DISEÑO DE MONITOREO INTELIGENTE SOBRE EL USO DE LAS TARJETAS DE CREDITO Y DEBITO

CARRERA:

ING. ADMINISTRACION DE EMPRESAS MENCION

COMERCIO INTERNACIONAL

ALUMNA: ROMINA RIVEROS M.

SANTIAGO - CHILE

2012

AGRADECIMIENTOS

Quiero agradecer en esta oportunidad a las personas que han estado conmigo en este proceso de la universidad y sobretodo en la realización del Proyecto de Título.

A mi Madre por creer en mí, y pese a los momentos difíciles, siempre tuve apoyo incondicional de su parte, sin ella no hubiese podido llegar hasta aquí.

A mi novio, Sebastián Silva, que estuvo conmigo en cada momento y siempre me aportó ideas de cómo llevar mi tesis de la mejor forma posible.

A Subgerente de Area de Fraudes de Banco Santander, Andrés Leniz, que pese a la confidencialidad del tema, me ayudó a desarrollar el tema de mi proyecto.

Y por último a mi profesora guía, Alejandra Acuña, por todo su disposición e instrucción, que gracias a ella pude llevarlo a cabo.

Gracias a todos.

Romina Riveros M.

INDICE

RESUMEN

La propuesta de mejora en el diseño de un monitoreo inteligente para las tarjetas de crédito y débito, tiene por finalidad de entregar un aporte para el Banco reduciendo los fraudes y mitigar incidencias resultantes de operaciones a través de los cajeros automáticos (clonación) .

Actualmente se dice que el 99.9% de los casos de éstos accede a la devolución de los dineros cuando se presenta una clonación en la red de cajeros automáticos por parte de Banco Santader, pero ¿quién nos garantiza que se está cumpliendo este procedimiento? Y si es así ¿por qué no evitar que los clientes se sientan desprotegidos?

Los contenidos de este proyecto se ha estructurado de la siguiente manera:

- En el primer capítulo, se presentan los antecedentes de contexto, la empresa, y los objetivos del proyecto.
- En el capítulo II, se presentan contextos de la investigación, marco teórico y la metodología.
- En el tercer capítulo, se presenta un análisis de la situación actual y un diagnóstico del problema.
- En el capítulo IV, se justifica la propuesta de mejora.
- Y finalmente, se presentan las conclusiones del proyecto.

CAPITULO I: ANTECENTES Y OBJETIVOS

INTRODUCCION Y ANTECEDENTES GENERALES

Actualmente son evidentes lo avances tecnológicos que ha sufrido la sociedad, con ello ha traído consigo en muchos de los casos una mejora en nuestro estilo de vida, sin embargo no podemos decir que ha habido del todo un progreso ya que hablar de progreso es referirse en concreto a algo mejor y es evidente que no se cumple del todo ya que el hombre siempre ha buscado la manera de dañar a sus semejantes con el fin de obtener algún provecho generalmente económico,

Existen diversos tipos de delitos informáticos, pero en esta investigación nos enfocaremos a hablar de *clonación de tarjetas en cajeros automáticos*, un delito muy común en la actualidad. Hoy circulan aproximadamente 18 millones de tarjetas de crédito y 33 millones de débito. Expertos financieros suelen recomendarlas como una herramienta de administración de dinero, el Skimming, también conocido como clonación de tarjetas de crédito o debito, consiste en la duplicación de tarjetas de crédito o debito sin el consentimiento del dueño de la tarjeta. Los delincuentes que se dedican a esto utilizan diferentes tipos de dispositivos electrónicos que los ayudan a clonar de las tarjetas y una vez clonadas dejarlas sin fondos efectuando de este modo un estafa.

El trabajo a realizar tiene por objeto mostrar incidencias ocurridas en Banco Santander por fraude en cajeros automáticos, detallando la situación actual de la institución frente a la prevensión e información de estos, desarrollando así un sistema de mensajería instantánea la que informa automáticamente al cliente la operación realizada, esto le permite saber en forma inmediata cuándo, dónde, a qué hora y en qué cajero automático se realizó **un giro o consulta de saldo** a través de su tarjeta de crédito o débito, para así alertar al cliente de alguna operación fraudulenta sobre sus productos y además aportar una idea para combatir con astucia este delito que tanto problemas trae y que nos hace vivir con miedo a los ciudadanos.

¿Por qué este proyecto solo cubre en caso de giros, consulta de saldos y no compras?

Porque en primera instancia el delincuente a lo menos debe saber cuánto dispone el cliente para girar o para ir a comprar, y es la única forma de confirmar la clave secreta para luego hacer el paso siguiente que sería comprar. Entonces se podría decir que al

detectar el primer giro no reconocido, se puede bloquear el plástico para evitar así los próximos cargos en la cuenta.

PLANTEAMIENTO DEL PROBLEMA

Desafortunadamente, el conocimiento de los estafadores ha dado pasos en paralelo bajo la creciente globalización tecnológica a nivel mundial, perjudicando integralmente a la industria financiera nacional e internacional con ingeniosos artificios que capturan la información personal de establecimientos y tarjetahabientes en cajeros automáticos, páginas web falsas, y a través de una gran diversidad de esquemas delictivos que impactan significativamente el desarrollo interbancario y los servicios de gestión y posventa financiera de las instituciones bancarias, sin que se percaten de los inminentes efectos de la materialización de pérdidas potenciales por riesgo de fraude que recaen sobre los sistemas de operaciones de tarjetas de crédito y afectan gravemente a la competitividad.

En el contexto de la banca y las finanzas, cuando se habla de riesgo, se hace referencia a la posibilidad de pérdidas causadas por variaciones en los factores que afectan el valor de un activo; por esa razón, es importante que se identifiquen, se midan, se controlen, y se efectúe un monitoreo continuo de los diversos tipos de riesgos a los que están expuestas las instituciones financiera en lo cotidiano de sus actividades.

JUSTIFICACION

Hoy en día los fraudes por clonación de tarjeta de crédito o a la vista no está cubierta en su totalidad por parte de los seguros “fraudes”, esto debido a que en la gran mayoría de casos el banco falla en contra del cliente argumentando que éste realizó la operación con su clave vigente, sea giro, compra, transferencias o hasta consulta de saldo.

En el útlimo tiempo las instituciones bancarias, como también así el gobierno, han hecho campaña para evitar el phishing, o correo fraude, debido al aumento por este tipo, sin embargo no han hecho campaña de la misma forma sobre la clonación de tarjetas.

El robo de identidad sería uno de los puntos a explotar por los delincuentes. Muchas veces el robo de un cajero automático para un banco es un daño mínimo, debido a que existen seguros comprometidos, pero es la población la que sufre el daño más importante al generarse temor e inseguridad.

ANTECEDENTES

La clonación de las tarjetas comenzó en los 90, era limitada. Actualmente es creciente el número de usuarios de plásticos, incluso se pagan por ese medio los salarios, las misiones, jubilaciones y pensiones. Realizamos diferentes tipos de transacciones bancarias, retiro de dineros, consultas, transferencias entre cuentas, todo a través de esta tecnología.

Los fraudes y estafas cometidos con los cajeros automáticos revelan un modus operandi con alto grado de sotisficación. En la mayoría de los casos los autores de estos delitos son expertos conocedores de la tecnología informática.

HISTORIA DE LA INSTITUCION

Historia Banco:

Banco Santander Chile es una Sociedad Anónima bancaria, que se instaló en Chile el 18 de julio del año 2002, cuando se celebró la junta extraordinaria de accionistas del Banco Santiago, donde se acordó la fusión de Banco Santiago con Banco Santander Chile, para posteriormente tomar el nombre de éste último.

A través del tiempo este banco ha crecido año a año, es por ello que se mostrarán las principales aristas de la constitución de este banco, su misión, fundamento y por supuesto las áreas en las que se basa este crecimiento.

Constitución de Banco Santander:

- Comienza el 15 de mayo de 1875, cuando la Reina Isabel II firma el real decreto que autoriza la constitución del banco Santander, desde sus orígenes fue un banco abierto al exterior, inicialmente ligado al comercio.

- Con la adquisición del Banco Santander Chile en 1982 el banco entra al mercado nacional.

- A partir del año 2000 se incorpora al Grupo el Banco Santiago. Con ello se afianza la posición del grupo como primera franquicia financiera en Latinoamérica.

- En 2002 marcó un hito importante en la historia de Banco Santander Chile. En ese año Santander Central Hispano adquirió al Banco Central de Chile con un 35% de las acciones de Banco Santiago. En consecuencia, la institución hispana pasó a controlar el 78,95% de los títulos de esa entidad. Como adicionalmente poseía el 89% del capital del ex Banco Santander Chile, decidió proponer la fusión de ambas instituciones financieras en la medida que ella añadiera valor para todos los accionistas. La evaluación de los términos para intercambiar las acciones de los dos bancos constituyentes fue encomendada a dos bancos de inversión de primer nivel. Estas entidades utilizaron varios parámetros para valorizar ambos bancos y en base a un promedio de estos valores, se determinó la razón de intercambio justa. En definitiva, en las respectivas Juntas de Accionistas se aprobó la fusión por absorción entre los Bancos Santander Chile y Santiago, entidades que ponderarían 47,5% y 52,5%, respectivamente, dentro del capital del banco resultante. Tras contar con todas las autorizaciones pertinentes, el 1º de agosto hizo su debut en la banca nacional el nuevo Banco Santander Chile, una de las instituciones más importantes y rentables en América Latina.

  Hasta hoy, es la mayor financiera del país, con una participación de Mercado del 20.9% y con una red de distribución que cubre de Arica a Punta Arenas.

En las últimas décadas ha experimentado profundas transformaciones, adecuándose al nuevo escenario financiero del siglo XXI, para así seguir cumpliendo con su rol en forma moderna, competitiva, rentable y con bajo riesgo.

FILOSOFIA INSTITUCIONAL

Visión

Ser un actor de primera línea en el mercado financiero chileno y un banco de referencia en Latinoamérica, que anticipe tendencias, ofrezca soluciones creativas y únicas, que constituyan una respuesta de calidad a los requerimientos de nuestros accionistas, clientes, empleados y de la sociedad en su conjunto. Con nuestra gestión contribuiremos fuertemente al desarrollo económico del país y al progreso de las personas.

Valores

Ser una Organización de referencia en cada uno de los mercados en la que estamos presentes. Tenemos vocación de liderazgo, valor a nuestros clientes, accionistas y colaboradores.

ANALISIS ESTRATÉGICO

Fortalezas

- Posición de liderazgo en el mercado.
- Importante monto de obligaciones con vencimientos programados, lo que disminuye el impacto de retiros inmediatos producto de un entorno incierto.
- Amplia red de distribución, con sucursales y oficinas en las principales ciudades del país que le han permitido acceder a su mercado objetivo y disminuir el riesgo por concentración geográfica.
- Diversidad en la colocación de sectores productivos.

- Planta de ejecutivos con experiencia, proactivos y ocupando cargos enfunción de sus capacidades.
- Nivel tecnológico y administración de su riesgo operativo.

Riesgos

- Las condiciones de un entorno que mantiene alta incertidumbre puede incidir en un incremento del riesgo de la cartera, lo cual requiere que la entidad continúe trabajando en la optimización de los procedimientos de control de riesgos y criterios de otorgamiento y administración de créditos.
- Vale indicar que este riesgo se ve mitigado por la estabilidad de los depósitos y por los altos niveles de sus activos líquidos.
- Concentración geográfica, dado el mayoritario porcentaje de sus colocaciones que se encuentran; las cuales son las más importantes del país y concentran la mayor cantidad de habitantes que desarrollan múltiples actividades.

OBJETIVOS DEL PROYECTO

OBJETIVOS GENERALES

Fidelizar a los Clientes de Banco Santander, para lograr que se sientan confiados, satisfechos y seguros de un banco que lo mantiene informado de sus cuentas, utilizando un diseño de soluciones tecnológicas que cubrirá las necesidades actuales en el área de manejo de información en tiempo real, a través de la mensajería de texto celular o vía email.

OBJETIVOS ESPECIFICOS

- Combatir los delitos en cajeros automáticos, prevenir el robo de identidad y reducir el fraude.

- Realizar mejoras en la red de cajeros automáticos con el diseño de tecnologías seguras para que nuestros clientes puedan estar tranquilos y puedan tener registro de la transacción realizada instantaneamente.

- Proveer de soluciones tecnológicas a las necesidades del cliente con el uso de sistemas de información masiva, como lo son mensajes de texto celular o SMS, utilizando los estándares de comunicación implementados por las diferentes operadoras de redes móviles a nivel Nacional e Internacional.

CAPITULO II: MARCO METEODOLÓGICO

METODOLOGIA DE LA INVESTIGACION

CARACTERISTICAS GENERALES

La investigación es un estudio de caso, que será realizado en forma mixta: cualitativa y cuantitativa. Se analizarán datos de fuentes primaria, en el área de riesgos de Banco Santander para realizar un análisis de datos sobre las incidencias de este tipo de fraude, y como fuente secundaria información obtenida de literatura para referencias, páginas internet de bancos, entidades emisoras y organismos que realizan estudios y encuestas para así obtener las condiciones internas y externas, y de esta manera justificar la propuesta.

Fuentes primarias: Información de cantidad de denuncias por fraudes (clonación), casos de reclamos de cliente en un período, tipos de dispositivos que ayudan a clonar tarjetas.

Fuentes secundarias: Información obtenida de la literatura, de tesis publicadas, testimonios de clientes que sufrieron este tipo de fraudes , como también encuestas para saber los beneficios que conlleva este proyecto.

Para desarrollar la metodología de este proyecto, fue necesario basarse en el principio *Benchmarkingfuncional o genérico*,quiere decir, tomar como referencia los mejores aspectos de lo que hay en el mercado, y en este caso incluir un servicio de un Banco de Venuezuela llamado Banco Venezolano de Crédito que cuenta con el servicio

de una importante empresa líder en el mercado **TotalTexto**, que fue creada para evitar fraudes bancarios y mantener alertas a los clientes entregando soluciones tecnológicas a la Banca.

El Banco Venezolano de Crédito fue la primera entidad bancaria en usar los servicios de notificación de transacciones de Totaltexto, empresa que se inició en el 2005 orientado a ayudar a disminuir y a prevenir el fraude con las tarjetas.

Este tipo de notificaciones fueron muy bien recibidas por parte de los clientes y contribuyeron a reforzar la imagen de las entidades bancarias, como también ayudó a Totaltexto a expandirse y entrar en otro Bancos como Banesco, Mercantil, Provincial, entre otros, para consolidar la presencia de ésta.

PROCEDIMIENTO ACTUAL EN CHILE AL OPERAR POR ATM

Cuando una persona natural realiza una operación en cajeros automáticos, por ejemplo un giro, consulta o transferencia, queda registrado inmediatamente en sus movimientos de la cuenta de origen (Cta. Cte. O T.Crédito), el cual se puede consultar o verificar desde el portal personal a través de internet o directamente en la cartola que el banco proporciona al cliente. Sin embargo, esta consulta no necesariamente es periódica por parte del cliente, por lo tanto existe una rango de tiempo donde éste desconoce si se cargó o no a su cuenta, en general siempre es así, pero el cliente se entera cuando el consulta.

El banco cuando se realiza transferencia a través del portal personas, envía automáticamente un mail al correo del titular e interesado si se ingresa, pero no cuando uno gira.

MODELO EXTRANJERO Y SOLUCIONES

Hoy en Venezuela se envían 170 millones de SMS al año producto de las transacciones bancarias que hacen los usuarios. La contribución que ha tenido la compañía para la efectividad de las cobranzas ha sido superior al 80% y dicen haber capturado más del 80% de las transacciones de banca SMS en su principal mercado que es el venezolano, ya que cuentan con oficinas y operaciones en Colombia, Panamá y pronto en Chile.

Cada vez que se recibe una notificación vía mensaje de texto, de algún movimiento bancario que ha hecho desde la cuenta **Banco Venezolano de Crédito** sobre algún consumo o compra que realizó desde un punto de venta o un retiro desde un cajero automático, por detrás está TotalTexto.

Esta empresa venezolana desde 2005 está dedicada al desarrollo de soluciones tecnológicas y al servicio de interconexiones de alto rendimiento con las operadoras móviles, orientada a cubrir las necesidades de clientes en el área de seguridad y manejo de información en tiempo real, ya que en menos de cinco segundos, aseguran sus ejecutivos, un usuario de la banca venezolana recibe su notificación a su teléfono celular Smartphone o terminal que cuente con plataforma Java.

La información fue suministrada por Jordán Dávila, líder del departamento de comercialización de la compañía quién junto a Jorge Falcón, director de Desarrollo Tecnológico y Darwin Morales, director de Tecnología, explicaron las contribuciones de TotalTexto hasta la fecha en las soluciones móviles para el sector bancario. Soluciones que van desde el proveer a las entidades bancarias de un sistema de monitoreo inteligente que les permita detectar de manera temprana cualquier movimiento que no sea ejecutado por los usuarios y deba ser notificado en tiempo real hasta la gestión de cobranzas de la entidades financieras. “Hoy en día somos responsables de la automatización de las cobranzas de todos nuestros clientes de la banca en el sentido de que cualquier notificación de estados críticos de pago o notificación de la cobranza de un instrumento financiero como tarjeta de crédito o un producto hipotecario, crédito a un vehículo, esas notificaciones de pago están siendo notificadas a través de SMS”.

En este sentido y en el país, la contribución que ha tenido TotalTexto para la efectividad de las cobranzas ha sido superior al 80%, al día de hoy se envían anualmente 170 millones de SMS, producto de las transacciones bancarias que hacen los usuarios y dicen haber capturado más del 80% de las transacciones de banca sms en su principal mercado que es el venezolano.

Hoy TotalTexto cuenta con presencia física y oficinas propias en Bogotá y Panamá y planean abrir operaciones en Chile producto de un acuerdo de colaboración con Visa que abarca el Cono Sur, Chile, Paraguay, Argentina y Uruguay para el servicio de notificación de transacciones a usuarios de plásticos Visa.

Totaltexto

VENEZOLANO DE CREDITO

MARCO TEORICO

CARACTERISTICAS PRINCIPALES

El fraude en tarjetas de crédito o débito es una de las más grandes amenazas a nivel mundial que recae y cuesta a titulares, establecimientos y emisores de las tarjetas; en términos generales, este tipo de fraude puede ser definido como.

"El uso de la tarjeta por parte del individuo sin que el portador de la tarjeta original, la entidad emisora esté consciente de que está siendo empleada ilícitamente y en la que no existe el compromiso por parte del defraudador en rembolsar los pagos de los débitos efectuados en la cuenta de la víctima[1]"

MARCO LEGAL DE LAS TARJETAS DE CREDITO Y DEBITO

Mediante el art. 5º de la Ley Nº 20.009, de 1 de abril de 2005, se introdujeron al derecho chileno varios tipos penales relativos al uso de tarjetas de crédito y débito y a las claves asociadas a las mismas, dando lugar a una serie de arduas cuestiones interpretativas.

1. Clonar una tarjeta de crédito implica obtenerla información que contiene su banda magnética y copiarla en otra tarjeta para cometer ilícitos.

   Respecto a la regulación de la conducta típica, este es un delito que infringe las leyes N°19.233 y N° 20.009 por delito informático y uso fraudulento de tarjetas de crédito y débito, respectivamente.

   Existen muchas formas diferentes a través de las cuales se comete este delito. Una de ellas es la utilización de una máquina con un chip que permite copiar la información de las bandas magnéticas, ubicadas en la puerta de cajeros automáticos, en los cajeros y receptores de compra en red. Luego, los datos se traspasan a un computador y son copiados a una tarjeta virgen. No obstante, a medida que las medidas de seguridad van aumentando, también los delincuentes realizan un up grade en las tecnologías para vulnerar los datos.

[1] Persona que se expone u ofrece a un grave riesgo en obsequio de otra.

2. La Ley N° 20.009 castiga el delito de uso fraudulento de tarjetas de crédito o débito con presidio menor en cualquiera de sus grados. Y se aplica en su grado máximo si la acción realizada produce perjuicios a terceros. Además, la Ley N° 19.223 establece la pena de presidio menor en su grado mínimo a medio para quien con ánimo de apoderarse, usar o conocer indebidamente la información contenida en la tarjeta, la intercepte, interfiera o accede a ella.
La clonación de tarjetas de crédito constituye lo que la doctrina jurídico penal considera un delito de falsificación de documento privado mercantil. Dicha clase de falsificación se encuentra regulada en el Código Penal, geográficamente en el Libro II, Título IV "De los crímenes y simples delitos contra la fé pública, de las falsificaciones, del falso testimonio y del perjurio"

   La disposición que contempla específicamente dicha materia se encuentra en el artículo 197 de dicho cuerpo legal, el cual señala: "El que con perjuicio de tercero, cometiere en instrumento privado alguna de las falsedades designadas en el artículo 193, sufrirá las penas de presidio menor en cualquiera de sus grados y multa de once a quince unidades tributarias mensuales, o sólo la primera de ellas según las circunstancias. Si tales falsedades se hubieren cometido en letras de cambio u otras clases de documentos mercantiles, se castigará a los culpables con presidio menor en su grado máximo y multa de dieciséis a veinte unidades tributarias mensuales, o sólo con la primera de estas penas atendidas las circunstancias".

   Por su parte el artículo 193, también del Código Penal, señala: "Será castigado con presidio menor en su grado máximo a presidio mayor en su grado mínimo el empleado público que, abusando de su oficio cometiere falsedad:

   1°Contrahaciendo o fingiendo letra, firma o rúbrica.
   2°Suponiendo en un acto la intervención de personas que no la han tenido.
   3°Atribuyendo a los que han intervenido en él declaraciones o manifestaciones diferentes de las que hubieren hecho.
   4°Faltando a la verdad en la narración de hechos sustanciales.
   5°Alterando las fechas verdaderas.

6°Haciendo en documento verdadero cualquiera alteración o intercalación que varíe su sentido.
7°Dando copia en forma fehaciente de un documento supuesto, o manifestando en ella cosa contraria o diferente de la que contenga el verdadero original.
8°Ocultando en perjuicio del Estado o de un particular cualquier documento oficial.

De tal forma, se puede aseverar que así como el artículo 193 limita estas conductas al actuar de funcionarios públicos, el art. 197 extiende la posibilidad de ser sujeto activo del delito a cualquiera que cometa alguna de las conductas descritas en el artículo 193, señalando además que constituye una agravante el hecho de que la falsificación recaiga en letras de cambio u otra clase de documentos mercantiles.

3. De la sencilla lectura de los artículos mencionados, es posible concluir que por la simple copia o adulteración ya sea de la tarjeta de crédito en sí misma o de la banda magnética de ésta (por cualquiera de los métodos desarrollados como el mecanismo de clonación) se estaría contraviniendo el artículo 197 en relación con el artículo 193 en el numeral sexto.

   En dicho punto es necesario hacer la siguiente observación, la ley 20.009 establece en su artículo quinto que la pena para la falsificación de tarjetas de crédito será la de presidio menor en cualquiera de sus grados, agregando a continuación que la pena se aplicará en su grado máximo si la acción realizada produce perjuicios a terceros. No obstante el Código Penal señala en el ya referido artículo 197, que si las falsedades se hubieren cometido en letras de cambio u otras clases de documentos mercantiles, se castigará a los culpables con presidio menor en su grado máximo y multa de dieciséis a veinte unidades tributarias mensuales, o sólo con la primera de estas penas atendidas las circunstancias.

   Claramente aquí se observa una incongruencia, pues la sanción establecida en el Código Penal es mayor que la impuesta por la ley 20.009. Si se aplicaran las normas señaladas podría enfrentarse ante el siguiente problema: para el caso que un sujeto clonara una tarjeta de crédito, es decir, se encuentre consumado el delito de falsificación, pero no alcanzó a utilizarla en el comercio (no se ha consumado la

estafa) y por ende no hay perjuicios a terceros, aplicando el principio de la especialidad, correspondería ser sancionado conforme a la ley 20.009, es decir, con la pena de presidio menor en cualquiera de sus grados, por tanto, el tribunal podría sancionar con presidio menor en su grado mínimo. Por otra parte, si el sujeto falsifica una letra de cambio, aplicando el inciso segundo del artículo 197, sufrirá la pena de presidio menor en su grado máximo y multa de dieciséis a veinte unidades tributarias mensuales según las circunstancias.

De la comparación de dichos artículos está clara que en ambos se exige el perjuicio a terceros para llevar la pena de presidio menor en su grado máximo, sin embargo la clonación de tarjetas de crédito no lleva aparejada una sanción pecuniaria, por lo tanto se puede concluir que la norma que regula dicha materia es más benevolente para los clonadores de tarjetas de crédito, que la falsificación regulada por el código penal, lo cual no nos parece tener una respuesta lógica.

4. La gravedad del delito y a los diversos bienes jurídicos que se ven afectados por la comisión del mismo, consideramos que la pena establecida en la Ley Nº 20.009, no es suficientemente severa en proporción al daño que el hecho punible genera; no solo en el usuario de una tarjeta de crédito clonada sino a la sociedad en general, la cual se percibe en la actualidad preocupada por la falta de seguridad en el tráfico jurídico al utilizar sus tarjetas de crédito como medio de pago de bienes y servicios".

CAPITULO III: SITUACION ACTUAL Y SOLUCIONES

FRAUDES EN TARJETAS

El fraude en tarjetas de crédito es una de las más grandes amenazas a nivel mundial que recae y les cuesta a titulares, establecimientos y emisores de las tarjetas cientos de millones de dólares por año.

<u>Esquemas de Fraude</u>

Debido al constante cambio de las tecnologías de la información, esto ha originado que se propaguen diversas alternativas para que los falsificadores usen métodos sofisticados para perpetrar un fraude.

- **Extravío o robo de Tarjetas**: Una tarjeta es extraviada cuando el tarjetahabiente original reciba su tarjeta de crédito y la pierde; y robada cuando un delincuente extrae la tarjeta y la usa de manera fraudulenta para comprar bienes o servicios de un negocio afiliado legítimo.

- **Tarjeta no presente:** Este crimen se basa en el robo de los datos de una tarjeta de crédito, la cual es usada para hacer una compra a través de un canal remoto como el teléfono. Como todo fraude, el dueño legítimo de la tarjeta no puede estar advertido de este fraude hsta que verifiquen su estado de cuenta.
  El problema para contrarrestar este tipo de fraudes reside en el hecho que ni la tarjeta ni el tarjetahabiente necesitan estar presentes en el punto de venta. Esto significa que los Comercios de Tarjetas no presentes no pueden revisar las características de seguridad física de la tarjeta para determinar si es genuina. Sin una firma o el PIN no es fácil confirmar que el cliente es el dueño de la tarjeta.Los emisores de tarjetas no pueden garantizar que la información entregada en un entorno le pertenezca al tarjetahabiente.

- **Robo de identidad:** El robo de identidad en tarjetas ocurre cuando el criminal usa información personal obtenida fraudulentamente para abrir o acceder a cuentas de tarjetas de crédito en nombre del usuario original; existen dos tipos de esquemas bajo esta modalidad y son:

  Fraude aplicado:Este fraude lo aplican criminales cuando documentos robados o falsos para abrir una cuenta en nombre de alguien más. Los criminales roban documentos como estados de cuentas para entrar al fraude. Alternativamente ellos usan documentos clonados para propósitos de identificación.

Toma de Cuentas: Los criminales toman posesión de la cuenta de otra persona.Primero consiguen información de la víctima.El criminal contacta al emisor presentándose como el genuino tarjetahabiente para que redirecciones sus datos a una nueva cuenta de correo.El criminal reporta la tarjeta como pérdida y pide que se la envíe un duplicado de la misma.Las formas más comunes se posesionarse de una cuenta ilegalmente son las mencionadas a continuación:

Phising & Pharming: Es una conocida técnica para obtener información confidencial de un usuario que consiste en enviar una cantidad enorme de mensajes por correo electrónico haciéndole creer al consumidor que los mensajes vienen de un banco, tratando de conseguir que la víctima potencial revele su información personal.

Con ayuda de un troyano, también es posible infiltrarse en la conexión entre la dirección IP y el nombre del servidor al que corresponde, esto se llama Pharming.

- **Falsificación o Clonación de Tarjetas**:Una tarjeta falsificada (clonada) es una tarjeta impresa, embozada o codificada sin permiso del emisor, o una que ha sido válidamente emitida y después alterada o recodificada. La mayoría de los casos de fraude por falsificación proviene de la información genuina de la tarjeta situada en la banda magnética de la misma, la cual es electrónicamente copiada en otra tarjeta a espaldas del legítimo tarjetahabiente.

  Después vende la información a nivel criminal mas alto en donde las falsificaciones son cometidas. En otros casos los datos obtenidos por clonaciones son usados para transacciones online. La mayoría de los tarjetahabientes no están advertidos del fraude hasta que llegue su nuevo estado con giros que ellos no hicieron.

  Tipologías relacionadas a este esquema delictivo son:

  Tarjeta alterada en el realce*:* Generalmente es utilizada en transacciones manuales, con plásticos originales deteriorando además la banda

magnética para obligar al comercio a que se realice con la máquina *imprinter o rastrilladora.*

Cualquier senal de manipulación del plástico como variación en la forma de los dígitos, pérdida de brillo del holograma, opacidad son indicios primarios de una tarjeta adulterada y se la puede presentar acompañada de una cédula falsa o auténtica.

Skimming & Scanning: Esquema de fraude que se realiza a través de ATMs, el delincuente copia o escanea la información financiera o personal de la tarjeta de crédito o débito de la víctima y luego la regraba en una tarjeta falsa, creando así una réplica que tiene los mismos alcances y limitaciones que su tarjeta personal.

Para llevar a cabo el fraude el delincuente utiliza un pequeño aparato denominado *skimmers* que se instalan en la ranura del ATM y que al momento que se inserte una tarjeta, copia inmediatamente su información, mientras un cómplice o el mismo estafador, se posiciona de tal manera que se puede percatar de los números del PIN y así al momento que la víctima abandona el cajero de su entidad bancaria, el criminal retira sus fondos con la tarjeta clonada.

A menudo, el tarjetahabiente no está consciente del fraude hasta que su estado de cuenta es entregado y muestra los giros que ellos no hicieron.

ANTECEDENTES GENERALES DE FRAUDE

Este proyecto está enfocado a la prevención de fraudes que afectan a los clientes Banco Santander. Para esto, a modo de muestra, se expondrá casos recientes de fraude y la estadística de fraude en la industria.

FRAUDES A NIVEL DE AMERICA DEL SUR

A nivel de nuestra región, se realizó en el año 2008 un índice de percepciones de corrupción y fraude de Transparencia Internacional, con una escala de calificaciones de 0 a 10, esto mide el nivel de corrupción percibido en cada uno de los países clasificados. Como se ve claramente, Chile obtuvo una calificación de un 6.9, esto nos indica que es

uno de los países menos corruptos de la zona, pero no deja de ser problemático, ya que la corrupción en nuestro país genera daños a largo plazo a las empresas, aumentando los costos en su operación:

Analizaré los índices de corrupción desde el año 2008 para Chile realizados por Transparencia Internacional.

Pais	2002	2003	2004	2005	2006	2007	2008	2009
Estados Unidos	7.6	7.7	7.5	7.6	7.3	7.2	7.3	7.5
Chile	7.5	7.5	7.4	7.3	7.3	7	6.9	6.7
Mexico	3.6	3.6	3.6	3.5	3.3	3.5	3.6	3.3
Brasil	4	3.9	3.9	3.7	3.3	3.5	3.5	3.7
Argentina	2.8	2.5	2.5	2.8	2.9	2.9	2.9	2.9

Tabla 1: Indice de corrupción y fraudes (Transparencia Internacional)

[2]

Se observa que Chile tiene índices de corrupción que han ido aumentando desde el año 2002, esto tiene una directa relación con la ocurrencia de fraudes en las empresas, esto es un factor importante a considerar, además de forma esencial deben entregar herramientas a nuestros clientes, para así reducir estas incidencias, evitando perdidas a las empresas, en este caso a Banco Santander.

FRAUDES EN CHILE

Se sabe que los fraudes son realizados por terceros no autorizados. Se verá que estos tipos de ilícitos, donde se muestra que el fraude con tarjetas (15%),es seguido por la documentación falsa (23%).

En este caso el perjuicio promedio económico fue de $912.000.000 al año 2009[3].

[2] Tabla desarrollada en base a datos obtenidos desde Transparencia Internacional

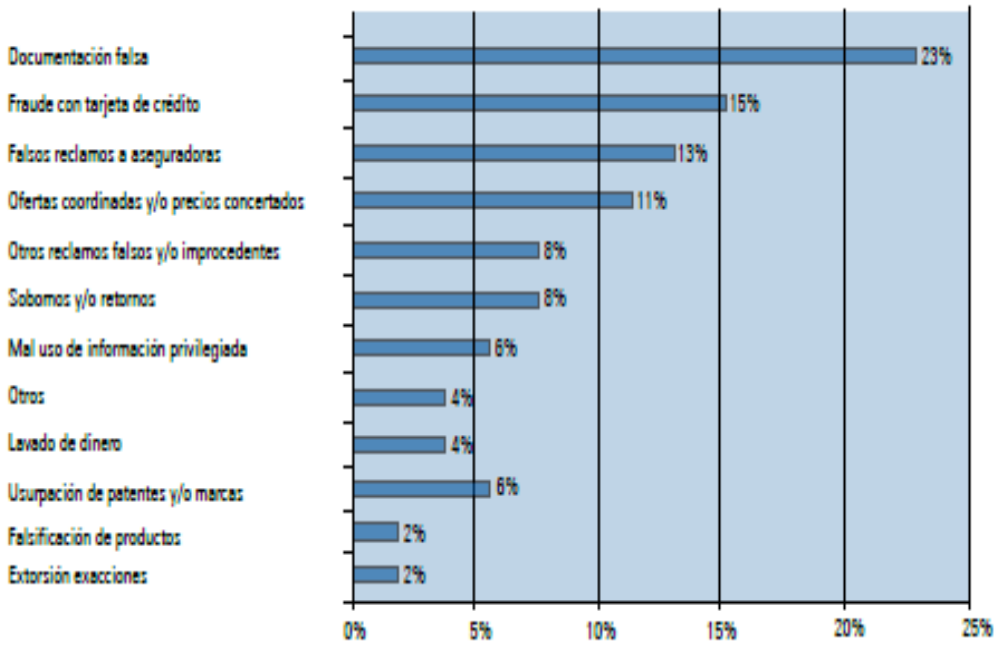


Ilustración 1: Fraudes cometidos en entidades financieras

Los fraudes tienen repercusiones mas profundas que el delito en sí, provoca problemas en el clima laboral, daño a la imagen corporativa, y lo más importante, la confianza de los clientes al momento de elegir una institución financiera.

También causa daño a la empresa ya que se pierde la fidelidad de los clientes al haberse sentado el precedente de que estos delitos ocurren constantemente.

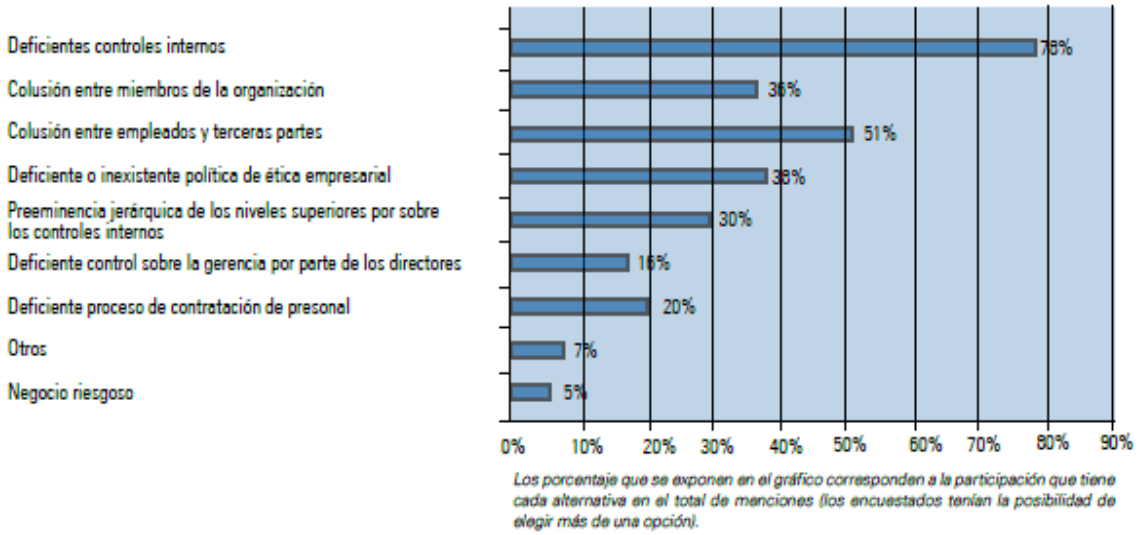


Ilustración 2: Condiciones que incentivan el fraude

[4]

A continuación se observará qué es lo que incita a la ocurrencia del fraude, y se puede observar claramente que la falta de controles internos con una frecuencia de un 78% tiene una directa correlación los mecanismos mas efectivos para controlar estos delitos, ya que, con una mejora de este monitoreo inteligente ayuda a detectar en tiempo real este tipo de fraude.

[4] KMPG en Chile (2009).”Encuesta de Fraude y Corrupción en Chile 2009”.

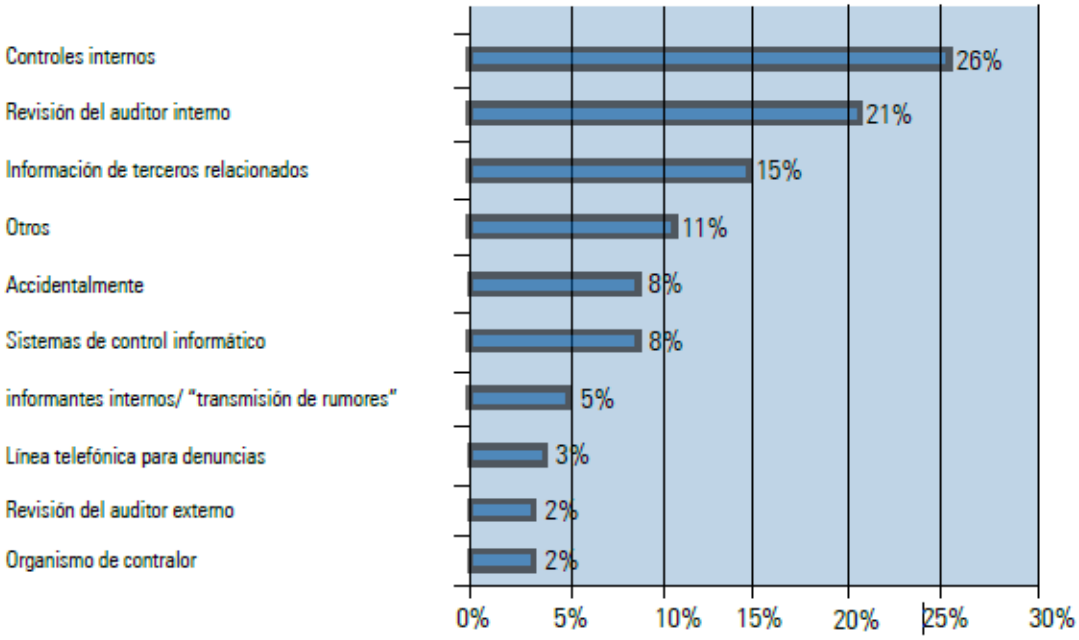


Ilustración 3: Mecanismos de detección de fraude

Según la información recopilada para este proyecto, hoy poy hoy es un problema importante que necesita ser revisado y la propuesta de mejora planteada es una buena alternativa.

El punto débil de la seguridad de las tarjetas de crédito son las bandas magnéticas, pues es allí donde van recogidos los datos del titular de la tarjeta, por la misma razón se piensa implementar una nueva tecnología “el chip inteligente”, que es más difícil vulnerar por parte de los delincuentes, que ha sido adaptado en la actualidad por muchos países, pero no en su totalidad, lo que provoca que los clonadores se instalen en Chile y en los países que aún no hayan optado por esta nueva tarjeta.Esta iniciativa, debiera lanzarse el próximo año y alcanzar una penetración de 100% en año 2014, que apunta a poner fin a la clonación de tarjetas, pero ¿quién nos dice que con el chip inteligente no podrá ser descifrado por los clonadores en un tiempo más?

REACCIONES ANTE UNA DETECCION DE UN FRAUDE

Son fundamentales para solucionar el problema y evitar futuros ilícitos. Este tipo de medidas deben ser consideradas con cuidado, pues una empresa que no realiza una investigación profesional, corre el riesgo de dañar o borrar evidencia esencial para fijar responsabilidades al presunto defraudador o, por lo menos, exigirle el resarcimiento del daño causado. Peor aún, una investigación que no se realiza profesionalmente puede ocasionar que la empresa nunca se entere sobre qué esta fallando en la organización o qué tipo de controles internos son los que necesita realmente y, por tanto, disminuir la probabilidad de padecer un nuevo ilícito en el futuro.

De hecho el 45% de quienes respondieron, afirmó que solicitaría servicios para la prevención y/o detección de fraudes a especialistas en la materia.

ACCIONES TOMADAS ANTE UN FRAUDE

De igual forma, el despido del presunto responsable del ilícito debe estar antecedido por una investigación profesional que explique qué paso, si actuó realmente solo o estuvo coludido con alguien y por qué fallaron los controles internos establecidos.

Además, contar con una investigación profesional sobre el fraude cometido ayuda a que la empresa no sea contra demandada por presunto despido injustificado y, en términos de aprendizaje organizacional, le da la oportunidad a la empresa de valorar la vulnerabilidad de sus procedimientos de trabajo, la lealtad de sus empleados y la eficacia de su contraloría.

Otro aspecto importante observado en este estudio es que tan sólo un 2% de las empresas que han detectado un fraude deciden implementar o corregir sus controles internos. Este es un dato muy serio que nos habla de la irresponsabilidad con que muchas empresas se conducen en materia de control de riesgos.

Organizaciones que sencillamente no hacen ningún tipo de ajustes a sus controles, una vez que han sido defraudados, son presa fácil para un nuevo ilícito. El fraude, como la corrupción, es un delito que comienza como un acto aislado y casi

imperceptible, que al ir probando su efectividad se va repitiendo en el tiempo, hasta alcanzar dimensiones más graves. Si la empresa que ha detectado un desfalco no reacciona a tiempo y aprende de los errores cometidos, está condenada a seguir padeciendo este tipo de ilícitos.

MODUS OPERANDI

¿ COMO SE CLONA UNA TARJETA DE DEBITO O CREDITO?

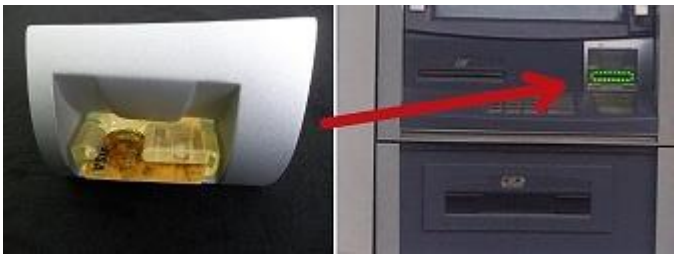
A continuación se presentará, cómo se realiza la clonación en cajeros automáticos:

El delincuente tiene en su poder un Skimmer de bolsillo (utilizado para leer y guardar la información de la tarjeta).

1. El dispositivo es instalado en un cajero automático o si el sujeto trabaja en una tienda, espera a que un cliente vaya a pagar y pasa la tarjeta tanto por el punto de venta como por el Skimmer(esta acción sólo toma 4 segundos).

2. Con los datos ya almacenados el malhechor va a su casa, conecta el Skimmer a una computadora y descarga la información.

3. Finalmente, el infractor utiliza una tarjeta en blanco con cinta magnética y la pasa por un codificador de tarjetas de créditos. Esto con el fin, de pasar la información desde la computadora hasta la tarjeta en blanco.



Además de clonar, el sujeto podría llegar hasta falsificar su cédula de identidad sino posee un cómplice dentro de un local comercial. Sin embargo, si el victimario sólo quiere realizar compras por internet, y no duplicar tarjetas fisicamente, llegaría solamente hasta el paso número tres.

TECNOLOGIAS MAS COMUNES PARA CLONAR TARJETAS EN ATMs[5]

[5] Estas imágenes fueron capturadas al interior de Sucusal Banco Santander de Isidora Goyenechea - Las Condes, donde se detectó clonador, son aparatos sofisticados para copiar tarjetas, y una cámara que grababa la clave al ser digitalizada.

CASO DE CLONACIONES

PRIMER CASO

A continuación, se mostrará el caso de un cliente que realiza el reclamo a la entidad bancaria correspondiente por clonación en cajero automático, y ésta falla contra cliente.

reclamos.cl
Neutralidad, Responsabilidad y Transparencia

SANTANDER- CLONARON MI TARJETA Y BANCO SE NIEGA A RESPONDER.

Jueves 07, Junio 2012, Número de Reclamo: 211424

Hace aproximadamente un mes, sufrí una clonación a mi tarjeta bancaria y me robaron toda la plata que tenía en ella. Reclamé al banco y me dijeron que mi caso iba a ser investigado. Luego de unas semanas, la respuesta de ellos fue que "se hizo un giro con una tarjeta válida y nunca hubo error en la introducción de la contraseña secreta". Apelé al resultado del caso y me volvieron a decir exactamente lo mismo. Hablé con SERNAC y me dijeron que era absolutamente ilegal lo que estaban haciendo, así que ahora quiero buscar a más gente que le haya pasado lo mismo para interponer una demanda colectiva a través de SERNAC.

Publicado por: IP 200.86.211.252
Jueves, Junio 7, 2012 - 19:26

SEGUNDO CASO

En el caso siguiente, se muestra a un cliente que deja la documentación en sucursal, para dejar constancia de la clonación ocurrida en 3 días (contablemente el 25/06/2012) para que posteriormente el Banco realice la investigación con el fin de que devuelva el monto reclamado.Además relata los hechos de cómo y cuando se percató de estos giros no reconocidos.

Santander

FORMULARIO ÚNICO DE RECLAMOS DE TARJETAS PARA TRANSACCIONES NO RECONOCIDAS POR EL CLIENTE Y DENUNCIA DE SINIESTRO SEGURO FRAUDE

(FORMULARIO VÁLIDO COMO: FICHA DE RECLAMO / CARTA RELATO DE LOS HECHOS / DECLARACIÓN JURADA)

I.- IDENTIFICACIÓN DEL CLIENTE:

APELLIDO PATERNO	APELLIDO MATERNO	NOMBRES	RUT
Schulz	Ogaz	Alfredo Christian	15.190.897-2
TELEFONO PARTICULAR	**TELEFONO COMERCIAL**	**CELULAR**	**CIUDAD**
		08-26579198	Santiago
DOMICILIO		**E-MAIL**	**FECHA DEL RECLAMO**
Jorge Matte Gormaz 2462 Depto 305		acschulz@uc.cl	25/06/2012

IMPORTANTE: SI LAS TRANSACCIONES RECLAMADAS CORRESPONDEN A TARJETAS DE CREDITO Y/O DEBITO DIFERENTES, DEBE LLENAR UN FORMULARIO POR CADA TARJETA.

II- IDENTIFICACIÓN TARJETA Nº: 589710 5001086168 29

TIPO DE TARJETA		DEBITO		MASTERCARD		VISA		AMEX
	X							

III.- CLASIFICACION DE TRANSACCION(ES) RECLAMADA(S):

X	AVANCE NO CORRESPONDE		COMPRA ANULADA		COMPRA DUPLICADA		RESERVA ANULADA
	COMPRA NO CORRESPONDE		MERCADERIA NO RECIBIDA		CREDITO NO PROCESADO		PAGO POR OTRO MEDIO
	ROBO / HURTO		PERDIDA / EXTRAVÍO		OTRO		

IV. TRANSACCIONES RECLAMADAS:

Nº TOTAL DE TRANSACCION(ES) RECLAMADA(S)	7	MONTO TOTAL RECLAMADO $	$795.463.-	MONTO TOTAL RECLAMADO US$	

NOMBRE ESTABLECIMIENTO COMERCIAL	FECHA (DD-MM-AA)	MONTO($ / US$)	NAC	INT	NORMAL	CUOTAS	PAT
Giro en Cajero Automático	25 06 2012	$132.849					
Giro en Cajero Automático	25 06 2012	$66.415					
Giro en Cajero Automático	25 06 2012	$132.277					
Giro en Cajero Automático	25 06 2012	$66.139					
Giro en Cajero Automático	25 06 2012	$198.902					
Giro en Cajero Automático	25 06 2012	$132.599					
Giro en Cajero Automático	25 06 2012	$66.302					

V.- RESEÑA DEL EVENTO / RELATO DE LOS HECHOS (LETRA IMPRENTA Y LEGIBLE)

El motivo de este reclamo es por giros en cajeros automáticos que se realizaron con fecha posterior al día 20 de junio del 2017. Ese día fue el último día que realicé un giro en un cajero automático, por la suma de $17.000.- Con fecha 25 de junio, revisé mi cartola de mi cuenta corriente por internet y me percaté que se realizaron siete transacciones que yo no realicé, las cuales se describen en la página anterior

VI.- USO EXCLUSIVO PARA CLIENTES CON RECLAMOS INTERNACIONALES

Tarjeta Involucrada:	Titular :		Adicional :	
Indicar Si estuvo en el extranjero:	Si :		No :	X
Fechas de Permanencia:	Desde :		Hasta :	
Indicar País(es)				
Indicar Ciudad(es)				

SOLO

Si analizamos éste, podemos observar que solo en un fin de semana, pudieron realizar 6 giros haciendo un total de $795.463, entonces ¿Por qué no detener que sigan realizando giros , y minimizar las pérdidas tanto para el cliente como para el Banco?

CAPITULO IV: COSTOS INCURRIDOS EN EL PROYECTO

PERDIDAS MONETARIAS

A continuación se presentará los costos que incurren por la inversión de implementar la mejora en el diseño de monitoreo de las tarjetas de crédito y débito, como también se mostrará el porcentaje de incidencias por este tipo de fraudes.

Banco Santander cuenta en promedio con 3.5 millones de cliente a lo largo de todo el país, cubriendo el territorio nacional con 499 sucursales. Para este análisis se consideró la cantidad de reclamos por clonación que llegaron a una sucursal del sector oriente, las cuales se compararon con otras del mismo sector quienes entregaron un promedio de 3 reclamos mensuales por sucursal. Si a lo anterior, decimos que el 85% de sucursales son quienes reciben este tipo de reclamos, sin considerar las sucursales ubicadas en zonas extremas tales como Punta Arenas, Isla de Pascua, Puerto Aysen, etc. tenemos un total de 424 sucursales, vale decir 17.384 reclamos al año por concepto de fraudes de clonación. Si por cada tarjeta clonada se realiza en promedio 3,2 operaciones, tenemos un total 55.629 compras y/o giros fraudes hechos, los cuales corresponden a un 0,05% del total de transacciones anuales que se realizan con estos productos del banco,

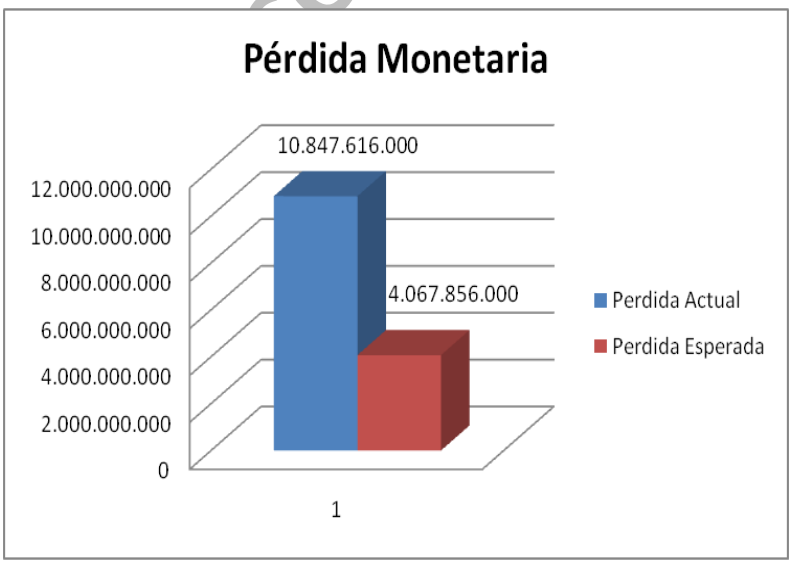


Ilustración 4 : Reporte pérdidas monetarias año 2011

dado este resultado, se tiende a creer que la cantidad de operaciones por fraude son mínimas, sin embargo este porcentaje reporta pérdidas para el banco, el cual responde en su gran mayoría como fraude, un total aproximado de $10.847 millones de pesos al año. (Ilustración 4)

PROYECTO DE INVERSION

Dado a que este proyecto de inversión no margina por concepto de ventas, el impacto al que se enfoca éste, es a reducir considerablemente la cantidad de pérdida monetaria por clonación la que bordea el 60%, aproximadamente un ahorro de 6.779 milones, desincentivando la cantidad de operaciones por alertar en tiempo real al cliente.

La tecnología actual con la que cuenta el banco ayuda a mitigar el costo de inversión, estimándose para un año un total de $678.174.600 pudiendo ser menor, debido a que este se estima por el total de operaciones realizadas al año según la participación que tengan los giros y consultas que se realicen, un 30% y 1% respectivamente, por ende la inversión anual de $678 millones ayudan a reducir una pérdida a $4.067 millones al año. (Ver imagen 5).

La inversión para este proyecto y su finalidad en sí no puede asegurar que se reducirá la cantidad de clonaciones, sin embargo está planteada para reducir la cantidad de operaciones que se realizan con las tarjetas, vale decir que si actualmente hay un promedio de 3,2 operaciones con tarjeta clonada, se estima que debería bajar a 1,2 e incluso mas (Ver Ilustración 5), ya que el sistema de monitoreo inteligente de las tarjetas avisará instantaneamente[6] al cliente cada vez que se efectue un giro o consulta de saldo, siendo este último quien de aviso inmediato a VOX (Servicio telefónico para Clientes de Banco Santander) para el bloqueo del plástico.

[6] Esto dependerá de las condiciones de cada operador móvil de los clientes.

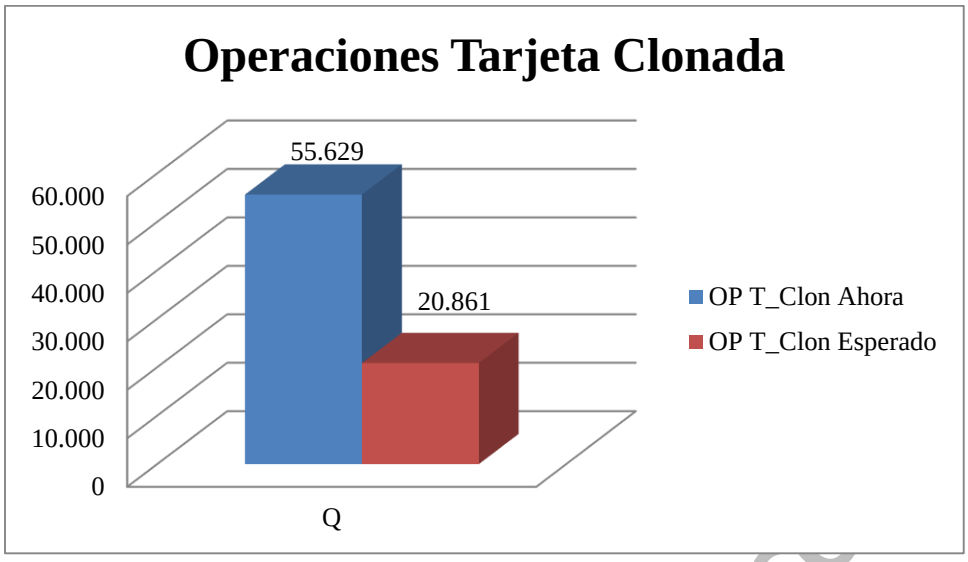


Ilustración 5: Muestra la reducción en la cantidad de clonaciones.

DEFINICIÓN DE RIESGO OPERATIVO

Se entiende por riesgo operativo a la posibilidad de ocurrencia de pérdidas financieras por deficiencias o fallas en los procesos internos, en la tecnología de información, en las personas o por ocurrencia de eventos externos adversos. Esta definición incluye el riesgo legal, pero excluye el riesgo estratégico y el de reputación.

Fuentes del Riesgo Operativo

1. **Procesos Internos**: Posibilidad de pérdidas financieras relacionadas con el diseño inapropiado de los procesos críticos, o con políticas y procedimientos inadecuados o inexistentes que puedan tener como consecuencia el desarrollo deficiente de las operaciones y servicios o la suspensión de los mismos.

2. **Personas** :Posibilidad de pérdidas financieras asociadas con negligencia,error humano, sabotaje, fraude, robo, paralizaciones, apropiación de información sensible, lavado de dinero, inapropiadas relaciones interpersonales y ambiente laboral desfavorable, falta de especificaciones claras en los términos de contratación del personal, entre otros factores.

3. **Tecnología de Información**: Posibilidad de pérdidas financieras derivadas del uso de inadecuados sistemas de información y tecnologías relacionadas, que pueden afectar el desarrollo de las operaciones y servicios que realiza la institución al atentar contra la confidencialidad,integridad, disponibilidad y oportunidad de la información.

4. **Eventos Externos**: Posibilidad de pérdidas derivadas de la ocurrencia de eventos ajenos al control de la empresa que pueden alterar el desarrollo de sus actividades, afectando a los procesos internos, personas y tecnología de información.

SISTEMA DE ADMINISTRACION DEL RIESGO OPERATIVO

Como principio general, las entidades financieras deben contar con una estrategia aprobada por el Directorio estableciendo principios para la identificación, medición, control, monitoreo y mitigación del riesgo operativo.

Las entidades financieras deberían desarrollar su propio enfoque y metodología para la gestión de riesgos, de acuerdo con su objeto social,tamaño, naturaleza y complejidad de operaciones y otras características.

Gráfico Sistema de Administración del Riesgo Operativo

La implementación del sistema de gestión de riesgo operativo debería considerar todas las etapas de gestión de riesgo, incluyendo la identificación,evaluación, medición, monitoreo y control.

1. **Identificación**: La identificación efectiva del riesgo considera tanto los factores internos como externos que podrían afectar adversamente el logro de los objetivos institucionales.

2. **Evaluación**: Todos los riesgos materiales deberían ser evaluados por probabilidad de ocurrencia e impacto a la medición de la vulnerabilidad de la entidad a este riesgo. Los riesgos pueden ser aceptados, mitigados o evitados de una manera consistente con la estrategia y el apetito al riesgo institucional. Cuando sea posible, la entidad debería usar controles internos apropiados u otras estrategias de mitigación, como los seguros.

3. **Medición**: Las entidades financieras deberían estimar el riesgo inherente en todas sus actividades, productos, áreas particulares o conjuntos de actividades o portafolios, usando técnicas cualitativas basadas en análisis expertos, técnicas cuantitativas que estiman el potencial de pérdidas operativas a un nivel de confianza dado o una combinación de ambos.

4. **Monitoreo**: Un monitoreo regular de las actividades puede ofrecer la ventaja de detectar rápidamente y corregir deficiencias en las políticas,procesos y procedimientos de gestión del riesgo operativo. El alcance de las actividades de monitoreo incluye todos los aspectos de la gestión del riesgo operativo en un ciclo de vida consistente con la naturaleza de susriesgos y el volumen, tamaño y complejidad de las operaciones.

5. **Control**: El control del riesgo operativo puede ser conducido como unaparte integral de las operaciones o a través de evaluaciones periódicas separadas, o ambos. Todas las deficiencias o desviaciones deben serreportadas a la gerencia.

6. **Reporte**: Debe existir un reporte regular de la información pertinente a la alta gerencia, al directorio, al personal y a partes externas interesadas,como clientes, proveedores, reguladores y accionistas. El reporte puede incluir información interna y externa, así como información financiera y operativa.

CUANTIFICACION DEL RIESGO OPERACIONAL

La cuantificación permite integrar las etapas del proceso, otorgando mayor objetividad a la gestión del riesgo operacional y permitiendo una mayor eficacia en la asignación de recursos para minimizar el impacto de las pérdidas operativas.
Basilea II [7]brinda un marco de referencia para la gestión integral de los riesgos, marco que es progresivamente adoptado por los supervisores y también por las entidades como una referencia de mejor práctica. Presenta tres métodos para el cálculo de los requerimientos de capital asociados al riesgo operacional:

- Método del Indicador Básico
- Método Estándar.
- Métodos de Medición Avanzada (AMA)

Los dos primeros no se caracterizan por ser sensibles riesgo, dado que determinan los requerimientos de capital en forma simplificada a través del producto entre los ingresos brutos anuales medios y el coeficiente de exigencia de capital. Ambos métodos son cuestionados, porque las entidades son penalizadas por el solo hecho de tener elevados ingresos brutos y porque el requerimiento de capital podría depender de las prácticas contables de cada país, posibilitando así el llamado arbitraje regulatorio. En los AMA el requerimiento de capital es determinado según la estimación del riesgo operacional al que realmente está expuesta la entidad. Para realizar dicha estimación se desarrollan modelos estadísticos de medición interna. En el marco de Basilea II, la posibilidad de utilizar modelos internos está sujeta a la aprobación del supervisor junto con el cumplimiento de

[7] Comité de Supervisión Bancaria de Basilea (**BCBS**, sigla de *Basel Committee on Banking Supervision* en inglés), la organización mundial que reúne a las autoridades de supervisión bancaria, cuya función es fortalecer la solidez de los sistemas financieros.

requerimientos cualitativos adicionales. El Comité de Supervisión Bancaria de Basilea reconoce la evolución de los métodos analíticos para la cuantificación del riesgo operacional, y por lo tanto no define un método específico. No obstante especifica que el horizonte de cálculo de pérdidas sea de carácter anual y que la entidad demuestre que el método seleccionado permite reflejar en la distribución eventos de escasa probabilidad de ocurrencia pero de alto impacto monetario. La metodología para determinar el requerimiento de capital por riesgo operacional utilizando los AMA es semejante al concepto de VaR (Value atRisk o Valor en Riesgo), propio del riesgo de mercado. A partir de la estimación de la distribución de pérdidas agregadas, el requerimiento de capital exigido por Basilea es el que acumula el 99,9% de las pérdidas en un año. Es decir, la entidad debe demostrar suficiente capital para absorber las pérdidas que surjan en el plazo de un año en el 99.9% de los casos,exponiéndose a una insuficiencia en el 0,1% de los casos restantes.

CONCLUSION

En este proyecto se ha tratado de analizar las incidencias y el impacto que tiene las clonaciones en nuestro páis en este último tiempo, demostrar que las medidas actuales no son suficientes para frenarlo y que cada vez con más frecuencia ataca a los procesos de negocio de las instituciones financieras; así como también presentar una mejora que resguardará en este caso a Banco Santander de una protección contra este fraude a través del diseño inteligente de Tarjetas de Crédito y Débito.

Como se ha podido mostrar en este trabajo, el control de la corrupción pueden ser hasta 4 veces más baratas que la propia investigación de estos actos ilícitos, sin considerar el costo y el desgaste administrativo que implica recuperar el dinero perdido.

Por lo tanto, la gestión y el responsable de las empresas se debe poner en la prevención del delito.La investigación del fraude, del abuso, de la corrupción, y del error no debe ser el interés primordial de la Alta Dirección de las Empresas. Su interés debe estar encaminado a fortalecer una cultura ética y a construir sistemas de control de riesgos, que disminuya la probabilidad de un peligro.

En otras palabras, uno de los objetivos esenciales es contar con un sistema de control interno y administración de riesgo es la reducción de fraudes y todo tipo de conductas impropias que puedan dañar la integridad de la empresa.

La gestión y la mejora de procesos es uno de los pilares fundamentales para el funcionamiento de las empresas, en este caso particular para evitar pérdidas, los procesos otorgan herramientas y opciones de cómo responder a los requerimientos de los clientes, con el objeto de entregar lo mejor en cada operación para el Banco.

Este nuevo diseño propuesto entrega a las entidades bancarias un mejor control en las operaciones que se realizan a lo largo de todo el país, para así mitigar la mayor cantidad de incidencias, además de disminuir la pérdida monetaria que se deriva de estos tipos de fraudes, mejorando su rendimiento en general.

BIBLIOGRAFIA

- KMPG en Chile (2009) Encuesta de Fraude y Corrupcion
- Asociación de Bancos e Instituciones Financieras (ABIF).
- Totaltexto Venezuela SMPP CA.
- Venezolano de Crédito. Banco Universal.
- David A Montague "Fraud Prevention Techniques for credit Card Fraud", Trafford Publishing, Canadá 2004.
- Noticias de Actualidad de implementación de tecnolog[ias http://www.altonivel.com.mx/1956 5-chile-implantara-las-tarjetas-de-credito-con-chip.html.
- Omar Briceño Cruzado; "Aplicación de la Distribución de Pérdidas (LDA) Para estimar el Requerimiento de Capital por Riesgo Operacional (CaR) utilizando @Risk y Stat Tools"; Foro de Análisis de Riesgos y Decisiones de Palisad 2010.http://www.palisade.com/downloads/UserConf/LTA10/Briceno_PaliasdeLima2010.pdf