smartcardalliance.org/

(2011). Smart Card Alliance report, "Smart Cards and Biometrics in a Privacy-Sensitive Secure Personal Identification System," Recuperado de http://www.smartcardalliance.org/

(2010). Smart Card Alliance report. Using Smart Cards for Secure Physical Access. Recuperado de http://www.smartcardalliance.org/

Estrada Cabrera y Ramos Alvarez (2011). El Fraude Informático: Consideraciones Generales, en Contribuciones a las Ciencias Sociales, Madrid, Editores S.A

Financial Fraud Action UK y la UK Cards Association. "Fraud The Facts 2010 The Definitive Overview of Payment Industry Fraud and Measures to Prevent it." Recuperado de. http://www.theukcardsassociation.org.uk/files/ukca/fraud_the_facts_2010.pdf

Anexo 1

Modelo de Encuestas

El objetivo de esta encuesta es conocer sus inquietudes y sugerencias con respecto al fraude con tarjetas de crédito. La información recopilada será totalmente confidencial y utilizada exclusivamente para evaluación global de la efectividad del proyecto.

Información del Encuestado

Sexo: Hombre___ Mujer___

Edad: 18 a 25___ 26 a 35___ 36 a 45___ 46 a 65___

Ocupación: Trabajo___ Negocio propio___ Estudiante___ Ama de casa___

1. **¿Posee usted alguna de las siguientes tarjetas de crédito: Visa, Mastercard, Diners, American Express?**
   SI___ No___

   Si la respuesta es no, puede abandonar la encuesta.

2. **¿Cuánta seguridad y/o confianza le inspira efectuar actualmente sus transacciones con tarjeta de crédito?**
   Mucha confianza___ Poca confianza___ Ninguna confianza___

3. **¿Ha sido usted víctima de algún tipo de fraude de tarjeta de crédito o débito?**
   No, nunca he sido víctima___

   Sí, he sido víctima de algún tipo de fraude ___

   Si la respuesta es no, pase a la pregunta 7.

4. **De los siguientes tipos de fraude ¿En cuales usted ha sido víctima?**

   Falsificación (Clonación) de tarjeta___

   Robo de tarjeta de crédito___

   Fraude por extravío de tarjeta de crédito___

   Fraude por compras en internet___

5. **¿Cuántas veces ha sido víctima de fraude con tarjetas de crédito o débito?**

   Una vez___ 2 a 3 veces___ Más de 4 veces___

6. **En promedio ¿A cuánto asciende el monto sustraído en el fraude?**

   Menos de $500___ Entre $501 y $1.000___ Más de $1.000___

7. **¿Ha recuperado parcial o totalmente el dinero robado?**

   Totalmente___ Parcialmente___ No lo he recuperado___

8. **Cuál fue el daño principal que sufrió producto del fraude?**

   Económico___ Físico___ Emocional o psicológico___ Laboral___

   Ninguno___ No sabe / no responde___

9. **¿Estaría dispuesto/a a contratar algún seguro contra fraudes de tarjeta de crédito?**

   Si___ No___ Noestoy seguro/a___

Anexo 2

Modelo de Entrevistas

1. ¿Actualmente, considera que la clonación de tarjetas afecta a un gran porcentaje de tarjetahabientes en el país?

2 ¿Si no existiera la resolución que obliga a las entidades bancarias a cambiar el tipo de tarjetas que se emiten actualmente por otras con chip, cuál sería el riesgo a mediano plazo?

3. ¿De acuerdo a su experiencia, cuáles son los problemas más importantes que podrían surgir en el proceso de implementación de estas nuevas tarjetas inteligentes?

4.¿Cuáles podrían ser los proveedores de las máquinas o software necesarios para la implementación?

5. ¿Cuáles son los beneficios para el banco y para la sociedad, por la emisión de tarjetas inteligentes?

Anexo 3

Resultado y/o Tabulación de Entrevistas

PREGUNTAS	Pacificard Jorge Armanza	Credimatic Carlos Aguirre	En Reserva nombre de Experto e Institución Financiera	Banco de Guayaquil Nombre Reserva
1. Actualmente considera que la clonación de tarjetas afecta a un gran porcentaje de tarjetahabientes en el país.	Sí, el costo hundido del negocio o rubro por falsificación de banda magnética podría decirse que del 100% del total de fraudes presentados es el 90% aproximadamente. El rango normal o razonable en montos por este rubro se encuentra entre el 0.3% y 0.7% del total de facturación anual, el monto no debería exceder el 1%, si pasa de ese porcentaje ya es considerado alarmante. La métrica para medir los fraudes es: Fraudes = % nivel de fraudes sobre facturación Sin embargo, podría considerarse que el fraude por falsificación de banda magnética se encuentra controlado en nuestro país en comparación con Latinoamérica	Estuvimos involucrados en un tema de skimming el año pasado y pudimos constatar lo siguiente: El porcentaje de afectación no lo conocemos con exactitud ya que antes de la resolución ley que obliga a los bancos a responder ante los casos de fraude no había un verdadero esfuerzo de parte de estos para evitarlo. Actualmente los bancos están luchando contra este fenómeno y según dicen el monto del fraude es bastante significativo.	Afecta a la población pero no tendría un porcentaje sobre los clientes afectados con este tipo de problemas.	SI, efectivamente, existe algunas bandas de clonadores que están operando en el país, recientemente hubo una falla de seguridad en uno de los bancos del país, mismo que ocasionó que se vean comprometidas muchas tarjetas.
2. ¿Si no existiera la resolución que obliga a las entidades bancarias a cambiar el tipo de tarjetas	Si no existiera la resolución, Mastercard y Visa Internacional te obligan a cambiar el tipo de tarjetas de todas formas, de hecho tenían un cronograma de migración	Si no existieran las resoluciones sobre el tema de fraude y actualmente las que obligan a los emisores de tarjetas a mejorar la	El riesgo a mediano plazo estaría primero en que no podríamos realizar transacciones en el exterior	El riesgo ya está presente, y se comprometería en mayor proporción, debido a que las mafias de clonadores estarían

que se emiten actualmente por otras con chip, cuál sería el riesgo a mediano plazo?	progresivo que iba hasta el 2015 aproximadamente. El riesgo a mediano plazo sería que el fraude de banda magnética migre es decir que el fraude existente en otros países migre hacia el nuestro y que la institución responda financieramente por esas estafas. Adicionalmente, el riesgo comercial de que no te acepten las tarjetas en otros países.	tecnología y seguridad, estaríamos en la situación en la cual el usuario del servicio termina pagando en primera instancia, pero a mediano plazo se restringiría el uso de medios de pago y afectaría la credibilidad del sistema.	en los países de Europa ya que ellos manejan sus transacciones solo con POS que aceptan tarjetas con CHIP, otro de los inconvenientes que tendríamos es al mantener una tarjeta con banda el acceso a la información es más fácil para realizar clonaciones o fraudes	operando sin ningún tipo de obstáculos
3. ¿De acuerdo a su experiencia, cuáles son los problemas más importantes que podrían surgir en el proceso de implementación de estas nuevas tarjetas inteligentes?	De orden tecnológico: Interoperabilidad, porque es una tecnología nueva que implica aprendizaje, por poner un ejemplo, antes al deslizar la tarjeta por el POS éste leía los datos de la banda rápidamente, con la nueva tecnología podría decirse que el chip conversa con el POS y se toma su tiempo para reconocer los datos que en él se encuentran. En resumen uno de los problemas surgiría por el cambio de tecnología, la curva de aprendizaje está en la parte más baja. Tema de fraude: Que la persona que conozca de fraudes se interese por otro tipo de fraudes, es decir que evolucione a temas de internet y fraudes internos.	Como en todo proceso de migración al principio se presentan muchas dificultades asociadas a temas técnicos, cambios de infraestructura, nuevos desarrollos, etc, pero lo que observamos es que aunque EMVco estandariza las tarjetas chip financieras cada marca está en la posibilidad de establecer sus propias condiciones, a esto hay que sumar que existen diferentes tipos de hardware (chip) para la implementación y se necesita adaptarse a lo que ofrece el fabricante. Esto indica que tendremos que manejar un ecosistema muy variado de tecnologías conviviendo en el mismo ambiente.	• Costos por la inversión que tendrían que realizar las Instituciones Financieras (adquisición de plásticos, programas para configuración del Chip y equipos). • Cambios en el manejo de la seguridad física de las instalaciones y los programas, así también dentro del manejo de la información. • Tiempo de la migración de la información de los tarjetahabientes. • Implementación y capacitación del personal. • Inducción del cliente sobre el nuevo manejo de las tarjetas con chip, protección de datos y claves asignadas para	Los costos, el tiempo de implementación, obtener el personal idóneo, la priorización de este tipo de proyectos, sobre otros que mantenga el banco.

			transacciones	
4. ¿Cuáles podrían ser los proveedores de las máquinas o software necesarios para la implementación?	Por parte del emisor nuestro proveedor autorizado es Gemalto. Los Pos también deben migrar. Los dueños de Datafast son: Banco Guayaquil, Pacificard y Banco del Pichincha. Por el momento las tarjetas con banda magnética y chip trabajarán conjuntamente en este proceso, pero poco a poco se irá eliminando las tarjetas con banda magnética.	Datacard provee el hardware o integra hardware de terceros. Por ejemplo la 280 tiene un grabador de chip marca Gemplus. También provee el software ya sea desarrollado por la empresa o producto de la adquisición de otras empresas que se dedican al desarrollo de este tipo de soluciones. Gemalto conocemos que provee mucho del hardware para chip y también tiene sus propios sistema para la administración de la personalización.	Vidortec/Datacard (www.vidortec.com.ec) Gemalto (www.gemalto.com) Medianet Datafast	Los proveedores que tienen certificación de cumplimiento con las franquicias, tanto para la generación de tarjetas, como para la venta de software de personalización, entre otros.
5. Cuáles son los beneficios para el banco y para la sociedad, por la emisión de tarjetas inteligentes?	1. Confianza y seguridad de cara al cliente, que se sienta seguro siempre que haga una transacción. 2. Para el Banco disminución de pérdidas y falsificación de banda magnética	Para el banco, a futuro tendrá una disminución en la demanda de transacciones en línea cuando empiece a implementarse la tecnología DDA y transacciones offline. Para la sociedad la posibilidad de aumento en la seguridad de sus transacciones aumentará la confianza en el uso de medios de pago y que vendrá acompañado de nuevas aplicaciones que pueden integrarse en el futuro en un mismo chip.	Protección de la información (mayor seguridad en las transacciones) Reconocimiento de tarjetas a nivel mundial para poder realizar transacciones dentro y fuera del país.	La seguridad de que no clonen la tarjeta, no solo a nivel país, sino al resto del mundo; las personas ya no serían víctimas de la clonación, y el banco dejaría de perder dinero por devolver al cliente lo que se han robado.

Anexo 4

RESOLUCIÓN JB-2014-2745

RESOLUCIÓN JB-2014-2745

LA JUNTA BANCARIA

CONSIDERANDO:

Que en el capítulo V "Riesgo operativo", 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 de la Junta Bancaria, constan, en el artículo 4, los numerales 4.3.8, 4.3.9, 4.3.10, que disponen la implementación de tarjetas inteligentes;

Que de las inspecciones que han realizado los supervisores de riesgo tecnológico de la Superintendencia de Bancos y Seguros en las instituciones del sistema financiero controlado; y, del análisis técnico realizado respecto del nivel de cumplimiento de los citados numerales, se ha determinado que la implementación de las disposiciones normativas ha demandado grandes esfuerzos humanos, técnicos y económicos para las entidades controladas; además, se ha observado la dependencia existente respecto de los proveedores de las tecnologías de la información locales e internacionales para la implementación de varias disposiciones normativas, así como la dependencia de las empresas comerciales para la implementación de tecnologías que permitan el procesamiento de tarjetas inteligentes;

Que por lo tanto, es necesario reformar las disposiciones transitorias del citado capítulo V, con el propósito de establecer un nuevo plazo para ser consecuentes con la realidad del sistema financiero, respecto del cumplimiento de la referida normativa; 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 el siguiente cambio:

ARTÍCULO ÚNICO.- En la primera disposición transitoria del capítulo V "Riesgo operativo", del título X "De la gestión y administración de riesgos", efectuar las siguientes reformas:

1. En el numeral 2, eliminar el 4.3.8.1.

2. Sustituir el numeral 4, por lo siguiente:

"**4.** Los numerales 4.3.8.1, 4.3.9.3, 4.3.10.2, 4.3.10.3, vencen el 19 de diciembre de 2014"

3. Incluir el siguiente numeral;

"**5** El numeral 4.3.8.21, vence el 19 de junio de 2015."

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

Ab. Pedro Solines Chacón
PRESIDENTE DE LA JUNTA BANCARIA

LO CERTIFICO.- Quito, Distrito Metropolitano, el diez de enero del dos mil catorce.

Lcdo. Pablo Cobo Luna
SECRETARIO DE LA JUNTA BANCARIA