REPUBLICA BOLIVARIANA DE VENEZUELA
UNIVERSIDAD CATÓLICA ANDRÉS BELLO

INCIDENCIA DEL FRAUDE ELECTRÓNICO EN LAS METAS DE EFICIENCIA Y CONTROL DE COSTOS EN LA BANCA VENEZOLANA.

TRABAJO ESPECIAL DE GRADO PRESENTADO COMO REQUISITO PARA OPTAR AL TITULO DE ESPECIALISTA EN INSTITUCIONES FINANCIERAS.
MENCION: ANALISIS Y GESTION DE LAS INSTITUCIONES FINANCIERAS

ROSANA MUÑOZ OVIEDO C.I. V- 11.229.947
PROFESOR: REINALDO LÒPEZ FALCÒN

JUNIO 2007

TABLA DE CONTENIDO

CAPITULO I

INTRODUCCIÓN

Las innovaciones tecnológicas en los medios de pago y comercio electrónico han generado una nueva economía y a su vez producido cambios profundos en las organizaciones, obligadas a crear nuevas estructuras para aprovechar las ventajas competitivas que ofrece esta tecnología. El negocio bancario no escapa de esta revolución que ha dado origen a un cliente más sofisticado y exigente.

En el negocio financiero y bancario, el uso de las citadas innovaciones seguirá creciendo porque el usuario busca comodidad y acceso a la realización de operaciones bancarias sin trabas de horarios.

A través de los medios de pago electrónico se realizan las operaciones de una forma más económica para el cliente y para la institución bancaria. Sin embargo, es imprescindible la seguridad en dichos medios; las negociaciones financieras requieren contar con sistemas altamente confiables de seguridad.

Cuando la banca advierte sobre la necesidad de reducir el tráfico de personas en las distintas agencias bancarias, de ninguna manera puede interpretarse como una invitación a que los clientes retiren sus cuentas y vuelvan a la vieja práctica de ahorrar bajo el colchón el producto de su trabajo. Todo lo contrario, de lo que se trata es de que, a través de las distintas opciones electrónicas, los usuarios puedan hacer la mayor cantidad de operaciones financieras sin tener que movilizarse al banco. No obstante, hay quienes por temor, o por tradición, se resisten a la tentación de usar las redes electrónicas. Cambiar la conducta del usuario es un reto cuesta arriba

que se ha planteado la banca y la seguridad en las transacciones electrónicas es el primer obstáculo a vencer.

En los últimos años, el incremento en los casos de fraude electrónico, atenta contra la necesidad que tiene la banca de incrementar las operaciones electrónicas y con esto disminuir sus costos de trasformación.

En una entrevista publicada por el diario Ultimas Noticias el 11 de Abril de 2007, el Sr. Julio Rivero, comisario del Cuerpo de Investigaciones Científicas, Penales y Criminalísticas (CICPC), señala que en Caracas clonan entre 3 y tarjetas bancarias al día, cifra aproximada ya que solo son las denuncias que se reciben en ese despacho. El Presidente del Consejo Bancario Nacional, Víctor Gill, también se pronuncia sobre el tema (entrevista publicada en el diario el Nacional el 14 de junio de 2007) y reconoce que en las últimas semanas, el sistema financiero y los ahorristas han sido víctimas frecuentes de fraude a través de cajeros automáticos y cuentas nómina. Señala también que una propuesta concreta para blindar los sistemas contra este tipo de delitos, es la introducción de una chip (microcircuito) en las tarjetas de débito y crédito, siendo el tiempo estipulado para que todo el sistema financiero cuente con este dispositivo es de entre uno y dos años.

La presente investigación está motivada por el impacto de que tiene el fraude electrónico en el sistema bancario del país y pretende analizar las incidencias del mismo en las metas de eficiencia y en la reducción de los costos operativos de la banca venezolana.

CAPITULO II

PLANTEAMIENTO DEL PROBLEMA

El importante incremento de los casos de fraude electrónico, generan alarma y preocupación en la directiva de los bancos, comerciantes y en el público en general. En el Instituto para la Defensa y Educación del Consumidor y del Usuario (INDECU) y en el Cuerpo de Investigaciones Científicas, Penales y Criminalísticas (CICPC), reposan gran cantidad de denuncias sobre clonación de tarjetas de crédito y débito y consumos o cargos no reconocidos.

Estas irregularidades ponen en peligro el futuro de las operaciones automatizadas y la reducción de los costos bancarios mediante el uso la tecnología, la cual busca disminuir la asistencia de público en las agencias bancarias y abaratar procedimientos eliminando papeles, cheques, planillas y personal bancario.

Por otra parte, en opinión del Dr. Grasso (2007) la banca enfrenta importantes retos para el año 2007 los cuales “son muy variados y muy complejos, ya que se espera que pronto sea aprobada la nueva Ley de Bancos con una mayor carga de regulaciones”. Entre las posibles regulaciones que serán impuestas están, las normas sobre el funcionamiento de la Unidad de Atención al Cliente y la solución de reclamos, en donde el banco deberá demostrar que el reclamo no es procedente, normas para el servicio de cajeros automáticos, creación del Concejo Nacional de Usuarios del Sistema Bancario, y en general, mayores facultades para la Superintendecia de Bancos e incremento de responsabilidades y sanciones para la Banca.

Al 31 de Marzo 2007, operan en Venezuela cincuenta y ocho (58) instituciones financieras, de las cuales cuarenta y ocho (48) son de capital privado y diez (10) pertenecen al Estado. Este gran número de instituciones ofrecen básicamente los mismos productos a sus clientes, razón por la cual, la competencia para incrementar cuotas de mercado, vendrá dada por la adecuación a los cambios impuestos, la capacidad de asumir los costos para implementarlos y la calidad de los servicios que ofrecen.

Uno de los cambios más importantes a realizar, será la incorporación de nueva tecnología, factor determinante en el logro de la efectividad y eficacia en las operaciones bancarias y en la disminución de los costos.

En este sentido, el investigador Antonio López Rodríguez, adscrito al Banco Central de Venezuela, señala: "Al comparar el nivel de los gastos de transformación en Venezuela con los registrados por la banca en otros países de la región se observa que, en promedio la banca venezolana registra valores de 11,4%, mientras que el promedio latinoamericano excluyendo a Venezuela se ubica en 5,8% "[1]

Del planteamiento formulado anteriormente, se deriva la necesidad que tiene la banca venezolana de disminuir sus costos, siendo un punto importante, la sustitución de medios de pagos tradicionales como los cheques, por medios de pagos menos onerosos y más eficientes, como los pagos electrónicos. Sin embargo, cabe preguntarse:

¿Cómo incide en este cambio el incremento del fraude mediante medios de pagos electrónicos?

---

[1] López Rodríguez, citado en: Bello R, Gonzalo. Operaciones Bancarias en Venezuela. UCAB. 2004. Pág. 302

CAPITULO III

OBJETIVOS DEL TRABAJO

OBJETIVO GENERAL

- Analizar las incidencias del fraude mediante medios de pagos electrónicos en las metas de eficiencia y reducción de los costos operativos de la banca venezolana.

OBJETIVOS ESPECÍFICOS

- Identificar las causas y procedimientos que originan el fraude mediante medios de pago electrónicos de la banca venezolana.

- Identificar los tipos de operaciones fraudulentas más comunes en Venezuela.

- Cuantificar el fraude mediante medios de pago electrónicos, como las tarjetas de débito y crédito.

- Identificar las instituciones bancarias venezolanas que reciben mayor número de reclamos por concepto de fraude en los medios electrónicos de pago.

- Formular alternativas en torno a las incidencias del fraude mediante medios de pago electrónicos en las metas de eficiencia y de reducción de costos de la banca venezolana.

CAPITULO IV

MARCO DE REFERENCIA

Banca electrónica en Venezuela

El Dr. Grasso Vecchio (2006) define la Banca Electrónica como el medio electrónico de distribución de servicios bancarios que nos permite movilizar nuestro dinero sin necesidad de entrar a la sucursal o agencia de nuestro banco. Se creó con el fin de aumentar los canales de distribución y de descongestionar las agencias. Dentro de lo que conforma una banca electrónica tenemos los cajeros automáticos, las tarjetas de débito y la banca a domicilio a través de medios electrónicos entre otros.

En Venezuela, la banca ha ido evolucionando hacia un negocio en el cual se prestan múltiples servicios, dentro de los cuales los no financieros están ganando terreno de forma significativa.

Como en otros países del mundo, la reducción que han experimentado los índices de intermediación financiera, han obligado a la banca a obtener mayor rentabilidad, por medio de la prestación de otros servicios entre los que se encuentran los sistemas de pago electrónicos, no considerados tradicionalmente como servicios financieros.

En los años 80, comienzan a constituirse los cajeros automáticos o ATM's (las siglas corresponden a *Automatic Teller Machin*), como una atractiva manera de ahorrar tiempo para los clientes bancarios y posteriormente una fuente de ahorro de costos para la gestión bancaria.

Para esa fecha comienzan las negociaciones, entre un grupo de bancos, entre los que se encontraban Provincial (hoy BBVA Banco Provincial), Venezuela, Caracas y Venezolano de Crédito, para la interconexión entre las redes y cajeros operativos en el mercado.

El 31 de Agosto de 1.987, se constituye la Corporación SUICHE 7B, C.A, como empresa de servicios de interconexión, bajo el lema "Su ingreso cómodo hacia la electrobanca: 7 días completos de banca a la semana". La propia corporación reconoce que este año transcurrió saturado de investigaciones, pruebas y ensayos.

Para agosto de 1.988, la Corporación SUICHE 7B, se encontraba constituida por tan solo 50 cajeros. Más adelante, motivado por el mejoramiento del "software utilizado, las normas y procedimientos implementados y a la acertada administración impulsada por el directorio, para fines de año se había incrementado el número a 109 cajeros automáticos en plena función y más de 70 puntos en operación"[2]

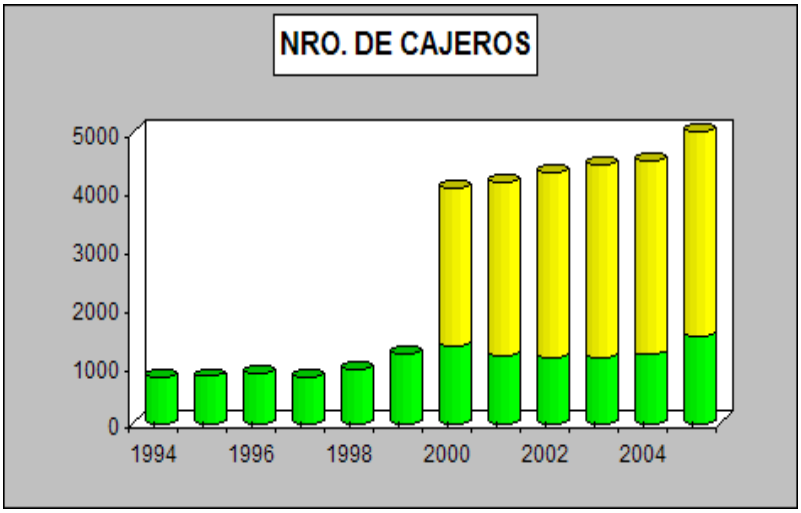
El 14 de Junio de 1.989 se constituye Proyectos Conexus C.A, mediante una alianza de los bancos Consolidado, Mercantil, Latino y Unión.

"Desde el 16 de agosto del año 2000, las Redes CONEXUS y SUICHE7B se encuentran interconectadas, permitiendo a todos los clientes del Sistema Financiero Venezolano el acceso a más de 4.000 cajeros automáticos distribuidos por toda la geografía nacional, estableciéndose las bases para la incorporación de nuevos servicios que permitirán seguir ampliando y dándole

[2] Reseñado en la página web de la Corporación Suiche 7B

valor agregado al portafolio de servicios financieros ofrecidos a través de los bancos miembros"[3]

Actualmente en la Red Conexus participan ocho (8) Instituciones Financieras: Corp Banca (antiguo Consolidado), Mercantil, Banesco (antiguamente Unión), Citibank, Fondo Común, Banpro, Central y Banplus.

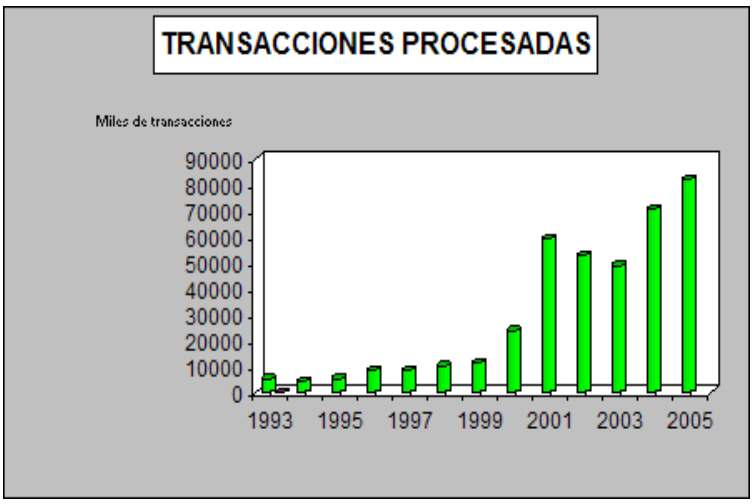


Fuente: Página web de la Red Conexus

Nota: Desde Julio 2000, las redes Conexus y Suiche 7B están interconectadas.

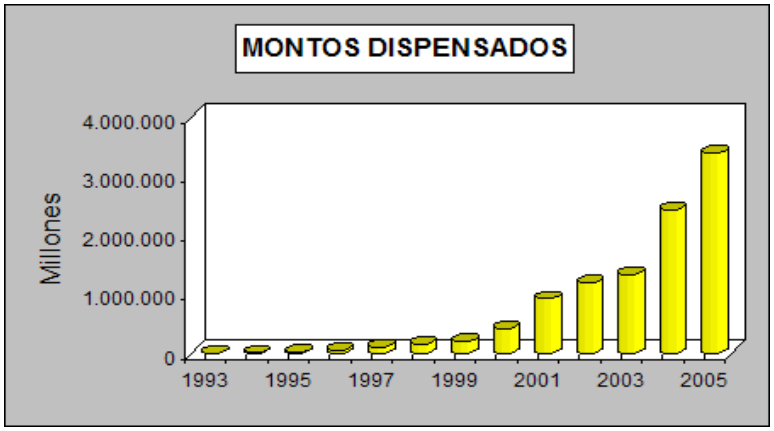
Año	1.994	1.995	1.996	1.997	1.998	1.999	2.000	2.001	2.002	2.003	2.004	2005
CONEXUS	794	811	875	808	932	1.206	1.333	1.155	1.116	1.127	1.177	1.492
SUICHE 7B							2.710	2.988	3.186	3.305	3.321	3.899

[3] Reseñado en la página web de la Red Conexus.



Fuente: Página web de la Red Conexus

Año	1.994	1.995	1.996	1.997	1.998	1.999	2.000	2.001	2.002	2.003	2.004	2.005
Nro. Tran. Procesadas (Miles)	4.328	5.437	8.386	8.494	10.098	11.443	23.766	59.334	53.005	49.090	70.675	82.212



Fuente: Página web de la Red Conexus

Año	1.994	1.995	1.996	1.997	1.998	1.999	2.000	2.001	2.002	2.003	2.004	2.005
Miles de Millones Bs. Dispensados	11.9	23.4	58.6	116.6	162.3	201.6	424.3	927.5	1.19,.5	1.339,4	2.009,6	3.389,4

Ventajas y Desventajas de la Banca electrónica

VENTAJAS	DESVENTAJAS
Procesos de mayor calidad por la reducida intervención humana. Menor Costo.	Dificultad por parte del cliente en el uso de nuevas tecnologías
Comodidad para el cliente, reduciendo tiempos de espera y sin necesidad de ajustarse al horario de atención de las oficinas.	Rechazo por parte de los clientes, por preferir el contacto humano.
Facilidad de distribución, por la amplia Red de Cajeros y el incremento de los centros de telecomunicaciones.	Dudas sobre la seguridad del sistema, especialmente si se trata de información confidencial o de operaciones financieras
Disponibilidad de acceso en diversos espacios físicos.	Incapacidad de algunas personas para operar con dispositivos electrónicos.

Riesgo Operacional y Seguridad de la Información.

Tradicionalmente el manejo de los riesgos en las instituciones financieras estaba centrado en los riesgos financieros, sin embargo, la presión constante de factores externos como la globalización y competencia en el mercado y el incremento de las regulaciones, y factores internos, como la automatización de procesos, la tecnología de la información y la banca electrónica; han fomentado cambios en la percepción del riesgo, ante lo cual se plantea que las instituciones financieras, no solo deben cumplir con estándares cualitativos sino también con estándares cuantitativos.

En Junio del 2004, el Comité de Supervisión Bancaria de Basilea, publicó el documento “Convergencia Internacional de medidas y normas de capital: marco revisado”, conocido como Basilea II, que propone establecer una

relación directa entre el requerimiento de capital de un banco y el grado de riesgo en que éste incurra, más específicamente, que el capital de los bancos sea suficiente para protegerse contra los diversos riesgos.

Entre los riesgos que se comienzan a cuantificar, se encuentra el riesgo operacional, que es la probabilidad de daños potenciales y pérdidas motivados a las formas de organización y a la estructura de sus procesos de gestión, debilidades en los controles internos, errores en el procesamiento de operaciones, fallas de seguridad e inexistencia o desactualización en sus planes de contingencias del negocio. Así como, la potencialidad de sufrir pérdidas inesperadas por sistemas inadecuados, fallas administrativas, eventos externos, deficiencias en controles internos y sistemas de información originadas, entre otros, por errores humanos, fraudes, incapacidad para responder de manera oportuna o hacer que los intereses de la institución financiera se vean comprometidos de alguna u otra manera.[4]

En el riesgo operacional cobra vital importancia, la Seguridad de la Información, que contiene el marco de políticas, procedimientos operacionales, la estructura organizativa y el uso del software para proteger la información de la destrucción, manipulación o revelación no autorizada, ya que uno de los activos más importante de la banca, es la base de datos de sus clientes (activo intangible).

Para las bases de datos (activos de información) se establecen medidas tendientes a mejorar la seguridad, las cuales pueden ser de dos tipos:

[4] Gaceta Oficial Nro. 37.703 del 30-06-03. Artículo 2.

- Las orientadas a mejorar el control interno, lo cual comprende la protección de la información para prevenir el fraude y garantizar su exactitud y confiabilidad.
- Las encaminadas a definir un plan de contingencia ante hechos no previstos, cuyo objetivo primordial es reducir el impacto de los mismos una vez han ocurrido.

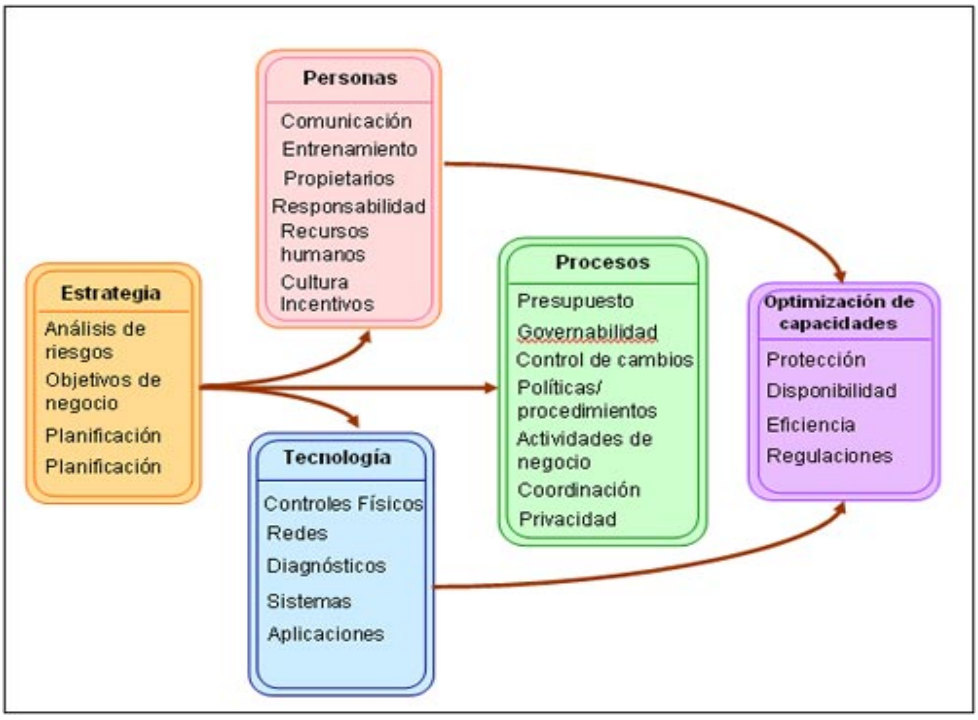
Entre las razones que justifican que un activo de información debe protegerse o asegurarse se encuentran las siguientes:

- Pérdida de información de la institución o corporación, lo cual lleva a una pérdida de la ventaja competitiva.
- Daño a la reputación de la corporación o institución y a la reputación profesional del equipo gerencial.
- Pérdidas financieras por desvío de fondos, documentos, investigaciones y pérdidas de clientes, como respuesta al incidente.
- Riesgo de envío de virus u otros códigos peligrosos.

La seguridad en la información concierne a tres áreas importantes a saber:

- Confidencialidad. La información debe estar disponible sólo para quienes tienen el derecho de acceder a ella
- Integridad. La información debe ser modificada solo por aquellos que estén autorizados a hacerlo.
- Disponibilidad. La información deber ser accesible para aquellos que la necesiten cuando la necesiten.

La Seguridad de la Información, hoy en día, no es sólo un aspecto tecnológico, por el contrario, es una solución integrada de negocio que combina recursos organizacionales, procesos y tecnología. (ver gráfico). Para que el dinero que se invierte en tecnología, no sea más que una perdida de dinero, las organizaciones deben contar con reglas, lineamientos, responsabilidades, procedimientos definidos y personal capacitado para la gestión de cada proceso. "Este concepto de seguridad de la información como una solución integral es esencial para la transformación de este nuevo enfoque, en una plataforma tangible, pragmática y operativa de seguridad, que brinde resultados cuantificables para el negocio."[5]



Fuente: Espiñeira, Sheldon y Asociados.

[5] Espiñeira, Sheldon y Asociados. PC-News.com. Abril 2005

A medida que el rol de seguridad de la información evoluciona, los directivos y ejecutivos de negocio reconocen que esta es sin duda, el primer paso en la relación entre la organización, sus clientes, socios de negocio, proveedores y empleados. En este sentido, la seguridad de la información acarrea enormes implicaciones para las organizaciones debido a que la confianza es la base para el intercambio, y su ausencia es una buena razón para hacer negocios con la competencia.

A pesar de las mejores tecnologías y arquitectura de seguridad, no hay manera conocida de proveer una protección de información completa. Así, la mitigación del riesgo es el único enfoque práctico que puede tomar toda organización.

Fraude electrónico

"Sugiere cualquier cambio no autorizado y malicioso de información contenida en bases de datos electrónicas, ya sea que medie o no el ánimo de lucro o un perjuicio a terceros. Es una nueva forma de acometer acciones que están reñidas con la legalidad; es una forma elegante donde no está presente la fuerza, sino la tecnología moderna, armonizando con pretensiones personales"[6]

"Toda conducta dirigida a la obtención de un provecho económico indebido mediante la apropiación, la falsificación, la interferencia y la reproducción de códigos, instrucciones o programas, tanto sobre instrumentos portables como sobre programas incorporados a sistemas de

[6] Galvis Sánchez, José. Los Fraudes en la Cibernética. Universidad Bicentenaria de Aragua. 1.998

procesamiento de datos, que permiten el acceso a dinero en efectivo o a bienes y servicios con cargo diferido a cuentas bancarias"[7]

El artículo 14 de la Ley Especial contra Delitos Informáticos, lo tipifica como delito de peligro y lo define como "manipulación de sistemas de información o datos, mediante la inserción de instrucciones falsas o fraudulentas que permitan obtener un provecho injusto en perjuicio ajeno"

La clonación de tarjetas de crédito y de débito se ha convertido en la forma más frecuente de realizar fraudes, a pesar de que el equipo para este proceso cuesta alrededor de diez mil dólares y su manejo es sofisticado. Los ladrones de cuello blanco y los hackers (término utilizado para referirse a un experto relacionado con las tecnologías de la información y las telecomunicaciones. Usando la palabra inglesa, quiere decir divertirse con el ingenio (cleverness), usar la inteligencia para hacer algo difícil), perfeccionan cada vez más sus métodos de sustracción de datos en entidades bancarias, manipulación de programas, falsificación de documentos comerciales, virus, gusanos -programas que se infiltran dentro de otros programas para modificar datos-, sabotajes informáticos, entre otros, son algunos de los delitos electrónicos reconocidos por la Organización de las Naciones Unidas (O.N.U)

En Venezuela el fraude vinculado estrictamente a operaciones a través de Internet, constituye un área de criminalidad relativamente limitada, aunque con perspectivas de expansión, considerando el grado de incorporación de usuarios a la red, que de acuerdo a estadísticas de la Cámara Venezolana

[7] Centro de Investigaciones Jurídicas, núcleo de estudios sobre delincuencia económica. Delincuencia Económica y Tecnologías de la información. UCAB. 2004

Fuente : Cámara Venezolana de Comercio electrónico- CAVECOM)

de Comercio Electrónico (CAVECOM) se ubicó al cierre del 2005 en 12% de la población total (ver gráfico 5)

De acuerdo con el profesor de Derecho Penal de la UCAB y la UCV, Juan Modelel[8], el fraude informático está contemplado dentro de lo que ley cataloga como delitos económicos, es decir, aquellas conductas que afectan el orden socioeconómico del país (sistema financiero, sistema de valores, propiedad intelectual e industrial, administración de sociedades e incluso hasta el medio ambiente). A su juicio, estos delitos no causan daño sólo al sistema económico, sino también a la administración de justicia del país, pues es una forma de encubrir otros delitos más graves, como el lavado de dinero.

Los fraudes con tarjetas de crédito falsificadas han sido definidos como el robo bancario de fin de siglo. Sólo en Estados Unidos, este delito cuesta a los bancos cuatro mil millones de dólares anuales. Este tipo de fraude se

[8] Modelel, Juan en: El fraude electrónico se supera a sí mismo. El Universal. 24/03/2007

inició con métodos rústicos para obtener la información del tarjetahabiente, mediante el papel carbón con el que se pasaban los bauchers.

Las instituciones bancarias desarrollan sistemas de monitoreo y nueva tecnología para prevenir transacciones fraudulentas, no obstante, los delitos avanzan para evadir los complejos sistemas de seguridad de los bancos y encuentran un campo fértil para sus operaciones delictivas donde existen vacíos legales a pesar de la promulgación el 06 de Septiembre de 2.001 de la Ley Especial sobre Delitos Informáticos, la cual tiene como objetivo principal, la prevención y sanción de los delitos cometidos contra sistemas o cualquiera de sus componentes o los cometidos mediante el uso de dichas tecnologías.

El tema del fraude en las operaciones electrónicas bancarias actualmente es tema de discusión en distintos escenarios. A continuación algunas noticias publicadas en la prensa nacional durante el año 2007.

El Provincial actualiza sus sistemas de seguridad: Desde el año 2005, el BBVA Banco Provincial ha venido adquiriendo todo tipo de equipos y sistemas a fin de garantizarles transacciones seguras y transparentes a sus clientes, al igual que lo ha venido haciendo buena parte de las entidades que conforman el sistema financiero venezolano. Desde los softwares más sofisticados, sistemas de circuitos cerrados en oficinas y cajeros automáticos, hasta teclados virtuales y láminas separadoras en los telecajeros son algunas de las herramientas que ha aplicado esta institución para minimizar el riesgo a sus clientes, al momento de hacer cualquier operación. En este sentido, Pedro García, gerente del Área de Prevención de Fraudes del Provincial, explica que la entidad fue pionera en la activación de diversos sistemas de seguridad que han permitido reducir hasta en 60% las estafas electrónicas. El Mundo 7 (15-05-07)

Mercantil resguarda la seguridad con teclado virtual: Con el fin de disminuir los riesgos de fraude, Banco Mercantil, subsidiaria de Mercantil Servicios Financieros, desarrolla acciones orientadas a diseñar sistemas seguros para sus clientes. Para ello utilizan innovaciones tecnológicas en cada uno de sus servicios. La banca electrónica (Mercantil en Línea Personas y Empresas) está encaminada a proteger los datos financieros del cliente cuando realiza sus transacciones en línea y evita la comisión de actos ilícitos, mediante la implantación de un teclado virtual y certificados digitales para la identificación del usuario. El Mundo 2. (15-05-07)

Transferencias fraudulentas y ofertas engañosas son los delitos más comunes: La pesca se ha transformado; pasó de ser una actividad recreativa y que sirve como una forma de sustento para las personas, para convertirse en una práctica en la Web con fines distintos a los antes descritos. Al *Phising o pesca* se le conoce como una acción perversa. El comisario Julio César Rivero, jefe de la División contra los Delitos Informáticos, explicó que es la simulación de una página Web y que a través de un link o conexión cambia el nickname (forma cómo me identifico en la red), y con ello engañar a las personas. Una de las más usadas es aparentar ser el portal de un banco. Un cliente recibe un correo y se le pide que actualice los datos, incluyendo número de cédula de identidad, de cuenta y clave secreta, y hacer clic en un enlace determinado. El Nacional 4 (12-05-07)

Microsoft Venezuela reúne a principales empresas del país para analizar la seguridad informática: En la segunda edición de la Semana de la Seguridad en Internet, Microsoft Venezuela reunió a los Jefes de Programas de Seguridad de la Información de las principales empresas e instituciones del país con el fin de dar a conocer normativas de beneficio para el

ecosistema y de la empresa, estándares y valor de una unidad de seguridad. Microsoft congregó como aliados a la Alianza Nacional de Usuarios y Consumidores (Anauco), el Banco Mercantil, la Cámara Venezolana de Comercio Electrónico (Cavecom-e), Cadena Capriles, Cecodap, Genesis Telecom, Hewlett-Packard de Venezuela, IDC, Isaca, Isec (Information Security Inc.) y El Nacional, para educar a la población sobre cuál es la mejor manera de protegerse ante los peligros de la red, proporcionando información, educación y asesoría para ayudar a usuarios, empresas y profesionales IT a hacer sus sistemas más seguros y prepararlos frente a cualquier amenaza de seguridad. Panorama Digital (17-05-07)

Tarjetas de Crédito para combatir el fraude electrónico Los casos de fraude electrónico en el mundo van en franco crecimiento. En los últimos dos años, pasaron de 30 millardos de dólares a 100 millardos, según cifras divulgadas en el XXI Congreso Latinoamericano de Seguridad Bancaria, realizado el año pasado en 2006.

Eso por un lado. Por el otro, resulta que, según Datanálisis, 41% de los venezolanos está preocupado por la seguridad.

Este es el contexto de un problema que abrió un nicho comercial. El Banco de Venezuela lanzó ayer un producto destinado a aprovecharlo. Se trata de una tarjeta de crédito Master Card, edición Titanio, cuyo valor agregado principal es que está blindada contra fraude electrónico, pérdida, robo o clonación.

El vicepresidente ejecutivo de Banca Comercial del banco, Claudio Melandri, indicó que con el producto se espera aumentar en 50% su base de tarjetahabientes, que actualmente supera las 700.000 personas.

Entre otras particularidades, Titanio promete devolver al cliente los montos por consumos que no haya realizado, dentro de las 48 horas previas al momento en que reportó la tarjeta como extraviada.

"Esto lo hacemos porque mucha gente no se da cuenta de inmediato cuando extravía o le roban la tarjeta". Las restituciones del dinero se realizarán también en 48 horas. El Universal 24/03/2007

Costos en la Banca y su relación con los sistemas informáticos

Al relacionar los sistemas informáticos con los sistemas de costos en la banca, el resultado es que dichos sistemas contribuyen a reducir los costos a través del fortalecimiento de la banca electrónica.

La banca venezolana presenta un importante desfase tecnológico en comparación con el nivel alcanzado en países industrializados. Este desfase se observa en el tipo de herramientas tecnológicas utilizadas, en la inadecuada infraestructura de telecomunicaciones y en la escasa penetración de los medios informáticos en la población, por lo cual la actualización tecnológica, ha cobrado una importancia vital, aunque en un primer momento supone, la erogación de inversiones significativas, pero en una segunda fase, estos procesos deberán tender hacia una racionalización de los costos, en la medida que las transacciones se realicen por vía electrónica, que pueden ser hasta ocho (8) veces menos onerosas que por vías físicas tradicionales.

En la presente investigación hay que tomar en cuenta los costos relativos al área bancaria, siendo más específicos, los Gastos de Transformación. Estos engloban gastos operativos: que son las erogaciones destinadas al pago de servicios externos, mantenimiento de la planta física, ciertas

obligaciones de carácter legal y realización de las inversiones en aplicaciones tecnológicas; y Gastos de Personal que son el conjunto de erogaciones asociadas a la política de contratación de personal tales como sueldos, salarios y otros beneficios laborales.

En el caso de la banca venezolana, el elevado nivel de los gastos de transformación, se presenta como uno de los rasgos característicos de su esquema de costos y se considera como un reflejo directo de la presencia de ineficiencias de carácter operativo.

El sistema financiero venezolano utiliza procedimientos muy atrasados y lentos y contrario a las expectativas de la banca, la implantación de servicios alternos como servicios en línea y cajeros automáticos, no alejaron a los clientes de las agencias bancarias de manera significativa continuando con la preferencia de hacer uso físico de la taquilla, lo que incide en los altos costos.

Un estudio realizado por Datanálisis para la Asociación Bancaria de Venezuela revelo interesantes resultados sobre los niveles de conocimiento en torno a los productos y servicios que presta la banca en Venezuela.

De una muestra de mil personas localizadas en 37 localidades urbanas del país, 69% manifestó conocer los productos y servicios del sector bancario. Los mayores niveles de información se concentran entre las personas de las clases socioeconómicas A, B y C.

Al preguntar qué medios conoce que le permitan recibir servicios de la banca o realizar operaciones a través de medios electrónicos, máquinas o desde la casa: 90.5% se refirió a los cajeros automáticos, 44% a los centros de atención telefónica, 14.4% a Internet, 15.1% a envíos por fax y 15.5% a la

domiciliación de pagos.

De los medios electrónicos que las personas dicen conocer, el más empleado es el cajero automático, que cuenta con un nivel de utilización de 76.5% entre los entrevistados. Los centros de atención telefónica son los preferidos del 55%, la domiciliación de pagos por 37.2%, mientras que los envíos por fax son empleados por un 21.4% y por último con un 18.8% el uso de Internet.

El hábito de ir al banco aún persiste entre el público, 46.4% indicó que siempre va a la agencia del banco a realizar cualquier operación. Mientras que 32.4% admitió que va a una oficina bancaria sólo cuando la operación requiere su presencia; otro 17.3% dijo preferir los cajeros automáticos.

Por último, entre los resultados arrojados por la investigación se puede encontrar las razones que esgrime el público para seleccionar un banco, estas son: solidez, seguridad y confianza (17.6%); cercanía (14.1%); cuenta de nómina (13.5%); buena atención (12.2%); rapidez en operaciones (9.1%); tradición y costumbre (8.5%) y paga buenos intereses (4.65). Los concursos y promociones solo impulsan la preferencia d 1.1% de los entrevistados.

Los clientes se encuentran abiertos a nuevas opciones, pero lo más importantes es que los clientes necesitan sentir seguridad a la hora de realizar sus transacciones, necesitan confiar plenamente en los servicios que la banca les ofrece, específicamente en los servicios ofrecidos a través de la banca electrónica.

Indicadores de Gestión Administrativa

Miden desde diferentes ángulos la Gestión Administrativa del Ente y por ende del dinero del público.

En este trabajo de investigación realizaremos el análisis de los siguientes indicadores:

(Gastos de Personal + Gastos Operativos) / Activo Total

Muestra la relación entre los Gastos de Personal y los Gastos Operativos con el Activo Total, es de hacer notar que mientras más bajo sea el coeficiente es más eficiente

(Gastos de Personal + Gastos Operativos) / Ingresos Financieros

Sirve para medir el gasto promedio en que incurre el Ente en su operación fundamental de intermediación.

CAPITULO V

TIPO DE INVESTIGACIÓN

Esta investigación presenta un diseño Bibliográfico, ya que la misma se basa, en la obtención y análisis de datos provenientes de materiales impresos u otros tipos de documentos.

También requiere, trabajo de campo, para obtener información sobre fraude electrónico y cantidad de reclamos que se efectúan al año, para cuantificarlos y determinar los bancos que presentan mayor cantidad de reclamos por este tipo de delito.

De acuerdo al problema planteado y en función de los objetivos que se quieren conseguir, la investigación es Exploratoria, siendo las principales fuentes de información la Superintendencia de Bancos y Otras Instituciones Financieras (SUDEBAN) y el Instituto para la Defensa y Educación del Consumidor y del Usuario (INDECU), en donde se logró recopilar información cualitativa relativa al fraude en el sistema financiero nacional.

CAPITULO VI

MARCO METODOLÓGICO

En toda investigación científica, es necesario, que los hechos estudiados, así como las relaciones que se establecen entre estos, los resultados obtenidos y las evidencias significativas encontradas en relación con el problema investigado, además de los nuevos conocimientos que es posible obtener, reúnan las condiciones de fiabilidad, objetividad y validez interna; para lo cual, se requiere delimitar los procedimientos de orden metodológico, a través de los cuales se intenta dar respuesta a las interrogantes objeto de investigación.

En consecuencia, el marco metodológico, de la presente investigación recoge fundamentalmente el cómo de la misma, es decir, los pasos a seguir desde que se inicia el estudio hasta su culminación, sobre las bases de la sistematización racional del fenómeno estudiado, en cuanto a los conocimientos obtenidos, en función de la demostración de los objetivos específicos y la temática abordada sobre el análisis de las incidencias del fraude mediante medios de pagos electrónicos en las metas de eficiencia y de reducción de los costos operativos de la banca venezolana.

CAPITULO VII

DISEÑO DE LA INVESTIGACIÓN

Para abordar el tema del fraude electrónico en Venezuela y su incidencia en los costos del sistema financiero nacional, se requiere un trabajo fundamentalmente exploratorio ya que en la actualidad, el fraude electrónico no es una práctica bien sedimentada, sobre la que existan datos cuantitativos o registros oficiales y en general material documental consistente. Además el medio bancario, es un ambiente de acceso restringido, debido a la confidencialidad requerida por la clientela y a las estrategias de negocios que implican el mantenimiento de ventajas competitivas.

Para esta investigación el diseño será bibliográfico, que utilizaremos referencias existentes, producto de trabajos realizados por el Centro de Investigaciones Jurídicas, Núcleo de Estudios sobre Delincuencia Económica y la Unidad de Investigaciones de Medios Electrónicos de Pagos de un importante banco del país.

CAPITULO VIII

PROCEDIMIENTO A SEGUIR

A fin de analizar las incidencias del fraude mediante medios de pagos electrónicos en las metas de eficiencia y de reducción de los costos operativos de la banca venezolana, se efectuarán los siguientes pasos.

1. Revisar en las bases de datos de las bibliotecas, la existencia de material bibliográfico sobre el tema en estudio.
2. Luego de conocer la información disponible que resulte oportuna para la investigación, el próximo paso será una lectura rápida para efectuar una primera selección.
3. Se iniciara la búsqueda y observación de los hechos presentes en los trabajos escritos consultados, que son de interés para la investigación.
4. Luego de esa primera selección, se hará una lectura más detenida, sacando los tips y puntos importantes para la investigación, haciendo uso de las técnicas e instrumentos ya señalados anteriormente.
5. Esa lectura será ampliada, es decir, será objeto de varias lecturas más detenidas y rigurosas de los textos, a fin de captar sus planteamientos esenciales y aspectos lógicos de sus contenidos para poder de esa manera extraer los datos útiles para el estudio a realizar.
6. Revisar y analizar las estadísticas suministradas por la Superintendencia De Bancos y Otras Instituciones Financieras (Gerencia de Estadísticas y Publicaciones) y por la Unidad de Estadísticas de un Banco del país.
7. Se procesarán los datos secundarios de información.
8. Se realizará el informe escrito.

CAPITULO IX

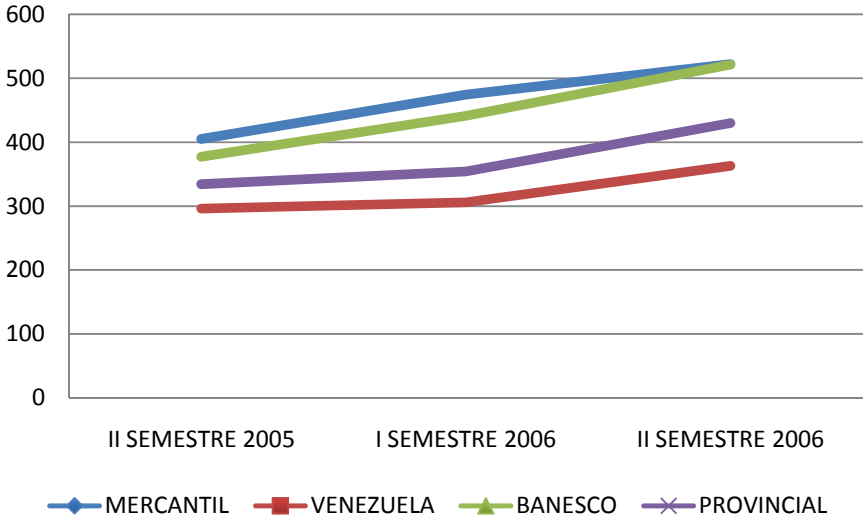
PRESENTACIÒN DE LOS RESULTADOS DE LA INVESTIGACIÒN

En primer lugar, es importante explicar que las metas de la banca venezolana en la actualidad, se traducen en la necesidad de lograr eficiencia, competitividad, productividad, fortalecimiento patrimonial, reducción de costos y excelencia e innovación en la calidad del servicio. Sin embargo, hasta la fecha la banca no ha podido reducir los altos costos operativos o de transformación, que en Venezuela son uno de los más altos de Latinoamérica, por lo que se hacen menos competitivos y funcionalmente poco operativos.

Los elevados gastos de transformación constituyen una situación problemática para las instituciones bancarias y uno de los rasgos característicos de su esquema de costos; esto es considerado como un reflejo directo de la ineficiencia de carácter operativo en el interior de las instituciones financieras y una consecuencia del uso de procedimientos muy atrasados y lentos. Parte de los elevados costos, se deben a que la mayoría de los clientes prefieren hacer uso físico de las taquillas, en vez de utilizar la banca electrónica, por razones de temor a la inseguridad o al fraude. Los elevados costos también se deben a gastos administrativos, manejo de efectivo, al tamaño de las oficinas y cantidad de sucursales y/o agencias distribuidas en todo el país.

A continuación se muestra el incremento de los gastos de transformación en los cuatro (4) bancos principales del país de acuerdo a la Cartera de Créditos y Depósitos Totales. (ver gráfico 6) y la relación de los mismos con el total de Ingresos Financieros (ver gráfico 7) y con el total activos (ver gràfico 8)

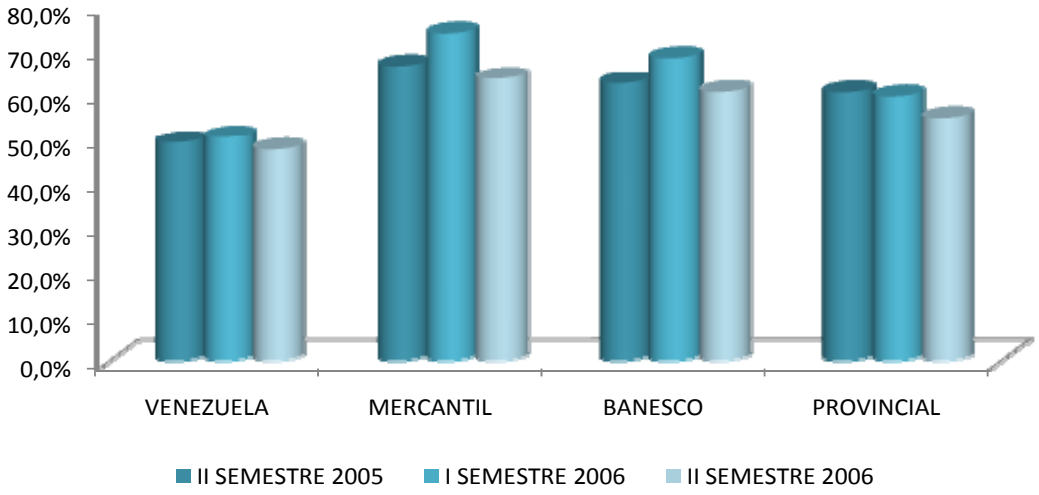
Gastos de Transformación (Millardos de Bs.)
Gráfico Nro.6



Fuente: Balances de Publicación. Asociación Bancaria Venezolana

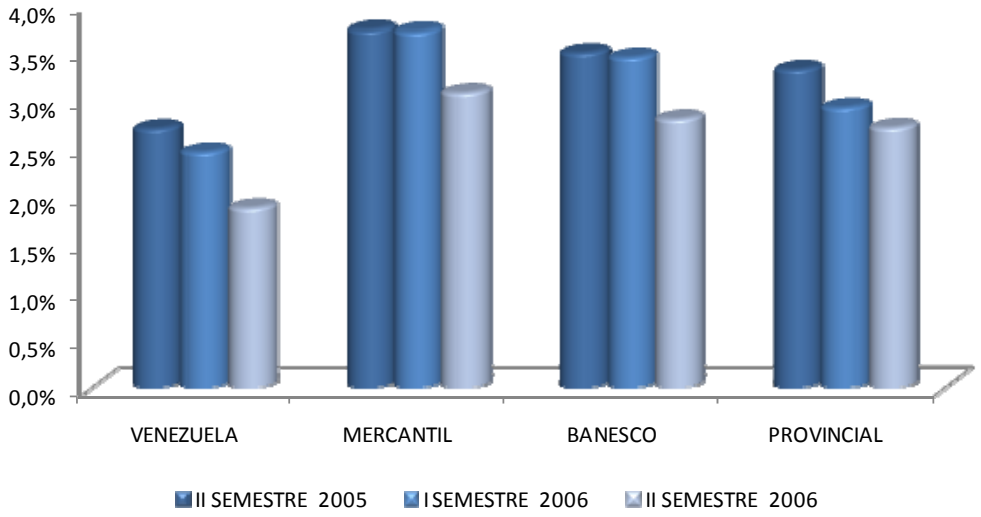
[redacted]

Gastos de Transformación/Ingresos Financieros (%)
Gráfico Nro.7



Fuente: Cálculos Propios. Balances de Publicación. Asociación Bancaria Venezolana.

Gastos de Transformación / Activos Totales (%).
Gráfico Nro. 8



Fuente: Cálculos Propios. Balances de Publicación. Asociación Bancaria Venezolana.

De los gráficos presentados concluimos que:

- ✓ Los gastos de transformación en los cuatro (4) principales bancos del país de han incrementado de manera constante en los últimos tres semestres. Banesco y Mercantil (banca venezolana) presentan mayores gastos que Venezuela y Provincial (banca extranjera)
- ✓ A pesar del incremento en los gastos de transformación observamos que los indicadores de eficiencia mejoran; esto debido a la expansión en el balance total de la banca, especialmente el incremento de la cartera de crédito.
- ✓ En base a los indicadores presentados, la banca venezolana se ubica dentro del promedio de la Banca Latinoamericana, sin embargo aún nos encontramos lejos de ser una banca eficiente, al compararnos con países desarrollados como EEUU o España.

Para alcanzar mejores indicadores de eficiencia, la banca debe disminuir sus gastos de trasformación y una de las maneras de hacerlo, es disminuyendo el volumen de clientes en las agencias bancarias, lo cual solo pueden conseguir, fortaleciendo la banca electrónica, sin embargo el incremento del fraude en las operaciones que se realizan vía cajeros automáticos o vía internet, es una de las causas que, imposibilita alcanzar las metas deseadas.

Comportamiento de la banca electrónica en Venezuela

El principal medio de uso para banca electrónica es la tarjeta de débito y en Venezuela hay aproximadamente 10 millones de usuarios (según cifras de la Superintendencia de Bancos y otras Instituciones Financieras al 31 de Diciembre de 2.006), lo que equivale a 380 tarjetas por cada 1.000 habitantes; luego están las tarjetas de crédito de las cuales hay unos cinco millones (según cifras de la Superintendencia de Bancos y otras Instituciones Financieras al 31 de Diciembre de 2.006), es decir, unas 190 tarjetas por cada 1.000 habitantes.

De acuerdo a Rodolfo Gasparri, Gerente de Tecnología de Banco Mercantil, se calcula que en el país un 30% de la población está bancarizada, cifra que esta dentro de los parámetros de las economías latinoamericanas, pero muy baja cuando se le compara con los países desarrollados cuya bancarización está por encima del 90%.

Gasparri señala que en el país hay potencial importante de crecimiento que debe canalizarse hacia los medios electrónicos. “El esfuerzo de los bancos en particular debe estar orientado a derivar transacciones hacia los medios electrónicos, y esa debe ser parte de la estrategia de los bancos”.

Sin embargo, de según Pedro García, miembro del comité de prevención de fraude de la Asociación Bancaria de Venezuela, cada día la banca recibe entre 300 y 500 reclamos de clonación de tarjetas de crédito y débito en todo el país, asumiendo el 90% de estos reclamos (el 10% restante queda en manos de los cuerpos de seguridad). Señala igualmente, Roberto León, presidente de la Alianza Nacional de Usuarios y Consumidores, Anauco, que Venezuela es el país donde se comete mayor número de fraudes bancarios electrónicos en la región y alerta sobre la falta de respuesta que los ahorristas reciben del sistema financiero.

Esta situación de inseguridad dificulta el crecimiento de la banca electrónica en Venezuela. Por referencias internacionales conocemos que una operación en taquilla tiene un costo promedio de USD 1,10, mientras que vía telefónica el costo promedios es de USD 0,60 y por internet USD 0,20.

Causas del fraude electrónico

De acuerdo a las estadísticas manejadas por la Unidad de Investigaciones de medios electrónicos de pagos de uno de los seis bancos más importantes del país, estas son las causas principales del fraude electrónico:

- Desconocimiento del negocio de tarjetas de crédito o débito por parte de las personas que tienen la responsabilidad sobre el comercio.
- Incumplimiento por parte de las personas que tienen la responsabilidad sobre el negocio de los mandatos y recomendaciones de las marcas, relacionados con los mecanismos de seguridad y

procedimientos, lo que ocasiona pérdidas por fraude, además de las correspondientes multas y sanciones.

- Falta de entrenamiento periódico del personal involucrado en las operaciones de tarjetas, sobre cursos, talleres actualizados que ofrecen las marcas en los diferentes productos, tanto operativos, como de prevención y seguridad.
- Afiliación de comercios que no reúnen los requisitos que exigen las marcas. Ejemplo: Ubicación, calidad, estructura física, documentos, clasificación de comercio, etc.
- Carencia de políticas y/o normativas severas por parte de la banca para aplicar castigos a los comercios que se confabulan con los estafadores y/o no aplican la normativa existente para la recepción de tarjetas.
- Ausencia de una educación adecuada dirigida a los comercios afiliados y los tarjetahabientes sobre las normas de seguridad para la recepción, manejo y custodia de las tarjetas.
- Falta de dispositivos de seguridad adicionales para los equipos electrónicos como cajeros automáticos (ATM's) o Puntos de Venta (P.O.S) (las siglas corresponden a *Point Of Sale*). Ejemplo: Cámara fotográfica, protectores especiales para pin-pad, etc.
- Falta de legislación severa sobre la materia de tarjetas de crédito y débito para castigar a los infractores.
- Carencia de conocimiento adecuado de las autoridades judiciales relacionadas con los delitos electrónicos con la tarjeta de crédito y débito.

Modalidades del fraude más comunes en Venezuela

Existen diversas formas utilizadas por los delincuentes en el fraude de medios de pagos electrónicos. Al consultar la Unidad de investigaciones de medios electrónicos de pagos de un importante banco del país, la misma, señaló las principales modalidades aplicadas actualmente para el fraude con tarjetas de crédito y débito.

Se describen a continuación:

- *Lectura no autorizada de Bandas Magnéticas. (Clonación o Skimming)*

Sin duda el delito informático más extendido, frecuente y notorio de cuantos se comenten hoy en día en Venezuela, consiste en la lectura no autorizada y almacenamiento de la información contenida en la banda magnética de tarjetas bancarias, mediante la utilización de dispositivos electrónicos que simulan ser los autorizados o por personas con acceso a estos medios de pago.

Es un delito que consigue un ambiente propicio dadas las necesidades y tendencias en el sistema financiero a sustituir los medios de pago tradicionales por medios electrónicos debido a menores costos y a mayor eficiencia.

La clonación de tarjetas ilustra claramente la articulación de mecanismos delictivos tradicionales con el uso de poderosas tecnologías digitales y hace pensar que se trata, más que de delitos cometidos en solitario, de la actuación de poderosas redes de delincuencia organizada.

El modus operandi es extremadamente sencillo. Mediante uso de lectoras ópticas o pescadoras, instaladas en comercios legales, se logra capturar de forma subrepticia la información del dueño de la tarjeta grabada en la banda magnética de ésta, al momento en que el cliente la entrega para el pago.

Es un mecanismo simple, rápido y que opera incluso ante la vista de las propias víctimas, quienes ignoran que mientras su tarjeta es solicitada para confirmar la validez, al mismo tiempo es sometida a un proceso que "captura" en este dispositivo la información que servirá para clonar la tarjeta.

Una vez que se han grabado las informaciones de las tarjetas, la pescadora es llevada a un sitio donde se encuentra el resto del equipamiento: una magnetizadora, un quemador de CD, una minicomputadora, y equipos de impresión del plástico (la tarjeta). Usando un software diseñado para ello, la información pescada de las tarjetas es transferida mediante la magnetizadora a una tarjeta virgen, la cual, por supuesto, ya tiene la información del tarjetahabiente, y con la cual se realizan operaciones fraudulentas.

- *Usurpación de identidad.*

Los estafadores usurpan la identidad de personas de buena solvencia económica, permitiéndoles aprovechar las buenas referencias crediticias y bancarias de la persona escogida, aportando direcciones y números de teléfonos donde tendrán una estadía temporal o cuenten con el apoyo de un cómplice que le secunde sus intenciones delictivas, evadiendo así su ubicación posterior.

- *Infidelidad de empleados*

Ocurre cuando trabajadores de una empresa emisora de tarjetas de crédito o débito se confabulan con delincuentes, a quienes les proporcionan datos de clientes o materiales que faciliten el delito. La implementación de mecanismos de seguridad a nivel de los sistemas computarizados tales como auditorías de consultas, inventario automatizado de plásticos vírgenes y grabados ha permitido a las empresas emisoras de tarjetas, controlar estas actividades desleales. De acuerdo al comisario Pablo Guzmán, ex director de la Policía Judicial, ahora contratado por la banca comercial como asesor de seguridad bancaria, trabajadores deshonestos, han vendido a los cabecillas de bandas organizadas para la estafa, el movimiento bancario de personas o empresas pudientes.

- *Transferencia indebida vía electrónica. (phishing)*

Consiste en el envío de correos electrónicos que, aparentando provenir de fuentes fiables (por ejemplo, entidades bancarias), intentan obtener datos confidenciales del usuario**.** Para ello, suelen incluir un enlace que, al ser pulsado, lleva a páginas web falsificadas. De esta manera, el usuario, creyendo estar en un sitio de toda confianza, introduce la información solicitada que, en realidad, va a parar a manos del estafador.

- *Cambio de tarjeta*

Los delincuentes le prestan su “colaboración” a clientes que no saben utilizar el cajero automático, le visualizan la clave y valiéndose de artimañas le cambian la tarjeta por una similar.

Bancos más fraudulentos y cuantificación del fraude

Según estadísticas obtenidas de la Superintendencia de Bancos y Otras Instituciones Financieras, durante el año 2005, el total de reclamos por clonación en el sistema financiero nacional fue de 7.619 casos, por un monto total de Bs. 4.226.405M, siendo el Banco Occidental de Descuento (B.O.D), la institución bancaria que más reclamos recibió por concepto de clonación (2.832 casos). A este le sigue el Banco Provincial, con 1.175 casos y Banesco con 1.074 casos.

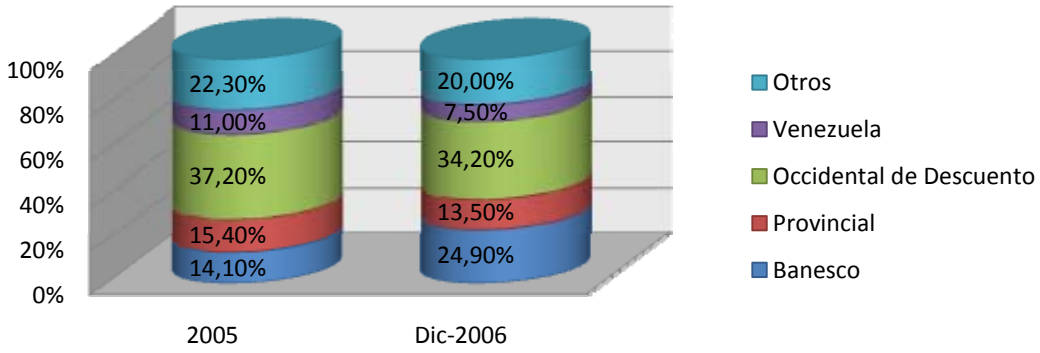
El número total de reclamos por banca electrónica (internet banking) fue de 840 casos por un monto total de Bs. 806.165M, siendo el banco con mayor número de reclamos Banesco, con 257 casos, seguido de Mercantil con 230 casos.

Entre el 1 de Diciembre y el 31 de Diciembre del 2006 (en la Superintendencia de Bancos señalaron que estas estadísticas no se realizaron sino en el último mes de año), el número total de reclamos por clonación fue de 10.160 casos por Bs. 8.298.277M y continúa siendo el Banco Occidental de Descuento (B.O.D), la institución que más reclamos recibió con 31.914 casos, a pesar de ubicarse en el octavo lugar de el ranking bancario de acuerdo al número de tarjetahabientes; seguido de Provincial con 12.631 casos.

El número total de reclamos por banca electrónica (internet banking) fue de 6.430 casos por un monto total de Bs. 8.710.661M, siendo el banco con mayor número de reclamos Mercantil, con 3.183 casos, seguido de Banesco con 1.104 casos.

En el siguiente gráfico se presenta la participación porcentual de los bancos con mayor número de reclamos por clonación.

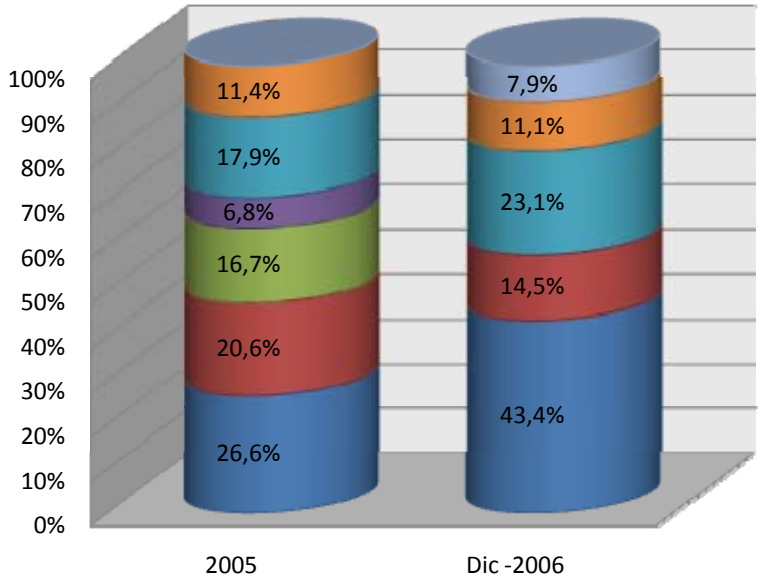
Bancos con mayor número de reclamos por clonación.
Gráfico Nro.9



Fuente: Superintendencia de Bancos y Otras Instituciones Financieras.

De las cifras presentadas, se concluye que el incremento del delito de fraude al 31 de Diciembre de 2.006 es importante, por cuanto, solo en el último mes de año, el número de reclamos presentados es mayor que el número de reclamos presentados en el 2.005. En las estadísticas observadas, llama la atención que el Banco Mercantil, no reporta en ninguno de los períodos, información sobre el número de reclamos que realizan los clientes, aún cuando en el reporte de reclamos procedentes, si reflejan información.

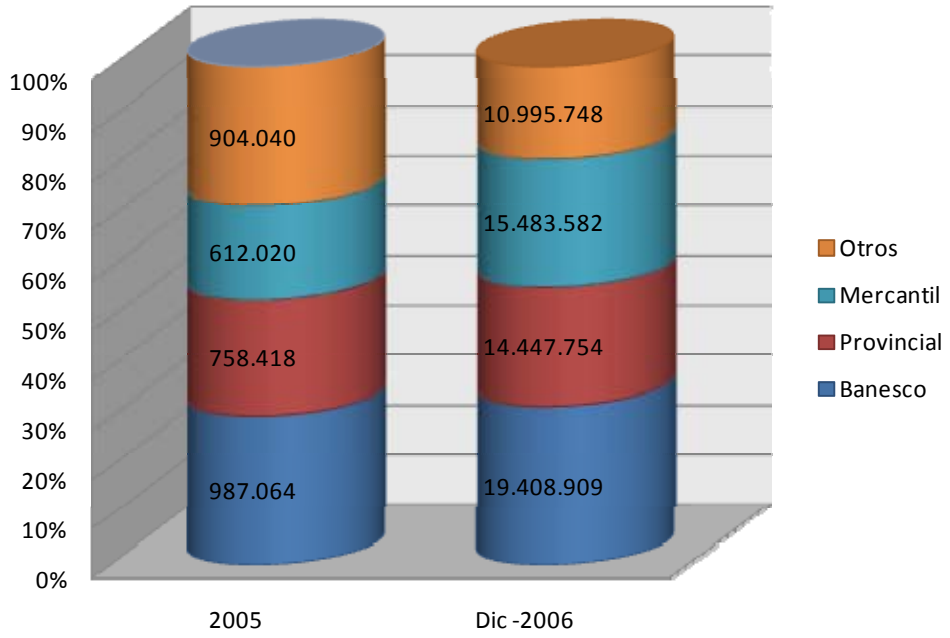
Los bancos con mayor número de **reclamos procedentes** por clonación de presentan en el siguiente gráfico.



Fuente: Superintendencia de Bancos y Otras Instituciones Financieras.

Los bancos con mayor monto en reclamos (en miles de Bs.) procedentes por clonación se presentan en el siguiente gráfico.

Bancos con mayor monto procedente en reclamos por clonación. (miles de Bs.)
Gráfico Nro.11



Fuente: Superintendencia de Bancos y Otras Instituciones Financieras.

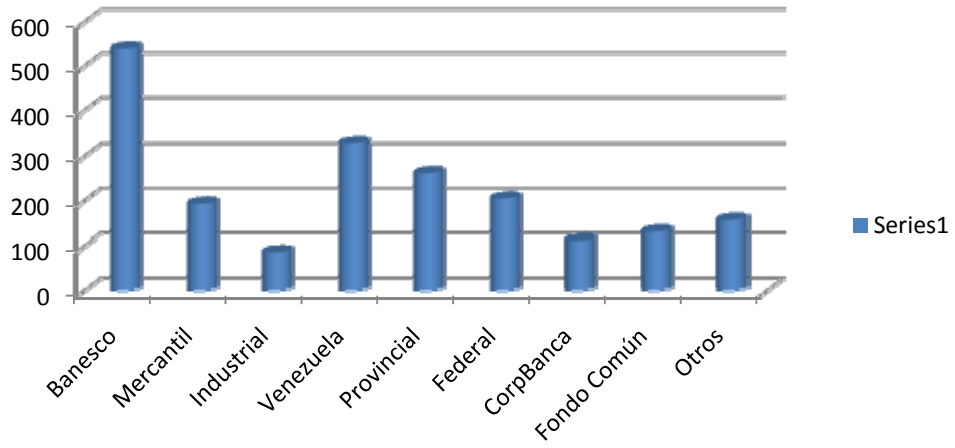
En los gráficos presentados se observa que el Banco Occidental de Descuento, presenta el mayor número de reclamos por clonación, no obstante, al observar el monto de reclamos procedentes, no es significativo, por lo que se encuentra incluido dentro “otros”.

En cuanto al tipo de producto que presenta mayor índice de clonación, observamos que al 31 de Diciembre de 2.005, las tarjetas de crédito presentaron un monto total en denuncias de Bs. 2.524MM Vs. Bs. 672MM en tarjetas de débito.

Entre el 01 y el 31 de Diciembre del año 2.006, la situación se revierte, ya que observamos un monto total en denuncias por tarjetas de débito de Bs. 4.582MM Vs. Bs. 1.975MM en tarjetas de crédito.

Sobre el tema consultamos al Instituto para la Defensa y Educación del Consumidor y del Usuario, quienes nos suministraron estadísticas del número de denuncias recibidas en la sala de conciliación y arbitraje durante el año 2.006, sin embargo estás se presentan a manera de referencia, púes en el citado instituto no se tipifican las denuncias recibidas.

Denuncias por Bancos recibidas en Sala de Conciliación y Arbitraje del INDECU. Año 2006
Gráfico Nro.12



Fuente: Sala de Conciliación y Arbitraje (INDECU).

También fue consultada la Unidad solucionadora de reclamos del producto tarjetas de débito de uno de los seis (6) principales bancos del país, sobre el tema del fraude y nos señalo que durante el año 2006 se recibieron reclamos por Bs. 23MM, de los cuales Bs. 12MM resultaron procedentes y pagados a los clientes Del total procedente, el 58.33%

corresponde a clonación y el resto de los reclamos se califica y cuantifica como Error Operativo.

Del total de reclamos procedentes, una media del 16%, fue reconocido como procedente por “Reglas del Negocio”, lo que significa que se reconoce, por el tipo de cliente que presenta el reclamo, consecuencias que puede traer no reconocerlo, reciprocidad que ofrece el mismo o sus empresas relacionadas o tipo de relación que maneja con algún ejecutivo de la institución.

Las causales principales de los reclamos no procedentes, en esa Unidad son:

- Timación (quitar o hurtar con engaño)
- Entorno (algún familiar o persona del entorno del cliente posee la clave y está retirando fondos sin autorización)
- Plástico robado y no denunciado
- Olvido o confusión del cliente
- Operación sin indicios de fraude

Un Ejecutivo de esta Unidad, nos señaló, que la banca no desvía su responsabilidad por el incremento cada vez más importante del número de casos de tarjetas clonadas, pero advierte que en la mayoría de los casos, la misma recae sobre los clientes ya que, generalmente, confían demasiado cuando realizan sus transacciones. Según esto, son los propios tarjetahabientes quienes facilitan su clave de seguridad a terceros o no hacen un empleo óptimo de los aparatos dispensadores de efectivo. En la mayoría de los casos, no se cuidan de que extraños merodeen cerca, al

momento de pulsar los dígitos, convirtiéndose así en presa fácil de los delincuentes.

Una de las consecuencias derivadas de la situación descrita anteriormente es que las primas de seguros de los bancos aumentan 40 por ciento por delitos electrónicos.

La ofensiva emprendida por la delincuencia organizada contra las instituciones financieras a través de los fraudes electrónicos, le ha costado a la banca un incremento mínimo de 60% en las pólizas de seguro que reponen los montos de dinero sustraído mediante la clonación de tarjetas de débito y crédito.

Esta situación ha hecho que las compañías aseguradoras aumenten el número de requisitos exigidos a las entidades bancarias para contratar pólizas, así como la definición de los montos máximos reconocidos en caso de hurto electrónico.

La delincuencia organizada en materia de fraude electrónico, es relativamente reciente, por lo que no ha generado aún suficiente información para describir patrones consistentes.

Esta unidad no maneja estadísticas en las cuales el fraude involucre a un empleado de la institución; las mismas son manejadas directamente por el Unidad de Seguridad y son confidenciales porque se involucra al Cuerpo de Investigaciones Científicas, Penales y Criminalísticas (CICPC).

Formulación de alternativas en torno a las incidencias del fraude mediante medios de pagos electrónicos.

Las alternativas que se presentan a continuación en referencia a la problemática analizada son de orden legal, tecnológico y de orientación al cliente o consumidor.

Aplicación de la Ley sobre Delitos Informáticos

La misma fue promulgada con el objeto de eliminar el desfase existente entre la realidad creada por nuevas tecnologías de la información y su regulación normativa; tipificando como delitos aquellas conductas que no se encontraban dentro de los ilícitos penales tradicionales y estableciendo sus correspondientes sanciones, atendiendo así al principio de legalidad que rige el ordenamiento jurídico penal del país.

Su aplicación serviría para combatir la impunidad de los ilícitos cometidos mediante el uso o aprovechamiento de las citadas tecnologías que permiten comisión de delitos a distancia, la encriptación, el ocultamiento de la identidad, lo cual atenta contra el proceso de investigación, impide que las autoridades recaben las pruebas necesarias para imputar la comisión del delito a un sujeto dado y que este sea enjuiciado y castigado.

La Ley se nutre de los lineamientos que sobre la materia plantea las Naciones Unidas y de experiencias del derecho comparado (Alemania, Gran Bretaña, Holanda, España, Francia, Italia, Chile y Perú).

Dentro del elenco de conductas que la ley prescribe como delitos informáticos, encontramos: el acceso no autorizado a sistemas informáticos,

el sabotaje a sistemas informáticos, agravando la pena cuando este resulte de la creación, introducción o transmisión de un virus; la prestación u oferta de servicios para sabotaje; el espionaje informático; la falsificación o eliminación de documento o la incorporación de éstos a sistemas informáticos; acceso indebido a sistemas para alterar registros o data; violación de privacidad, revelación debida de data o información de carácter personal, difusión y exhibición de material pornográfico a niños y adolescentes, entre otras.

Por otra parte, dentro de las sanciones se contemplan penas accesorias por la comisión de delitos informáticos, tales como: el decomiso o incautación de las herramientas y dispositivos utilizados para perpetrar el delito, la inhabilitación para el ejercicio de ciertas funciones, cuando el delito se hubiere cometido con abuso de la posición de acceso a la data o información en razón del cargo o función. El alcance real o en la práctica de este instrumento legal todavía es difícil determinarlo por su corta existencia, sin embargo constituye un avance en el contexto jurídico o regulatorio al que hay que hacer seguimiento para profundizar, ampliar y perfeccionar.

Promulgación de la nueva Ley de Bancos

La reforma a la Ley General de Bancos y otras Instituciones Financieras contempla la regulación de las operaciones realizadas con instrumentos de pagos electrónicos. La figura de banca virtual se incluyó por vez primera en la Ley en 2002, fecha en la cual entró en vigor el texto vigente. La Ley de Bancos establece en su artículo 67 y hasta el 73 del capítulo IV, sección tercera, relativa a los servicios bancario virtuales"- las transferencias, los servicios desmaterializados, banca virtual y las prohibiciones al respecto. Los técnicos que adelantan la reforma tienen instrucciones de regular en esta Ley

todas las operaciones que se realicen vía pagos electrónicos, por lo cual está previsto una regulación mayor a este tipo de operaciones.

Migración al Chip (Microcircuito)

Para lo cual los bancos deben realizar importantes inversiones en tecnología como: cambio en los terminales usados en los establecimientos por unos aptos para la lectura del Chip (algunos comercios cuentan ya con estos aparatos, pero están activos sólo como procesadores de banda magnética); el costo de cada aparato es de aproximadamente U.S.$ 130, y depende del convenio con el banco, si el costo será asumido por éste o por el establecimiento.

Adicionalmente, los cajeros automáticos contarán con un dispositivo de lectura del Chip (microcircuito), lo cual no implicará adquirir un nuevo cajero automático.

Una tarjeta con chip o microcircuito, contiene una especie de microcomputadora capaz no sólo de almacenar información sino también de ejecutar programas, lo cual aporta ventajas en al menos dos sentidos; por una parte, el diminuto procesador efectúa validaciones más exhaustivas que las realizadas por otras tecnologías anteriores y, de esta manera, cumple procesos que hacen más segura una transacción, en segundo lugar, la introducción de una computadora diminuta permite la añadidura de programas por parte de los bancos u otras empresas que establezcan convenios con las instituciones financieras vinculadas con la lealtad de los clientes.

Otra de las virtudes que se le adosan al chip o microcircuito es la posibilidad de portar la información, es decir, el usuario de una tarjeta inteligente, lleva consigo el historial de las operaciones comerciales que se han seleccionado para ser guardadas en el objeto. Así, los requerimientos de almacenamiento en los locales o instituciones financieras son menores pues una parte reposa en cada uno de los plásticos emitidos y sólo se harían respaldos de los datos más necesarios.

Alternativas al fraude mediante medios de pago electrónicos basadas en campañas de educación al consumidor

Recomendaciones de seguridad sugeridas por la Gerencia de Riesgo Operacional OyT del Banco Mercantil para prevenir fraudes en cajeros automáticos:

Recomendaciones básicas:

- ✓ Seleccione el cajero que cumpla con las condiciones de seguridad apropiadas para garantizar su protección personal.

- ✓ Asegúrese de que sólo usted conoce, utiliza y ve su clave personal.

- ✓ Siga las instrucciones de la pantalla del cajero automático cuando utilice su tarjeta y asegúrese que la tarjeta se mantiene segura durante y después de utilizarla.

Cómo seleccionar un cajero automático:

- ✓ Cuando sea posible, utilice los cajeros automáticos con los cuales esté familiarizado. De no ser así, seleccione cajeros en lugares bien iluminados, en buenas localidades y donde se sienta confortable y seguro.

- ✓ Observe cuidadosamente los alrededores antes de acercarse a un cajero automático. No lo utilice si observa individuos sospechosos en los alrededores, si el área se encuentra aislada, solitaria o es peligrosa. Evite utilizarlos a altas horas de la noche o por el contrario, a horas muy tempranas, cuando hay poco tránsito y pocas personas.

- ✓ Evite abrir su bolso, monedero o cartera mientras se encuentra en la línea de espera del cajero automático. Tenga su tarjeta lista en la mano antes de acercarse al cajero automático.

- ✓ Si algo en el cajero automático le parece sospechoso o fuera de lo corriente, es posible que el cajero automático haya sido alterado. Hágale caso a su intuición. No lo utilice si observa algún elemento adjunto a la abertura donde se inserta la tarjeta o en el teclado. Verifique si hay instrucciones inusuales en la pantalla, si existen pantallas en blanco o sospechosas. Informe a la entidad financiera sobre la posible alteración del cajero y diríjase a otro cajero automático

- ✓ Tenga cuidado con personas desconocidas que le ofrezcan ayuda en un cajero automático si su tarjeta se queda atascada o tiene dificultades con la transacción. No deje que nada ni nadie lo distraiga mientras se encuentra en el cajero automático y si tiene dificultades, comuníquese de inmediato con su banco.

Al utilizar el cajero:

- ✓ Asegúrese que las otras personas en la línea de espera mantienen una distancia prudente de usted. Al introducir su clave asegúrese de que no lo estén observando.

- ✓ Párese cerca del cajero automático y proteja el teclado con su mano al introducir su clave secreta.

- ✓ Siga las instrucciones en la pantalla. No teclee su clave hasta que el cajero automático no se lo solicite

- ✓ Si cree que el cajero automático no está trabajando correctamente, oprima la tecla “Cancelar”, retire su tarjeta y diríjase a otro cajero. Informe a su institución financiera acerca del problema.

- ✓ Nunca fuerce la tarjeta para introducirla en la ranura.

- ✓ Conserve el comprobante de la transacción para que pueda comparar sus recibos de cajero automático con su estado de cuenta mensual.

- ✓ Si su tarjeta se traba, queda retenida o se pierde, o si alguien interfiere con usted en un cajero automático, repórtelo inmediatamente al banco y/o a la policía.

- ✓ No se apure durante la transacción. Guarde cuidadosamente su tarjeta y el efectivo que retiró, antes de alejarse del cajero automático.

- ✓ Si utiliza un cajero automático interior, es decir, ubicado en pequeños locales que requieren su tarjeta para abrir la puerta e ingresar, no permita que personas desconocidas ingresen con usted.

Cuidado de su clave secreta

- ✓ Memorice su clave secreta. No la escriba. Si lo hace, no lleve la información consigo. Nunca tenga la clave junto con la tarjeta.

- ✓ Su clave secreta no debe ser conocida por ninguna persona. No la divulgue a nadie, ni a su familia, ni a personal del banco.

- ✓ Cuando asigne una clave, no utilice combinaciones obvias o que se puedan adivinar fácilmente, como por ejemplo su fecha de nacimiento.

- ✓ Cambie su clave secreta periódicamente. Si sospecha que ha sido descubierta, cámbiela inmediatamente.

CAPITULO X

CONCLUSIONES

A continuación se presenta una visión global en torno a los principales hallazgos y resultados de la investigación.

En primer lugar, las incidencias del fraude mediante medios de pagos electrónicos en las metas de eficiencia y reducción de los costos operativos de la banca venezolana, se traducen en que dicho fraude obstaculiza el logro de estas metas que buscan lograr eficiencia, competitividad, productividad, fortalecimiento patrimonial, reducción de costos y excelencia e innovación en la calidad del servicio. De allí que uno de los mayores retos es la consolidación de una banca electrónica que ofrezca seguridad y confianza en su utilización, por parte de los clientes, para lo cual es indispensable promover hábitos, con la consecuente disminución de costos operativos y aumento de la calidad en el servicio, ya que el venezolano es apegado a la utilización de la agencia y presenta resistencia al empleo de mecanismos electrónicos y banca por internet.

Como síntesis de la situación expuesta anteriormente se puede decir que se requiere con urgencia afianzar la relación de los sistemas informáticos y la organización, porque esto es lo que permitirá la reducción de los sistemas de costos operativos en la banca, lo cual será factible a su vez mediante la reducción del fraude electrónico. Este último fue cuantificado en la presente investigación. De acuerdo a datos suministrados por la Superintendencia de Bancos y otras Instituciones Financieras (SUDEBAN), durante al año 2.005 fueron denunciados en las distintas instituciones financieras del país, la cantidad siete mil seiscientos diez y nueve (7.619) casos y diez mil ciento sesenta (10.160) solo durante el mes de diciembre del año 2006. Ambas

cantidades ascienden a la suma de Bs. 4.226.405M y Bs. 8.298.277M, respectivamente.

En otro orden, se identificaron las instituciones bancarias venezolanas que reciben mayor número de reclamos por concepto de fraude mediante medios de pago electrónico resultan procedentes. El orden jerárquico resultante al 31 de diciembre de 2.006 fue el siguiente: el primer lugar correspondió a Banesco, seguido de Mercantil y Provincial. En la actualidad, estas instituciones están buscando alternativas para combatir esta problemática.

Las causas y procedimientos que originan el fraude mediante medios de pagos electrónicos en la banca venezolana son múltiples y diversos. Entre las más resaltantes, cabe destacar el desconocimiento en el uso de la tecnología por parte de los usuarios, de los comerciantes, falta de entrenamiento del personal involucrado en el sistema, afiliación de comercios que no reúnen los requisitos que exigen las marcas, carencia de políticas y normativas por parte de la banca para aplicar faltas y castigos a los comercios que se asocian con los estafadores y falta de legislación severa sobre la materia de tarjetas de crédito y débito para castigar a los infractores.

En cuanto a las modalidades del fraude se encuentran la clonación de tarjetas, infidelidad de empleados, cambio de tarjeta, entre otros.

Los actuales medios de pago electrónicos como tarjetas de crédito, débito y los que están en proyecto, caso monederos electrónicos, tienen una gran importancia tipificada en el alto uso o demanda de dichos medios por parte de los clientes. En el caso de las tarjetas de créditos, estas permiten solucionar situaciones de emergencia, cuando por ejemplo a un ciudadano se le presenta un problema de salud y no cuenta con un seguro médico para

ingresar a una clínica. Las tarjetas de débito, por su parte, es el medio de uso más extendido a nivel nacional. Los monederos electrónicos a pesar de ser un producto nuevo y cuya introducción está en fase de prueba en el país, ha sido probado con éxito en otras latitudes y los especialistas argumentan que una vez que las personas conozcan sus beneficios, se masificará rápidamente.

La característica principal que distingue al tipo de tarjetas señalado es la utilización del chip o microcircuito. Dada la importancia expuesta de cada uno de estos medios de pago electrónicos hay que profundizar la búsqueda de alternativas al fraude que se comete mediante dichos medios.

La Ley de Bancos garantiza al público que los reclamos más frecuentes como descuentos indebidos en los cajeros automáticos, cargos inexistentes, en tarjetas de crédito, ineficiencia al momento de entregar los estados de cuentas, tienen que ser atendidos en un máximo de treinta (30) días. En este lapso, el banco deberá entregarle un informe a la persona que interponga el reclamo, donde se indiquen las causas que motivaron los cargos no reconocidos u omisiones presentadas, así como la decisión adoptada.

CAPITULO XI

BIBLIOGRAFIA

Acedo Mendoza, Carlos, “Instituciones Financieras”. Editorial Carhel C.A. Caracas, 1984

Asti vera, Armando, “Metodología de la Investigación”, Editorial Kapeluz, 1.973

Bello R, Gonzalo, “Operaciones Bancarias en Venezuela: Teoría y Practica”. Universidad Católica Andrés Bello. Caracas, 2004.

Centro de Investigaciones Jurídicas. Núcleo de Estudios sobre Delincuencia Económica “Delincuencia Económica y Tecnologías de la Información”. Universidad Católica Andrés Bello. Caracas, 2004.

Espiñeira, Sheldon y Asociados. Seguridad de la Información: Un nuevo enfoque para el control de riesgos de negocio. (Documento en línea). Disponible: http://www.pc-news.com. 25 de Abril 2005.

Galvis Sánchez, José, “Los Fraudes en la Cibernética”. Fondo Editorial Universidad Bicentenaria de Aragua. Maracay, 1998

Gillespie, Cecil, “Introducción a la Contabilidad de Costos”. Unión Tipográfica Editorial Hispano – Americana. México, 1984

Grasso Vecchio, José. Cambios que enfrenta la Banca. 16/02/2007. (Documento en línea). Disponible: http://finanzasdigital.com/noticias_opiniones

Grasso Vecchio, José. Banca Electrónica. 16/10/2006.(Documento en línea). Disponible: http://finanzasdigital.com/noticias_opiniones

Herrera Labarca, Raul, "Los delitos contra la Banca. Recopilación de casos y su posible prevención". Consorcio Asegurador Bancario. Caracas, 1.989.

Lahoud, Daniel. El Margen y los Costos para la Banca Venezolana. Revista Negotium. Año 2. Nro. 5. Noviembre 2006

Modelel, Juan. El fraude electrónico se supera a sí mismo. 24/03/2007 (Documento en línea). Disponible: http://www.eluniversal.com

Universidad Nacional Experimental Libertador (UPEL) Vice-Rectorado de Investigación y Post-Grado. "Manual de Trabajos de Grado de Especialización, Maestría y Tesis Doctorales". Caracas, Julio 1998

Venezuela, Ley Especial contra Delitos Informáticos (2001). Gaceta Oficial de la República de Venezuela número 37.313 del 30 de Octubre de 2.001.

Página web de la Corporación Suiche 7B.
http://www.suiche7b.com.ve

Página web de Proyecto Conexus.
http://www.redconexus.com

www.eluniversal.com

www.delitosinformaticos.com

www.ultimasnoticias

www.elmundo.com.ve

www.panorama.com.ve