UNIVERSIDAD SAN FRANCISCO DE QUITO

Colegio de Administración para el Desarrollo

FRAUDE AL SISTEMA FINANCIERO Y A SUS CLIENTES

Roberto Fabián Núñez Ávila

Jorge Moncayo, MBA., Director de Tesis

Tesis de grado presentada para el cumplimiento parcial de los requisitos de graduación para la obtención del título de Licenciado en Administración de Empresas

Quito, Diciembre 2013

UNIVERSIDAD SAN FRANCISCO DE QUITO

Colegio de Administración para el Desarrollo

HOJA DE APROBACION DE TESIS

Fraude al Sistema Financiero y a sus clientes

Roberto Fabián Núñez Ávila

Jorge Moncayo, MBA.
Director de Tesis _____

Magdalena Barreiro, PhD.
Decana del Colegio de Administración _____
para el Desarrollo

Quito, Diciembre 2013

© DERECHOS DE AUTOR

Por medio del presente documento certifico que he leído la Política de Propiedad Intelectual de la Universidad San Francisco de Quito y estoy de acuerdo con su contenido, por lo que los derechos de propiedad intelectual del presente trabajo de investigación quedaran sujetos a lo dispuesto en la Política.

Asimismo, autorizo a la USFQ para que realice la digitalización y publicación de este trabajo de investigación en el reposito virtual, de conformidad a lo dispuesto en el Art. 144 de la Ley Orgánica de Educación Superior.

Firma _____

Nombre: Roberto Fabián Núñez Ávila

CI: 1716964414

Fecha: Quito, Diciembre 2013

DEDICATORIA

Dedicado para Dios y toda mi familia que hicieron posible para que yo pueda alcanzar mis sueños y metas, por darme fuerza, el ejemplo, motivación y lo más importante darme la mano cuandomás lo necesitaba, por eso y por todo lo que son es para ustedes esta tesis en agradecimiento por todo su amor.

AGRADECIMIENTOS

Agradezco a Dios por cuidarme y guiarme siempre

A mi esposa e hija por ser la inspiración de todos los días.

A mi madre por su bondad y amor incondicional.

A mi padre por su ejemplo y ayuda.

A mi hermana por su esfuerzo y cariño.

A mi hermano por sus consejos y compañía.

A mi sobrino por su bondad y colaboración.

A toda mi familia por el apoyo a lo largo de mi vida.

A la universidad por ensenarme a ser: Un buen estudiante, buen profesional, buen hijo, buen hermano, buen padre, pero sobre todo un buen ser humano.

A mis maestros por brindarme a más de enseñanza, sus experiencias y consejos de vida.

A mi director de tesis por guiarme a lo largo de este trabajo y aconsejarme de la mejor manera.

RESUMEN

Los tipos de fraudes en el sistema financiero bancario ha crecido de manera significativa a media que ha ido aumentando la tecnología, ha generado millonarias pérdidas a las instituciones bancarias y a sus clientes no solo en el país sino también en todo el mundo, los cotos de las inversiones en las instituciones bancarias son muy altas para controlar la vulnerabilidad que poseen, pero esta inversión y control no son suficientes. En el Ecuador los tipos de fraudes han crecido cada año debido a que el país posee una moneda muy valorada en el mundo como lo es el Dólar Americano, así los hackers y/o delincuentes con sus bandas organizadas se han ubicado en nuestro país. Los clientes conocen muy poco sobre los métodos de fraudes que existen en la actualidad y como evitarlos. Es común escuchar sobre nuevos tipos de fraudes que cada día captan más dinero y hacen daño a las instituciones financieras y de sus clientes.

ABSTRACT

The types of financial frauds in the banking system have grown significantly. As technology has increased, it has generated millions in losses to banks and their customers not only in the country but also worldwide. The investment costs of banking institutions are too high to control the vulnerability they have, but this investment and control are not enough.

In Ecuador, types of scams have grown every year. Since the country has a highly valued currency in the world, such as the U.S. Dollar, hackers and / or offenders with organized gangs have been located in our country. Customers know very little about the methods of fraud that exist today and how to avoid them, it is common to see unimaginable types of fraud every day capture more money from the banking system, financial institutions and their customers.

Contenido

CAPITULO 1

Planteamiento del problema

En la actualidad no existe un estudio detallado sobre los tipos de fraudes en el sistema financiero bancario. Además el fraude y el lavado de activos han traído grandes pérdidas económicas a las instituciones financieras, que han tratado de identificar para poder controlar y por el desarrollo tecnológico avanzado se ha vuelto casi imposible contrarrestarlos por los altos costos de inversión para su control por su alta vulnerabilidad. Por lo que es necesario realizar una investigación que permita establecer mediante gestión de riesgos la identificación y nivel de afectación de los tipos de fraude a los que debe enfrentar el sistema bancario y sus clientes.

En el presente la inseguridad se ha convertido en un hecho que afecta a todos los ecuatorianos sin discriminación de raza, extracto social, edad, género, etc. La población se encuentra insatisfecha por las medidas que se han tomado, porque no ha existido una reducción de la inseguridad en la ciudad de Quito, en relación a los fraudes y sus distintas modalidades que afectan a todos y que son temas recurrentes entre los ecuatorianos.

La ciudadanía conoce lo mínimo sobre los fraudes bancarios, cómo son afectados, quienes delinquen. Por otro lado, la tecnología desarrolla nuevos métodos para favorecer a los usuarios sobre los diferentes riesgos como: Los hackers, Loop Libanes, Skimming, cheques y/o documentos microborrados, el Phishing, falsificación de firmas en cheque y documentos valorados, transferencias SMS, Pharming, y los diferentes tipos de intrusiones innovadores, que son modalidades que se utilizan en contra del sistema financiero bancario, que hace lo necesario y toma medidas internas necesarias a través de software para la mitigación de riesgos, la prevención de fraudes, cuidar sus activos y clientes.

Hipótesis

Los fraudes externos realizados a las instituciones financieras, son realizados en complicidad de un empleado de la misma institución.

El desarrollo tecnológico ha sido bien aprovechado por las instituciones financieras para mejorar su seguridad contra los fraudes.

Las instituciones financieras ante los fraudes, no han tomado las prevenciones necesarias para controlarlos.

Preguntas de Investigación

- ¿Cuáles son los tipos de fraudes más utilizados que afectan al sistema financiero?
- ¿Cuál es el tipo de fraude que ha causado más pérdidas económicas a las instituciones financieras?
- ¿Cuáles son los fraudes externos e internos y quienes lo comentes?
- ¿Cómo ha llegado a beneficiar el desarrollo tecnológico a los antisociales?
- ¿Cuáles son las prevenciones que han tomado las instituciones financieras en los últimos 10 años?
- ¿Qué virtudes y deficiencias presenta el sistema financiero en la actualidad?
- ¿Cómo deben actuar los clientes para minimizar el riesgo que tienen ante los fraudes?

Objetivos de la investigación

Objetivo General

Conocer cuáles son actualmente las principales modalidades delictivas que afectan al sistema financiero y a sus clientes, así presentar un plan de mitigación de riesgos las cuales ayuden a disminuir los riesgos que posee el sistema financiero.

Objetivos Específicos.

Analizar las principales modalidades de fraude al sistema financiero ecuatoriano.

Evaluar cuál es la modalidad que ha causado más pérdidas económicas a las instituciones financieras.

Analizar los tipos de fraudes externos e internos, y quienes los cometen.

Investigar el desarrollo tecnológico constante que existe en la actualidad y como ha llegado a beneficiar a los antisociales.

Justificación

Los fraudes que se comenten al sistema financiero no afectan solo a los clientes sino también a los activos de las instituciones, los métodos de prevención han sido importantes para intentar disuadir los tipos de fraude, el rol de la Superintendencia de Bancos y Seguros es determinante para que exista una prevención de fraudes.

En el país existen estudios sobre seguridad ciudadana que poseen datos sobre tipos de fraudes que afectan a los usuarios de las instituciones financieras y son registrados en la Policía Nacional, Fiscalía, Instituto Nacional de Estadística y Censos (INEC). En muchas ocasiones los fraudes pasan desapercibidos y no son comunicados por vergüenza del hecho en el caso de los clientes o de las instituciones financieras.

Las modalidades más utilizadas se encuentran: Cheque firma falsificada, cheques micro borrado, retiro ahorros firmas falsas, phishing, pharming, malware, skimming, estafa piramidal, transferencias SMS.

Las estructuras del sistema financiero se encuentran bien protegidas, y para los antisociales es más complicado asaltar oficinas, es por ese motivo que se ha incrementado los tipos de fraudes

Viabilidad

Es posible llevar la investigación, existen muchos órganos de control que poseen datos actualizados los cual son de fácil acceso. La investigación sobre el fraude en las instituciones financieras es un tema de actualidad en la sociedad ecuatoriana el cual en los últimos años ha tenido mayor movimiento y control por parte de entidades como la Superintendencia de Bancos.

Marco conceptual

Teoría del patrón del delito.-Profesor de criminología Paul Brantingham, PhD.

Esta teoría trata de dar explicación al hecho de que la distribución de los daños en los escenarios urbanos no es uniforme ni aleatoria, sino que presenta patrones claramente identificables particularmente, estos autores estuvieron influenciados por el enfoque de las actividades rutinarias, planteando que la distribución de las actividades claves de la comunidad, y se relaciona con la familiaridad que el infractor tiene con ciertos espacios urbanos y no con otros.

Los elementos claves son:

La disminución de la distancia: Este patrón se debe tomar en cuenta para determinar cómo sería el área de búsqueda de objetivos o víctimas de un único factor. El área de mayor intensidad búsqueda es la más cercana al lugar, decayendo en la intensidad de búsqueda al aumentar la distancia. Esto es lógico por el gasto y el esfuerzo necesario

para viajar más lejos. Además, el infractor dispone de un mayor conocimiento espacial y sobre posibles objetivos y rutas de escape en las zonas de frecuencia.

Espacios de actividades y conocimiento: Las personas que cometen delitos tienen patrones espacios temporales de movimiento similares a los de todo el mundo. Del mismo modo que cualquier persona realiza sus actividades cotidianas en sus espacios de actividad y alrededores, los infractores tienden a cometer los delitos en sus espacios de actividad y conocimiento, cerca de las rutas que habitualmente emplean.

Patrón de delitos para un individuo: En los espacios de actividad y conocimiento deben existir objetivos atractivos para el delincuente, y que el infractor y objetivo han de coincidir en el espacio y el tiempo, así que los patrones de actividad de infractores y víctimas tienen que coincidir en esos mismos puntos y que la víctima sea evaluada como un buen objetivo.(Brantingham, 1995)

Teoría de la oportunidad del delito.- Felson y Clarke (1988). 10 formas para practicar la prevención del delito

En la prevención situacional del delito, la oportunidad se considera la causa principal del delito.

- ✓ Las oportunidades juegan un rol importante en las causas del delito.
- ✓ Los delitos de oportunidad son muy específicos.
- ✓ Los delitos de oportunidad se concentraron en tiempo y espacio.
- ✓ Los delitos de oportunidad dependen de movimientos de movimientos y actividad diaria
- ✓ Un delito genera la oportunidad para otro.

- ✓ Algunos productos generan mayor ventaja a la comisión de los delitos de oportunidad.
- ✓ Cambios sociales y tecnológicos generan nuevosdelitos de oportunidad.
- ✓ El delito puede ser prevenido mediante la reducción de las oportunidades.
- ✓ La reducción de oportunidades no en todas las oportunidades será garantía que el delito se desplace totalmente. El desplazamiento del delito en gran escala no es común.
- ✓ El enfoque conjunto por parte de las autoridades y de la comunidad en la reducción de oportunidades, puede producir que el delito decline de manera importante en una jurisdicción diferente. (Felson y Clarke, 1988).

Factor macro de la inseguridad.

Es uno de los principales factores que pone en riesgo a las personas a sus bienes e incluso a las instituciones financieras. El Ecuador ha sufrido directamente los problemas que tiene nuestro vecino Colombia, los problemas más fuertes para el Ecuador han sido: el narcotráfico, el narcotráfico, el tráfico de armas y sustancias químicas, el lavado de dinero. En los últimos años estas problemáticas en el país se han ido aumentando, La presencia de la Policía Nacional ha su personal y el gobierno ha invertido triplicando su presupuesto brindándoles un mejor sueldo, mejorando e incrementando el armamento y vehículos, pero lamentablemente no ha sido suficiente para lograr controlar la inseguridad actual.

El gobierno actual ha mejorado algunas variables que afectaban de manera continua los ciudadanos y estas son: La justicia politizada, la impunidad, la inseguridad jurídica y la falta de una política de rehabilitación social, en la que las cárceles no sean escuelas del delito

Análisis económico

La economía en el Ecuador ha crecido en los últimos años debido a varios factores, al tener en circulación una moneda como el Dólar Americano, hemos tenido baja inflación en los últimos años son respecto a los demás países de nuestra región, el precio del petróleo que se ha mantenido estable, al ser una zona de tránsito de droga, estos y muchos más factores han generado que en nuestro país circule mucho dinero, además los planes emergentes que ha manejado el gobierno nos han mantenido con estabilidad por el momento.

Inflación

Inflación mensual		
Año	**Mes**	**Valor**
2011	Diciembre	5,41%
2012	Enero	5,29%
2012	Febrero	5,53%
2012	Marzo	6,12%
2012	Abril	5,42%
2012	Mayo	4,85%
2012	Junio	5%
2012	Julio	5,09%
2012	Agosto	4,88%
2012	Septiembre	5,22%
2012	Octubre	4,94%
2012	Noviembre	4,77%
2012	Diciembre	4,16%
2013	Enero	4,10%
2013	Febrero	3,48%
2013	Marzo	3,01%
2013	Abril	3,03%
2013	Mayo	3,01%
2013	Junio	2,68%
2013	Julio	2,39%
2013	Agosto	2,27%
2013	Septiembre	1,71%
2013	Octubre	2,04%
2013	Noviembre	2,30%

Ilustración1:Inflación Ecuador. (Banco Central del Ecuador 2013)

Alcance y metodología

	Métodos	Técnicas	Resultados
Fundamentación teórica	1. Analítico sintético 2. Inductivo deductivo. 3. Hipotético deductivo 4. Sistémico 5. Triangulación.	Revisión bibliográfica y por internet	Pilares y bases teóricas de la investigación. Enfoque integrador
Diagnostico	1. Histórico lógico 2. Revisión documental 3. Recolección de información 4. Datos estadísticos.	Entrevistas Cuestionarios	Informe sobre el estado actual del problema
Propuesta	1. Analítico sintético 2. Inductivo deductivo 3. Sistémico. 4. Modelación.		Material de estudio de metodología de la investigación con enfoque integrador
Validación	Criterio de expertos	Entrevistas Cuestionarios	Criterios especializados para afinamiento de la propuesta.

Ilustración 2:Investigación Socioeducativa. Dr. Rafael Fraga

CAPITULO 2

Definición de términos

Fraude

"Cualquier acto ilegal caracterizado por engaño, ocultación o violación de confianza. Estos actos no requieren la aplicación de amenaza de violencia o de fuerza física. Los fraudes son perpetrados por individuos y por organizaciones para obtener dinero, bienes o servicios para evitar pagos o perdidos de servicios, o para asegurarse ventajas personales o de negocios." (UAF, 2011)

Activos

"Los bienes, activos financiero, propiedades de toda clase, tangibles o intangibles, muebles o inmuebles, con independencia de cómo se hubieran obtenido, y los documentos o instrumentos legales, sea cual fuere su forma, incluida la forma electrónica o digital, que acrediten la propiedad u otros derechos sobre dichos bienes, incluidos, sin que la enumeración sea taxativa, créditos bancarios, cheques de viajero, cheques bancarios, giros, acciones, títulos, obligaciones, letra de cambio, cartas de crédito, y los intereses, dividendos u otros ingresos o valores que se devenguen o sea generados por esos fondos o u otros bienes." (UAF, 2011)

Actividades de alto riesgo

"Aquellas que por sus características particulares representan un mayor riesgo para las personas naturales y jurídicas que integran el sistema de seguro privado de ser utilizadas en el cometimiento del delito de lavado de activos." (UAF, 2011)

Bienes procedentes de una activad delictiva

"Se entenderá por bienes procedentes de una actividad delictiva todo tipo de bienes procedentes de una actividad delictiva todo tipo de activos, tanto materiales como inmateriales, muebles o inmuebles, tangibles o intangibles, así como los documentos o instrumentos jurídicos con independencia de su forma, incluida la electrónica o la digital, que acrediten la propiedad de dicho activos o un derecho sobre los mismos, con inclusión de la cuota defraudada en el caso de los delitos contra el Servicio de Rentas Internas, cuya adquisición o posesión tenga su origen en un delito." (UAF, 2011)

Cliente

"Persona natural o jurídica con la que una persona o entidad establece, de manera ocasional o permanente, una relación contractual de carácter financiero, económico o comercial." (UAF, 2011)

Código de Ética

"Recopilación de políticas relacionadas con las normas de conducta ética y legal que sus accionistas, personal directivo y empleados deben observar en el curso de sus operaciones de negocios para prevenir el lavado de activos y financiamiento de delitos." (UAF, 2011)

Colaborador cercano

"El que se beneficia del hecho de estar cercano a una persona políticamente expuesta, como por ejemplo su colaborador de trabajo, asesor, consultor, socio personal, entre otros." (UAF, 2011)

Elementos de prevención de lavado de activos

"Son políticas, procedimientos, documentación, estructura organizacional, órganos de control interno, infraestructura tecnológica, formación del personal y divulgación de normas y principios." (UAF, 2011)

Etapas de prevención de lavado de activos

"Se refiere a la identificación, medición, control y monitoreo del riesgo de lavado de activos." (UAF, 2011)

Empresa pantalla

"Compañía que no tiene una presencia física en el país donde fue legalmente constituida y autorizada para funcionar." (UAF, 2011)

Factores de riesgo

"Son las circunstancias y características particulares del cliente, operación y ubicación en la que se realiza, que determinan la mayor o menor probabilidad de que se trate de una operación inusual." (UAF, 2011)

Financiamiento de delitos

"Es el proceso por el cual una persona natural o jurídica, provee o recolecta fondos por el medio que fuere, directa o indirectamente, a sabiendas de que serán utilizados o con la intención deliberada de que se utilicen, en todo o en parte, para cometer un acto o actos delictivos, por parte de una organización criminal o por un delincuente individualmente considerado." (UAF, 2011)

Financiamiento del terrorismo

"Actividad por la cual cualquier persona deliberadamente provea o recolecte fondos por el medio que fuere, directa o indirectamente, con la intención ilícita de que se utilicen o a sabiendas que serán utilizados, en todo o en parte para cometer un acto o actos de terrorismo, por una organización terrorista o por un terrorista." (UAF, 2011)

Instituciones del sistema financiero

"Son aquellas que se encuentran sujetas a la supervisión, vigilancia y control de la Superintendencia de Bancos y Seguros y autorizadas por ésta para realizar actividades de intermediación financiera." (UAF, 2011)

Industrias de alto riesgo

"Aquellas que por su ubicación geográfica, su nicho de mercado, por el perfil personal y financiero de sus accionistas y demás características particulares, representan un mayor riesgo para las personas naturales y jurídicas que integran el sistema de seguro privado de ser utilizadas en el cometimiento del delito de lavado de activos." (UAF, 2011)

Inspectores de riesgos

"Personas naturales o jurídicas autorizadas por la Superintendencia de Bancos y Seguros, cuya actividad es la de examinar y calificar los riesgos en forma previa a la contratación del seguro y durante la vigencia del contrato." (UAF, 2011)

Indemnización

"Es un importe que está obligado a pagar contractualmente el asegurador en caso de producirse un siniestro, con la finalidad de conseguir una reposición económica en el patrimonio del asegurado afectado por un siniestro." (UAF, 2011)

Indicadores

"Son elementos que permiten detectar la posible presencia de operaciones de "lavado de activos" relacionadas con la tipología." (UAF, 2011)

Lavado de activos

"Es el proceso por el cual los bienes y ganancias monetarias de origen delictivo e ilícito, se invierten, integran o transforman en el sistema económico financiero legal con apariencia de haber sido obtenido de forma ilícita y procurando ocultar su verdadera procedencia, así como su real propiedad y el ejercicio de su dominio y control.

Es el mecanismo a través del cual se oculta el verdadero origen de dineros provenientes de actividades ilegales, tanto en moneda nacional como extranjera, para introducirlos como legítimos dentro del sistema económico de un país." (UAF, 2011)

Oficial de cumplimiento

"Es el funcionario de alto nivel, que debe contar con suficiente independencia para la toma de decisiones, responsable de verificar la aplicación de la normativa inherente a la prevención de lavado de activos, ejecutar el programa de cumplimiento tendiente a evitar que la entidad sea utilizada para lavar activos; y, velar por la observancia e implementación de los procedimientos, controles y buenas prácticas necesarios para la prevención de lavado de activos." (UAF, 2011)

Operación o transacción económica inusual e injustificada

"Es aquella operación o transacción que no guarda correspondencia con los patrones regulares de las actividades económicas que habitualmente realiza el cliente, y cuyo origen no puede ser justificado." (UAF, 2011)

Operaciones y Transacciones

"Son todas aquellas actividades realizadas bajo un identificador único de cliente y de producto financiero en cada institución." (UAF, 2011)

Paraísos fiscales

"Aquellos que se caracterizan por tener legislaciones impositivas y de control estatal laxas, y que han sido clasificados como tales por el Servicio de Rentas Internas." (UAF, 2011)

Reporte de Operaciones y Transacciones Inusuales e Injustificadas (ROII´s)

"Reporte en el que se detallan todas las inusuales generadas en las operaciones y transacciones de un cliente que no hayan podido ser debidamente justificadas. Estos reportes de operaciones y transacciones inusuales e injustificadas deben contar con los debidos sustentos." (UAF, 2011)

Señales de alerta

"Son aquellos elementos que evidencian los comportamientos particulares de los clientes o usuarios y las situaciones atípicas que presentan las operaciones o transacciones que pueden encubrir actividades de lavado de activos o de financiamiento del terrorismo. Hay que tener en cuenta que no todas las operaciones que presentan comportamientos atípicos e inusuales son operaciones ilegales, por tal razón, el hecho de identificar señales de alerta no significa que la operación deba ser reportada de forma inmediata a las autoridades." (UAF, 2011)

Superintendencia de Bancos y Seguros

"Entidad encargada de la supervisión y control del sistema financiero con la finalidad de proteger los intereses del público y en materia de prevención de lavado de dinero, a través de la práctica de inspecciones, tendientes a verificar la existencia de políticas y cumplimiento de procedimientos que permitan evitar que se utilice al sistema financiero para lavar activos." (UAF, 2011)

Supervisores

"Las autoridades competentes designadas, para cumplir funciones de supervisión, control o registro, que deberán asegurar el cumplimiento de los requisitos para combatir el lavado de activos y el financiamiento de terrorismo." (UAF, 2011)

Tipologías

"Clasificación y descripción de técnicas utilizadas por las organizaciones criminales para dar apariencia de legalidad a los fondos de procedencia lícita o ilícita y transferirlos de un lugar a otro o entre personas para financiar sus actividades criminales." (UAF, 2011)

Usuario

"Es aquella persona natural o jurídica a la que, sin ser cliente, la institución controlada presta un servicio." (UAF, 2011)

Banca electrónica

"Son los servicios suministrados por las instituciones del sistema financiero a los clientes a través de internet en el sitio que corresponda a uno o más dominios de la

institución, indistintamente del dispositivo tecnológico a través del cual se acceda.” (UAF, 2011)

Banca móvil

“Son los servicios suministrados por las instituciones del sistema financiero a los clientes a través de equipos celulares mediante los protocolos propios de este tipo de dispositivos.” (UAF, 2011)

Tarjetas

“Para efectos del presente capítulo, se refiere a las tarjetas de débito, de cajero automático y tarjetas de crédito.” (UAF, 2011)

Canales electrónicos

“Se refiere a todas las vías o formas a través de las cuales los clientes o usuarios pueden efectuar transacciones con las instituciones del sistema financiero, mediante el uso de elementos o dispositivos electrónicos o tecnológicos, utilizando o no tarjetas.” (UAF, 2011)

Antispyware

“Es un software que sirve para lograr eliminar programas espías que pueden estar instalados en el computador.” (UAF, 2011)

Antimalware

“Este software nos ayuda a la eliminación y detención de todo software que quieren causar daño.” (UAF, 2011)

CAPITULO 3

Tipos de fraudes

Fraudes internos:

Son cometidos por los empleados de una empresa, sacan provecho de su conocimiento e información que manejan para su beneficio.

Fraudes externos:

Son cometidos por personas externas a la empresa que no tienen relación alguna.

Fraudes mixtos:

Este tipo de fraude es cometido por personas externas con la colaboración de empleados de la empresa.

Tipos de seguridad

Seguridad Pública

Thomas Hobbes quién fue uno de los impulsores para implementar el orden público basado en la preponderancia a la intervención del gran Estado, porque se tenía la desconfianza hacia las otras personas. El gran Estado tenía se basaba en la preservación de la integridad de todas las personas. (Hebbert, 2010, pag.98)

Seguridad Física

Es la creación de barreras estructurales que sirven para proteger de amenazas que puedan afectar, estas barreras no son para protegerlos de personas, sino también de la naturaleza.

Seguridad Bancaria

La seguridad de las entidades financieras es un tema complejo y de alta responsabilidad, por cuanto comprende velar por la integridad física de los clientes y funcionarios bancarios, así como salvaguardar el patrimonio de la entidad correspondiente. La gama de ilícitos de tipo económico a la que se encuentran expuestas las instituciones financieras, por el giro de su actividad son los asaltos, estafas y secuestros, entre otros.

A muchos se les antoja que los bancos y cooperativas de ahorro son los centros para obtener el dinero, de forma delictiva, de menos esfuerzo, sin riesgo. Este planteamiento simplista para unos, muy estudiado para otros, es el que define el perfil de los delincuentes o asaltantes de bancos desde hace mucho tiempo.

Por otro lado, las instituciones bancarias se han visto en la obligación de ir cumpliendo con medidas de seguridad dispuestas por la Junta Bancaria, para cambiar los niveles de riesgo, para resguardarse de robos y atracos que cualitativa y cuantitativamente, pueden considerarse como ¨buenos trabajos¨, con el consiguiente riesgo de las personas y la pérdida de bienes y valores.

La seguridad bancaria presenta múltiples facetas, ha sido el primer sector que necesitaba un planteamiento serio de seguridad. Se ha iniciado en la toma de conciencia de la seguridad como un problema ciudadano del día a día y ha servido, en gran medida, para el establecimiento de las bases de muchas empresas de seguridad y de la formación de profesionales y técnicos especializados.

Desde la perspectiva de la lucha contra los actos antisociales, presenta una gran implicación en la vida cotidiana de cualquier país por estar ¨más cerca del cliente¨. Las entidades han multiplicado en pocos años, el número de agencias y continuamente se

establecen nuevos servicios bancarios, se realizan más gestiones y de forma más rápida. Este contacto habitual para todo tipo de usuarios, hace que muchas agencias tengan varios centenares de visitas diarias en búsqueda de esos pequeños y grandes servicios.

Esta situación, a lo largo de los años de mayor dependencia bancaria, ha hecho que se considere a los bancos como establecimientos en los que se tiene depositado la confianza de los clientes. Por todas las razones implícitas a la propia actividad y contenido, las entidades bancarias y sus clientes están permanentemente situadas en la mira de los delincuentes.

La seguridad y la eficacia son parte integrante de la calidad del servicio en las entidades bancarias. Uno de los conceptos que más pueden influir en la ¨calidad del servicio¨ es el de la atención personalizada y directa, con mayor contacto con el cliente, sin barreras intermedias, en un ambiente cómodo, relajado y en medida de lo posible, acogedor, situado en un ambiente abierto, en contacto y sin la ¨presión agresiva de la seguridad¨ que, en muchos de los casos perturba el diálogo e incluso, el ambiente de blindaje quizás podría generar cierta angustia.

Las agencias bancarias deben aspirar a obtener y ofrecer, dentro del principio de ¨puertas abiertas y máximo contacto directo¨, una garantía de seguridad implícita y explícita no necesariamente disuasoria, al menos, en el interior de la propia agencia. La estética y el ambiente relajado no están en contraposición con la seguridad.

En las agencias bancarias se comenzó protegiendo el dinero mediante cajas fuertes y cámaras acorazadas; con posterioridad, se protegió a los empleados con barreras, como los vidrios blindados y la incorporación de vigilantes armados que, en muchos casos, se mantienen después de la incorporación de puertas esclusas, cabinas, control de accesos, etc.

Pero si bien cada una de las medidas de prevención y protección puede considerarse un elemento eficaz en sí mismo, la suma de todos ellos puede llegar a repercutir en el funcionamiento de la agencia sin aportar grandes dosis de eficacia. La seguridad y la eficacia, están directamente relacionadas con los niveles de control, procedimientos y gestión de los accesos, y son un elemento básico de la prevención y la protección de las agencias bancarias.

Seguridad Privada

Relativas a aquellas actividades destinadas a precautelar y proteger la vida e integridad física de las personas, así como dar seguridad a patrimonios de personas naturales o jurídicas; realizadas por personas naturales o jurídicas bajo alguna de las modalidades normadas en la Ley y debidamente autorizadas y registradas ante la autoridad competente.

Esta actividad es desempeñada por sociedades, empresas o compañías privadas de vigilancia armada. Se trata de personas jurídicas cuyo objeto social es prestar servicios remunerados de protección armada a bienes muebles y a personas naturales, servicio de escolta, transporte de valores y demás tarea que le sean afines. (Rafflin, 2008, pag.17)

CAPITULO 4

Sistema Financiero

El Sistema Financiero es conjunto de mercados, instituciones que tiene como objeto dirigir el ahorro generado por los prestamistas hacia los prestatarios, consiguiendo así el desarrollo ordenado y equilibrado de la economía del país.

Clasificación del Sistema Financiero

El mercado de capitales

Son las transacciones de mediano y largo plazo, que realizan las instituciones financieras para poder financiar la formación de activos fijos, a través de la concesión de créditos, la circulación o emisión pública de títulos de valores.

El mercado de dinero monetario

Son las operaciones de corto plazo que efectúan las instituciones financieras con el objetivo de financiar el capital de trabajo del consumo de las personas y de las empresas.

Grupos de instituciones financieras

Entidades bancarias:

Bancos nacionales, Bancos extranjeros, Bancos Privados y Bancos del Estado.

Entidades financieras:

Cooperativas, Compañías Financieras, Mutualistas, Corporación Financiera Nacional.

Entidades de apoyo:

Casa de Cambios, Compañías de Seguros.

Otras instituciones:

Instituto Ecuatoriano de Seguridad Social (IESS), las casas de valores. Estas instituciones no están bajo el control de la Superintendencia de Bancos.

Función de las entidades bancarias

Según la Ley General de las Instituciones del Sistema Financiero Ecuatoriano menciona que sus funciones son:

- Recibir recursos del público para depósitos de ahorro, cuentas corrientes, depósito a plazo.
- Emisión de obligaciones y cedulas garantizadas con sus activos y patrimonio.
- Comprar o vender oro, plata o moneda que sea de circulación.
- Otorgar préstamos hipotecarios y prendarios, con o sin emisión de títulos, así como préstamos quirografarios.
- Efectuar cobros, pagos y transferencias.
- Negociar letras de cambio, pagares, facturas y otros documentos que representen obligaciones de pago.
- Comprar y conservar objetos, muebles en depósitos, propiedades raíces.
- Negociar títulos valores y descontar letras documentarias sobre el exterior, o hacer adelantos sobre ellas.
- Adquirir, conservar o enajenar, por cuenta propia valores de renta fija de los previstos en la Ley de Mercado de Valores.
- Emitir bonos de prenda, pólizas de acumulación.

Estructura Funcional

En las instituciones financieras se posee una estructura organizacional y funcional que están encargadas de las diferentes divisiones que existen, cada una con su función específica. La siguiente es una estructura que ayudara a entender las funciones y responsabilidades que tiene cada departamento.

Junta accionistas

Es el organismo soberano que manifiesta a través del voto de la mayoría de accionistas los votos para adoptar cuantos acuerdos y resoluciones estime, siempre de acuerdo al estatuto y Leyes vigentes.

Directorio.-

Es el organismo administrativo que representa a la sociedad accionaria en sus relaciones externas y al que corresponde la gestión empresarial.

El Directorio está compuesto por:

Presidente

Vicepresidente

Vocales principales y suplentes.

Estos se reúnen periódicamente y sus funciones son:

Nombramiento del Gerente General y otros funcionarios.

Aprobar presupuestos.

Dictar políticas financieras, crediticias, administrativas y operativas/

Convocar a Junta General de Accionistas

Autorización de adquisición de activos fijos importantes e hipotecas sobre ellos.

Aprobación de nuevas oficinas

Gerente General.-

Responsable de la administración general del banco, además define los objetivos, coordinación, control, planes, organización y dirección. Ejerce la representación legal, extrajudicial y jurídica del banco. Además supervisa la eficiencia de todos los departamentos del banco y presenta proyectos y presupuesto general al Directorio

Auditor Interno.-

Funcionario a cargo de la asesoría y control de todas las áreas y operaciones del banco

CAPITULO 5

Control Interno

‘‘ Control interno es un proceso, ejecutado por la junta directiva o consejo de administración de una entidad, por su grupo directivo (gerencial) y por el resto del personal diseñado específicamente para proporcionarles seguridad razonable de conseguir en la empresa las tres siguientes categorías de objetivos: ’’(Estupiñan, 2006, pag.25)

Eficiencia en todas las operaciones

Confiabilidad de la totalidad de la información financiera

Cumplimiento de leyes y regulaciones

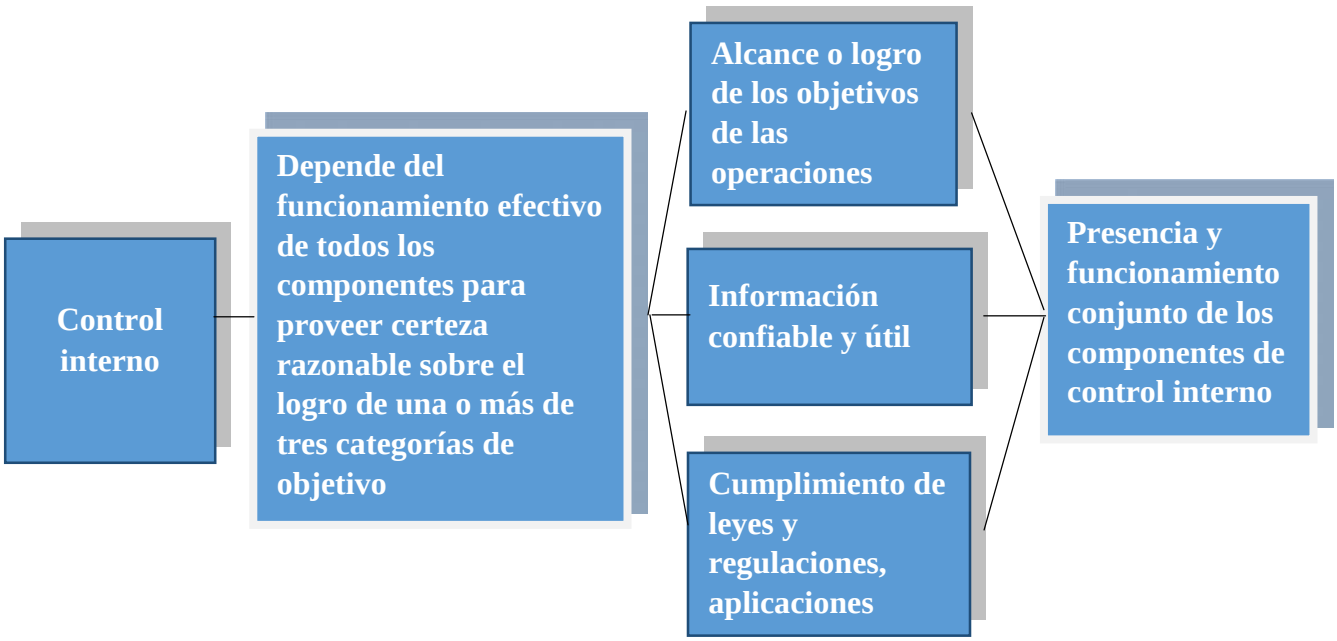


Ilustración3:Control Interno. (Análisis de informe COSO I y II, 2006)

Componentes de Control Interno

El control interno posee de cinco componentes, que son como la administración los maneja, y se clasifican en:

Ambiente de control

Establece el entorno de una organización que influye en las actividades del personal para el control de sus actividades, además es el fundamento de los demás componentes de control interno.(Estupiñan, 2006, pag.27)

Ilustración 4: Control Interno. (Análisis de informe COSO I y II, 2006)

Evaluación de riesgos

Es la identificación de la entidad y el análisis de riesgos importantes para lograr los objetivos, construyendo una base para determinar el manejo de riesgos.

En las entidades es vital que se generen objetivos globales y actividades relevantes, para utilizarlos como identificadores los cuales deberán ser analizados los factores de riesgos que amenazan.

Todos los niveles involucrados tienen la responsabilidad de la evolución del riesgo, y la autoevaluación deberá ser revisada por los auditores internos para el cumplimiento de objetivo, enfoque, alcance y procedimiento.(Estupiñan, 2006, pag.29)

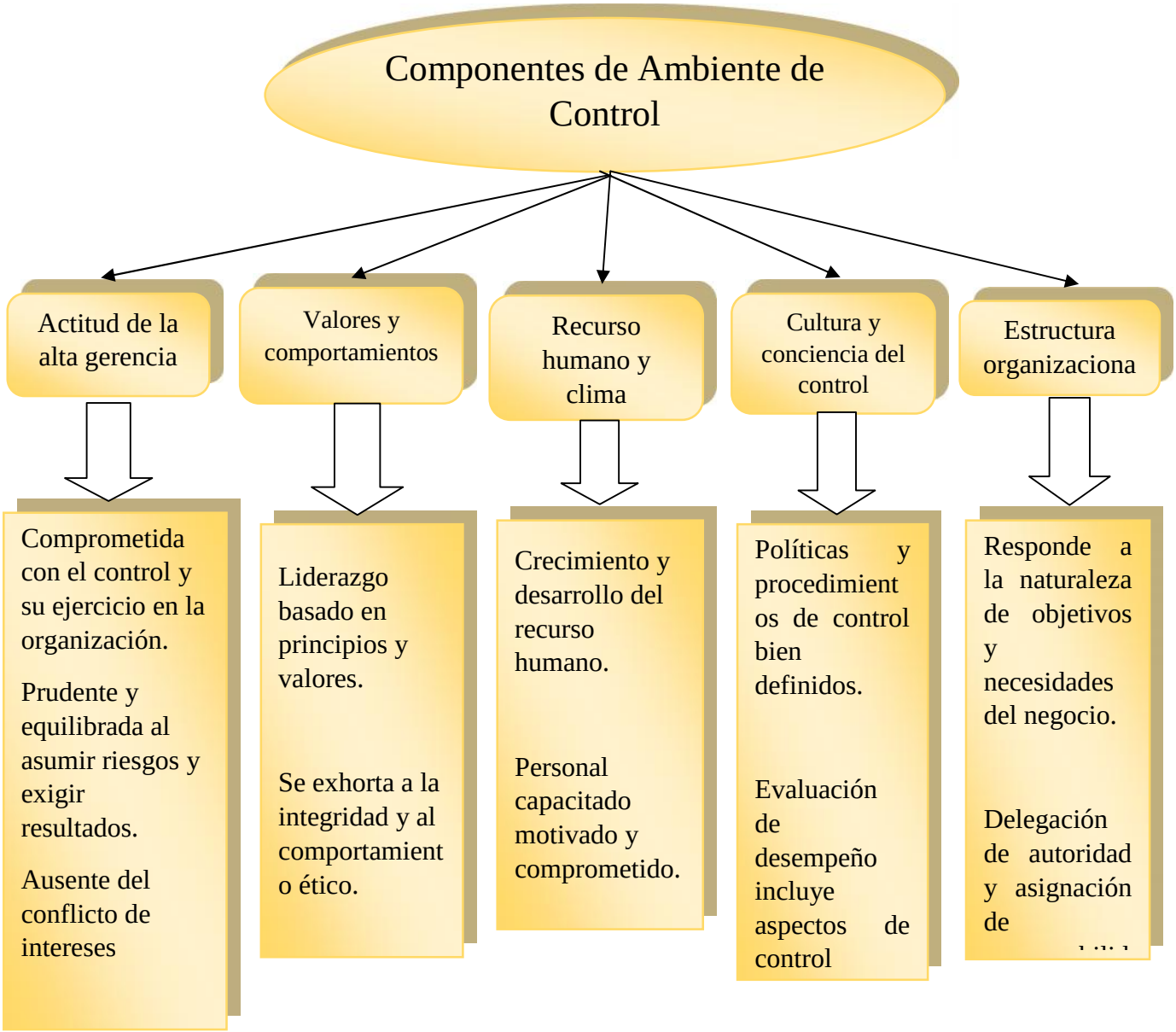


Ilustración 5:Control Interno. (Análisis de informe COSO I y II, 2006)

Las empresas deben tolerar todo tipo de riesgos que son tanto de fuentes externas como de fuentes internas y que deben ser analizados por la gerencia.

La gerencia analiza e identifica los riesgos de sus objetivos generales y específicos para que no afecte su capacidad de:

- Auxiliar sus recursos y bienes
- Ventaja competitiva
- Mejorar y mantener su imagen
- Aumentar y tener estable su solidez financiera
- Sustentar su crecimiento

Categorías de los objetivos

Objetivos de cumplimiento

Enfocados en la adhesión a las leyes, reglamentos y políticas que han sido difundidas por la administración.

Objetivos de operación

Están vinculados a la eficiencia y efectividad de las operaciones de la empresa.

Objetivos de la información financiera

Se refiere a la adquisición de información financiera confiable.

‘

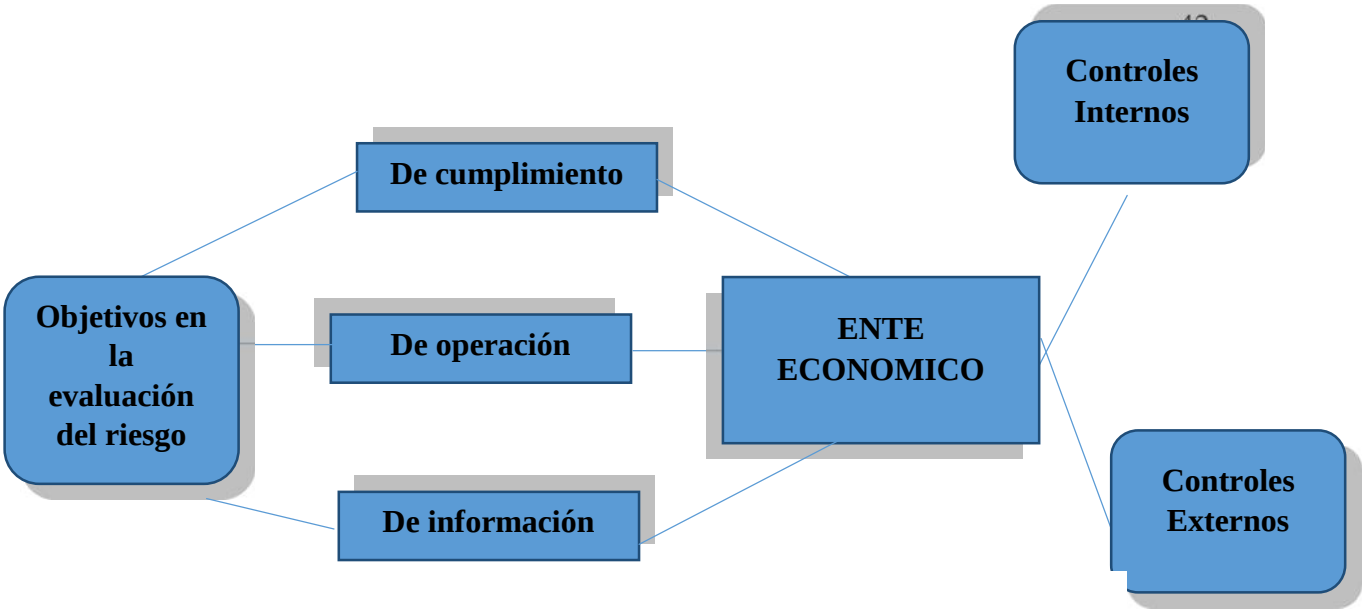


Ilustración 6: Control Internocon base en los ciclos transaccionales. (Análisis de informe COSO I y II, 2006)

Actividades de control

Son realizadas por la gerencia y todo el personal de la organización para cumplir con el cronograma asignado y estas actividades las constituyen las políticas, sistemas y procedimientos que ayudan a que las directrices de la gerencia sean llevadas a cabo.(Estupiñan, 2006, pag.32)

Incluyen actividades detectives, preventivas y correctivas, las actividades de control pueden ser computarizadas, operacionales, manuales, específicas y preventivas, no importa su forma de control lo importante es que se enfoque en los riesgos que sean reales o potenciales para la empresa. Por tal motivo las actividades de control son fundamentales para la meta de cumplir con los objetivos.(Estupiñan, 2006, pag.32)

Controles de procesamiento de información

- Seguridades físicas
- Revisión de desempeños operacionales
- Revisión de informes de actividades y desempeño
- Análisis de registros de la información

- Finanzas y seguros
- Indicadores de desempeño
- Salvaguarda de activos
- Segregación de funciones
- Reconciliaciones
- Aprobaciones y autorizaciones
- Verificaciones

Tipos de controles

Detectivos

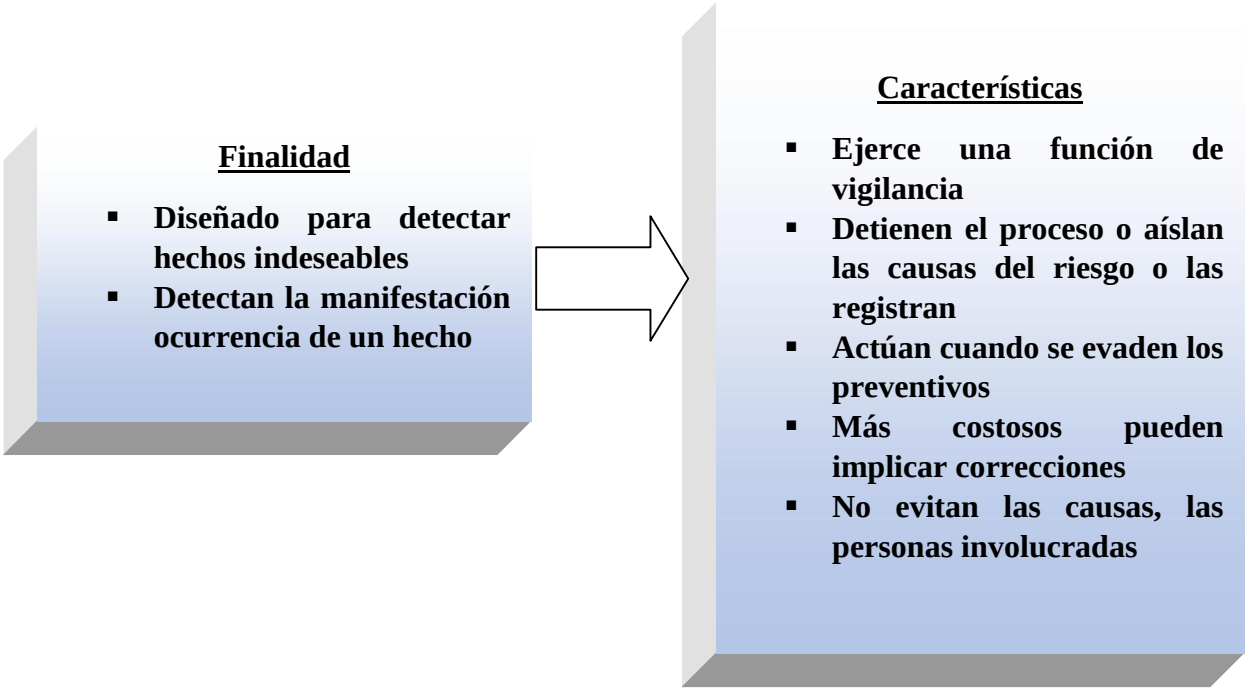


Ilustración 7: Control Internocon base en los ciclos transaccionales. (Análisis de informe COSO I y II, 2006)

Preventivos

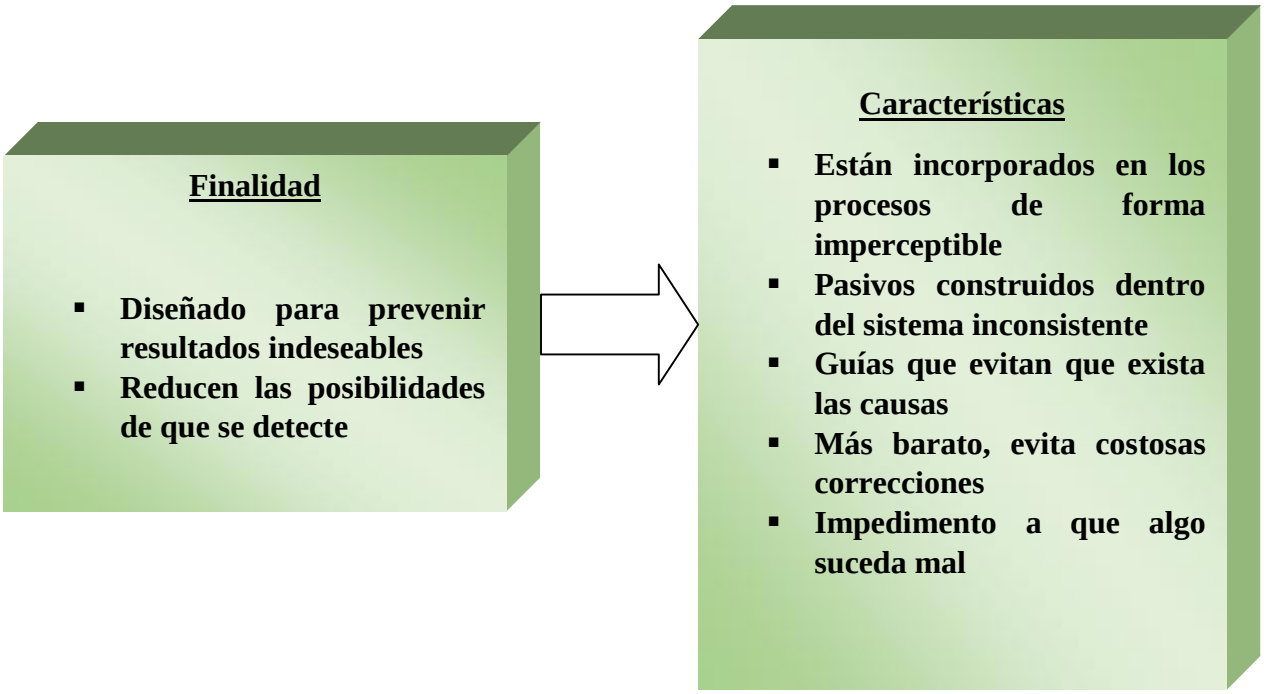


Ilustración 8: Control Interno. (Análisis de informe COSO I y II, 2006)

Correctivos

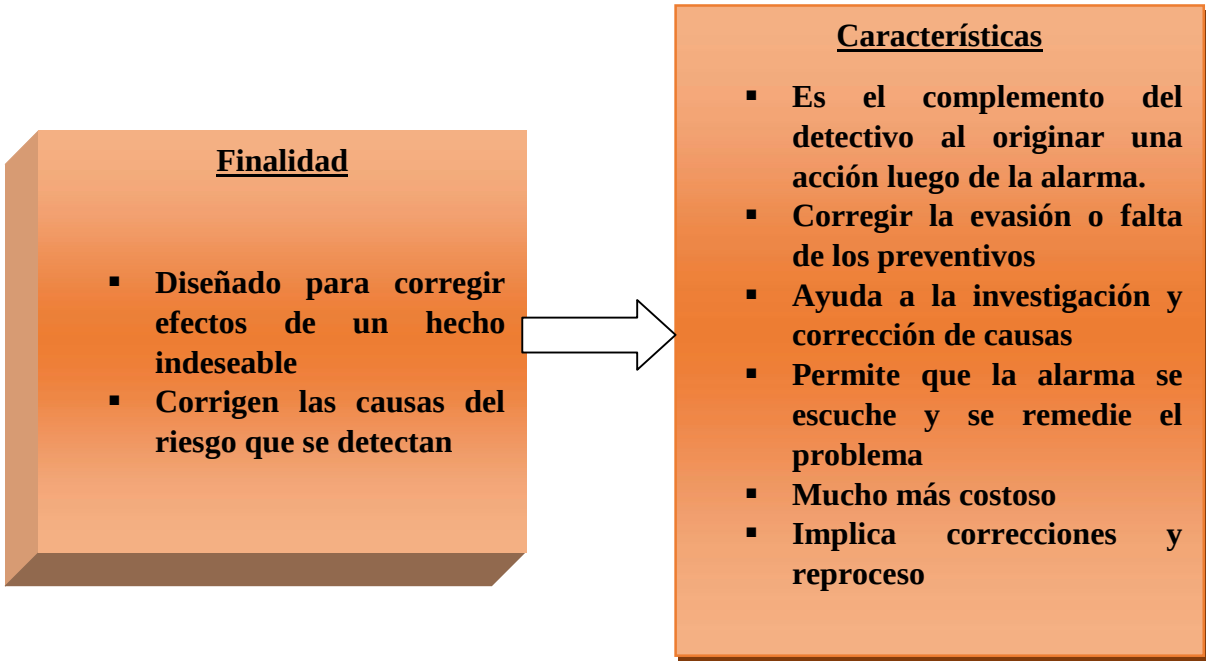


Ilustración 9: Control Interno. (Análisis de informe COSO I y II, 2006)

Información y comunicación

Los sistemas de información y de comunicación están esparcidos y todos contemplan uno o más objetivos de control. Simboliza la identificación, capturando e intercambiando información de tal manera ayuda para que la gente de la organización lleve a cabo sus responsabilidades pertinentes. (Estupiñan, 2006, pag.33)

Controles generales

Se incorpora el control del centro de procesamiento de los datos y la seguridad física, mantenimiento de software y hardware.

Se debe atender a los controles:

- Ayudan al cumplimiento de los controles específicos.
- Contribuyen en los procedimientos de control de saldos significativos
- Implanta un buen ambiente de control (moralidad, actitud, disciplina)
- Procedimientos y políticas presupuestales
- Valoración en base en control presupuestario
- Control de las desviaciones presupuestales
- Contabilidad por áreas de responsabilidad
- Presupuesto de inversiones de capital

Supervisión

Proceso elaborado para revisar la calidad del sistema de control interno de la organización, este proceso incorpora las siguientes actividades:

- Función de controlar
- El proceso de supervisar lo ejecutado con lo programado

- Fijar si hay desviaciones y acoger las medidas de solución
- El propósito del control es corregir el cumplimiento de los objetivos de la organización
- Supervisiones autónomas (Auditoria externa)
- Auto Evaluaciones (Revisiones de la Gerencia)
- Inspección a través de la ejecución de operaciones

CAPITULO 6

Exigencias de la Resolución de la Junta Bancaria: JB-2012-2148

LA JUNTA BANCARIA

CONSIDERANDO:

"Que las instituciones del sistema financiero deben contar con los controles necesarios para proteger los intereses del público, de acuerdo con lo señalado en el artículo

1 De la Ley General de Instituciones del Sistema Financiero; Entre los riesgos operativos que enfrentan, se encuentran el "fraude interno" y el "fraude externo", los cuales se ocasionarían a través del uso de la tecnología de información y comunicaciones; Por tal razón es importante que las instituciones del sistema financiero integren suficientes medidas de seguridad para mitigar el riesgo de fraude por el uso de la tecnología de información y comunicaciones. "El Comité de Supervisión Bancaria de Basilea ha definido y recomienda principios para la administración del riesgo de operación, a fin de que sean aplicados por las instituciones financieras y también consideradas por los supervisores al evaluar la gestión realizada por las entidades controladas"1; Que el control por parte del supervisor no consiste únicamente en garantizar que las instituciones controladas posean el capital necesario para cubrir los riesgos de sus actividades, sino también en alentarlas a que desarrollen y utilicen mejores técnicas de gestión de sus riesgos que les permitan ser más eficientes y competitivas en un entorno de globalización; Que por tales motivos es necesario reformar dichas normas, con el propósito de establecer medidas de seguridad en la tecnología de información y comunicaciones; y, En ejercicio de la atribución legal que le otorga la letra b) del artículo 175 de la Ley General de Instituciones del Sistema Financiero, acceso controlado al interior del cajero automático por parte del personal

técnico o de mantenimiento que disponga de las respectivas llaves. Estas cerraduras deben operar con llaves únicas y no genéricas o maestras;

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

2. Incluir como tercera disposición transitoria, la siguiente:

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

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

Principalmente son canales electrónicos: los cajeros automáticos (ATM), dispositivos de puntos de venta (POS y PIN Pad), sistemas de audio respuesta (IVR), señal telefónica, celular e internet u otro similares;

4.3.8 Medidas de seguridad en canales electrónicos.- Con el objeto de garantizar que las transacciones realizadas a través de canales electrónicos cuenten con los controles, medidas y elementos de seguridad para evitar el cometimiento de eventos fraudulentos y garantizar la seguridad y calidad de la información de los usuarios así como los bienes de

los clientes a cargo de las instituciones controladas, éstas deberán cumplir como mínimo con lo siguiente:

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

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

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

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

4.3.8.5 Las instituciones del sistema financiero deberán contar en todos sus canales electrónicos con software antimalware que esté permanentemente actualizado, el cual permita proteger el software instalado, detectar oportunamente cualquier intento o

alteración en su código, configuración y/o funcionalidad, y emitir las alarmas correspondientes para el bloqueo del canal electrónico, su inactivación y revisión oportuna por parte de personal técnico autorizado de la institución;

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

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

4.3.8.8 Ofrecer a los clientes los mecanismos necesarios para que personalicen las condiciones bajo las cuales desean realizar sus transacciones a través de los diferentes canales electrónicos y tarjetas, dentro de las condiciones o límites máximos que deberá establecer cada entidad. Entre las principales condiciones de personalización por cada tipo de canal electrónico, deberán estar: registro de las cuentas a las cuales desea realizar transferencias, registro de direcciones IP de computadores autorizados, el ó los números de telefonía móvil autorizados, montos máximos por transacción diaria, semanal y mensual, entre otros. Para el caso de consumos con tarjetas, se deberán personalizar los cupos máximos, principalmente para los siguientes servicios: consumos nacionales, consumos en el exterior, compras por internet, entre otros;

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

4.3.8.10 Las instituciones deberán establecer procedimientos de control y mecanismos que permitan registrar el perfil de cada cliente sobre sus costumbres transaccionales en el uso de canales electrónicos y tarjetas y definir procedimientos para monitorear en línea y permitir o rechazar de manera oportuna la ejecución de transacciones que no correspondan a sus hábitos, lo cual deberá ser inmediatamente notificado al cliente mediante mensajería móvil, correo electrónico, u otro mecanismo;

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

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

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

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

4.3.8.15 Mantener como mínimo durante doce (12) meses el registro histórico de todas las operaciones que se realicen a través de los canales electrónicos, el cual deberá contener

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

4.3.8.16 Incorporar en los procedimientos de administración de la seguridad de la información, controles para impedir que funcionarios de la entidad que no estén debidamente autorizados tengan acceso a consultar información confidencial de los clientes en ambiente de producción. En el caso de información contenida en ambientes de desarrollo y pruebas, ésta deberá ser enmascarada o codificada Todos estos procedimientos deberán estar debidamente documentados en los manuales respectivos. Además, la entidad deberá mantener y monitorear un log de auditoría sobre las consultas realizadas por los funcionarios a la información confidencial de los clientes, la cual debe contener como mínimo: identificación del funcionario, sistema utilizado, identificación del equipo (IP), fecha, hora, e información consultada. Esta información deberá conservarse por lo menos por doce (12) meses;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

4.3.9.6 Establecer y ejecutar procedimientos de auditoría de seguridad en sus cajeros automáticos por lo menos una vez al año, con el fin de identificar vulnerabilidades y mitigar los riesgos que podrían afectar a la seguridad de los servicios que se brindan a través de estos. Los procedimientos de auditoría deberán ser ejecutados por personal capacitado y con experiencia; y,

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

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

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

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

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

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

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

4.3.11.2 Realizar como mínimo una vez (1) al año una prueba de vulnerabilidad y penetración a los equipos, dispositivos y medios de comunicación utilizados en la ejecución de transacciones por banca electrónica; y, en caso de que se realicen cambios en

laplataforma que podrían afectar a la seguridad de este canal, se deberá efectuar una prueba adicional.

Las pruebas de vulnerabilidad y penetración deberán ser efectuadas por personal independiente a la entidad, de comprobada competencia y aplicando estándares vigentes y reconocidos a nivel internacional. Las instituciones deberán definir y ejecutar planes de acción sobre las vulnerabilidades detectadas;

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

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

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

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

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

4.3.11.8 La institución del sistema financiero deberá implementar mecanismos para impedir la copia de los diferentes componentes de su sitio web, verificar constantemente

que no sean modificados sus enlaces (links), suplantados sus certificados digitales, ni modificada indebidamente la resolución de su sistema de nombres de dominio (DNS);

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

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

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

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

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

4.3.14 Corresponsales no bancarios.- Las instituciones financieras controladas que presten servicios a través de corresponsales no bancarios deberán sujetarse en lo que corresponda a

las medidas de seguridad dispuestas en los subnumerales 4.3.8, 4.3.10 y 4.3.11.”

(Resolución JB, 2012).

CAPITULO 7

Delitos que más afectan al sistema financiero ecuatoriano

Loop Libanes

Este tipo de modalidad trata en que el delincuente coloca un hilo dental, u otro objeto parecido, en la lectora del cajero automático, así cuando el cliente inserta su tarjeta, el cajero no detecta su presencia y la retiene sin pedir la clave al cliente. Ahí es cuando el delincuente entra en acción y se acerca al cliente para decirle que ingrese tres veces su clave para que el cajero le devuelva su tarjeta, incluso los delincuentes en ocasiones utilizan letreros falsos colocados en el cajero. Cuando el cliente se aleja el delincuente retira el hilo dental de la lectora, y con la clave procede a retirar dinero de la cuneta del cliente.

Cambiazo

Trata en reemplazar la tarjeta del cliente por otra, cuando el cliente se acerca a un cajero automático cuando está realizando una transacción, el delincuente le distrae o se la quita con la excusa de limpiársela, en ese instante se la cambia por otra tarjeta. El cliente ingresa la tarjeta cambiada y digita su clave, el delincuente se fija en la clave ingresada, la tarjeta es retenida por ingresar la clave incorrecta, el cliente piensa que está segura porque se encuentra retenida, sin saber que su tarjeta fue cambiada.

Skimming

Es un sistema que se utiliza para copiar toda la información de las bandas magnéticas de las tarjetas de crédito y de débito, a la vez los delincuentes filman el momento que los clientes ingresan sus claves.

Los equipos que se utilizan pasan desapercibidos para los clientes, porque llevan los mismos colores de los equipos originales del cajero.

La única forma de darse cuenta del fraude es revisando los estados de cuenta.

Elementos para funcionamiento del skimming

Cámara

Este elemento es ubicado hacia el teclado numérico del cajero automático, por tal motivo debe estar en un lugar estratégico para que no sea identificado y para que capture la imagen a la hora que el usuario ingrese su contraseña, en algunas ocasiones para obtener esta información los antisociales lo hacen mediante: observación directa, telescopios, cámara de fotos, celulares, colocación en el teclado de talco, grasas, harinas, etc.

Skimmer

Suplanta a la lectora de la banda magnética del cajero automático para obtener la información de la tarjeta la cual se guarda en una memoria SIM que tiene incorporada.

Forma de instalación

El antisocial de antemano ya conoce y escoge el cajero automático.

Trabaja en equipo, por lo menos con un acompañante

Para adicionar estos equipos al cajero utiliza cinta doble face

Los equipos los llevan en mochilas e incluso bajo su ropa.

Phishing y Pharming

Son sistemas que se utiliza en todo el mundo por expertos “hackers” que realizan páginas web falsas que son idénticas a las originales, estos hackers viajan a diferentes

países para que se sea difícil rastrearlos. Los fraudes se realizan a diario a clientes de diferentes bancos, a los cuales se les sustrae toda la información necesaria de sus cuentas bancarias. Muchas veces esta información es vendida en diferentes países, esto hace más difícil rastrear a los delincuentes.

Phishing

Este método de fraude utiliza diferentes modalidades como páginas web, email, redes sociales, chat, etc. Así los hackers logran direccionar al cliente a una página web falsa de su banco. De esta manera logran sustraer información confidencial del usuario y de sus cuentas, como número de cedula, nombres completos, claves secretas, coordenadas de tarjeta, direcciones, números de teléfono, toda esta información es necesaria para realizar la estafa al cliente.

Pharming

Este método de fraude utiliza un tipo de virus ya sea host o troyano que logra filtrarse en los computadores que no están protegidas con antivirus, la forma de filtración de estos virus son a través de email, chat, páginas web. Las personas más propensas a este tipo de fraude son las que utilizan el internet sin precaución y hacen caso a todo lo que aparezca en su computador como promociones, pop up, juegos, links desconocidos. Al momento que ingresa el host y se instala en el computador para cuando el cliente ingresa a la página web de su banco no se dirija a la original sino a una falsa, donde le solicitaran todos sus datos personales.

Clickjacking

También se lo conoce como secuestro de clicks es un método en el cual hay sitios web en los que se esconden botones y diálogos que convencen al usuario envié su

información o instale programas que poseen descifradores de claves. Por lo general estos aparecen en páginas desconocidas que generan mucha desconfianza.

CAPITULO 8

Montos y porcentajes de fraudes

	2009	2010	2011	2012
Fraudes ATM's - Dup. Tarj. Skimming	1.721.027	726.574	1.933.376	2.229.869
Cuentas por Cobrar Varias	537.700	1.350.168	651.363	1.462.963
Fraudes Canales Internet	0	566.079	1.310.738	148.681
Fraudes Tarjetas de Crédito	734.579	426.233	739.238	342.550
Otras Pérdidas Operacionales	610.188	425.611	690.632	451.683
Otros Activos/Faltantes de Caja	505.756	211.386	334.708	194.511
CashManagement	0	0	0	81.501
Fraudes IVR	0	0	131.291	2.090
TOTAL FRAUDES	**1.115.944**	**636.997**	**1.156.631**	**729.785**

Ilustración10: Fraudes (OMSC, 2012)

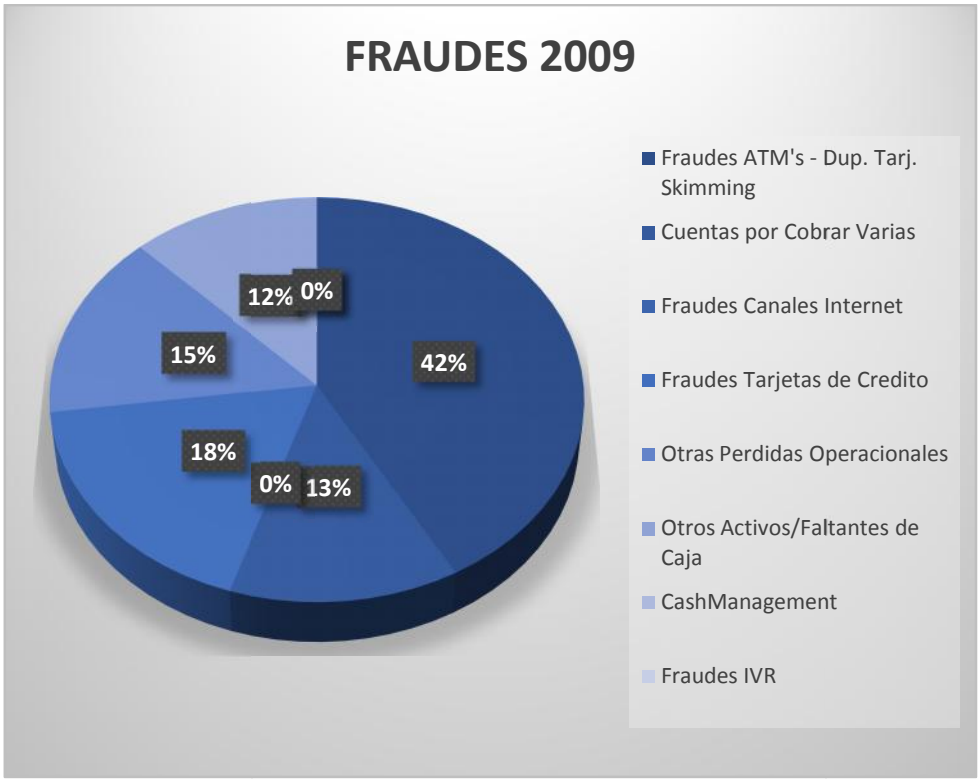


Ilustración 11: Fraudes (OMSC, 2009)

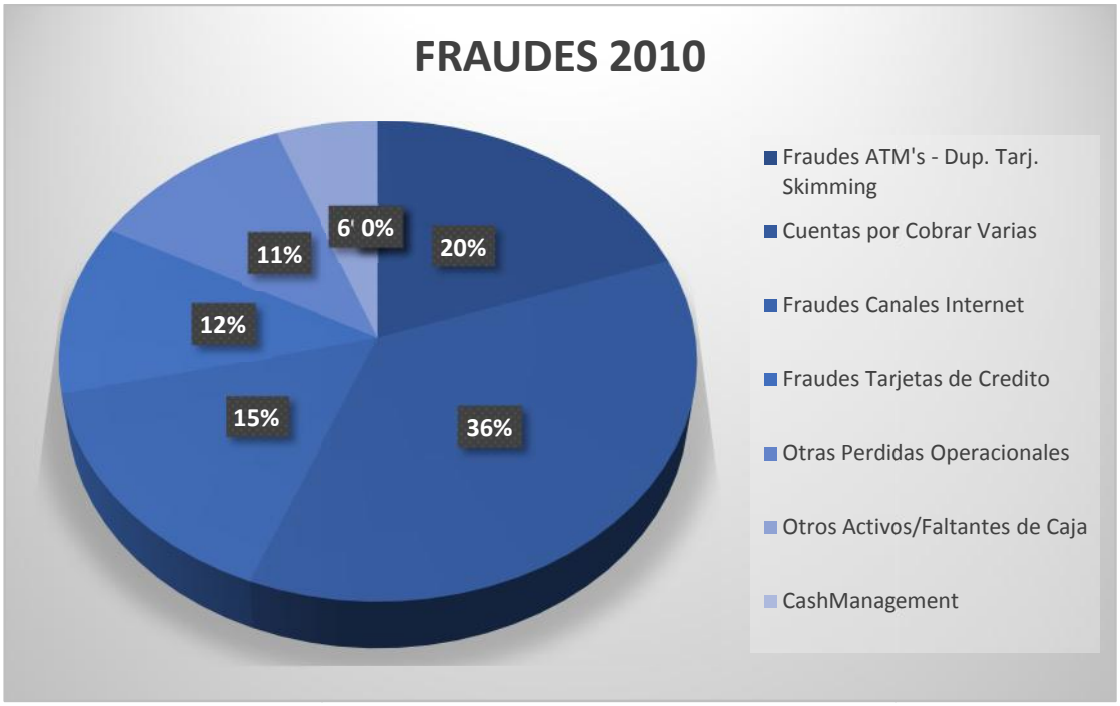


Ilustración 12: Fraude. (Análisis de informe OMSCI, 2010)

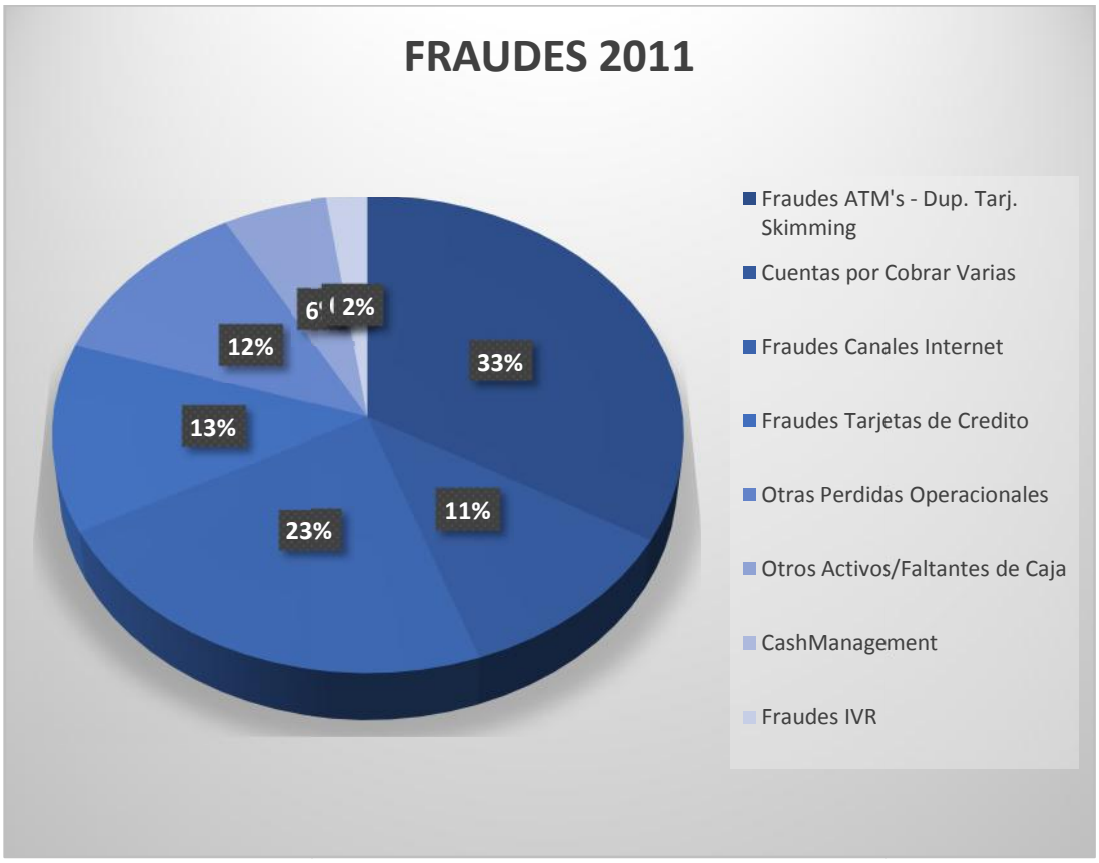


Ilustración 13: Fraude. (Análisis de informe OMSCI, 2010)

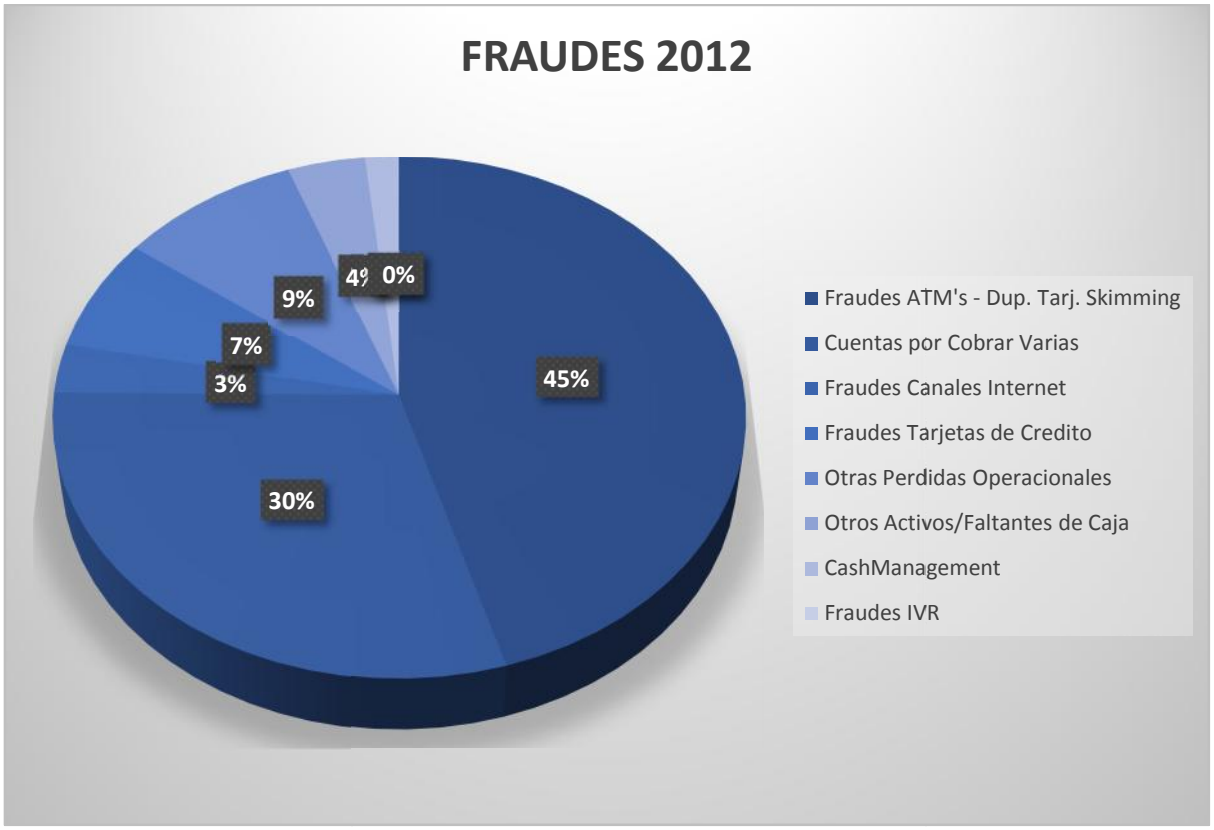


Ilustración 14: Fraude. (Análisis de informe OMSCI, 2010)

Fraude externo 2012 hasta Junio	**2012**	
Fraudes ATM'S - Dup. Tarjeta. Skimming tarjetas duplicadas	1.960.132,08	50%
Cuentas por Cobrar Varias. Multas de organismos de control	1.084.507,72	27%
Otras Pérdidas Operacionales. Cheques Falsificados Microborrado	407.072,11	10%
	271.642,19	7%
Otros Activos/Faltantes de Caja. Asaltos y robos	145.882,90	4%
Fraudes Canales Internet por Phishing y Pharming	81.620,44	2%
Fraudes IVR. Fraudes por compra de minutos para celulares	1.495	0,04%
TOTAL	**3.952.352,44**	**1,00**

Ilustración15: Fraudes (OMSC, 2012)

Ilustración 16: Fraude. (Análisis de informe OMSCI, 2010)

PERDIDA REAL	**2009**	**2010**	**2011**	**2012 hasta Septiembre**
Otras pérdidas Operacionales	610.188,32	425.611,10	690.632,39	583.184
Cuentas por Cobrar Varias	537.700,02	1.350.168,49	651.362,50	1.462.963
Otros Activos/Faltantes de Caja	505.756,22	211.386,21	334.708,24	194.511
Pagos por Cuentas de Clientes	378.023,92	726.051,88	299.014,54	225.102
Fraudes Microcrédito	0,00	-53.000,00	0,00	0,00
Demandas Clientes	0,00	600.000,00	0,00	0,00
Fraudes Canal Internet	0,00	566.079,00	1.310.738,00	148.681
Fraudes IVR	0,00	0,00	131.291,00	2,09
Fraudes Tarjetas de Crédito	734.578,81	426.233,36	739.237,87	342,55
Fraudes ATM'S-Dup. Tarjeta. Skimming	1.721.027,19	726.573,88	1.933.376,11	2.229.869
TOTAL	**4.487.274,48**	**4.979.103,92**	**6.090.360,65**	**4.844.654,64**

Ilustración17: Fraudes (OMSC, 2012)

Reclamos clientes 2010	jun-10	jul-10	ago-10	sep-10	oct-10	nov-10
ATM's Tarjetas de débito en poder del cliente	148	116	146	123	138	112
Casos ATM's cliente no presta la tarjeta de debito	62	50	56	62	49	106
Casos investigación	116	171	186	253	144	161
Casos de investigación – Apelación	18	14	14	23	16	24
TOTAL	**344**	**351**	**402**	**461**	**347**	**403**

Ilustración18: Fraudes (OMSC, 2012)

VALORES FRAUDES 2011		
FRAUDES	**MONTO**	**PORCENTAJE**
PHISHING	754.244,88	25,50%
CHEQUE MICROBORRADO	248.978,24	8,42%
RET. AHORROS FIRMAS FALSIFICADAS	310.774,10	10,51%
SMS	10.668,00	0,36%
CASH. MAG	25.000,00	0,85%
CHEQUE FIRMA FALSIFICADA	1.224.734,32	41,40%
VARIOS	383.619,32	12,97%
TOTAL	**2.958.018,86**	**1,00**

Ilustración19: Fraudes (OMSC, 2012)

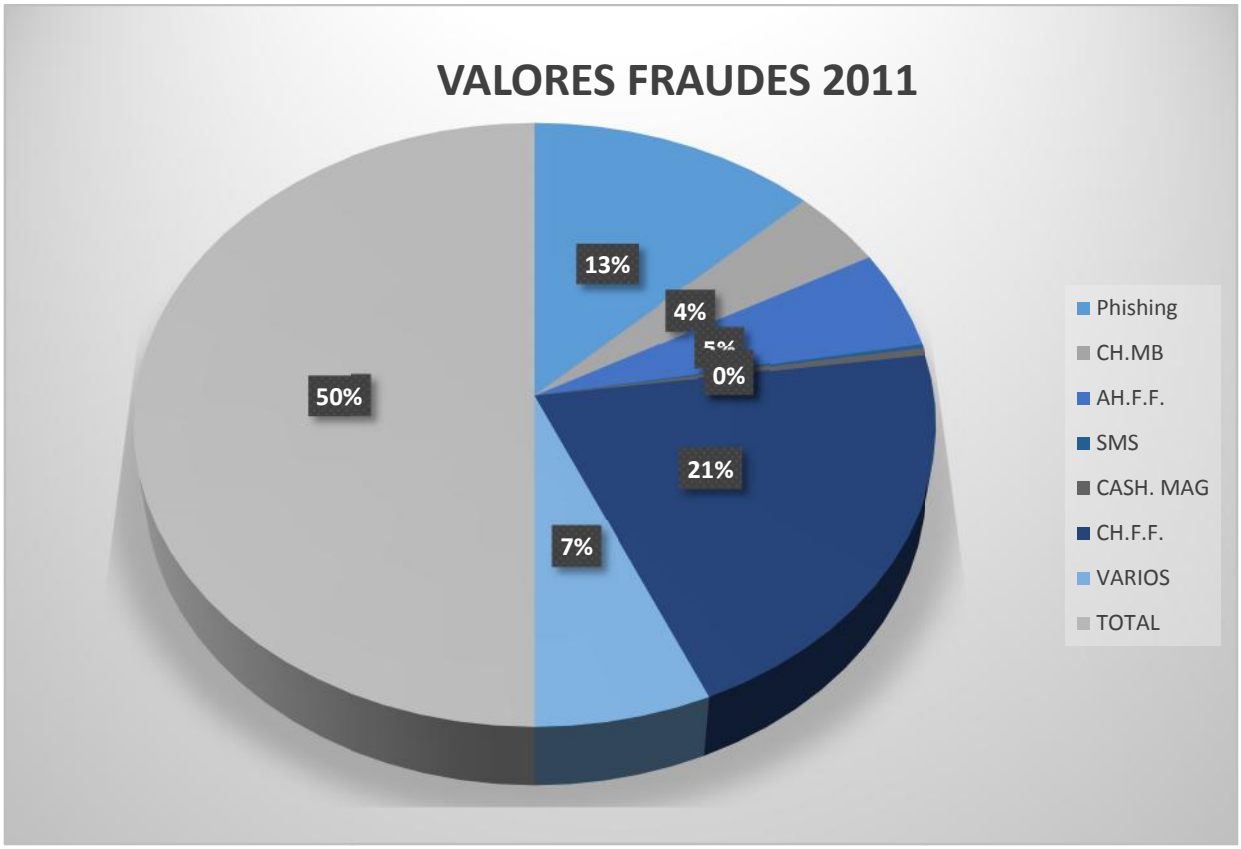


Ilustración 20: Fraude. (Análisis de informe OMSCI, 2010)

VALORES FRAUDES 2011		
FRAUDES	**NUMERO CASOS**	**PORCENTAJE**
PHISHING	245	39,64%
CHEQUE MICROBORRADO	14	2,27%
RET. AHORROS FIRMAS FALSIFICADAS	74	11,97%
SMS	13	2,10%
CASH. MAG	1	0,16%
CHEQUE FIRMA FALSIFICADA	207	33,50%
VARIOS	64	10,36%
TOTAL	**618**	**1,00**

Ilustración21: Fraudes (OMSC, 2012)

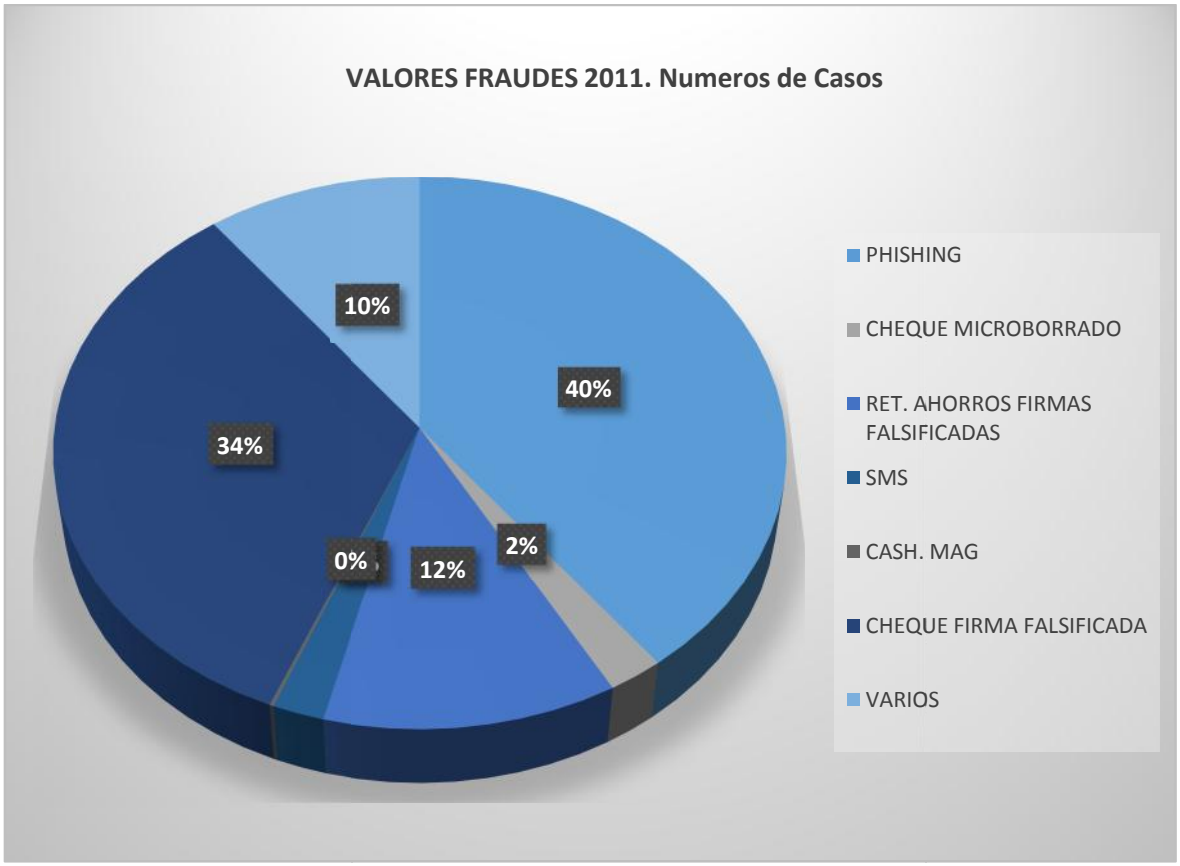


Ilustración 22: Fraude. (Análisis de informe OMSCI, 2010)

CAPITULO 9

Medidas de prevención

Por parte del banco

Los supervisores y vigilantes asignados por agencia deben realizar la inspección cada cierta hora durante el día, en cada agencia dependiendo de su tamaño existen supervisores, vigilantes y motorizados, además en cada ATM hay motorizados y supervisores, ellos son los que se encargan de verificar que no exista ningún dispositivo extraño en los ATMS.

Proceso de sistema de control ATM

Ilustración 23: ATM con cámara oculta y lector de tarjetas falso

Ilustración24: Teclado cajero automático

- Observar la cámara y espejos superiores del ATM
- Observar la lámpara del ATM se encuentre alumbrando correctamente
- Observar que en los parlantes del ATM no se encuentre ningún dispositivo que no pertenezca al ATM
- Observar y verificar que la pantalla del ATM funcione correctamente
- Observar y verificar el funcionamiento de la lectora de tarjetas
- Observar y verificar que el protector del lector de tarjetas tenga instalado el Braket
- Observar y verificar el buen estado del teclado
- Observar y verificar que este en buen estado el protector del teclado
- Observar y verificar el buen estado del dispensador de billetes
- Observar y verificar que no exista ningún dispositivo extraño que no pertenezca al ATM

Ilustración 25: Teclado y dispensador de billetes.

Ilustración 26: Cajerosautomáticos

Cajero automático

Antes de ingresar la clave en el cajero debe tener en cuenta que nadie lo esté observando, es recomendable proteger con la mano el teclado del cajero a la hora de ingresar la clave.

Es recomendable utilizar los cajeros durante el día.

Procure no retirar demasiado efectivo del cajero, de preferencia hágalo acompañado o utilice la banca electrónica.

Memorizar la clave de la tarjeta y no escribir en papeles o documentos.

No permitir que su clave sea vista por extraños.

Si usted existe algún tipo de inconveniente a la hora de hacer un retiro se debe notificar al banco.

Se recomienda cambiar su clave del Cajero Automático periódicamente

No entregar la clave a desconocidos, aunque sean funcionarios del banco o policías.

Las tarjetas son de uso personal no se debe entregar la tarjeta del cajero automático a nadie

En caso de pérdida de la tarjeta del cajero, se deberá notificar inmediatamente para que sea anulada.

Antes de que utilice el cajero automático observar que no exista nada extraño en la ranura por donde ingresa la tarjeta, si existe algo deberá notificarlo.

En el caso de que su tarjeta fuese retenida por el cajero:

No solicite ayuda de terceras personas.

Deberá cancelar la operación que está siendo efectuada.

Reportar inmediatamente al centro de atención.

Banca Electrónica o Banca Virtual

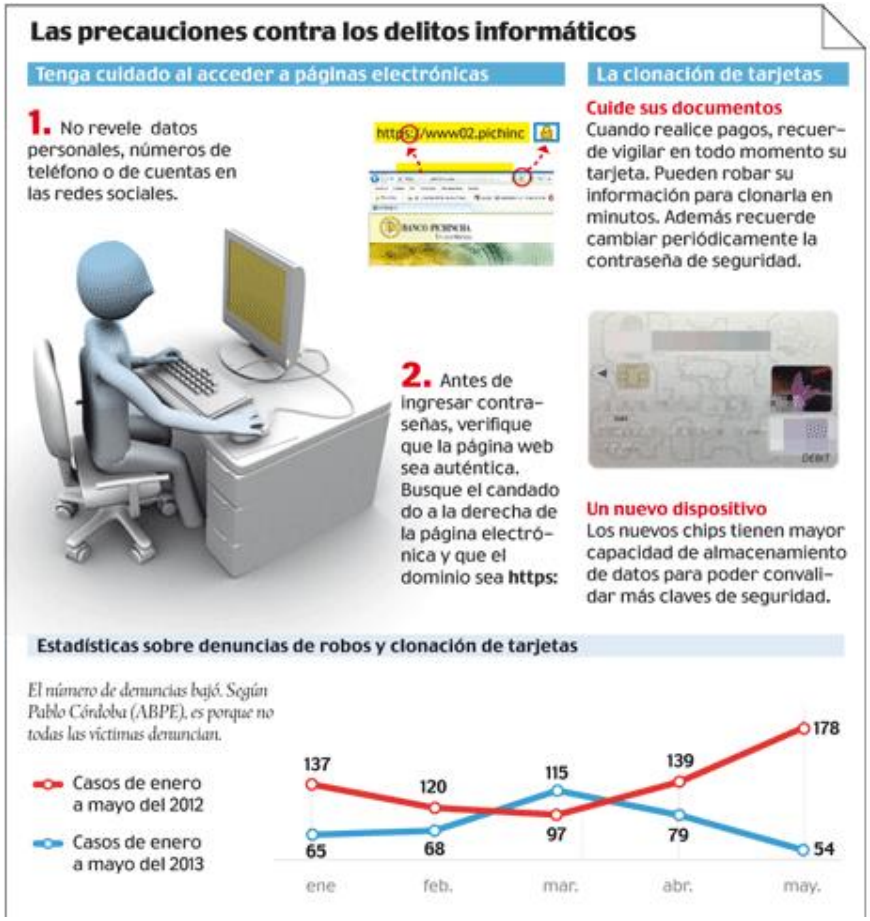


Ilustración 27: Dirección Nacional de la Policía Judicial, (2013)

Seguridades que ofrecen la Banca Electrónica o Banca Virtual

La Banca Electrónica o Banca Virtual se encuentra protegida con tecnología SSL (Secure Socket Layers), esta seguridad sirve para que la información que viaja no sea descifrada por terceras personas.

En algunas páginas de Banca Electrónica, existe la imagen de un candado, este le garantiza la seguridad del sitio a la hora de realizar una transacción. Cuando se da un clic en este candado se obtiene información del certificado de actualización y la fecha de la página web.

En la Banca Electrónica se ofrece un teclado seguro que consiste en cambiar la posición de los numero cada vez que ingresa, esto ayuda a evitar que terceras personas puedan descubrir su clave y no caer en programas como el clicligger que sirve para capturar las coordenadas de las contraseñas de los clientes.

Cuando se intenta acceder a la Banca Electrónica con una clave errónea, el sistema bloquea la clave.

Para realizar una transferencia o pagos la Banca Electrónica ofrece seguridad a sus clientes solicitando claves de su tarjeta de coordenadas.

La Banca Electrónica se desconecta automáticamente por inactividad, consiste en que si durante un periodo de tiempo su ordenador se encuentra en estado de inactividad automáticamente se desconectara, en ocasiones aparecerá en la pantalla: Debe iniciar sección, Acceso no autorizado o automáticamente se cierra la pestaña.Los portales de Banca Electrónica poseen certificados deseguridad y algunas certificaciones sonAutoridad de Certificación como VeriSign.

Ilustración 28: Teclado de ingreso Banca Electronica

Los Bancos nunca solicitan datos o copias de la tarjeta de coordenadas mediante ningún medio electrónico, carta o chat.

Procure usted mismo escribir la dirección de la página web de su banco en su explorador de Internet y no intente ingresar desde un link que le direccione directamente.

Trate de no hacer transacciones en computadores que no sean de su confianza.

Siempre tenga actualizado sus navegadores de internet a sus últimas versiones, porque brindan mayor seguridad.

No ingrese o abra mensajes que sean sospechosos.

Se recomienda cambiar su clave de Banca Electrónica o Banca Virtual periódicamente, siempre que se realice un cambio de clave de seguridad el sistema le solicita los números de su tarjeta de coordenadas.

Se recomienda no utilizar redes inalámbricas desconocidas porque expone a su máquina.

Instale un buen antivirus en su computador y manténgalo con las últimas actualizaciones.

Al encontrarse en la página web de su banco presione la tecla F11 así podrá verificar si la dirección es correcta.

Procure borrar los archivos temporales de internet después que salga de la Banca Electrónica.

Siempre el URL de la página web debe comenzar con https://. La s del final le brinda la seguridad que es la original, en caso de que no tenga la s al final no ingrese al sitio.

Ilustración29: Seguridad página web Banco

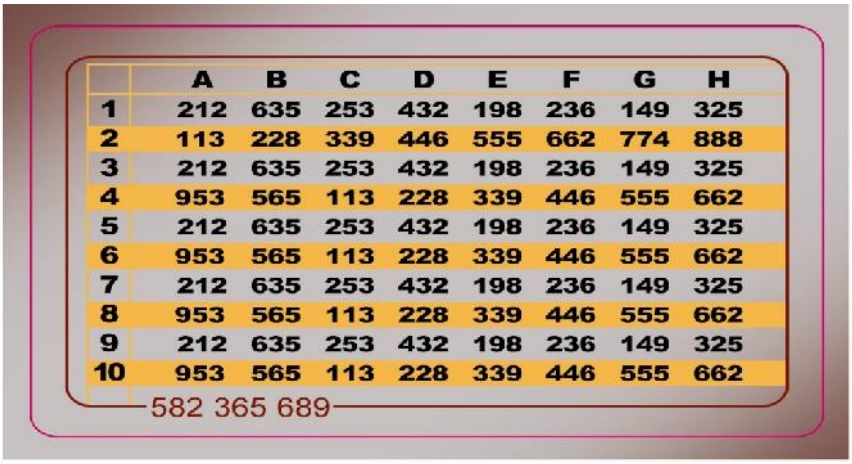
Tarjeta de Coordenadas para Banca Electrónica

Su banco nunca le solicitara claves o coordenadas de su tarjeta por teléfono o medios electrónicos.

No entregue a otras personas su tarjeta de coordenadas.

No tome fotos, saque copias o tenga por escrito las coordenadas de su tarjeta.

Mantener su tarjeta de coordenadas en un lugar seguro y solo llevarla cuando la vaya a utilizar.



	A	B	C	D	E	F	G	H
1	212	635	253	432	198	236	149	325
2	113	228	339	446	555	662	774	888
3	212	635	253	432	198	236	149	325
4	953	565	113	228	339	446	555	662
5	212	635	253	432	198	236	149	325
6	953	565	113	228	339	446	555	662
7	212	635	253	432	198	236	149	325
8	953	565	113	228	339	446	555	662
9	212	635	253	432	198	236	149	325
10	953	565	113	228	339	446	555	662

582 365 689

Ilustración 30: Tarjeta de coordenadas

Chequera

El momento que le entregan su chequera se debe verificar el sello y la secuencia numérica que posee cada una.

No se debe mantener los cheques firmados en blanco o sin valor

Las chequeras deben ser exclusivas para uso personal

Cuando no se utilice la chequera se recomienda mantenerla en un lugar seguro que no sea visible.

Tarjeta de Débito y Tarjetas de Crédito

A la hora que el banco le entregue su tarjeta, recuerde que debe verificar que esta se encuentre en un sobre de seguridad completamente sellado.

En el momento que reciba su tarjeta por parte del banco, no olvide firmar al reverso.

No prestar a nadie su tarjeta de débito o Tarjeta de Crédito.

No debe perder de vista ni un instante cuando haya entregado su tarjeta de débito o de crédito para pagar su cuenta.

En el caso de que existan inconvenientes a la hora de deslizar su tarjeta de débito o de crédito en el dispositivo electrónico de un local o tienda comercial, asegúrese que le muestren el recibo de anulación o cancelación de la misma.

CONCLUSIONES

¿Cuáles son los tipos de fraudes más utilizados que afectan al sistema financiero?

Los fraudes en los cajeros automáticos o ATMS ha ido creciendo en los últimos años de forma significativa, esto debido a la gran vulnerabilidad en las claves de las tarjetas de los clientes, pero son varios los tipos de fraudes que afectan al sistema financiero cada año, estos son los más utilizados por los antisociales: En año pasado fraudes como ATM's – Duplicación de Tarjetas. Skimming causaron el 50% de las pérdidas totales, Cheques Falsificados Microborrado con el 10%, Fraudes Tarjetas de Crédito con el 7%, Otros Activos/Faltantes de Caja. Asaltos y robos, el total en dólares de fraudes en el 2012 fue de USD3.952.352,44. Cabe mencionar que cada día aumenta la tecnología y esto facilita a los delincuentes crear nuevos métodos para fraudes financieros.

¿Cuáles son los fraudes externos e internos y quienes lo comentes?

Los fraudes externos son cometidos por personas de afuera de la empresa que no tienen relación alguna.

Los fraudes internos son cometidos por los empleados de una empresa, sacan provecho de su conocimiento e información que manejan para su beneficio.

En la mayoría de ocasiones los fraudes son realizados por bandas organizadas que tienen como cómplice a un empleado.

¿Cómo ha llegado a beneficiar el desarrollo tecnológico a los antisociales?

El desarrollo tecnológico ha facilitado a los antisociales a que puedan realizar fraude a las instituciones financieras y a sus clientes, la clonación de bandas magnéticas de las tarjetas, las pequeñas cámaras de seguridad que se utilizan para robar las claves de seguridad, los

virus que atacan a los computadores de los clientes, son muestras de la tecnología que poseen los antisociales y burlan las seguridades de las instituciones financieras.

¿Cuáles son las prevenciones que han tomado las instituciones financieras en los últimos 10 años?

Las instituciones financieras siguen varios procesos para mitigar el riesgo que existe para los clientes. Las inversiones en tecnología son altas la Banca Electrónica se encuentra protegida con tecnología SSL (Secure Socket Layers), esta seguridad sirve para que la información que viaja no sea descifrada por terceras personas. Se educa e informa a los clientes de manera continua a los clientes para que puedan tomar medidas de prevención.

¿Qué virtudes y deficiencias presenta el sistema financiero en la actualidad?

Las virtudes que posee el sistema financiero son los software y hardware en los cuales invierten, en la actualidad la banca electrónica posee los más altos estándares de seguridad como cerrar automáticamente la página cuando se detecta inactividad, se ofrece un teclado seguro que consiste en cambiar la posición de los numero cada vez que ingresa, esto ayuda a evitar que terceras personas puedan descubrir su clave y no caer en programas como el clicligger que sirve para capturar las coordenadas de las contraseñas de los clientes, el chip que se debe incluir en las tarjetas de débito y crédito hasta febrero del 2014 estas son las principales seguridades que ofrecen las instituciones financieras para controlar los fraudes. Las deficiencias que se presentan son por la parte de la educación al cliente para que colabore con la lucha contra el fraude, muchos de estos se los realiza por la falta de conocimientos del cliente a la hora de utilizar los servicios de los bancos, por lo tanto no sirve de nada las millonarias inversiones que realizan si a los clientes no se les capacita para usar de la mejor manera estos sistemas.

¿Cómo deben actuar los clientes para minimizar el riesgo que tienen ante los fraudes?

Los clientes deben utilizar las herramientas que les ofrecen los bancos y hacer caso a las sugerencias que les ofrecen.

Limitaciones del estudio

El estudio se limita solo a fraudes que ocurren a los bancos y a sus clientes, existe muy poca información sobre los datos de clientes afectados, los bancos no presentan datos exactos por cuidar su reputación, en ocasiones las personas afectadas tampoco presentan la denuncia.

RECOMENDACIONES

Se presentan a continuación las medidas que deben ser optadas tanto por las instituciones financieras como por los clientes, para neutralizar los diferentes tipos de fraudes:

Actualización constante de datos personales por parte del cliente.

Constante comunicación entre banco y cliente a través de mensajes de texto o correos electrónicos.

Difusión de medidas de prevención para evitar y conocer los tipos de fraudes que existen.

Campañas a través de medios de comunicación, sobre procedimientos de seguridad que deben tomar los clientes de instituciones financieras.

Creación de nuevos departamentos de inteligencia por parte de las instituciones financieras.

Campaña de educación sobre manejos adecuados de los servicios bancarios.

Aumento de inversión en tecnología por parte de las instituciones financieras para prevención de fraudes.

Conciencia por parte del cliente de las instituciones financieras a la hora de utilizar la banca electrónica, cheques, tarjetas.

REFERENCIAS

Estupiñan, R. (2006). Control Interno y Fraudes. Bogotá, Colombia.

Casnovas, P. & Ayuso, M. (2006).*Modelos de Seguridad y Cálculos de Riesgo, Editorial Atelier, Barcelona, España.*

Torrente, D. (2006).*Desviación y Delito, Alianza Editorial, Madrid.*

Baugman, Z. (2008).*Comunidad: en busca de Seguridad en un Mundo Hostil*, Siglo XXI Editores, Madrid.

Beck, U. (2007).*La Sociedad de Riesgo Global,* Siglo XXI Editores, Madrid.

Dammer,L. (2008).*Seguridad Ciudadana, Experiencias y Desafíos, Valparaíso Chile, Programa URBAL.*

INEC, Instituto Nacional de Estadística y Censo. Censo de población. http://www.ecuadorencifras.gob.ec/

UAF, Unidad de Análisis Financiero. Terminología. http://www.uaf.gob.ec/index.php/

Frigo, E. (2008).*Hacia un modelo Latinoamérica de Seguridad Privada, los nuevos desafíos en la región, Primer Congreso Latinoamericano de Seguridad,* Bogotá.

Núñez, J. (2011). Critica a la ideología de la seguridad ciudadana, Flacso-Ecuador.

López, C. J. (2009). *Ciencia y política de riesgo,* Alianza Editorial.

Hebbert, P. (2010).*Seguridad Privada, Pirámide México.*

Agra, C. (2008).*La seguridad en la Sociedad de Riesgos*, Ed. Atelier, Barcelona.

ANEXO A: ENCUESTA REALIZADA AL SR. MS. KLEVER PARRA BONILLA, JEFE DE SEGURIDAD DEL BANCO PICHINCHA, EL DÍA LUNES 09 DE DICIEMBRE DEL 2013

¿Cuáles son los tipos de fraudes más utilizados que afectan al sistema financiero?

En el sistema financiero, específicamente el bancario, se encuentra un sinnúmero de delitos de fraude, que van de la mano con la tecnología, estos son más avanzados cada día y son aplicados en el país como en los de todos los de la región latinoamericana. Por nombrar algunos de estos delitos tenemos los que se les atribuye a la delincuencia común, para situarlos en una primera variable están los que actúan como saca pintas, paquetazos, escopolamina, sustitución de identidad o sustitución de ejecutivos. En otra variable podemos situarlos a los que actúan como pishing (pescando identificación de claves) y robo de claves, tarjetas de crédito y skimming en cajeros automáticos (grabación de claves de usuarios). No se deja de lado la variable de robo a la institución bancaria por delincuentes sea en exteriores o al interior así como por parte del cajero o empleado del banco.

¿Cuál es el tipo de fraude que ha causado más pérdidas económicas a las instituciones financieras?

Las instituciones financieras han tratado de controlar las causas por las que tienen pérdidas económicas y es así que conforme avanza la tecnología, también tiene repercusión en el delito. La empresa financiera ha tenido que tratar constantemente con pérdidas por el pago de cheques adulterados denominados cheques con microborrado que supera el millón de dólares por la astucia de quienes logran pasar los filtros por los elementos utilizados, o por haberse procesado mal durante el pago del mismo. Otro de los fraudes constantes que se deben tratar son los que se refieren a las tarjetas de crédito, por cuánto no se ha logrado

totalmente en educar en seguridad de estos documentos a los clientes que son fácil presa de los anuncios, premios, ventajas que les ofrecen vía internet y caen en la provocación y entregan sus claves personales mediante las cuales son objeto de fraudes que luego son atribuidos al sistema bancario sin atribuirse el perjuicio causado por los clientes. Por último podríamos indicar como otro fraude constante y a diario que sucede en las instituciones bancarias es el skimming, elemento instalado en el cajero automático para grabar las claves de los usuarios sin que se de cuenta de que en ese cajero automático se encuentra instalado un pequeño grabador que recopila la información (clave) personal para luego copiar en cualquier otro tipo de tarjeta y perjudicar al cliente y a la institución financiera.

¿Cuáles son los fraudes externos e internos y quienes los cometen?

Entre los fraudes externos podemos citar el robo a las instituciones financieras y a los vehículos blindados transportadores de valores, en ambos casos existe el enfrentamiento armado y posiblemente muertos y heridos. En cambio los hurtos internos podríamos citar a los faltantes existentes al interior del área de cajas que son atribuidos al personal de cajeros sea por pagos indebidos o faltante de cantidades mínimas que no han sido controlados durante el horario de atención.

¿Cómo ha llegado a beneficiar el desarrollo tecnológico a los antisociales?

La tecnología es desarrollada conforme las necesidades de la ciudadanía para facilitar las operaciones económicas que el tiempo lo requiere, esto es para reemplazar portar el dinero en efectivo desarrollando la tarjeta de crédito personal que permite realizar transacciones y que en definitiva reemplazó al efectivo. Al mismo tiempo la delincuencia se encuentra atenta a cada tecnología que aparece que es impuesta al consumidor con sus fortalezas esto es la inmediatez para sus operaciones, mientras que sus debilidades se encuentran en el uso

y seguridad que el portador da al documento. No se descarta que la tecnología también es analizada y bien aprovechada por los delincuentes ¨científicos¨ que se dedican a descifrar los seguros y que inmediatamente son vendidos como los hiciera de un CD de una película por estrenar.

¿Cuáles son las previsiones que han tomado las instituciones financieras en los últimos 10 años?

La utilización de la violencia en contra de las instituciones financieras y sus clientes ha hecho que se tomen medidas radicales para proteger a las instituciones y clientes en general. El Estado a través de la Ley de Seguridad Pública, El Ministerio de Justicia, el Ministerio Coordinador de Seguridad Interna, la Secretaría de Riesgos y Seguridad y la Superintendencia de Bancos y Seguros del Ecuador, llegaron a la conclusión de que ante la ferocidad delincuencial que acosaba con gravidez a las instituciones y clientes, debían fortalecer a las instituciones con medidas de aseguramiento para los locales bancarios y proteger a clientes que eran asaltados dentro de sus instituciones. ¨velar por la estabilidad, solidez y correcto funcionamiento de las instituciones financieras con el fin de proteger a los depositantes a través de una adecuada administración integral de los riesgos¨, disponiendo a la Junta Bancaria que ¨en virtud del incremento y aparición de nuevas modalidades delictivas que se cometen en perjuicio de las instituciones del sistema financiero, y fundamentalmente de los usuarios de dichos establecimientos, la implementación de medidas efectivas de seguridad con la finalidad de establecer mecanismos y procesos que coadyuven en la prevención de siniestros y actos delictivos¨.

¿Qué virtudes y deficiencias presenta el sistema financiero en la actualidad?

Mediante la aplicación de la Resolución Bancaria, JB-2011-1851, del 11 de Enero del 2011, se impuso la aplicación de condiciones mínimas de seguridad, como manuales y

políticas de seguridad y protección (procedimientos operativos, vigilancia armada, sistemas electrónicos, alarmas, cctv, vidrios blindados, cajas fuertes temporizadas), contenidos fundamentales para la seguridad de las instituciones, en particular de sus empleados y usuarios, establecimientos, bienes y patrimonio, así como para el resguardo en el transporte de efectivo y valores. Las deficiencias se podrían determinar en más concientización a la ciudadanía de que no se expongan ante la delincuencia y que utilicen los servicios gratuitos como son el acompañamiento policial, las alternativas bancarias de transferencias de efectivo, uso de cheques gerenciales y utilización de transportadoras de dinero, servicios que lamentablemente no son utilizados por la impaciencia y por la desconfianza del usuario.

¿Cómo deben actuar los clientes para minimizar el riesgo que tienen ante los fraudes?

Los clientes deben estar conscientes de que cuando se acude a una institución bancaria, sea para depositar y/o retirar efectivo, el riesgo de un asalto es un aliado imperceptible y que no se trata sólo de hombres si no que también están involucrados niños y mujeres que se encuentran al asecho de quién ingresa y quien sale y de que por medio hay el efectivo que es lo que buscan. No es necesario de que crean o no, o que porqué uno puedo o no ser asaltado, no es cuestión de suerte, lo que se requiere es conocer cuáles son las formas de minimizar el riesgo de ser asaltado y por defenderse y no permitir la pérdida se produce la muerte del cliente.

Las causas y proliferación de los delitos y fraudes podemos citar por: Retiro de excesivas cantidades de dinero; desconocimiento de los servicios y alternativas que ofrece la banca para evitar el manejo de efectivo; exceso de confianza e ingenuidad de clientes que retiran grandes cantidades.

Cómo podemos mejorar la seguridad: Evitar el manejo innecesario de altas sumas de efectivo utilizando cheques de gerencia o cheques certificados; pago de servicios utilizando el servicio de débito automático con su institución bancaria; Uso de cajeros automáticos y ventanillas; Convenios de pago a empleados a través del SAT; No delegar a terceros o mensajeros el retiro o depósito de grades sumas de dinero; No comentar transacciones con personas desconocidas; Informar al personal de Seguridad si observa a personas sospechosas al interior del banco; Buen uso de sus claves personales e intransferibles de tarjetas.

ANEXO B: ENCUESTA REALIZADA AL SR. ING. PEDRO NÚÑEZ, SUPERVISOR REGIONAL DE SEGURIDAD DEL BANCO PICHINCHA, EL DÍA VIERNES 13 DE DICIEMBRE DEL 2013

¿Cuáles son los tipos de fraudes más utilizados que afectan al sistema financiero?

Los fraudes bancarios se perfeccionan conforme la tecnología avanza, se libera de obstáculos, vive una constate carrera en contra de la misma evolución que también experimentan técnicas de seguridad y que tienden avanzar en paralelo, es muy parecido a la eterna ley de la oferta y la demanda. La delincuencia de pronto se interesa por un tipo de objetivo o delito, lo golpea varias veces y saca sus beneficios, así tenemos, al menos en nuestro país los delitos denominados como saca pintas, paquetazos, phishing, skimming, microborrados, falsificación de documentos de identificación, con los que más se afecta tanto las instituciones como a los clientes de la banca.

¿Cuál es el tipo de fraude que ha causado más pérdidas económicas a las instituciones financieras?

Son varios los delitos que causan pérdidas económicas a los bancos, podría enunciar los que se refieren al fraude informáticos, transferencias internas no identificadas, uso de

equipo al interior de cajeros automáticos, mal uso de claves de usuarios, pago indebido de cajeros, transacciones mal acreditadas. Los fraudes que son aceptados por la institución financiera tienen un techo regulado por la empresa seguradora, se puede decir entonces, que una institución financiera no pierde porque se encuentra asegurado su capital.

¿Cuáles son los fraudes externos e internos y quienes los cometen?

La seguridad se ha convertido hoy en día en una inversión, no se puede considerar un gasto y de eso están convencidos los empresarios, ejecutivos y comerciantes, conscientes de que pueden ser el blanco más deseado de la delincuencia, quienes tienen el mayor tiempo necesario para estudiar al sistema y a la víctima que por supuesto es quien transporta el dinero o sea el delincuente está presente como lo está el efectivo. Los fraudes externos podría señalarse a quienes utilizan las herramientas tecnológicas actuales para cometer ilícitos utilizando los cajeros automáticos, las claves personales de clientes que exponen sus datos en ofertas realizadas a través del internet; y, los fraudes internos de igual manera por mal manejo de la información confidencial y que entregan muchas de las veces al interior de la institución bancaria.

¿Cómo ha llegado a beneficiar el desarrollo tecnológico a los antisociales?

La seguridad total no existe, todos podemos ser víctimas de un delito, debemos ser realistas, el delito bancario especialmente, aumenta y preocupa, no se puede desconocer las estadísticas que los países indican, los hombres de negocios deben estar atentos para no dejarse arrebatar su patrimonio que incluye naturalmente dinero en efectivo, bines y hasta información confidencial. La tecnología beneficia a delincuentes siempre y cuando la posean y esa cuestión también les cuesta, por eso se realiza la oleada delictiva o auge en el robo bancario, robo a blindados, secuestros extorsivos, robo de vehículos, narcotráfico y luego comienza nuevamente el ciclo que lo único que cambia es el área de operaciones. En

los países vecinos se vende el delito y la tecnología que son importados de países desarrollados. Equipo nuevo instalado, el mismo será violado en el menor tiempo posible, algo parecido como hecho la ley, hecho la trampa.

¿Cuáles son las previsiones que han tomado las instituciones financieras en los últimos 10 años?

Las instituciones financieras aseguran sus activos (capital, talento humano, bienes), sin embargo, ha exagerado el cobro de los servicios entregados al cliente, sus ganancias han sido significativas, especialmente cuando era conocido que colaboraban a candidatos presidenciables y parlamentarios que realizaban leyes para favorecer y/o pagar beneficios personales. La ley bancaria era impuesta por sus accionistas, hasta que la misma cambió en el aseguramiento de locales y clientes. Poco a poco y de acuerdo a la visión institucional, montos de capital, mercado de servicios, número de agencias, número de clientes, también se tomaba en cuenta la seguridad institucional en mayor porcentaje, hoy no se habla en constancia de asaltos bancarios, si no de vehículos blindados, debido a la capacidad de seguridad e implementación de equipo electrónico que permite primero disuadir al delincuente que tiene que pensar dos veces para ingresar, luego a la capacidad de aviso de alarmas, y el tiempo de reacción por parte de cuerpos de seguridad y de policía.

¿Qué virtudes y deficiencias presenta el sistema financiero en la actualidad?

A partir del 2011, mediante una resolución de la Junta Bancaria, se ha realizado cambios notables a favor de las instituciones y de los clientes a través de la instalación de equipos que sirvan para conocer quiénes son los delincuentes para poderlos al menos identificar al interior de la agencia bancaria así como en los cajeros automáticos para conocer al

delincuente que opera esos equipos. La prevención es el objetivo de cada institución, los departamentos de seguridad y riesgos se esmeran en encontrar las mejores soluciones para cada tipo de delito, el laboratorio que se realiza por cada actividad fraudulenta e implementación de sistemas probados beneficia a la institución y a sus clientes. Las instituciones bancarias no pueden abarcar la seguridad de sus clientes fuera del área comercial, digamos que esa parte le corresponde a los entes gubernamentales de seguridad ciudadana, así como entregar lo necesario para que toda la ciudadanía conozca procedimientos de seguridad no sólo comercial sino hasta familiar, un gran reto pero con resultados que pueden ser satisfactorios, que sean reconocidos y que la sociedad se beneficie por tener un país cero delincuencia.

¿Cómo deben actuar los clientes para minimizar el riesgo que tienen ante los fraudes?

Cuando se habla de fraudes contra las personas estamos haciendo referencia a situaciones por lo general más complicadas, traumáticas, y en muchos casos hasta fatales. Lo primero que se puede hacer, aunque suene ridículo es no ir al banco. Las transacciones lo hagamos por teléfono, por internet o cualquier otra vía, siempre será más seguro que ir personalmente a un lugar donde el riesgo es alto como un banco. Si se debe ir, la discreción será la primera aliada manteniendo en reserva nuestra información financiera, no dejar que nadie sepa que concurrimos a un banco a sacar una importante suma de dinero. Se debe evitar los movimientos rutinarios, utilizando diferentes días, horarios, sucursal bancaria y de vez en cuando enviar a un familiar que lo haga por nosotros. Recordar que la rutina le da seguridad al delincuente.