Facultad de Ciencias Económicas y Administrativas
Escuela de Auditoria.

PROPUESTA PARA MINIMIZAR LOS RIESGOS DE FRAUDES COMETIDOS CON LAS TARJETAS DE CREDITO BANCARIAS

Tesis Para Optar Al Titulo De Contador Público
Auditor Y Al Grado De Licenciado En Sistemas De
Información Financiera Y Control De Gestión

Tesista: CRISTIAN RECABAL CONTRERAS

Prof. Guía: Arturo Cornejo A.

Valparaíso, Diciembre 2009

RESUMEN

Actualmente la mayoría de los bancos internacionales de diversos países latinoamericanos, trabajan con el programa de seguridad de la información con la implantación de las normas de seguridad en la industria de los medios de pago (PCI DSS) Programa dirigido principalmente a la auto evaluación del propio banco y de los comercios donde son usadas las tarjetas de crédito de los bancos emisores en materias de seguridad de la información financiera.

Con esto los bancos son capaces de minimizar en cierta medida los riesgos que se cometan fraudes con sus respectivas tarjetas de crédito en cuanto a fuga de datos y posterior uso indebido de estos.

El presente proyecto de tesis tiene como objeto en cierta parte promover la implantación de estas normas de seguridad de la información en los medios de pago y capacitar a los comercios catalogados como mas riesgosos en cuanto a la importancia de efectuar una adecuada validación de los datos personales de los clientes que compran en esos comercios

Para cumplir con esto se recopilara información en Visa y Mastercard a través de su pagina Web en todo lo concerniente al programa de seguridad de la información PCI, se aplicara una encuesta a los distintos departamentos de prevención fraude de los 6 bancos que alcanza la muestra para confirmar primero que todo que medidas y sistemas utilizan para minimizar los riesgos de fraude con este tipo de tarjetas y segundo proponer las políticas y procedimientos en cuanto a la implantación del programa acá en chile y las respectivas capacitaciones con los funcionaros de los comercios catalogados de acuerdo a la encuesta como mas riesgosos.

Se encontró como era de esperar que la mayor parte de los departamentos de fraude encuestados desconoce las nuevas normas de seguridad de la información que actualmente se aplican en el exterior y pronto en chile, además que se detecto que solo un mínimo porcentaje de los departamentos encuestados realiza capacitaciones sobre la validación y uso de las tarjetas de crédito.

MARCO TEORICO

Partiendo de una idea general tenemos que tener presente

EL SISTEMA FINANCIERO CHILENO

Este se define según la SBIF como el conjunto de empresas, que debidamente autorizadas por la superintendecia operan en la intermediación financiera. Entendiéndose por intermediación el proceso mediante el cual una entidad, generalmente bancaria o financiera, traslada los recursos de los ahorrantes directamente a las empresas que requieren de financiamiento.

En chile existen 26 bancos que componen este sistema dentro de los cuales podemos mencionar:

Banco de Chile, Banco Internacional, Scotiabank Sud Americano, Banco de Crédito e Inversiones, Corpbanca, Banco Bice, HSBC Bank (Chile), Banco Santander-Chile, ABN AMRO Bank (Chile), Banco Security, Banco Falabella, Deutsche Bank (Chile), Banco Ripley, HNS Banco, Banco Monex, Banco Penta, Banco Paris, Banco Bilbao Vizcaya Argentaria, Chile (BBVA), Banco Itaú Chile y Banco del Desarrollo.

Además de los anteriores, hay 5 Sucursales de Bancos Extranjeros, que son:

Banco do Brasil S.A., Citibank N.A., JP Morgan Chase Bank, N. A., Banco de la Nación Argentina, The Bank of Tokyo-Mitsubishi UFJ, LTD.

Finalmente, existe un Banco Estatal, que corresponde al Banco del Estado de Chile.

A todos ellos se agrega el Banco Central de Chile que no es fiscalizado por la Superintendencia.

NACIMIENTO DE LOS BANCOS

Los bancos nacen en la edad media donde los cambistas realizaban, sentados en una banca y una mesa, todo tipo de operaciones financieras a las personas que las requerían, préstamos, etc. Se realizaban a modo de compra y venta de algo, ellos daban dinero a personas que quisieran dejarles algo a cambio, como una financiera o caja de trueque. De allí en adelante los bancos comenzaron a delimitar su territorio, primero fue con cadenas y guardias para que los cambistas puedan trabajar tranquilamente y luego se apostaron en su propio edificio, detrás de un mesón donde se realizaban esta clase de trámites. Con el tiempo, los bancos se fueron transformando en oficinas y, a parte de prestar dinero, ofrecían a los clientes guardárselo en un lugar seguro donde ellos pudieran ir a retirarlo las veces que quieran y cuando quieran. El primero de los bancos en Chile, fue, por supuesto, el Banco Estado, por allá por 1855 el Presidente de Chile Don Manuel Montt y su primer ministro Don Antonio Varas crearon la caja de crédito hipotecario. Una institución financiera del Estado que, gracias a una serie de estrictos reglamentos le prestaba dinero a quién mas lo necesitara, para comenzar una empresa o para comprar tierras y propiedades. Con los años, los servicios de la Caja se fueron ampliando, llegando hoy a ser uno de los mas grandes bancos de Chile y principalmente el mas popular. Otro de los bancos pioneros en Chile fue el Banco de Chile. Creado en 1893 se transformó en el primer banco privado del país y prestaba dinero y ofrecía guardarlo a las personas mas adineradas del país. Hoy en día tenemos alrededor de 6 bancos netamente chilenos, dentro de ellos obviamente están los dos antes mencionados, el Banco de Crédito e Inversiones, hoy en día llamado BCI, Banco Santander Santiago, y banco Edwards, actualmente perteneciente al Banco de Chile.

Además dentro del país se han instalado numerosos bancos internacionales, gracias a la gran inversión extranjera existente en el país. Si bien algunos son escasos con no más de dos o tres sucursales existentes solo en Santiago, cuentan con un número muy reducido de clientes, la mayoría extranjeros que necesitan tener sus inversiones en esos bancos dada la cantidad de viajes que realizan.

Si hablamos de bancos y financieras de alta popularidad, podemos mencionar el boom que se ha visto de los bancos que han sacado las multitiendas al mercado. Es un nuevo concepto en banco. Con tasas de interés para el público masivo y la mayor ventaja que dicen tener es la posibilidad de tener abierto, de Lunes a Domingo a toda hora del día en horario de mall, de esta manera el gancho comercial de estos nuevos bancos populares

es la posibilidad de ir al banco a depositar, pagar o consultar, en los días libres de los fines de semana. Los nuevos bancos, tanto Ripley como Falabella, han visto incrementada su capacidad de clientes y hoy en día no solo ofrecen créditos de consumo e hipotecarios, sino que están comenzando a ofrecer cuentas corrientes y la administración de tarjetas de crédito bancarias.

OTORGAMIENTO DE LICENCIAS BANCARIAS

Toda empresa bancaria, para establecerse como tal requiere de la autorización de la Superintendencia de bancos e instituciones financieras (SBIF) para lo cual debe presentar un prospecto que defina las características fundamentales de la empresa proyectada. La autorización está sujeta a las disposiciones legales vigentes y a los criterios establecidos por un organismo supervisor. Al respecto, la nueva legislación establece como requisitos esenciales para la aprobación de una solicitud de licencia la verificación de la solvencia e integridad de los accionistas fundadores.

Para el cumplimiento de la solvencia, la ley establece que los accionistas fundadores de un banco deberán contar con un patrimonio neto consolidado equivalente a la inversión proyectada, esto es, un mínimo de 800 unidades de fomento; [1] mientras que para el cumplimiento de la integridad, los accionistas fundadores, además de su trayectoria comercial, deben estar en condiciones de demostrar que no deben haber tenido conductas dolosas o culposas, graves o reiteradas, que puedan poner en riesgo la estabilidad de la institución que se propone establecer o la seguridad de sus depositantes.

Las conductas a las que se refiere la ley dicen relación con las actividades comerciales y Con la administración financiera, en particular, la bancaria.
La Superintendencia verificará el cumplimiento de los criterios señalados, lo que significa que se analizarán caso a caso las solicitudes para su resolución, pudiendo además el Banco Central pronunciarse acerca de los efectos que la autorización de nuevos bancos pueda producir para la estabilidad del sistema financiero o el cumplimiento adecuado de las obligaciones contenidas en la Ley Orgánica del Banco Central. Luego, en caso de aprobación de la solicitud, se comprobará previamente si la nueva institución bancaria se

[1] Superintendencia de Bancos e Instituciones Financieras de chile otorgamiento de licencias bancarias.Diciembre 2001 www.sbif.cl.

encuentra preparada para iniciar sus actividades. En particular, si cuenta con los recursos humanos y tecnológicos y con los procedimientos y controles para iniciar sus funciones, caso en el cual se procederá a conceder la autorización para su funcionamiento.

MARCO NORMATIVO PARA LA EMISION Y OPERACIÓN DE TARJETAS DE CREDITO

El uso de medios de pago electrónicos es una tendencia generalizada en Chile y en otras economías. En nuestro país, la utilización de las tarjetas de crédito como medio de pago se ha incrementado significativamente durante los últimos años, fenómeno que se ha visto reforzado por el ingreso de nuevos emisores a la industria y por el mayor número de entidades afiliadas a estos esquemas de pago. En la actualidad, se estima que circulan en Chile más de 12 millones de tarjetas de crédito, bancarias y no bancarias, y que un porcentaje significativo de la población cuenta con al menos uno de estos instrumentos. Este desarrollo ha contribuido a que una parte relevante de la población utilice habitualmente este tipo de instrumento como medio de pago para efectuar sus compras de bienes y servicios. [2] En este contexto, es de interés público que estos medios de pago cumplan con altos estándares de eficiencia y seguridad, que contribuyan a fortalecer y preservar la confianza de la población y extender su uso a sectores diversos de la economía. El Banco Central de Chile, por mandato de su Ley Orgánica Constitucional, debe velar por el normal funcionamiento de los pagos. Por lo anterior, está facultado para dictar las normas que deben acatar las empresas cuyo giro consista en la emisión u operación de tarjetas de crédito que se encuentren bajo la fiscalización de la Superintendencia de Bancos e Instituciones Financieras, que en ejercicio de sus facultades legales, debe fiscalizar el cumplimiento de tales normas.

[2] Banco Central de Chile Capitulo III J.1 Compendio de Normas Financieras del Banco Central. Octubre 2005. www.bcentral.cl.

CONCEPTO LEGAL DE TARJETA

Una tarjeta es un instrumento mercantil de pago, definiéndose como “toda tarjeta o cualquier otro medio que permite a su usuario efectuar operaciones como:

Pago por medios electrónicos que suponga el uso de tarjeta, especialmente en el punto de venta;

Retirada de billetes, depósito de billetes y cheques, y operaciones por medio de mecanismos electrónicos, como distribuidores automáticos de billetes y cajeros automáticos;

Pago con tarjeta por medios no electrónicos; se incluyen las operaciones que exigen una firma y la entrega de un Comprobante.

Pago por medios electrónicos realizado por un particular sin emplear una tarjeta, como las operaciones bancarias desde el propio domicilio.

Este instrumento está compuesto por:

- Los datos del documento, esto es, el número de la tarjeta.
- Los datos del emisor, es decir, la entidad.
- Los datos identificativos del titular de la tarjeta.
- Firma del titular.
- La fecha de caducidad.

TIPOS DE TARJETAS

Los tipos de tarjetas son varios, aunque los principales son los siguientes:

• Tarjeta de crédito: Tarjeta que emite una Entidad de Crédito y cuya característica principal es que los pagos que se realicen con la tarjeta suponen un crédito entre el titular de la misma y la Entidad de Crédito.

• Tarjeta de débito: Tarjeta que emite una Entidad Financiera y cuya característica principal es, a diferencia de la anterior, es que los pagos que se realicen con la tarjeta se cargan directamente a una Cuenta Bancaria del titular de la tarjeta.

La principal diferencia entre estos dos tipos de tarjeta es que la primera supone un medio de financiación, ya que el cargo en la Cuenta es aplazado, mientras que en la de débito el cargo es inmediato y, por lo tanto no supone un medio de financiación.

TARJETA DE CREDITO BANCARIA

Podemos entender por **"tarjeta de crédito"**, cualquier documento que le permita a su titular o usuario, disponiendo de un crédito del emisor, adquirir bienes o servicios en establecimientos afiliados al correspondiente sistema, sin perjuicio de las prestaciones adicionales al titular.

Consiste en una **tarjeta de plástico con una cinta magnética** en la que se almacena información del propietario, que puede emplearse como medio de pago o como instrumento de crédito. Su uso está sujeto a distintas tarifas, sea por concepto de comisiones cuando se usa como medio de pago, o de intereses en el caso que dé lugar a una operación de crédito. Las tarjetas de crédito son intransferibles y deben emitirse a nombre de su titular.

El uso de la tarjeta da lugar al cobro mensual de parte de la institución emisora tanto del capital usado como de los intereses, comisiones y seguros que correspondan.

Operadores de Tarjetas de Crédito

- Transbank S.A.- Código SBIF: 267 - Operador de tarjetas
- Nexus S.A.- Código SBIF: 268 - Operador de tarjetas
- Tarjetas de Chile S.A.- Código SBIF: 681 - Emisor de tarjeta Diners
- Fidelity National Information Services S.A. (Antes Certegy S.A)- Código SBIF: 684 - Operador de tarjetas

TIPOS DE FRAUDE CON TARJETA

Existen básicamente dos formas de actuación de las personas que se dedican a este tipo de delitos:

- por un lado la obtención de la tarjeta física como tal,
- y por el otro la grabación de los datos de la banda magnética para su posterior utilización, ya sea a través de una nueva tarjeta o utilizando los datos en compras realizadas a través de Internet.

En el primero de los casos, en los que los delincuentes se hacen físicamente con la tarjeta, una forma de obtenerla discretamente para así poder actuar es la siguiente:

- Se coloca en la ranura, donde se debe introducir la tarjeta, una nueva ranura que llevará una especie de “tope” para que la tarjeta, al ser introducida, no llegue al cajero. De este modo se ha conseguido que la tarjeta quede bloqueada.
- Aprovechando el hecho, uno de los delincuentes se acercará al usuario de la tarjeta y le comentará que a él le ha sucedido lo mismo, y que debe marcar una serie de números y para terminar su clave personal, que el delincuente estará mirando y memorizando.
- El siguiente paso, una vez que el dueño de la tarjeta se ha ido, confiado de que resolverán su problema, consiste en que un segundo delincuente (cómplice del primero) se acerque al cajero y retire la tarjeta, con lo que ya disponen de la tarjeta y de la clave personal.

Otra de las formas frecuentes de actuar consiste en obtener los datos de la tarjeta y posteriormente grabarlos en otra para poder operar con ella.

Existen en el mercado una multitud de lectoras/grabadoras de bandas magnéticas, que facilitan a los delincuentes esta tarea.

Algunas de las formas de conseguir estos datos son:

- En algunos casos, cuando vamos a acceder a un cajero interno de un banco, vemos que al lado de la puerta existe un dispositivo que presumiblemente debe abrir paso a los clientes si pasan su tarjeta por el mismo. Pues si bien es cierto que

- este dispositivo existe en algunas entidades bancarias, en otras son colocados por delincuentes que en el momento en el que pasamos la tarjeta por el lector están grabando los datos de su banda magnética. Para poder operar solo tienen que reproducirla y conseguir la clave secreta, que consiguen colocando una cámara que graba como pulsamos los números. Una recomendación ante un dispositivo de este tipo es antes de pasarlo por el lector probar si la puerta está abierta, ya que en ocasiones ocurre que pasamos la tarjeta sin comprobar antes si la puerta abre o no por si sola.

- En otras ocasiones colocan un cajero falso, consistente en el display con el teclado numérico y la ranura para la tarjeta, sobre el cajero verdadero. Este tipo de operaciones se hace en cajeros de calle que no cuentan con cámara de seguridad. De esta manera graban los datos de la tarjeta y la clave secreta. El dueño de la tarjeta únicamente cree que el cajero esta estropeado, ya que al pulsar la clave personal le sale un mensaje en el que se le indica que la operación ha sido cancelada.
- Tampoco se debe ser confiados cuando se va a comprar a una tienda, o pagamos con tarjeta en un restaurante, ya que se han dado casos en los que los propios empleados de este tipo de establecimientos han utilizado lectores de bandas magnéticas para grabar los datos de las tarjetas,

  Utilizándolos posteriormente para realizar compras. Es recomendable no perder de vista la tarjeta en este tipo de operaciones, aunque bien es cierto, por ejemplo, que no siempre es posible acompañar al camarero hasta el lugar donde se encuentra el lector de la tarjeta

No es necesario en todos los casos hacer una copia material o física de la tarjeta de crédito para llevar a cabo un uso fraudulento de la misma, se pueden hacer compras a través de Internet, es decir, a través de comercio electrónico utilizando el número de tarjeta y la fecha de caducidad. Es importante tener claro que la tarjeta de crédito comienza a ser un mecanismo de pago no del todo seguro, ya que podemos ser victimas sin enterarnos hasta el momento en el que la utilicemos de nuevo.

CLONACION DE TARJETAS DE CREDITO

El rápido crecimiento de las economías regionales y el fenómeno de globalización propiciaron en los últimos años importantes cambios en el manejo económico financiero a nivel mundial y especialmente en nuestro país, facilitando el incremento de uso de tarjetas de crédito como sustituto del tradicional papel moneda o dinero, cuyos orígenes ya datan de la edad media.

En este contexto de realidades, han proliferado también nuevas metodologías en los fraudes, que para llegarse a concretar con éxito, se nutren de tecnología de avanzada para intentar vulnerar las barreras de seguridad, que día tras día las empresas imponen a sus productos para dar mayor seguridad a los usuarios del sistema.

Se entiende por sistema de tarjeta de crédito al conjunto complejo y sistematizado de contratos individuales cuya finalidad es:

a) Posibilitar al usuario efectuar operaciones de compra o locación de bienes o servicios u obras, obtener préstamos y anticipos de dinero del sistema, en los comercios e instituciones adheridos.

b) Diferir para el titular responsable el pago o las devoluciones a fecha pactada o financiarlo conforme alguna de las modalidades establecidas en el contrato.

c) Abonar a los proveedores de bienes o servicios los consumos del usuario en los términos pactados.

Se entenderá por:

a) Emisor: Es la entidad financiera, comercial o bancaria que emita Tarjetas de Crédito, o que haga efectivo el pago.

b) Titular de Tarjeta de Crédito: Aquel que está habilitado para el uso de la Tarjeta de Crédito y quien se hace responsable de todos los cargos y consumos realizados personalmente o por los autorizados por el mismo.

c) Usuario, titular adicional, o beneficiario de extensiones: Aquel que está autorizado por el titular para realizar operaciones con Tarjeta de Crédito, a quien el emisor le entrega un instrumento de idénticas características que al titular.

d) Tarjeta de Compra: Aquella que las instituciones comerciales entregan a sus clientes para realizar compras exclusivas en su establecimiento o sucursales.

e) Tarjeta de Débito: Aquella que las instituciones bancarias entregan a sus clientes para que al efectuar compras o locaciones, los importes de las mismas sean debitados directamente de una cuenta de ahorro o corriente bancaria del titular.

f) Proveedor o Comercio Adherido: Aquel que en virtud del contrato celebrado con el emisor, proporciona bienes, obras o servicios al usuario aceptando percibir el importe mediante el sistema de Tarjeta de Crédito.

Las tarjetas de crédito se clasifican según distintos criterios:

EL TIPO DE TITULAR	Tarjetas individuales
	Tarjetas corporativas o empresariales
	Tarjetas industriales
SEGÚN LA FUNCIONALIDAD DEL PRODUCTO	Tarjetas de compra
	Tarjetas de compra y crédito
	Tarjetas múltiples (compra, crédito y débito)
SEGÚN LA COBERTURA GEOGRÁFICA O REGIONALIZACIÓN	Tarjetas internacionales
	Tarjetas nacionales
	Tarjetas regionales
SEGÚN LOS SERVICIOS O LOS LÍMITES DE COMPRA	Clásicas
	Gold
	Platinum

1. Tipo de titular

Las tarjetas individuales son personales e intransferibles y el único autorizado a utilizarlas es el titular.

Las tarjetas corporativas o empresariales cubren las necesidades del personal de las empresas. En este caso el sujeto del crédito es la empresa y sus empleados son los titulares autorizados.

Las tarjetas industriales dan seguridad a las operaciones de compras institucionales que efectúan las empresas a proveedores de distintos insumos.

2. Funcionalidad del producto

La tarjeta de compra suplanta momentáneamente al efectivo, al vencimiento del resumen de cuenta se tiene que pagar la totalidad de las compras. La función de crédito es transitoria**.**

La tarjeta de compra y crédito le suma a la anterior la posibilidad de financiar los consumos. El poseedor, sólo está obligado a pagar parte de sus compras, el llamado monto mínimo, y puede financiar el monto restante según lo pactado con el emisor.

La tarjeta múltiple reúne las funciones de compra, crédito y débito. Incluye la posibilidad de utilizar los cajeros automáticos y otras terminales electrónicas. Por medio de esta tarjeta se puede, con la función de débito, girar contra el límite de compra de la tarjeta, retirando adelantos en efectivo de los cajeros automáticos, o contra fondos disponibles en la cuenta corriente o caja de ahorro.

3. Cobertura geográfica

Las tarjetas internacionales pueden utilizarse en todos los países en que la marca tenga presencia. En nuestro país, pertenecen a este grupo American Express, Diners, Visa y Mastercard.

Las tarjetas nacionales tienen cobertura en todo el territorio nacional. .

Las tarjetas regionales: a este subgrupo pertenece una gran cantidad de tarjetas emitidas por distintas empresas de localidades del interior del país y que, por lo general, cubren un reducido territorio. Ejemplo tarjeta Xtra acá en la región.

4. Servicios y los límites de compra

Las tarjetas de crédito se clasifican en Clásicas, Gold y Platinum. Estas dos últimas poseen mayores beneficios que una tarjeta clásica en cuanto a los servicios otorgados a sus usuarios, como por ejemplo: acceso a salones VIP en Aeropuertos, seguro sin costo para alquiler de automóviles en el exterior, servicios telefónicos exclusivos para socios de

este tipo de tarjetas, etc. Los límites de compra son superiores a los de las tarjetas clásicas o, en algunos casos ilimitados.

Las primeras tarjetas de crédito aparecieron aproximadamente en la década de 1950. Con su uso surgió también la comisión de delitos en perjuicio de los propios tenedores, los comerciantes que recibían las tarjetas y las empresas emisoras.

"Dinero plástico", así se denomina a estas piezas, del tamaño de una tarjeta de presentación, que permite comprar productos y obtener servicios cuyo pago queda diferido. Las diferentes maniobras se fueron llevando a cabo y se siguen practicando aprovechando fallas en el sistema de control y seguridad (Pese a que se incorporan adelantos tecnológicos tendientes a detectar en tiempo oportuno el fraude) y el mismo desarrollo tecnológico que permite también anular o superar las defensas implementadas.

En consecuencia, las nuevas formas de protección, pese a ser cada vez mas sofisticadas, no han servido para impedir el fraude.

Los viejos controles de vigencia y titularidad de tarjetas de créditos basados en la distribución de planillas con listados de morosos e inhabilitados fueron reemplazados por:

- holagramas
- dígitos encriptados verificadores tanto en el anverso como en el reverso
- incorporación de lugares inviolables para estampar la firma
- *fotografías
- firmas incorporadas al plástico
- aparatos y dispositivos conectados a una base de datos que al simple paso de la tarjeta, por contacto directo refleja en una pantalla y directamente imprime sobre el ticket o factura la conformidad indicativa de que la operación crediticia está aprobada.

En algunos países (entre ellos Alemania, Francia, España, Paraguay), se han incorporado nuevas figuras delictivas para penar las maniobras de fraude, incorporándolas al Código Penal o en leyes especiales.

En nuestro país se dictó la ley 20.009 que limita la responsabilidad de los usuarios de tarjetas de crédito por operaciones realizadas con tarjetas extraviadas, hurtadas o robadas pero sus disposiciones no incorporan nuevos delitos, por lo que sólo es posible enjuiciar penalmente algunas de las conductas censurables, en la medida en que resulte posible encuadrar el caso en las normas punitivas tradicionales:

Lo que es absolutamente insuficiente por la falta de adecuación de determinadas acciones notoriamente enderezadas a aprovechar el mercado en el que se opera con tarjeta de crédito para burlar a sus legítimos usuarios, los comerciantes adheridos y las empresas organizadoras del sistema.

La aplicación de la legislación que podemos denominar "clásica" genera conflictos doctrinales y jurisprudenciales, acrecienta la inseguridad y facilita la actividad de grupos especializados en el fraude con tarjetas de crédito.

Maniobras adulteradoras y falsificadoras.

ADULTERACIÓN

Fue la primera en evolución de estos dos delitos, citándose a modo de ejemplo:

Pegado: es la más antigua y ya está en desuso; se realizaba a través del levantamiento mediante objetos cortantes, de los números embozados en las tarjetas como así también el nombre del titular y su reemplazo por datos de otras tarjetas, guardando el "arte" o gráfico de la tarjeta para que le confiera una apariencia de confiabilidad.

Planchado y regrabado: maniobra más evolucionada y actual que consiste en el aplastamiento de los datos embozados en los plásticos y su posterior regrabado con datos ajenos a la misma, al igual que en el afeitado y pegado.

Falsificación

Para este delito se debe contar con mayor estructura, ya que requiere la obtención de máquinas aptas para: el embozado del soporte (plásticos blancos), diseño de gráficos, grabado de datos en bandas magnéticas, diseño de hologramas y por supuesto, de una verdadera organización delictiva que obtenga los datos de usuarios de tarjetas vigentes. Por último, la utilización de las mismas en comercios adheridos y la reventa de los elementos adquiridos

Estas maniobras fueron combatidas mediante el agregado a los plásticos de nuevas medidas de seguridad tales como: hologramas, bandas magnéticas, isologotipos, embozado de seguridad, fotografía del usuario, firma digitalizada, tintas reactivas ultravioletas y, hace un par de años, a partir del mes de octubre de 1997, en Japón, como parte de un gran proyecto a escala establecido por el gobierno japonés con una de las

empresas de tarjetas de crédito, para desarrollar nuevas formas de pago relacionadas con el auge cada vez mayor del comercio electrónico, se implementó el "Microchip" como nueva medida de seguridad, lo que permite al usuario disfrutar de la experiencia de tener una tarjeta multifuncional a través de la combinación entre una tarjeta de crédito y de pago con fondo "recargable" por medio de terminales que posibilitan "leer" los fondos disponibles y las últimas transacciones con el plástico.

LA TARJETA DE DEBITO

Es aquella que las instituciones bancarias entregan a sus clientes para que al efectuar sus compras o locaciones los importes de las mismas sean debitadas directamente de una cuenta de ahorro o corriente bancaria del titular.

Uno de los recaudos tendientes a evitar el apoderamiento de las tarjetas remitidas al cliente o titular del instrumento de crédito, es la prescripción que impide darlas de alta en el sistema (para que se pueda operar con ellas) hasta que no se recepcione el acuse de recibo por parte del destinatario. Se procura evitar las maniobras que se llevan a cabo a partir de la sustracción de las tarjetas durante su distribución, porque incluso en muchos casos llega el sobre que la contiene hasta el domicilio indicado y cae en manos de terceros (encargados, empleados y hasta parientes del titular del plástico).

DELITOS CON TARJETAS DE CRÉDITO.

Las tarjetas de crédito utilizadas para defraudar, pueden ser:

a) tarjetas genuinas obtenidas con documentación falsa o de terceros;

b) Tarjetas genuinas sustraídas o halladas;

c) tarjetas genuinas adulteradas;

d) tarjetas totalmente falsificadas.

e) tarjetas genuinas utilizadas para defraudar por sus legítimos usuarios, en forma personal o en colusión con terceros.

Entre las modalidades más recientes se encuentran los fraudes en el telemarketing (mediante compras ordenadas por teléfono o Internet), donde el damnificado puede ser el comprador o el comerciante vendedor.

Delitos cometidos por el titular de la tarjeta.

Aquí se dan también diferentes situaciones:

Se Obtiene la tarjeta y hace en pocos días numerosas compras en distintos comercios; luego no paga y como no tiene solvencia el emisor se perjudica.

Habrá cometido delito de estafa si al solicitar la tarjeta lo hace mediante el suministro de datos falsos sobre sus bienes o ingresos.

Y hay **estafa** en estos casos porque el solicitante:

- Obtiene una tarjeta por parte de la entidad emisora por medios fraudulentos
- Usa la tarjeta para hacerse de bienes o dinero, sin posibilidad de cobrar o recuperar por imposibilidad de ubicar a la persona que usa la tarjeta o por ser absolutamente insolvente, hecho este ocultado al emisor de la tarjeta.

También habrá estafa si el titular **adultera la tarjeta** para ocultar su caducidad y efectúa compras, concurriendo ese delito con el de uso de documento privado falso.

- Uso de la tarjeta y desconocimiento posterior de las compras efectuadas.

El titular de la tarjeta cambia su firma o pone un garabato. Después alega que la compra no es suya. Es estafa.

- Entrega de la tarjeta a un tercero y posterior desconocimiento de las operaciones.

Alega que debe tratarse de una tarjeta clonada y desconoce la firma puesta en los recibos. Es estafa. Incluso hay casos en que el titular acompaña al que compra y coloca la firma falsa.

Delitos de terceros que sustraen o falsifican tarjetas de crédito y los que las utilizan sin ser los titulares autorizados.

1.- Normalmente se trata de un titular que obtuvo la tarjeta con documentos falsos o nombre supuesto o por haberla hallado, sustraído o comprado a delincuentes que las tienen como productos de sus ilícitos.

2.- Una vez en posesión de la tarjeta se usa un documento también ajeno para falsificar la cedula de identidad del que la usará como propia: falsificación de documento público que concurrirá materialmente con la estafa.

3.- Sustracción de la tarjeta enviada por correo

4.- Utilización de una tarjeta perdida.

5.- La firma del cupón y el delito de falsificación: El adquirente con tarjeta debe firmar un cupón o ticket, lo que por lo común se hace tratando de imitar la firma que obra en el documento de identidad o en la tarjeta. Hay falsificación de documento privado en concurso ideal con estafa.

6.- Con una tarjeta falsificada: La tarjeta puede ser falsificada de numerosas maneras: la banda magnética, la numeración en relieve, la parte impresa, etc.. A medida que aparecieron los distintos fraudes, las empresas emisoras han ido tomando nuevas medidas de seguridad; es cada vez mas difícil falsificar los plásticos con éxito. Pero se siguen falsificando. En este caso se pudo haber empleado la modalidad del "planchado" y "regrabación" de la tarjeta, maniobra que consiste en borrar uno o más números con calor hasta alisarlos y pegar encima, con el mismo método, el número extraído de otra tarjeta. Las tarjetas falsas se han utilizado para: hacer compras en los comercios, con lo que se configura estafa en concurso ideal con falsificación de documento privado; obtener dinero de los Cajeros Automáticos en relación a cuentas de terceros, lo que genera problemas de calificación legal, habida cuenta que se "engaña" a un aparato mecánico, que es quien expide el dinero: por el delito de hurto. Con una máquina lectograbadora e información de los números de cuenta que había obtenido -no sabemos por qué medio- tomaba cualquier tarjeta y le grababa los números de cuenta. Si la tarjeta todavía no tenia PIN (clave), le grababa una y extraía el dinero que el titular pudiera tener en la cuenta. Operó durante un tiempo y hubo que montar todo un largo operativo para detenerlo. Al calificar el hecho como hurto, las causas prescribieron. ¿Es posible equiparar el caso de fraude con la tarjeta de crédito con el fraude sobre aparatos mecánicos de que habla la jurisprudencia y la doctrina? Es estafa: El sentido común nos dice que no es igual introducir una moneda falsa en un expendedor automático -que entrega un chocolatín-con la introducción de una tarjeta falsa, con la que se saca dinero de una cuenta. En efecto, en el primer caso se obra automáticamente, es decir ante cualquiera que coloque algo que simule la moneda obrará expidiendo el chocolatín. En la tarjeta de crédito los datos incorporados electrónicamente van a impactar sobre un

programa preestablecido por el emisor de la tarjeta, que contiene una serie de instrucciones. Allí se indica que sólo se expedirá el dinero al poseedor de la tarjeta, cuya clave se ingrese simultáneamente por el cajero, que la cuenta tenga fondos o posibilidad de hacer extracciones y que no esté excedida, vencida, etc. Esta verificación la puede hacer -y en realidad la hace- un cajero de carne y hueso cuando en vez de hacer el trámite en un cajero automático se concurre a la ventanilla del Banco a sacar dinero con la tarjeta del Banco; esto constituye indudablemente estafa, que no advierte entonces la diferencia entre un caso y otro. En los casos de tarjetas de crédito, se está engañando a un programa que el Emisor introdujo en la máquina para evitar el uso de cajeros humanos y hacer más ágiles las transacciones. Es el Emisor, bajo este error, el que libera los fondos a quien no corresponde. Además, la ley penal sólo dice que se pena al que defraudare a otro con engaño. Es decir no habla del error, tampoco de quién o cómo lo debe sufrir. Hay una evidente disposición patrimonial perjudicial unida en relación causal por un error. Este error, ciertamente, no es humano, pero no deja de ser error. La ley penal no exige en absoluto la existencia de un error humano, sólo pide que alguien simule ser quien no es y aparente tener bienes o créditos que no tiene. Y ese ardid puede funcionar tanto frente a un ser humano o frente a una computadora, a quien otro ser humano instruyó de la misma forma que al cajero para pagar en ciertos casos, y no en otros. Ambos pueden ser engañados de la misma forma y caer en error de igual manera. No veo porqué hacer diferencia. La existencia de un engaño y la inexistencia de un apoderamiento (en realidad la máquina entrega engañada) determina claramente la estafa.

7.- Con una tarjeta retenida: Una variante que usada frecuentemente consiste en impedir la devolución de la tarjeta por el cajero automático, haciendo creer al poseedor que el cajero (la máquina) se la ha "tragado".

8.- Tarjeta obtenida intimidando al tenedor para que la entregue o acompañe a los delincuentes hasta el cajero para hacer extracciones de dinero

CONSUMACION Y TENTATIVA

La estafa por medio de tarjetas clonadas se consuma cuando se le entrega al estafador la mercadería mal habida.

Es posible la tentativa a partir del momento en que el autor hace uso de la tarjeta en el comercio. Antes hay actos preparatorios

Acciones legales por abuso o fraude.

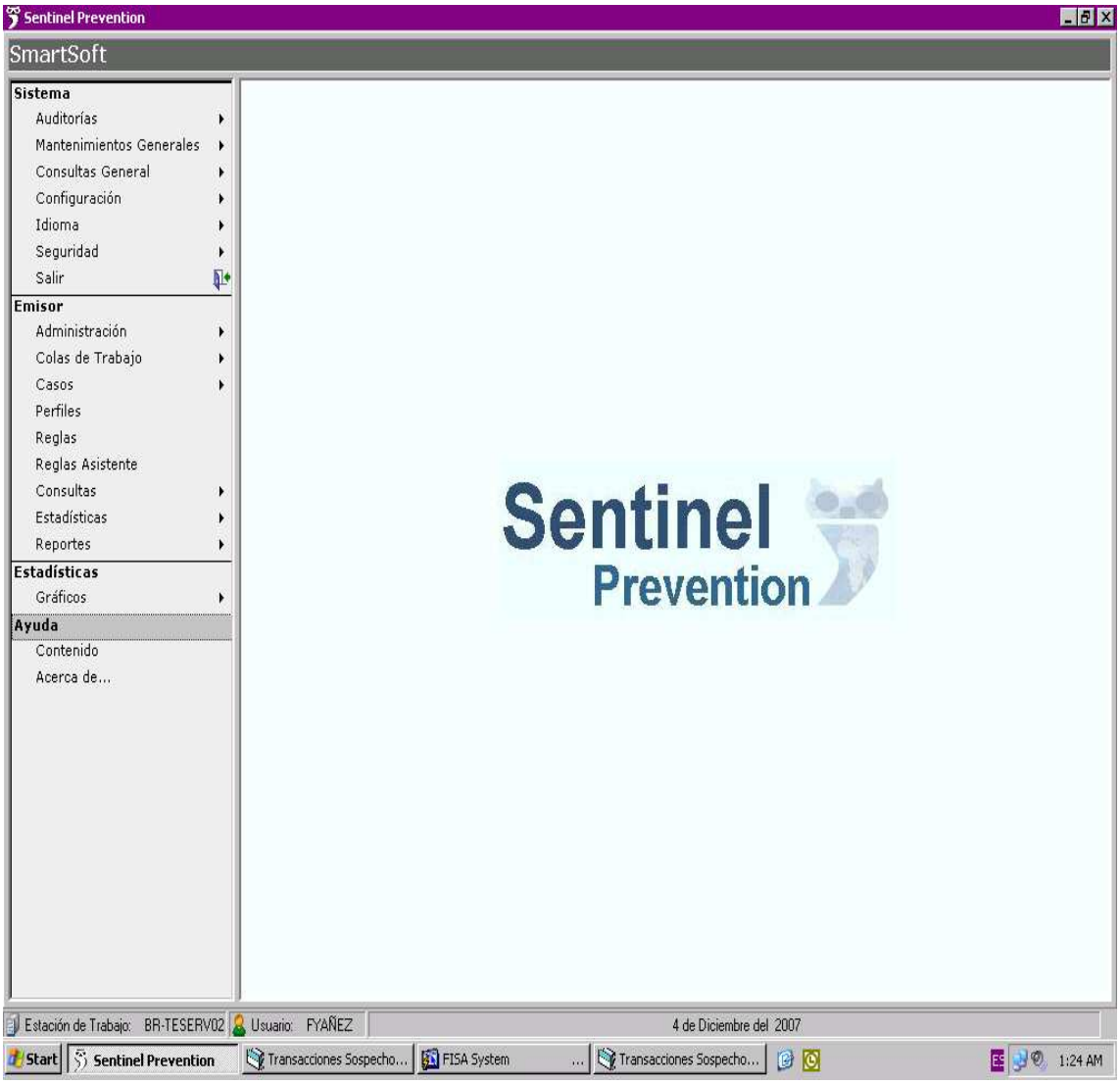
Ante el fraude, las posibilidades son:

1º) Acción penal. Querella por estafa, abuso de firma en blanco o el delito que corresponda (después de analizar los elementos de juicio) si las compras o las operaciones fraguadas se han producido mediante falsificación, apoderamiento de la tarjeta, etc.

2º) Acción civil en el fuero penal.

3º) Acción civil en el fuero comercial. La acción por rectificaciones, errores, etc., de la cuenta corriente bancaria prescribe a los cinco años (Art. 790 Código Comercio). Pero hay precedentes en el sentido de que existe una carga de impugnación de los resúmenes de cuenta corriente dentro de un cierto plazo (Art. 793 C.Com.), sin perjuicio de la posibilidad de revisarlos en sede judicial de acuerdo al Art. 790 Comercio.

SISTEMA DE MONITOREO UTLILIZADO POR LAS DISTINTAS ENTIDADES QUE ALCANZO LA MUESTRA



De acuerdo a la muestra los 6 bancos encuestados trabajan con similares sistemas de monitoreo de transacciones en línea, en distintas versiones siendo la más utilizada por los bancos la siguiente: “Sentinel Prevention”. Sistema que permite la detección y seguimiento de fraudes para la sección emisora de una empresa de tarjetas de crédito, mediante el uso de la tecnología para la detección y análisis de fraudes conocida como Reglas de negocios, Perfiles e Indicadores.

Una de sus características principales es que permite el monitoreo y seguimiento de

Los casos sospechosos, por parte del departamento de Seguridad de la entidad Bancaria, lo que brinda a la gerencia una visión en el ámbito general del comportamiento del fraude y la efectividad del seguimiento por parte de cada una de las oficinas de seguridad.

CARACTERISTICAS DEL SISTEMA

Se compone de una Interfase gráfica utilizable en los sistemas Microsoft Windows 95 o superiores.
Existe un Manejo de la seguridad del sistema, por medio de claves de acceso a la base de datos, para cada usuario.
También posee una definición detallada de privilegios, para cada usuario, a las opciones utilizadas en el sistema.
Permite una ayuda en línea, es bilingüe (Ingles – Español). Es Totalmente operacional en redes (sistema multiusuario). Posee una definición de reglas de negocios y perfiles para detectar la actividad sospechosa de fraude en Tarjeta habientes.
Es posible una ejecución automática de reglas de negocios e indicadores tanto para Comercios como para Tarjeta habientes.
Se puede efectuar una revisión de la actividad sospechosa de fraude, de lo general a lo específico, determinando las reglas de negocios o parámetros que permitirán la detección de la actividad sospechosa de fraude.
Se puede realizar una medición del desempeño de reglas de negocios o indicadores establecidos para la determinación de actividad sospechosa de fraude.

BENEFICIOS

Permite la detección de la actividad sospechosa de fraude, además de una ejecución automática de reglas de negocios y perfiles, permitiendo que el personal de Seguridad invierta su tiempo en el análisis y seguimiento de los casos sospechosos.
Permite el envío automático de correos electrónicos (email's), con el resultado de los distintos procesos a direcciones de correo predeterminadas. Permite a los departamentos de seguridad de las distintas entidades el acceso a la información, mediante la utilización de una interfaz web, facilitando a cada entidad el monitoreo y seguimiento de la actividad sospechosa de fraude.

Brinda la visión del comportamiento del fraude por Unidad Estratégica de Negocios, mostrando además, la efectividad en la prevención, detección y seguimiento de la actividad fraudulenta.

Se puede evaluar la efectividad de las reglas de negocios e indicadores en la detección del fraude, mediante la valoración del aporte brindado por cada regla.

El sistema SENTINEL se encuentra totalmente integrado en la detección y análisis de fraude, tanto en la parte emisora como en la adquirente, lo que facilita el seguimiento de cualquier transacción sospechosa de fraude hasta llegar a confirmar o descartar el fraude.

Una de las características que tienen en común todas las opciones del sistema es el manejo de las tablas de datos. Son todas aquellas tablas donde se encuentran datos organizados en columnas y renglones como un tipo de hoja electrónica.

Estas tablas, contienen los datos utilizados por el sistema para trabajar.

Como se explicó anteriormente, la tabla está cuadriculada, tiene renglones que representan registros individuales de datos y columnas que definen las características del registro. Mostrando, al lado derecho de la tabla, la información asociada al registro (renglón) seleccionado.

TIPOS DE AUDITORIAS QUE POSEE EL SISTEMA

AUDITORIA CALENDARIZACION DE TAREAS

En esta opción es posible consultar la calendarización de tareas que se han asignado a las reglas de negocios establecidas. Lo que permite llevar un control de cuáles reglas de negocios están siendo aplicadas.

Despliega, al lado izquierdo de la pantalla, una lista que incluye la información correspondiente al código y nombre de la regla que se calendarizó, tipo de regla (si es una regla simple o si fue creada mediante el Asistente), fecha y hora de la última ejecución de la regla y el nombre de la Unidad Estratégica de Negocios a la que está asociada la regla y en la parte derecha de la pantalla, los datos correspondientes a la auditoria de calendarización para la regla seleccionada.

AUDITORIA EVALUACION DE REGLA

Es posible consultar qué usuario ha realizado cambios sobre alguno de los campos de la tabla de transacciones.
Despliega, al lado izquierdo de la pantalla, una lista completa de las Unidades Estratégicas de Negocios que se han ingresado en el sistema y en la parte derecha de la pantalla, los datos de la auditoria de evaluación para la Unidad Estratégica de Negocios seleccionado del Listado de Unidades Estratégicas de Negocios.

Muestra la siguiente información:

Campo: campo de la tabla de transacciones que ha sido modificado.
Fecha Hora: fecha y hora en que se realizó la modificación.
Usuario: usuario que ejecutó la acción.

AUDITORIA CATEGORIAS DE COMERCIO

Permite consultar, para cada Unidad Estratégica de Negocios registrada en el sistema, los comercios (MCC's) que tiene asociados así como los que se han desligado.
Despliega, al lado izquierdo de la pantalla, una lista completa de las Unidades Estratégicas de Negocios que se han ingresado en el sistema y en la parte derecha de la pantalla, los datos de la auditoria de MCC's para la Unidad Estratégica de Negocios que haya sido seleccionado en el Listado de Unidad Estratégica de Negocios.

Muestra la siguiente información:

Fecha Hora: fecha y hora en que se realizó la acción.
Usuario: usuario que ejecutó la acción.
Código: código del MCC al que se le ejecutó la acción.
Descripción MCC: descripción del MCC al que se le ejecutó la acción.
Acción: acción que se realizó, presenta dos opciones: asociar o desasociar.

AUDITORIA DE PAISES SOSPECHOSOS

Acá es posible ver los países que se consideran sospechosos.
Despliega, al lado izquierdo de la pantalla, la lista completa de las Unidades Estratégicas de Negocios que tienen países sospechosos asociados y en la parte derecha de la pantalla, la lista de países sospechosos asociados a cada Unidad Estratégica de Negocios.

Muestra la siguiente información:

Fecha Hora: fecha y hora en que se realizó la acción.
Usuario: usuario que ejecutó la acción.
Código: código del país al que se le ejecutó la acción.
Nombre: descripción del país al que se le ejecutó la acción.
Acción: acción que se realizó, presenta dos opciones: asociar o desasociar.

AUDITORIA PRIVILEGIOS

En esta opción podemos apreciar los privilegios de acceso del sistema asignados a cada usuario. Lo que permite llevar un control de a quién y cuándo se le concedió o denegó algún privilegio.
Despliega, al lado izquierdo de la pantalla, una lista completa de los usuarios del sistema y en la parte derecha de la pantalla, los datos de la auditoria de privilegios para el usuario seleccionado del Listado de Usuarios.

Muestra la siguiente información:
Fecha Hora: fecha y hora en que se realizó la acción.
Responsable: usuario responsable de otorgar o denegar el privilegio.
Opción Seguridad: privilegio afectado.
Acción: acción que se realizó, presenta dos opciones: otorgar o denegar.

AUDITORIA EFECTIVIDAD DE REGLAS

Es posible consultar las modificaciones realizadas a los índices establecidos como parámetros para la medición de la efectividad de las reglas de negocios establecidas para la detección de transacciones sospechosas de fraude.
Despliega, al lado izquierdo de la pantalla, una lista completa de las Unidades Estratégicas de Negocios que se han ingresado en el sistema y en la parte derecha de la pantalla, los datos de la auditoria, que muestra las variaciones sufridas por los índices.

Muestra la siguiente información:
Usuario: usuario responsable de variar los índices.
Fecha y Hora: fecha y hora en que se realizó la acción.
Índice Filtrado: porcentaje asignado al filtrado dentro del porcentaje de efectividad.
Índice Acertación: porcentaje asignado a la acertación dentro del porcentaje de efectividad.
Índice Ahorro: porcentaje asignado al ahorro dentro del porcentaje de efectividad

MONITOR DE ALERTAS DE FRAUDES

Opción que permite consultar la información referente a las alertas de fraude que han sido enviadas.
Esta información es presentada en dos carpetas, que muestran la siguiente información:

Temas Relacionados

Registro de Envíos
Reporte de advertencias

Registro de envíos

Carpeta que muestra el registro de la información correspondiente a las alertas que se han enviado.
Presenta al lado izquierdo de la pantalla, una lista completa de las Unidades Estratégicas de Negocios que se han ingresado en el sistema y en la parte derecha de la pantalla, la

información correspondiente a las alertas enviadas a la Unidad Estratégica de Negocios seleccionada.

La información que muestra es la siguiente:
Fecha: fecha en que fue enviada la alerta.
Hora: hora a la que se envió la alerta.
Nombre Archivo: nombre del archivo en que se envió la alerta.
Email Dirigido a: dirección de correo electrónico de la persona a la que se envió la alerta.
Email Copia a: dirección de correo electrónico de la persona a la que se envió copia de la alerta.

REPORTE DE ADVERTENCIAS

Fecha: fecha en que se presentó la alerta.
Hora: hora en que se presentó la alerta.
Nº Error: número del error que provocó la alerta.
Fuente: objeto que provocó la alerta. Puede se provocado por errores de código, problemas con el acceso a la Base de Datos, problemas de envío de correos.
Descripción: descripción del tipo de alerta.
Alertas

Opción que permite seleccionar los usuarios a quienes se desea notificar de una alerta de fraude, presenta las siguientes opciones:

Correos
Opción que permite seleccionar los usuarios a quienes se desea notificar de una alerta de fraude, presenta dos opciones:

Dirigido...: usuario a quien será enviada la alerta de fraude.

Copia...: usuario a quien será enviada copia de la alerta de fraude.
Para cada uno de los destinatarios es posible establecer horarios de envíos de alertas, de tal manera que es posible configurar que al usuario A se le envíen alertas de la UEN 1 entre las 19:00 y las 23:00, y al usuario B se le envíen alertas de las misma UEN pero

entre las 23:00 y las 05:00. La opción muestra la pantalla que permite establecer el horario de envío de e-mails.

En la parte derecha de la pantalla de Horario de Envío de E-mails se muestra la lista de usuarios con sus diferentes direcciones de e-mail que han sido seleccionados para el envío de alertas en la UEN actual, en la parte izquierda de la pantalla se muestra el horario establecido para cada uno de los días de la semana. La calendarización para el envío de alertas se realiza a nivel de dirección de e-mail, para cada e-mail se establece un horario de envío. Para agregar una dirección de e-mail en el horario se presiona "clic derecho" sobre la dirección de e-mail que se desea calendarizar.

En la opción Incluir en horario se debe seleccionar la hora en la que se va a iniciar el envío de alertas a dicha dirección así como la hora en la que se va a suspender el envío de alertas al e-mail en cuestión.

Existe la opción de copiar el horario establecido para un día de la semana a cualquier otro día, esto con el fin de facilitar el trabajo en la definición del horario. La copia del calendario se realiza del día en que se encuentre posicionado a los días seleccionados. Luego de presionar el "botón" Copia de Horario se confirma la copia y se refleja el horario en los días seleccionados.

PERIODO DE TIEMPO DE ALERTAS

Esta opción brinda la posibilidad de elegir el período de tiempo para el que se desea el envío de alertas, presenta dos opciones:

Transacciones del día actual: al seleccionar esta opción se realiza el envío de las alertas que se han generado el día actual, de acuerdo con la frecuencia especificada.

Transacciones de hace: al seleccionar esta opción se especifica, en horas, el lapso de tiempo que se utilizará como referencia para el envío de las alertas generadas.

FRECUENCIA

Opción que brinda la posibilidad de establecer la frecuencia del envío de las alertas
Enviar cada: opción que permite especificar, en horas, la frecuencia con que se desea se envíen las alertas.
Próximo envío: opción que permite especificar el día y la hora a partir de cuando y retrocediendo el tiempo establecido en la opción Transacciones de hace, se generará el envío de la siguiente alerta.

INFORME

Opción que permite especificar el formato que tendrá el archivo además del tipo de informe que se desea enviar.

Formato Archivo: formato que tendrá el archivo que contiene la notificación de la alerta, esta opción presenta las siguientes alternativas: Documento Word (WORD), Documento Excel (EXCL), Documento HTML (HTML) y Documento PDF (PDF).
Tipo Informe: tipo de informe que se desea enviar en la notificación de la alerta, esta opción ofrece dos posibilidades:

LISTADO DE TRANSACCIONES

Transacciones por Tarjeta habiente

Funciones especial

Esta pantalla presenta una función especial la cual es detallada a continuación:

Seguridad de Alertas

Permite definir y la configuración de seguridad de claves, además muestra el historial de claves utilizadas.

Esta pantalla cuenta con dos carpetas:

CONFIGURACION

Carpeta que permite definir la seguridad para el manejo de alertas, los campos a ingresar son los siguientes:
Tipo Protección: define el tipo de protección a utilizar, ya sea archivos sin encriptación para el cual no se debe usar una clave, archivos encriptados o archivos auto desencriptables, para estos será necesario definir una clave y un algoritmo de encriptación.
Algoritmo de Encripción: algoritmo a utilizar para encriptar la información (podrá escoger entre dos AES- Rijndael ó Twofish).
Clave: clave a utilizar para encriptar la información.

HISTORIAL DE CLAVES

Carpeta que muestra el historial de claves utilizadas, la información que se muestra es la siguiente:
Fecha: fecha en que se creo la clave.
Usuario: usuario que definió la clave.
Clave: clave que se utilizó.

CLASIFICACION DEL COMERCIO

Esta opción de menú facilita la creación de un catálogo en el que se clasificarán los comercios (MCC's), que utilizará el sistema como base para la definición de reglas de negocios que identifiquen transacciones que pueden ser consideradas sospechosas de fraude. Permitiendo el ingreso, modificación y eliminación de registros de información.

La información a digitar será la siguiente:

Código: campo de diez caracteres correspondientes al código para la clasificación del comercio.
Descripción: descripción de la clasificación del comercio.
Comentario: espacio que permite el ingreso de observaciones que se consideren necesarias para el MCC.

CODIGOS DE RESPUESTA

Esta opción de menú permite el registro de los códigos que podrán ser recibidos como respuesta o resultado de una transacción. Facilitando el ingreso, modificación y eliminación de registros de datos.
La información a digitar será la siguiente:
Código: campo de diez caracteres, correspondiente al código para la clasificación del código de respuesta.
Descripción: descripción del código de respuesta.
Tipo: clasificación del código de respuesta, básicamente este dato se utiliza en la construcción de reglas.
Comentario: espacio que permite el ingreso de observaciones que se consideren necesarias para el código de respuesta.

CODIGOS DE SALIDA

Esta opción de menú registra los Códigos de Salida que podrán ser utilizados en la construcción de las reglas de negocios que se utilizarán para la determinación de actividades sospechosas de fraude en cada país. Permite ingresar, modificar y eliminar registros de datos.
Deberá digitar la siguiente información:
Código: campo de diez caracteres correspondientes al código para la clasificación del código de salida.
Descripción: descripción del código de salida.
Comentario: espacio que permite el ingreso de observaciones que se consideren necesarias para el código de salida.

PUNTOS DE ENTRADA

Esta opción de menú permite el registro de los distintos Puntos de Entrada que puede presentar una transacción, ya sea por medio de banda magnética o manual. Estos puntos podrán utilizarse en la construcción de las reglas de negocios que se utilizarán para la determinación de actividades sospechosas de fraude en cada Unidad Estratégica de Negocios. En ella se puede ingresar, modificar y eliminar registros de datos.
La información a digitar será la siguiente:

Código: campo de diez caracteres correspondientes al código para la clasificación del punto de entrada.
Descripción: descripción del punto de entrada.
Comentario: espacio que permite el ingreso de observaciones que se consideren necesarias para el punto de entrada.

TIPOS DE FRAUDE

Esta opción de menú permite el registro de los distintos Tipos de Fraude que se le podrán definir a una transacción sospechosa de fraude que, se ha comprobado, corresponde a un fraude. En ella se puede ingresar, modificar y eliminar registros de datos.
La información a digitar será la siguiente:
Código: campo de cuatro caracteres correspondientes al código para la clasificación del tipo de fraude.
Descripción: descripción del tipo de fraude.
Comentario: espacio que permite el ingreso de observaciones que se consideren necesarias para el tipo de fraude.

CONSULTA GENERAL

Opción que permite la consulta de datos generales del sistema.

Temas Relacionados
Sincronización de Reglas
Herramientas de Prevención de Fraude
Reglas Eliminadas

SINCRONIZACION DE REGLAS

Esta opción de menú muestra las reglas que se están trabajando en modo sincronizado. Bajo un grupo de sincronización se encuentran varias reglas, todas de diferentes Unidades Estratégicas de Negocios que comparten los mismos criterios en su definición.

HERRAMIENTAS DE PREVENCION DE FRAUDES

Esta opción de menú muestra en forma consolidada todas las herramientas de prevención de fraude que se tienen configuradas por Unidad Estratégica de Negocios. En la consulta se da la opción de listar las Reglas Emisor, Reglas Adquirente, Indicadores y Perfiles. Es posible consultar cada una de estas herramientas conjuntamente o en forma separada. Se deben seleccionar las herramientas que se desean incluir en la lista y refrescar la pantalla. (Ver anexo 2)
La información que se despliegue será la siguiente:
Id: identificador de la herramienta de prevención de fraude.
Nombre: nombre de la herramienta de prevención de fraude.
Última ejecución: fecha y hora de la última vez que se ejecutó la herramienta de prevención de fraude.
Tipo: Tipo de herramienta de prevención de fraude, los tipos de herramientas que maneja Sentinel son:

- ü Regla Adquirente Asistente.
- ü Regla Emisor Simple.
- ü Regla Emisor Asistente.
- ü Indicador Adquirente.
- ü Perfile Emisor.

REGLAS ELIMINADAS

Esta opción de menú muestra una auditoria de las reglas que ha eliminado cada uno de los usuarios del sistema que tiene el privilegio de eliminar reglas.
En la parte izquierda de la pantalla se muestra la lista de usuarios con privilegios para eliminar reglas y en la parte derecha las reglas que cada usuario ha eliminado.
La información que se despliegue será la siguiente:
Usuario: usuario del sistema con privilegio para eliminar reglas.
Descripción: número de las reglas que ha sido eliminada.
Tipo Regla: tipo de regla que ha sido eliminada.
Fecha: fecha y hora en la que se eliminó la regla.

Ver anexo Nº 1 Con ejemplos de comercios más riesgosos

CRIMINALIDAD INFORMÁTICA

1. Una de las trabas que se presenta para configurar un tipo específico de delito informático (DI) es, previamente, formular una definición adecuada que comprenda todas las modalidades posibles de ilícitos.

Retomando los elementos de la definición clásica de delito, entendemos por DI a aquella conducta típica –tipificada o establecida como ilícito por la ley-, antijurídica –contraria a derecho- y culpable –con intención dolosa o por negligencia-, cometida contra el soporte lógico de un sistema informático o de tratamiento automatizado de información ("programas o instrucciones" y "datos de cierta naturaleza o importancia"), generalmente mediante elementos Computacionales.

El Mensaje del Gobierno con el cual en Septiembre del 2005 se presentó un nuevo proyecto de ley, entiende por delito informático a toda conducta atentatoria de bienes jurídicos o valores sociales relevantes (patrimonio, fe pública, privacidad, etcétera), que suponga el uso de medios informáticos en alguna de sus fases de ejecución, quedando incluidas en la categoría aquellas conductas que recaen directamente en objetos no corporales asociados al desarrollo tecnológico informático (tales como documentos electrónicos y datos).

Se trata de una materia relacionada con otros ámbitos, tales como la protección de datos personales porque los atentados contra ellos o los casos de apropiación indebida de datos relevantes como los nominativos debieran ser establecidos como delitos; con la protección legal del software, porque su trascendencia hace que el uso ilegal o su copia, con o sin fines de venta o comercialización posterior –el caso del “pirateo”-, deba ser sancionada en sede penal; con la transferencia electrónica de fondos, porque muchos delitos informáticos han consistido en el redondeo computacional de cuentas bancarias o en el uso fraudulento de tarjetas de crédito; y con el flujo de datos transfronteras, porque la mayoría de los llamados "hackers" o penetradores de sistemas y "crakers" o destructores de los mismos actúan telemáticamente vía redes computacionales y de un Estado a otro.

2. El "objeto material" de todo delito es la entidad, persona o cosa sobre que recae la conducta reprochable penalmente. Una idea es esencial y obvia, no obstante lo cual los

legisladores de la ley 19.223 nunca lo entendieron: …no debe hablarse de criminalidad informática o de delitos computacionales, para sancionar eventuales atentados o abusos ilícitos que se cometan contra la totalidad de un sistema informático.

En materia de criminalidad informática sólo es necesario tipificar o crear nuevos delitos para castigar aquellas conductas que atenten contra el soporte lógico de un sistema, contra el software entendido en sentido amplio, …contra ciertos datos y/o documentos relevantes procesados y almacenados en un ordenador (que pueden ser manipulados, hurtados o atisbados, destruidos) y contra los programas o instrucciones que determinan el funcionamiento del mismo (los que pueden ser modificados, copiados ilegalmente y sin autorización,.).

Lo dicho se debe a la naturaleza física del soporte lógico, porque se trata de impulsos electromagnéticos, de bienes intangibles o inmateriales, no apropiables o aprehensibles físicamente, que no son de aquellas cosas corporales muebles susceptibles de apoderamiento y que puedan serle privadas en forma permanente a la víctima, lo que obsta para que se configuren los delitos tradicionales llamados patrimoniales (hurto, robo, apropiación indebida).

3. Una distinción es necesaria. Cuando hablamos de “bienes jurídicos” conculcados por un delito aludimos a valores esenciales para la sociedad que, por su importancia, el derecho penal los protege mediante la tipificación o consagración de hipótesis, casos o conductas que atentan en su contra. Es diferente en ciencia jurídica cuando hablamos de “objeto material”, porque nos referimos a la cosa o persona sobre la cual recae la conducta típica, al llamado “cuerpo del delito”, a la casa destruida, al auto robado, a la persona injuriada, entre otros.

Cuando se copia o se daña un programa computacionalmente, se lesiona la propiedad intelectual o copyright del titular del soft, que se verá menoscabado cuando por ejemplo no se le compre la licencia previa o no se pague el derecho de uso.

Cuando se copian o alteran datos almacenados o procesados en un sistema informático sólo deben sancionarse penalmente las conductas que vulneren datos relevantes o cuya naturaleza los haga dignos de ser protegidos en sede penal. Los bienes jurídicos afectados debieran ser ciertos y particulares datos de especial y relevante naturaleza,

tales como los nominativos o íntimos (que constituyen privacidad), los financieros o valores (que constituyen el patrimonio), y los estratégicos o relacionados con los secretos industriales.

4. Únicamente porque la tecnología computacional, los archivos y documentos electrónicos, las bases de datos, los discos duros, los correos electrónicos y la red Internet son herramientas esenciales de una empresa o de un servicio público, una conducta ilícita puede realizarse mediante soportes computacionales y violando su confidencialidad o reserva. Por eso es que suele afirmarse que no estamos frente a “nuevos delitos”, sino más bien ante nuevas formas de ejecutar las conductas típicas para atentar contra bienes jurídicos tradicionales (hurtos, daños, apropiaciones indebidas, fraudes, falsificaciones de documentos, y bienes jurídicos tales como patrimonio, fe pública, privacidad, etcétera).

Por ende, consideramos que la criminalidad informática o los abusos dolosos son más bien un tema ético, de detección de las llamadas "vulnerabilidades" y de seguridad preventiva para el uso y el acceso a los documentos almacenados en sistemas computacionales, que un asunto de tipificación legal de delitos idóneos, y mecanismos técnicos simples como las claves de acceso o "passwords" o más complejos como los perfiles de acceso, la encriptación o codificación y la autentificación de identidades mediante firmas y certificados digitales son una opción necesaria de ser revalorada por las empresas y servicios públicos.

MODALIDADES DE DELITOS INFORMÁTICOS

La expresión o la categoría de los "fraudes informáticos" se utiliza para aludir a todas las posibles alteraciones o manipulaciones tanto de los datos (al recopilarlos, procesarlos, estando almacenados o al transmitirlos telemáticamente) como de los programas de un sistema computacional.

El concepto, a diferencia de la noción tradicional de fraude o estafa, no se restringe a los delitos con ánimo de lucro, con una connotación pecuniaria o contra el patrimonio.

Ejemplos de fraudes informáticos son el redondeo electrónico de cuentas bancarias y la introducción de programas virus.

2. Lo que se ha llamado "espionaje informático" se refiere a la obtención ilícita, dolosa y sin autorización de datos o información relevante y de programas computacionales.

Caben aquí las conductas de los "hackers", la copia ilegal de programas sin fines de venta (el "hurto" de software o la copia sin comercialización posterior -porque el “pirateo” está sancionado en la ley de propiedad intelectual-).

3. La noción de "sabotaje informático" alude a los atentados que causan daños, destruyen o inutilizan un sistema computacional. Para ser exactos, la expresión debe reservarse para los atentados ilícitos que se cometan contra el software o soporte lógico -datos y programas- de un sistema informático, ya que el daño o la destrucción del hardware es una conducta de muy poca ocurrencia y comprendida en los delitos tradicionales.

Los ejemplos más clásicos -en consideración a sus efectos- son las bombas lógicas, las conductas de los “crakers” y los virus computacionales.

NORMATIVA VIGENTE SOBRE DELITOS INFORMATICOS

LEY 19.223

A pesar de la vigencia desde junio de 1993 de la Ley 19.223, que contempla penas que van desde 61 días hasta 10 años, el tema de la sanción legal de la criminalidad informática en Chile no está resuelto. De manera que a pesar que la ley se contemplo como una gran innovación para el derecho chileno, queda mucho por hacer con respecto al tema y nuevos proyectos de ley acorde con los progresivos avances en la Tecnologías de la Información.

El artículo primero de la ley 19.223 sanciona a quien maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento. La pena establecida es presidio menor en su grado mínimo a medio, esto es, de 61 días y hasta 3 años.
También se sanciona como delito contra un sistema de información si como consecuencia de estas conductas se afectaren los datos contenidos en el sistema, y se aplicará la pena señalada en el inciso anterior en su grado máximo, es decir, de 3 años y 1 día a 5 años.

El Articulo segundo, a quien con el ánimo de apoderarse, usar o conocer indebidamente la información intercepte, interfiera o acceda a un sistema de tratamiento de información, será castigado con presidio menor en su grado mínimo a medio o de 61 días y hasta 3 años. Se trata de una hipótesis de acceso no autorizado a información contenida en sistemas de tratamiento de información, dentro de los cuales están los electrónicos o informáticos, o de un caso de “hacking”, pero no de un mero acceso y por el sólo hecho de acceder sino con la exigencia de concurrencia de un elemento subjetivo adicional –ánimo de apropiación, uso o conocimiento-.

El Articulo tercero, muy similar o relacionado con el artículo 1º, castiga a quien maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información, y será castigado con presidio menor en su grado medio o de 541 días a 3 años. A algunos ha llamado la atención la excesiva severidad con que se aborda la destrucción de estos objetos, sin atender mayormente al valor económico o a la cuantía de los mismos.

El Articulo cuarto, a quien maliciosamente revele o difunda los datos contenidos en un sistema de información, el que sufrirá la pena de presidio menor en su grado medio -541 días a 3 años-, y si quien incurre en estas conductas es el responsable del sistema de información la pena se aumenta en un grado –de 3 años y 1 día hasta 5 años-

PROYECTOS DE LEY MODIFICATORIOS EN CURSO

Se reseñan dos iniciativas en curso o trámite parlamentario, que apuntan a, considerando los delitos tradicionales del Código Penal, establecidos como tales para proteger ciertos y determinados bienes jurídicos, agregar o incorporar nuevos casos o supuestos en que de la mano de la tecnología informática se atente contra dichos valores esenciales.

PROYECTO DE LEY (1º, Moción parlamentaria, Boletín 2974-19, complementada con una indicación del Ejecutivo):

"Artículo 1°.- Modificase el Código Penal de la sig uiente forma:

"1.- Sustitúyase el artículo 146, por el siguiente: "Articulo 146.- El que por cualquier medio abriere o registrare la correspondencia o los papeles de otro sin su voluntad o accediere a la información de otro contenida en redes, soportes lógicos o sistemas de tratamiento automatizado de información sin su voluntad sufrirá la pena de presidio menor en sus grados medio a máximo si divulgare o se aprovechare de los secretos que ellos contienen, y en el caso contrario la de reclusión menor en sus grados mínimo a medio. Esta disposición no es aplicable entre cónyuges, ni a los padres, guardadores o quienes hagan sus veces, en cuanto a los papeles, cartas o información contenida en redes, soportes lógicos o sistemas de tratamiento automatizado de información, de sus hijos o menores que se hallen bajo su dependencia. Tampoco es aplicable a aquellas personas a quienes por ley, reglamento o contrato con el titular de la información les es lícito instruirse de comunicaciones o informaciones ajenas."

Esta propuesta de ley buscó resolver la problemática que plantea el tipo de acceso ilegal o hacking contemplado en la Ley 19.223, eliminando la exigencia de concurrencia del elemento subjetivo especial "ánimo de apropiación, uso o conocimiento" y sancionando el mero hecho del acceso.

“2.- Incorpórese el siguiente numeral 9°, nuevo, al artículo 485: “9° Destruyendo, alterando, inutilizando o dañando de cualquier otro modo los datos, programas o documentos electrónicos de otros contenidos en redes, soportes lógicos o sistemas de tratamiento automatizado de la información".

“3.- Sustitúyase el inciso primero del artículo 487, por el siguiente: “Los daños no comprendidos en los artículos anteriores, serán penados con reclusión menor en su grado mínimo o multa de once a veinte unidades tributarias mensuales. Igual pena se impondrá al que impidiere u obstaculizare el funcionamiento de un sistema de tratamiento automatizado de la información".

Se contempla acá el entorpecimiento u obstaculización del funcionamiento de un sistema informático, hipótesis que apunta a un método de ataque informático denominado de “denegación de servicios”, consistente, como se ha explicado, “en la ejecución de un programa que realiza miles de solicitudes simultáneas a un sitio, a veces coordinados entre sí, aminorando la velocidad con la que el servidor recupera las páginas o en algunos casos, inutilizándolo por completo”.

Artículo 2°.- Derogase la ley Nº 19.223, publicada en el Diario Oficial el 7 de junio de 1993, que tipifica figuras penales relativas a la informática”.

PROYECTO DE LEY (2º, Proyecto o Mensaje del Gobierno2):

Artículo 1º.- Introducen las siguientes modificaciones al Código Penal:

* El proyecto propuso regular las conductas de falsificación de documentos electrónicos, clonación y adulteración de tarjetas de crédito junto a los delitos de falsificación, inherentes a o que se han presentado en el contexto de las transacciones no presénciales entre contratantes, en los artículos 193 y 197 del Código Penal.

1) Incorpórese el siguiente inciso segundo, nuevo, al artículo 193: "Con la misma pena se castigará al empleado público que, abusando de su oficio, forjare o alterare un documento público electrónico o incurriere, respecto de un instrumento público electrónico, en alguna de las falsedades previstas en los numerales 2°, 3°, 4° y 7° precedentes.".

2) Sustitúyase el inciso segundo del artículo 197 por los siguientes incisos: "Si tales falsedades se hubieren cometido en letras de cambio u otra clase de documentos mercantiles, se castigará a los culpables con presidio Al decir de los redactores del Mensaje, “el… proyecto propone una serie de modificaciones al Código Penal, con el objeto de recepcionar en los tipos penales tradicionales nuevas formas delictivas surgidas a partir del desarrollo de la informática”, y “de esta forma… llenar los vacíos o dificultades que aún después de la Ley Nº 19.223 subsisten en nuestro ordenamiento penal”. menor en su grado máximo y multa de dieciséis a veinte unidades tributarias mensuales, o sólo con la primera de estas penas atendidas las circunstancias.

Del mismo modo se castigará al que forjare o alterare tarjetas de crédito, débito o pago provistas de banda magnética u otro dispositivo técnico de almacenamiento de datos. En las mismas penas de los incisos anteriores incurrirá respectivamente el que, con perjuicio de tercero, forjare o alterare un documento privado electrónico suscrito por medio de firma electrónica.".

3) Sustitúyase el artículo 284 por el siguiente: "Artículo 284.- El que fraudulentamente comunicare o se aprovechare de secretos comerciales, industriales o profesionales de la persona, empresa o institución a la que presta o ha prestado servicios, sufrirá la pena de reclusión menor en su grado medio y multa de once a veinte unidades tributarias mensuales". Este artículo, sobre violación de secretos del comercio, alude a los casos en que el acceso a la información contenida en un sistema computacional puede afectar patrimonialmente a su titular, como ocurre precisamente con la revelación de datos tales como sobre secretos industriales o comerciales. Esto es importante, porque en Chile “….la información con valor económico carece de protección penal, como lo demuestran la inexistencia de un delito de espionaje industrial o comercial y el alcance muy limitado del delito de comunicación de secretos de fábrica”.

4) Incorporase el siguiente inciso segundo, nuevo, al artículo 468: "En las mismas penas incurrirá el que, alterando indebidamente el funcionamiento de un sistema de tratamiento automatizado de la información o los datos contenidos en el mismo, o valiéndose de cualquier otra manipulación informática o artificio semejante, modificare una situación patrimonial en perjuicio de otro.".

5)

Incorporase el siguiente artículo 470 bis: "Artículo 470 bis.- A los queen perjuicio de otro

obtuvieren indebidamente servicios de telecomunicaciones mediante conexiones clandestinas o fraudulentas o mediante cualquier maniobra técnica que permita neutralizar, eludir o burlar los mecanismos de control del legítimo acceso al servicio, en beneficio de tercero y a título oneroso, se aplicarán las penas del artículo 467. En caso de reiteración, los hechos se considerarán como un solo delito, y la regulación de la pena se hará tomando por base el monto total de lo defraudado. Cuando el perjuicio no excediere de una unidad tributaria mensual, se aplicarán las penas del Nº 3 de dicho artículo.

Al decir del Mensaje del Gobierno, “la inclusión de este nuevo artículo. 470 bis permite comprender las hipótesis de clonación de celulares, el acceso a señales satelitales cifradas sin pagar, y la obtención ilegítima de señal de televisión por cable mediante conexiones clandestinas o fraudulentas o mediante cualquier maniobra técnica que permita neutralizar, eludir o burlar los mecanismos de control del legítimo acceso al servicio”.

INTIMIDAD Y PRIVACIDAD DE LAS PERSONAS ANTE EL ROBO DE DATOS PERSONALES

No puedo dejar pasar como ejemplo para este proyecto de tesis el delito detectado en octubre del año 2008 donde un ex empleado de empresas bancarias, donde se procesan millones de datos personales, copió una base de datos con los antecedentes de las tarjetas de crédito de 19.000 personas, y con ellos, clonó tarjetas de crédito y giró fondos de cajeros automáticos. La primera lectura ha llevado a procesarlo por los delitos de clonación de tarjetas, adulteración o falsificación de ellas, que son instrumentos privados mercantiles. Esto es correcto, porque se trata de un delito patrimonial.

El tema no es nuevo. Así lo demuestran casos de delitos cometidos en Chile casi simbólicos como el que afecto a la empresa Falabella hace muchos años, y lo que ha sido la tipificación de delitos informáticos en el Derecho Comparado o en la legislación extranjera desde 1978 a la fecha.

Los alcances del atentado vía conductas dolosas que deben ser tipificadas como delito penal quedaron en evidencia con el caso de un periodista inglés del diario The Sun, que adquirió ilícitamente los antecedentes de los titulares de un millón de tarjetas de crédito de manos del empleado de un call center en Nueva Delhi.

Lo que no debe dejarse de lado es entender que previamente se accedió sin autorización a miles de datos personales o nominativos de los tarjeta habientes. Esos datos o antecedentes son parte de la intimidad o privacidad de esas personas, y el mero hecho de obtenerlos indebida y dolosamente ya debiera ser sancionado en conformidad al artículo 2º de la ley 19.223, sobre delitos informáticos.

La protección penal de la intimidad y delitos informáticos, son temas que admiten por cierto un trato metodológico y deontológico separado o autónomo, pero deben abordarse en conjunto porque entendemos que la privacidad o intimidad, tanto en cuanto datos personales o nominativos procesados computacionalmente, es en las Sociedades de la información del Siglo XXI, un bien jurídico fundamental cuyo mal uso o abuso debe sancionarse penalmente, con penas privativas de libertad o mediante la tipificación de delitos informáticos. De cara a o desde la perspectiva de la criminalidad informática o computacional, junto con el patrimonio de las personas y empresas uno de los bienes jurídicos más afectados y que requiere de mayor tutela es la privacidad o intimidad de las

personas. La intimidad, tanto en cuanto a datos personales procesados computacionalmente, es un bien jurídico carente de tutela idónea en el derecho tradicional, y no basta su consagración constitucional en el artículo 19Nº4 de la Constitución de 1980 ni descansar en la labor de la jurisprudencia conocedora de los Recursos de Protección. Dicho resguardo frente a la informática -o al procesamiento abusivo y doloso de datos personales- es esencial.

A mayor abundamiento -y desde otra perspectiva-, al año 2008 se afirma que “el robo de identidad” -un concepto para nada jurídico- es uno de los “cibercrímenes” -o delitos informáticos cometidos en el “ciberespacio“- que más se ha incrementado en el último tiempo, por ejemplo de cara a la obtención ilícita y dolosa de los datos personales incluso de nosotros los estudiantes universitarios. Se dice, concretamente, que cada vez hay más información confidencial y sensible en bases de datos, ya no sólo en el ámbito de las finanzas sino también en otros sectores como el educativo, y donde se intenta obtener información financiera, estados de cuentas corrientes o información clínica de los estudiantes.

Antes de la clonación, en este caso hubo un robo de identidad o de datos personales de los tarjeta habientes, lo que en definitiva les causó un perjuicio. ¿Podemos pensar que ello se debió a la negligencia de los bancos donde trabajó el ingeniero informático que luego cometió las estafas? Si él efectivamente era un funcionario externo (que accedía a los sistemas a consecuencia de un outsourcing), ¿el banco que externalizó, adoptó las necesarias medidas de seguridad para fiscalizarlo y para proteger los datos de sus clientes? Los hechos parecen indicar lo contrario.

El tema de los delitos contra la intimidad esta abiertamente debatido actualmente tanto en chile como en el derecho comparado, lo mismo que los delitos contra el honor. Se cuestiona mucho la necesidad de protección “penal” para atentado contra bienes jurídicos sobre los que pareciese ser mas eficaz la tutela civil que la penal. En legislaciones europeas se han derogado los delitos contra la intimidad y el honor (violación de correspondencia, injurias y calumnias), siendo reemplazados por ilícitos civiles, donde pareciera que el concepto de sanción-indemnización es mucho mas efectivo que el de sanción-multa y evidentemente también mas efectivo que el de sanción-privación de libertad.

Por otro lado se cuestiona esta visión por cuanto al trasladar el ilícito al ámbito civil se esta patrimonializando la protección de la intimidad, el cual, en tanto bien jurídico

diferenciable de la propiedad, debiera tener protección propia. Pero es ineludible que el concepto de indemnización se vincula únicamente con las reparaciones patrimoniales.

Si bien la propiedad no es un bien jurídico protegido por la protección de datos personales, como si lo es la intimidad, es innegable que los datos personales en tanto cosas incorporales tienen una potencia patrimonial que permite comercializar con ellos. Esta es una razón más que suficiente para avalar la posición de las modernas legislaciones que sacaron del ámbito penal la protección de la intimidad y la ubicaron en sede civil.

Por tanto el tema de la clonación y eventual uso, de tarjetas de crédito, debiera ser, un ilícito pluriofensivo, en tanto en sede penal es un delito contra el patrimonio (el uso de la tarjeta clonada) y contra la fe publica (la clonación, adulteración o falsificación misma), y en sede civil debiera ser un ilícito contra la intimidad sancionado con una indemnización pecuniaria.

El tema es muy discutible, pero en principio parece una alternativa si bien garantista, efectiva. Como bien dice el profesor, con el mal llamado “robo de identidad” se produce un perjuicio contra la “victima” y al parecer una sanción penal no repara ningún perjuicio al afectado, es mas bien una sanción social, a diferencia de la indemnización que resguarda mucho mas efectivamente un bien jurídico individual como lo es la intimidad, y como es obvio es mas concreta la reparación del “perjuicio” del afectado.

(Ver anexo Nº 2 con ejemplo de base de datos que posee actualmente una entidad bancaria)

PROCESO DE CERTIFICACIÓN DE SEGURIDAD DE LA INFORMACIÓN VIGENTE EN CHILE NORMAS ISO 17799

Hoy por hoy el mundo de la seguridad se debate en dos posturas de instituciones muy respetables, las cuales han regido el mundo de las normas internacionales por muchos años, cada uno en diferentes lugares del mundo; y cada uno con una aproximación diferente. Por una parte tenemos a ISO y por otra parte tenemos a NIST cada una de estas instituciones ha propuesto un marco de trabajo para el tema de la seguridad informática.

Lo primero que debemos aclarar es la procedencia de las dos organizaciones la ISO es bien conocida en el mundo como la organización que se encarga de fijar las normas aceptadas en Europa y en buena parte del mundo. Por su parte en USA su contraparte en la materia es el NIST. Cada una tiene una postura frente al manejo de la seguridad informática.

Ante la necesidad de fijar un estándar en la industria la ISO adapto el estándar ingles una norma que había sido promulgado con anterioridad el BS7799, que había tomado una gran fuerza como documento base en seguridad informática, documento que poseía en su momento dos versiones 7799-1 código de practicas para la administración de seguridad en informática y 7799-2 las especificaciones para la administración de seguridad en informática. Ambos documentos creados con propósitos bastante diferentes, el primero como una guía general para encargados de seguridad en corporaciones y el segundo como una guía en la implementación de seguridad en organizaciones, tal y como aparece en los respectivos documentos. Cuando fue publicado el estándar vigente a diciembre del 2001 se basaba en el primer documento mencionado. El que sirve como guía de implementación, pero no explica particularidades de los sistemas ni su implementación particular.

Por otra parte para el profesional en informática el precio de estos documentos puede llegar ha hacerlos poco viables en principio, dado que el documento que esta disponible en Internet para bajar por un precio cercano a los U$S100 (cien dólares) sin embargo no deja de ser un estándar importante para tener en cuenta ya que arroja luces sobre muchos de los aspectos básicos de la implementación en seguridad desde la compra de equipos hasta planeación de contingencia.

Por su parte debido a un acta del congreso de 1987 el NIST debió desarrollar una serie de estándares que permitieran a las instituciones operar de manera segura con

documentos considerados no clasificados pero que sin embargo requerían mantenerse confidenciales por políticas de privacidad gubernamental. Dado esto y que han existido con anterioridad una serie importante de requerimientos por parte de la mayoría de agencias gubernamentales, se desarrollaron una serie de estándares que permiten tomar como base el sistema actual y convertirlo en un sistema seguro.

Normativas como ISO 17799 asisten en la implantación y especialmente en la gerencia de día-a-día para enfrentar la proliferación de comunicación y discontinuidad de tecnología. Es por esta razón que componentes de esquemas como ISO asisten en la realización de seguridad tanto financieras como de red informática.

ISO 17799 provee bases fundamentales para la seguridad en la administración de redes. Una vez implantada la misma propicia mejoras concurrentes con los avances en tecnología y proliferación de comunicación. La vulnerabilidad de sistemas es una situación que cambia a diario, no es una situación de semanas o meses, es de días u horas.

Para implantar ISO 17799 se requiere capacitar al personal no necesariamente y únicamente en aspectos tecnológicos sino que también en el trabajo de equipo y asegurar un adecuado avance del sistema de gerencia concurrente con la realidad tecnológica y comunicación.

NORMAS ISO 17799 - BS 7799

ISO/IEC 17799 es una norma mundial para gestionar la seguridad de la información que entrega un marco de trabajo para revisarla y mejorarla en cualquier tipo de empresa, abarcando las mejores prácticas a través de un conjunto integral de 127 controles.

Básicamente es un set de controles que incluyen las "mejores practicas" en seguridad de la información. Un estándar genérico de seguridad reconocido internacionalmente

Muchas organizaciones han declarado su intención de certificarse o están alineando sus procesos. Principalmente instituciones financieras que ya habían adoptado el BS7799 o British Standard. Podemos decir que desde los eventos del 11 de septiembre de 2001 en Nueva York, surgió boom de seguridad informática.

CERTIFICACIÓN

Más que todo es realizada por un tema de competitividad. Ya que si un competidor se certifica antes esto podría servir como un diferenciador en el mercado.
Claramente se ve la necesidad de la certificación en cuestiones de procesamientos de datos informáticos. Pero igual de importante puede ser para una firma consultora que ejecuta auditorias o un despacho de abogados que llevan a cabo la fusión de dos empresas. Ellos tendrán que garantizar que la información de sus clientes se encuentra protegida y que no habrá fugas o pérdidas de información.

Lo que se puede hacer con respeto al ISO 17799

1.- Ignorarlo.
2.- Al implementar políticas de seguridad en las empresas, tomar el ISO como una guía e intentar cubrir todos sus puntos.
3.- Desarrollar todas las políticas del ISO 17799 y continuamente verificar que se cumplan.
4.- Buscar la certificación completa.

ETAPAS A CUMPLIR

1. Hojas de operación (planning) de la Continuidad del Negocio

Evitar interrupciones a las actividades económicas y a los procesos críticos del negocio, evaluando los efectos de incidentes o de desastres importantes.

2. Control de Acceso del Sistema

Controlar el acceso a la información. Prevenir el acceso desautorizado a los sistemas de información. Asegurar la protección de servicios network. Prevenir el acceso desautorizado a los computadores. Detectar actividades no autorizadas. Asegurar la información al usar recursos móviles, el computador y servicios de telecomunicaciones de una red

3. Desarrollo y Mantenimiento del Sistema

Asegurando la construcción de sistemas operacionales. Previniendo la pérdida, modificación o el uso erróneo de los datos en sistemas o aplicaciones. Proteger el secreto, la autenticidad y la integridad de la información. Asegurar que los proyectos y actividades de ayuda se conduzcan de una manera correcta. Mantener la seguridad del software del sistema y de los datos de la aplicación.

4. Seguridad física y ambiental

Prevenir el acceso a personas no autorizadas a la información, que pudieran ocasionar daños o interferencia. Prevenir la pérdida o daño en los activos que causaran interrupción a las actividades económicas. Prevenir el hurto de recursos con información y un mal tratamiento de ellos.

5. Conformidad

Evitar la ambigüedad de cualquier obligación criminal o civil, estatutos reguladores o contractuales que tengan relación con cualquier requisito de seguridad. Asegurar la conformidad entre sistemas de seguridad y políticas o estándares de la organización. Maximizar la eficacia y reducir al mínimo la interferencia externa a los procesos o sistemas.

6. Seguridad del Personal

Reducir riesgos de error, hurto, fraude o el uso erróneo por parte del recurso humano. Asegurarse de que los operadores estén enterados de amenazas y se preocupen de la seguridad de la información, y que estén equipados para utilizar la política corporativa de seguridad en el curso de su trabajo normal. Reducir al mínimo el daño de incidentes y de mal funcionamiento de la seguridad y aprender de tales incidentes.

7. Organización de la Seguridad

Manejar seguridad de la información dentro de la compañía. Mantener la seguridad de los recursos de la organización, del tratamiento de la información y de los activos de la información alcanzados por terceros. Mantener la seguridad de la información cuando el

tratamiento de la información ha sido responsabilidad de un outsourcing (organización externa).

8. Administración del Procesador y de la Red (Conectividad)

Asegurar la operación correcta y segura de los recursos que realizan tratamiento de información. Reducir al mínimo el riesgo de fallas de los sistemas. Proteger la integridad lógica del software y de la información. Mantener la integridad, disponibilidad del tratamiento y de la comunicación de la información. Asegurar y salvaguardar la información en redes y la protección de la infraestructura que se utiliza. Prevenir las interrupciones de las actividades económicas y daños a los activos, además de la pérdida, modificación o el uso erróneo de la información intercambiada entre las organizaciones.

9. Clasificación y control del activo

Mantener la protección apropiada de activos corporativos y asegurarse de que los activos de la información reciben un nivel apropiado de protección.

10. Política De la Seguridad

Proporcionar a la dirección o gerencia la ayuda para la seguridad de la información.

ESTANDAR DE SEGURIDAD DE DATOS DE LA INDUSTRIA DE PAGOS CON TARJETAS DE CRÉDITO (PCI DSS)

Las principales empresas de tarjetas de crédito en el extranjero (Visa, Mastercard) están luchando por detener los incidentes de fraude financiero que han afectado a varias organizaciones y a sus consumidores. Consecuentemente, las organizaciones que aceptan transacciones de pagos con tarjeta tienen que comprometerse a cumplir PCI DSS para finales de 2008. Las organizaciones que no puedan cumplir, se arriesgan a no tener permitido el tratamiento de información de titulares de tarjeta y a sanciones de hasta US$ 500.000 si los datos son perdidos o robados. Este Informe de tesis examina los requerimientos necesarios para cumplir con PCI DSS, las implicaciones del no cumplimiento y cómo es de eficaz el papel que juegan la administración de registros de sucesos y la administración de vulnerabilidad de red en la consecución del cumplimiento.

Las tarjetas de crédito tanto en chile como en el extranjero están muy extendidas y su uso para pagos online se está incrementando drásticamente. Había 1.300 millones de tarjetas de crédito en circulación en USA en 2004, con un 76% de Americanos contando con al menos una tarjeta de crédito. Las ventas de comercio electrónico al detalle en USA durante el año 2006 fueron US$ 33.900 millones, un 25% de incremento sobre el mismo trimestre en 2005.

Sin embargo el fraude por tarjetas de crédito (25%) fue la forma más común de robo de identidad informada en 2006. Considerando que dicho año las instituciones financieras y empresas perdieron más de US$ 48.000 millones debido al robo de identidad, y US$ 5.000 millones fueron perdidos por particulares, se puede decir que el fraude por tarjetas de crédito está llegando al fondo de los bolsillos de todos. El fraude del comercio electrónico también está elevándose, alcanzando los US$ 3.000 millones en 2006 con un incremento del 7% sobre el 2005. El presente capitulo examina las consecuencias del robo de información de titulares de tarjetas y aborda las siguientes cuestiones clave:

¿Qué es la directiva PCI?

¿Por qué para su negocio es importante cumplirla?

¿Cuáles son las consecuencias de no cumplirla?

¿Qué soluciones hay disponibles para abordar la directiva PCI?

Robo y fraude de información de titulares de tarjetas – algunos casos reales en el extranjero.

18 de Febrero de 2005 – Bank of America acusado de haber perdido más de 1,2 millones de registros de clientes – aunque dijeron que no había evidencia de que la información hubiera caído en manos criminales.

16 de Junio de 2005 – CardSystems, proveedor de procesamiento de pagos para comercios, fue demandado en una serie de casos de la acción popular alegando que falló al proteger la información personal de 40 millones de clientes. El negocio de CardSystems encaraba el colapso ya que VISA y American Express cortaron sus lazos con la empresa, prohibiéndola procesar información de sus tarjetas. CardSystems fue posteriormente adquirida por otra empresa.

9 de Febrero de 2006 – Se estimó que alrededor de 200.000 cuentas de tarjetas de débito fueron reveladas por comercios al detalle desconocidos, aparentemente OfficeMax y otros. Estas incluían cuentas relacionadas con comerciantes de bancos y sociedades de crédito a escala nacional tales como CitiBank y Wells Fargo.

31 de Enero de 2006 – Boston Globe y The Worcester Telegram & Gazette expusieron involuntariamente 240.000 registros de tarjetas de crédito y débito, junto con información de ruta de cheques personales, impresos en papel usado reciclado para envoltorios para la distribución de periódicos

12 de Enero de 2007 – MoneyGram, un proveedor de medio de pago, informó que un servidor de la empresa fue ilegalmente accedido desde Internet el mes pasado. Contenía información de unos 79.000 recibos de pago de clientes, incluyendo nombres, direcciones, números de teléfono y, en algunos casos, números de cuenta bancaria.

17 de Enero de 2007 – TJX Companies Inc. anunció públicamente que había experimentado una intrusión no autorizada en el sistema electrónico de procesamiento de información de tarjetas de crédito/débito. En la que es considerada como la más fascinante brecha de seguridad hasta la fecha, hasta 45.700.000 números de cuenta de tarjetas de crédito/débito y más de 455.000 registros de devolución de mercancía (conteniendo nombres y números de permiso de conducción de clientes) fueron robados del sistema de TI de la empresa.

Los grandes detallistas online no son las únicas organizaciones en el punto de mira. La atención pública puede estar fijada en las grandes pérdidas de información, pero los

expertos en fraude financiero dicen que los hackers están fijando el objetivo cada vez más en pequeños sitios web comerciales. En algunos casos, los criminales son capaces de conseguir acceso en tiempo real a la información de las transacciones de sitios web, permitiéndoles robar números válidos de tarjeta de crédito y rápidamente realizar gran número de compras fraudulentas. Los pequeños negocios electrónicos ofrecen menos victimas, pero a menudo suponen un objetivo más sencillo, debido a defectos en las aplicaciones utilizadas para procesar pedidos o por una sobre confianza en la subcontratada seguridad del sitio.

El ciber crimen y la amenaza que acompaña al robo de identidad reducen la confianza del usuario y consumidor, ralentizando la aceptación del comercio electrónico. Como resultado, la seguridad informática, actividad crítica que ayuda a proteger estos sistemas, ha pasado a una posición de importancia.

DIRECTIVA DE LA INDUSTRIA DE PAGOS CON TARJETA (PCI)

El marco de seguridad de datos de la Industria de Pagos con Tarjeta (PCI) fue creado por American Express, Discover Financial Services, JCB, MasterCard Worldwide, y Visa Internacional. Antes de 2004, cada una de las asociaciones tenía un conjunto propietario de requerimientos de seguridad de la información que a menudo eran agobiantes y repetitivas para los participantes en redes de varias marcas. Posteriormente las asociaciones crearon un conjunto uniforme de requerimientos de seguridad de la información para todas las marcas nacionales de tarjetas (exclusiva de boutiques y etiquetas privadas). Estos requerimientos han pasado a ser conocidos como el Estándar de Seguridad de Datos PCI (PCI DSS), que rige en todos los canales de pago: Venta al detalle, por correo, por teléfono y comercio electrónico.

PROGRAMA PCI SEGURIDAD DE LA INFORMACIÓN DE LAS TARJETAS DE CREDITO BANCARIAS, UTILIZADO ACTUALMENTE EN EL EXTRANJERO Y PRONTO EN CHILE

Programa de Seguridad de la Información (AIS) es el nombre del programa de cumplimiento en relación con la seguridad de la información de las tarjetas de crédito bancarias. La seguridad de la información de tarjetas se ha convertido en una verdadera preocupación en todo el mundo, tanto para los bancos que emiten tarjetas de crédito como para los comercios que las aceptan y, por supuesto, para los clientes que las utilizan. En muchos países, se han producido casos en los cuales delincuentes acceden a sistemas informáticos, roban la información de tarjetas y utilizan estos datos para cometer fraudes. En la mayoría de los casos, estos sistemas informáticos han sido operados por comercios que aceptan tarjetas de pago o por vendedores que procesan pagos en su nombre.

Como respuesta a este problema, se han creado las Normas de Seguridad de la Información de la Industria de Medios de Pago (PCI DSS). Se trata de un conjunto de requisitos y procesos comunes al sector, desarrollados por Visa en asociación con MasterCard Internacional y respaldados por otros importantes sistemas internacionales de tarjetas de pago.

Como banco adquirente, las PCI DSS deben convertirse en una prioridad para su propio negocio. De hecho, en virtud de las condiciones de la Normativa Operativa de Visa y Mastercard Internacional, un banco adquirente es responsable, no sólo de la seguridad de sus propios sistemas, sino también de la seguridad de los sistemas de su completa red de comercios y de las de sus agentes o servidores de pago.

Se ha desarrollado un conjunto de herramientas y recursos adecuados para convertir la implantación de las PCI DSS en una tarea lo más sencilla posible.

- Dentro de sus propios sistemas del banco
- Dentro de los sistemas de sus comercios
- Dentro de los sistemas de servidores de pago

Mediante la implantación de estas normas, todas las partes cumplen con el programa AIS y, automáticamente, satisfacen las exigencias y las recomendaciones establecidas por otros sistemas internacionales de tarjetas de pago, como American Express, Diners Club, JCB y Discover.

Las PCI DSS se componen de un conjunto de requisitos y procedimientos normalizados comunes a todo el sector. Su objetivo es garantizar la seguridad permanente de los datos valiosos de la cuenta del titular de una tarjeta.

Consta de 12 requisitos clave.

1. Instalar y mantener una configuración de cortafuegos para proteger la información

2. No utilizar contraseñas ú otros parámetros de seguridad provistos por vendedores

3. Proteger la información almacenada

4. Cifrar la información de las tarjetas y la información confidencial al enviarla por redes públicas.

5. Utilizar y actualizar regularmente programas anti-virus

6. Desarrollar y mantener sistemas y aplicaciones seguros

7. Restringir el acceso a la información basándose en el principio de “necesidad de saber”

8. Asignar un ID único para cada persona que tenga acceso al ordenador

9. Restringir el acceso físico a la información de tarjetas

10. Rastrear y controlar todos los accesos a los recursos de la red y a la información de tarjetas

11. Comprobar regularmente los sistemas y procedimientos de seguridad.

12. Mantener una política dirigida a la seguridad de la información

Mediante la implantación de estas PCI DSS, todos los comercios cumplirán automáticamente los requisitos y las normas establecidas por todos los medios internacionales de tarjetas de pago y sus bancos adquirentes.

Las PCI DSS se aplican a todos los bancos adquirentes, a todos los comercios que aceptan tarjetas de pago y a todos los servidores de pago que almacenan o transmiten información de tarjetas de pago.
En el marco de la Normativa Operativa de Visa y Mastercard Internacional, se ha especificado que todos los bancos adquirentes deben cumplir dichas normas.
Los bancos adquirentes también son responsables de garantizar que:

- Todos los comercios a los que representan cumplen las normas
- Todos los proveedores de servicios de pago cumplen las normas

Se debe tener en cuenta que, desde la perspectiva de la Normativa Operativa de Visa y Mastercard Internacional, su organización (Banco) es responsable de todos los servidores de pago (con independencia de si el banco o sus comercios mantienen o no relación directa con ellos).
.
Entre dichos servidores de pago pueden incluirse:

- Proveedores de cuentas de comercio

- Vendedores directos

- Proveedores de puntos de venta electrónicos

- Proveedores de aplicaciones informáticas

- Servidores de pago

- Procesadores de pagos

- Proveedores de almacenamiento de información
- Proveedores de alojamiento web

- Proveedores de compras electrónicas

- Proveedores de programas informáticos

- Agentes intermediarios de servicios de pago

En el entorno actual, la seguridad se debe de tener en cuenta en cualquier tipo de negocio. En todo el mundo, se considera una expectativa general, y a menudo una exigencia legal, que los negocios protejan a sus clientes y salvaguarden toda la información relacionada con ellos.
Con independencia de las exigencias estipuladas en la Normativa Operativa de Visa y Mastercard Internacional, las PCI DSS aportan seguridad a todos los negocios dentro de la cadena de pago.
En concreto, es capaz de:

- Identificar los riesgos inherentes al modo en que almacena o transmite la información de las tarjetas

- Proporciona una ruta clara de acción y corrección para abordar dichos riesgos

- Garantiza que sus servidores de pago no pongan su negocio a riesgo

- Demuestra que sus comercios y servidores asociados toman en serio la seguridad
Además, minimizando el riesgo de poner a riesgo la información, puede:

- Protegerse contra responsabilidades financieras
- Protegerse contra el riesgo de costes legales y de investigación

- Protegerse contra el riesgo de recibir la atención negativa de los medios de comunicación

El hecho es que, a medida que las tecnologías y medios de aceptación de tarjetas han ido evolucionando, el fraude de las tarjetas de pago ha ido ganando en sofisticación. Todos los negocios que almacenan o transmiten información de tarjetas son un objetivo potencial.

El modo concreto en que las PCI DSS afectan a su negocio y el modo en que deben implantarse dependerán de:

- El tamaño y la naturaleza de su propio negocio
- El ámbito y la naturaleza de su red de comercios
- El número y el tipo de servidores de pago contratados por usted y/o por sus comercios

Al planificar el programa de cumplimiento PCI DSS, o al considerar una actualización de los sistemas, puede resultar útil tener en cuenta los siguientes principios:

1. Los sistemas de aceptación de tarjetas que no almacenan la información de las tarjetas más allá de la autorización inicial de la operación constituyen siempre la opción más segura.

2. Si existe un motivo comercial para el almacenamiento de la información, éste debe realizarse en todo caso de conformidad con las PCI DSS.

3. Los sistemas que no cumplan las PCI DSS expondrán su propio negocio, a sus comercios y a sus servidores de pago a un nivel de riesgo grande (y totalmente innecesario).

Visa Mastercard trabajan activamente con una amplia gama de vendedores y de servidores de pago para garantizar que los sistemas disponibles:

1° No almacenen más información que la necesaria pa ra realizar la autorización inicial de la operación.

2° Almacenen la mínima información de tarjetas que sea absolutamente necesaria para el negocio y siempre de conformidad con las PCI DSS.
Se aconseja encarecidamente que los bancos se encarguen de que su completa red de comercios implante este tipo de soluciones. Así, garantizarán que ellos como banco y todos sus comercios se benefician de un nivel de protección óptimo

Se recomienda que, además de implantar las PCI DSS en su propio negocio, se efectúe también algún tipo de validación. Esta validación podría adoptar la forma de una auditoria

interna realizada por un departamento interno o una auditoria externa efectuada por un Asesor de Seguridad Acreditado, es decir, un auditor especializado, acreditado por Visa y/o MasterCard para ayudarle en el cumplimiento de las PCI DSS.
Lo mas probable es que en el futuro estas empresas exijan la validación o la acreditación.
A continuación, podremos ver como se establecen las PCI DSS dentro de un negocio.

La implementación de las PCI DSS en los comercios implica:

- Descubrir de qué modo funciona su negocio.

- Determinar si maneja la información de tarjetas de un modo seguro.

- Poner en práctica medidas correctivas para hacer frente a todos los riesgos asociados.

El primer paso debe ser familiarizarse con las PCI DSS y relacionar su contenido con su propio negocio.
Las PCI DSS se basan en mejores prácticas establecidas para la protección de datos (como la norma ISO 17799 mencionadas anteriormente). Familiarizándose con su contenido, sabrá lo que todos los sistemas internacionales de tarjetas de pago consideran el nivel mínimo de protección.

Una vez familiarizado con las PCI DSS, el siguiente paso sería crear un equipo de proyecto. La prioridad inmediata de este equipo sería analizar el modo exacto en que se procesa la información de las tarjetas en sus sistemas y definir todos los recorridos de información relacionados.

Este ejercicio revelará dos hechos críticos:

- Identificará todos los sistemas en los que la información de tarjetas está almacenada
- Revelará cuáles de estos sistemas se hallan bajo su control directo.

Dependiendo de la naturaleza de su negocio, es probable que algunos de estos sistemas se hallen bajo el control de servidores intermediarios de pago o un vendedor.

Su organización (desde la perspectiva de la Normativa Operativa de Visa y Mastercard Internacional) es responsable, con independencia del lugar y del medio en que se almacene y transmita la información.
Una vez dibujados los recorridos de la información de su negocio, se debe identificar cualquiera de los sistemas en los que se almacena la información de tarjetas.
Durante estas fases iniciales del proceso de implantación, debe:

- Obtener una orientación sobre el ámbito del trabajo correctivo que puede ser necesario para cumplir las PCI DSS.

- Evaluar la cantidad de recursos que pueden ser necesarios y el tiempo que llevara para concluir el proceso, aproximadamente En esta fase del proceso, también se debe tener en cuenta si debe contratar, y en qué condiciones, los servicios de un Asesor de Seguridad Acreditado, es decir, un auditor especializado acreditado por Visa y/o MasterCard para ayudarle con el cumplimiento de las PCI DSS.

Trabajando solo o en asociación con un Asesor de Seguridad Acreditado, el comercio implantará las actividades correctivas necesarias, introduciendo todos los cambios legales, de procedimientos y de sistemas necesarios.
Una vez introducidos los cambios, el comercio podrá cumplir con las PCI DSS.
Si decide contratar los servicios de un Asesor de Seguridad Acreditado, recomendamos que éste audite y acredite independientemente el negocio. Así se verificará si todos sus sistemas cumplen con las PCI DSS.
Si prefiere, el propio equipo de proyecto puede ser el que realice una completa comprobación y un ejercicio de auto-acreditación.
Una vez concluida satisfactoriamente la fase de acreditación (o de auto-acreditación), estará preparado para presentar ante Visa y Mastercard un informe sobre su cumplimiento.
En virtud de las condiciones de la Normativa Operativa de Visa y Mastercard
Internacional, será necesario confirmar su cumplimiento anualmente. A fin de garantizar que sigue cumpliendo las normas, se debe llevar a cabo una auditoria o una acreditación regular e incorporar a sus procesos empresariales rutinarios.

VENTAJAS Y DESVENTAJAS DEL PIN PASS

Con sólo cuatro dígitos los consumidores podrán acceder a créditos y efectuar compras sin la necesidad de presentar la cédula de identidad ni de firmar un recibo por la transacción. Esta fórmula se llama Pin Pass y es el nuevo nombre que se le adjudicará a la clave secreta de la tarjeta de crédito bancaria que reemplazará la firma del comprador.
La modalidad es la misma que actualmente se ocupa con Redcompra y en una primera etapa se podrá utilizar sólo en los comercios autorizados como Shell, Copec, Salcobrand y supermercado Líder, para luego masificarse a todos los establecimientos comerciales adheridos al sistema de pago con tarjetas de crédito en Chile.

Para el gerente general de Transbank**,** Carlos Johnson**,** lo principal de este cambio es entregar comodidad, rapidez y seguridad a los usuarios. La iniciativa se ejecutará en dos períodos para asegurarse que la cobertura de la tarjeta esté en todos los locales y al alcance de los consumidores para que no exista ningún tipo de problemas a la hora de hacer la compra.

DESVENTAJAS

Actualmente, la ley de contrato obliga una firma para asegurar el consentimiento de la transacción y que no exista ningún fraude. En este sentido hay un tema que puede resultar crítico del punto de vista de seguridad, específicamente con el problema de la clonación de tarjetas. Actualmente, si una tarjeta es clonada, los peritos de la policía pueden detectar el fraude por la falsificación de la firma. Ahora, con la nueva implementación del Pin Pass, la firma desaparece, por lo tanto, sería más complejo descubrir algún tipo de fraude.

Si el objetivo es entregar mayor seguridad, sería mejor ocupar algo que nadie pueda robar como, por ejemplo, la huella digital del dueño.
La huella es un sistema que ya está siendo utilizado por empleadores, en Isapres y otros lugares, para identificar a los usuarios.

Una compra en persona no es igual a una compra en línea. En tales transacciones existen otras medidas ocupadas para crear y asegurar el contrato.

Con la utilización de Pin Pass se facilita el abuso de las tarjetas por parte de ladrones o por familiares no autorizados. Los cajeros no van a comprobar la identidad de las personas a través de la cédula de identidad, será fácil para quienes se sepan el código Pin Pass, utilizarla sin autorización del dueño. Este sistema no es muy diferente del que opera actualmente con Red Compra que se supone funciona bien y seguro.

La idea del dinero plástico es buena principalmente por la comodidad y seguridad. Sin embargo, hay que tener un buen comportamiento y conocimiento de cómo funcionan las tarjetas, ya que están sujetas a cobros que siempre son de sorpresa para el cliente. Además, es sabido desde hace años que el sistema de tarjeta de crédito es bastante vulnerable, dado que sólo se requiere del número de la tarjeta, el código de verificación y la firma del cliente para realizar una transacción. Por lo mismo, hay personas que prefieren no usarlas. No obstante, esta tendencia debiera cambiar debido a las constantes mejoras para incentivar el uso de las mismas con mayor seguridad.

.

PROBLEMA

El Fraude es el delito mas temido por las entidades bancarias y financieras, por las corporaciones publicas y privadas y por la sociedad en general, es el delito mas extendido en el mundo y el mas difícil de investigar y penalizar debido a las distintas alternativas que tienen los defraudadores para infringir la ley.

Si bien en nuestro país no existen cifras oficiales proporcionadas por los bancos afectados se puede decir a partir de información extraoficial que la mayor cantidad de fraudes son cometidos con tarjetas bancarias tanto de debito como de crédito registrando solo el año pasado en Europa fraudes de este tipo que alcanzan los 600 millones de Euros y que afectan a una gran cantidad de clientes de los distintos bancos a nivel mundial.

En Chile el monitoreo de transacciones a través de distintos sistemas computacionales como por ejemplo sistemas que son una especie de centinela donde existe un ejecutivo llamado analista de fraude que constantemente esta observando las transacciones mas sospechosas e inusuales de los clientes es la medida inicial que tienen las instituciones bancarias para poder disminuir los fraudes bancarios con tarjetas de crédito. Pero esto no basta debido a que el seguimiento se realiza una vez que la transacción fue efectuada resultando imposible de detectarla antes de que el cliente la realice.

El presente proyecto de tesis propone políticas y procedimientos tendientes a minimizar los riesgos de que se cometan fraudes con las tarjetas de crédito bancarias que emiten los bancos de nuestro país a diciembre del 2009.

OBJETIVOS

Se hace necesario en toda investigación plantear dos niveles de objetivos los Generales y Específicos.

OBJETIVO GENERAL

Cuestionar los actuales sistemas de monitoreo de transacciones que existen en los bancos de nuestro país.
Proponer nuevas políticas y procedimientos tendientes a minimizar los fraudes que se producen con las tarjetas de crédito bancarias en los comercios catalogados por los bancos como más vulnerables.

OBJETIVOS ESPECIFICOS

Explicar en que consisten los actuales sistemas de monitoreo de transacciones que realizan los bancos del país.

Proponer nuevas políticas y procedimientos que permitan minimizar los riegos de fraudes.

Detectar los comercios más vulnerables de ser defraudados encuestando a los analistas de fraude de los distintos bancos que alcance la muestra.

Identificar los actuales controles que existen en los comercios calificados como más riesgosos para proponer nuevas políticas y procedimientos a seguir.

METODOLOGIA.

A continuación se presentan las 5 etapas a través de las cuales se va a desarrollar el presente proyecto de tesis, mediante una investigación exploratoria descriptiva.

Etapa Nº 1: Recopilación de Información.

Acciones:

1.-Recopilar información en las paginas Web acerca de cuales son los bancos que realizan el monitoreo de transacciones en línea de sus clientes llamados tarjeta habientes.

2.- Recopilar información acerca de los beneficios que se obtienen cuando los bancos aplican un sistema de monitoreo de transacciones con tarjetas de crédito bancarias.

3.- Recopilar información acerca del funcionamiento del sistema de monitoreo que aplica Banco Ripley llamado SENTINEL PREVENTION.

4.- Recopilar información acerca de las distintas alternativas de monitoreo en línea de transacciones que ejecutan los demás bancos de nuestro país

5.- Recopilar antecedentes en los respectivos departamentos de Prevención de Fraudes de cada Banco que abarca la muestra para determinar el flujo de clientes que se monitorean día a día y cuales son las políticas y protocolo de trabajo que utilizan al momento de descartar una transacción.

6.- Recopilar información general de cuales son los principales fraudes que se cometen con las tarjetas de crédito bancarias ya sea clonaciones, duplicación de paginas Web (Phishing) Robos, fraudes internos, etc.

Etapa Nº 2: Determinación de la Población Objetiva.

1.- Determinar el tamaño de la población objetiva, considerando los siguientes criterios:

- Bancos Chilenos inscritos en la Superintendencia de Bancos e Instituciones Financieras.

- Bancos que emiten tarjetas de crédito bancarias (Visa, Mastercard) y que ofrezcan a sus clientes algún sistema de monitoreo antifraudes de las transacciones que realizan en línea.

- Bancos que tengan un departamento de Prevención de Fraudes establecido.

Se determino una población objetiva de 6 bancos chilenos que emiten tarjetas de crédito visa y mastercard con presencia tanto a nivel nacional como internacional.

Etapa Nº 3: Elaboración y Aplicación de la Encuesta.

- Elaborar una encuesta que permita determinar a través de la experiencia el grado de conocimiento que tengan los analistas de fraudes de los bancos que conforman la muestra, respecto de cuales son los principales fraudes que se cometen con las tarjetas de crédito bancarias y en que comercios ocurren la mayor cantidad de estos desfalcos.

- Validar el instrumento a través de un experto en el área.

- Aplicar la encuesta a los analistas de fraude de cada banco en estudio. Dicha encuesta se realizara de forma personal.

Etapa Nº 4: Elaboración de la Propuesta.

- Elaborar la propuesta en la que se plantea a los analistas de fraudes de cada banco en estudio que trabajan en el monitoreo de transacciones en línea sobre cuales son los distintos fraudes que se cometen con las tarjetas de crédito bancarias en nuestro país ya sea clonación, uso de paginas web fraudulentas, fraudes internos, robos, etc.; y entregar

una información general de cuales son los comercios donde se registran los mayores fraudes y donde se presume esta la génesis del problema.

- Presentar la propuesta a un experto en el tema.

- Recoger las sugerencias planteadas por el experto.

- Realizar los ajustes necesarios para tener la versión final de la propuesta a presentar.

- Difundir la propuesta ya ajustada entre los analistas de fraude de cada banco a través de una capacitación y entrega de folletos explicativos. Esta será realizada de forma personal con los analistas.

Etapa Nº 5: Análisis de resultados y redacción del Informe de Tesis.

- Tabular la información que se obtuvo con la aplicación de la encuesta en gráficos y tablas.

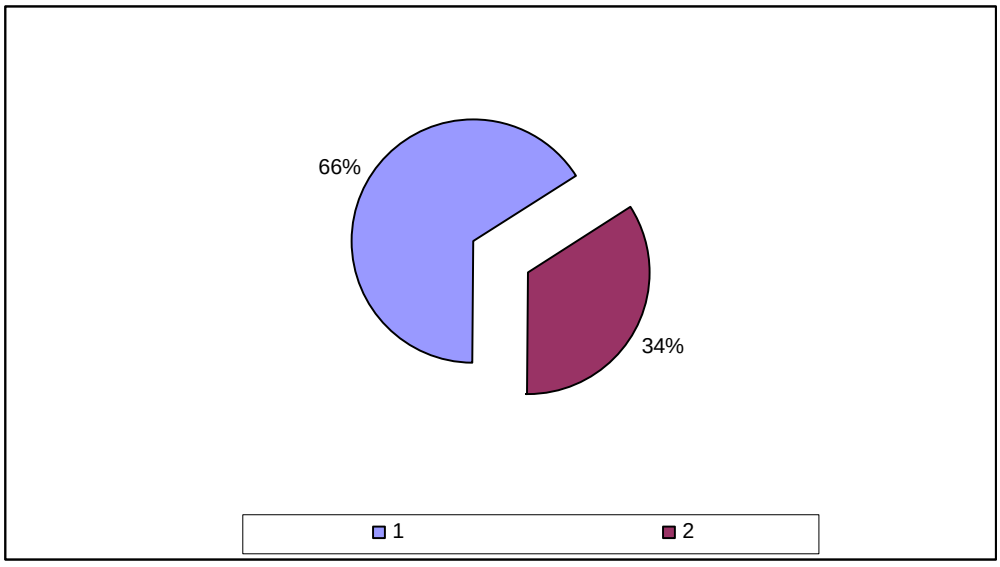
- Analizar los resultados obtenidos a través de la encuesta. Este análisis se realizara a través de procedimientos tales como tablas de distribución de frecuencias y medidas de tendencia central (moda).

- Redactar el informe final con las conclusiones respectivas de acuerdo a las pautas establecidas.

RESULTADOS Y DISCUSION

En el desarrollo de la tesis Propuesta para minimizar los fraudes con tarjetas de crédito bancarias, realizada a través de la metodología antes descrita. Se contó con el apoyo del supervisor del departamento de prevención de fraudes de Banco Ripley para la confección de la encuesta. Esta se aplico a los 32 funcionarios de los respectivos bancos que alcanzaron la muestra como lo fueron: Banco Chile, Banco Santander, Banco BCI, Banco Paris, Banco Falabella y Banco Ripley, todos estos funcionarios forman parte de la población Objetivo.

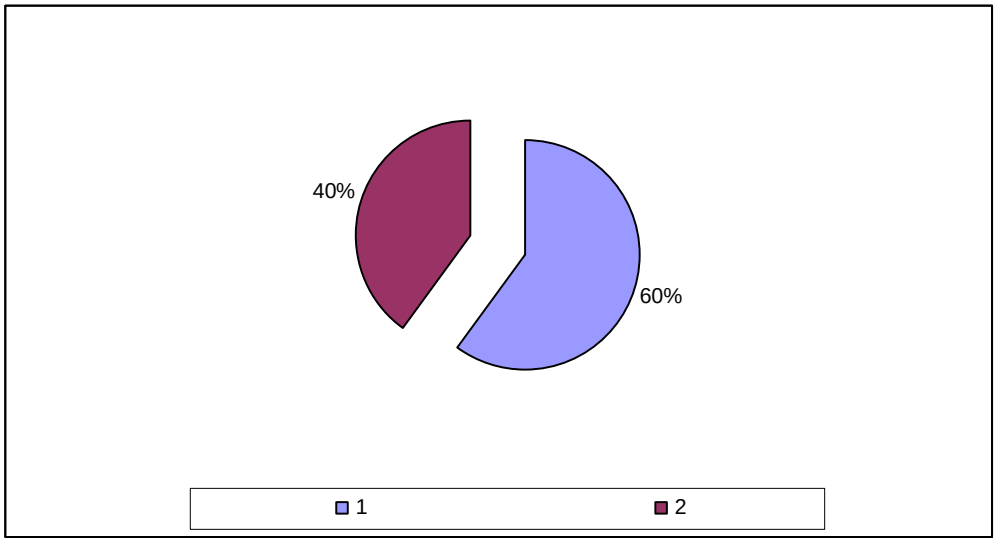
Grafico Nº 1: Porcentaje de bancos que posee un área establecida de prevención de fraudes



Fuente elaboración Propia, año 2009

De acuerdo al estudio se determino que aproximadamente de los 26 bancos que existen actualmente en nuestro país un 66% de ellos posee un área establecida de prevención de fraudes donde se monitorean las distintas compras que realizan los clientes en línea aproximadamente 17 de 26 bancos funciona con esta área. El otro restante argumenta que por un tema de falta de interés y de recursos por parte de la gerencia nacional no poseen un área de prevención establecida.

Grafico Nº 2: Bancos donde se realizan llamados telefónicos para confirmar las compras de los clientes.

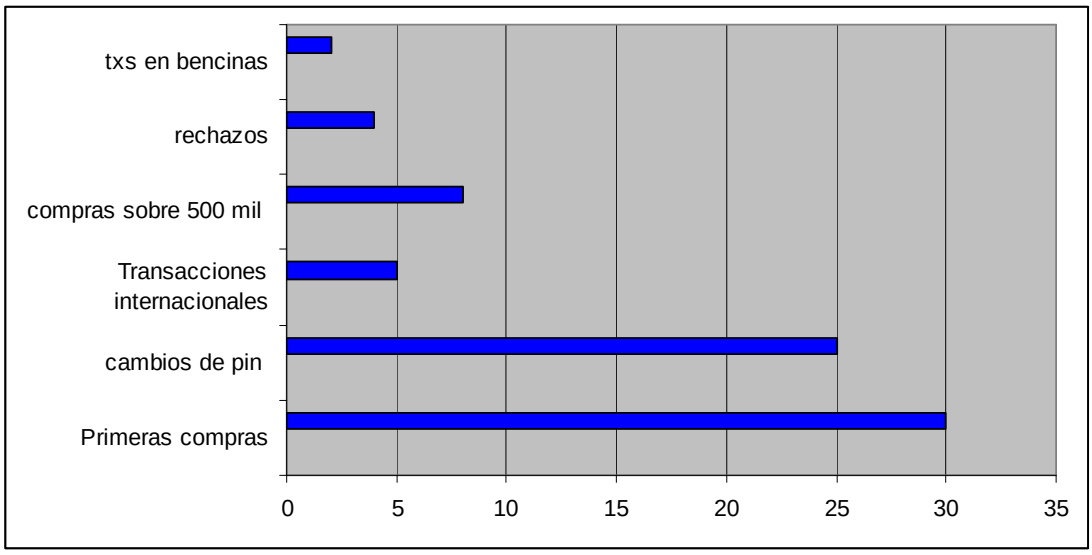


Fuente elaboración Propia, año 2009

Este grafico nos muestra los bancos que poseen un área establecida de prevención de fraudes y que de manera habitual contactan a sus clientes para confirmar las respectivas compras que realizan con las tarjetas de crédito. Sobre un universo de 17 bancos que tienen un departamento establecido se determino que solo un 40% de ellos aprox. 7 bancos realizan los llamados telefónicos. El resto de los bancos argumenta que no lo hacen más que todo por un tema de no divulgar tanto la existencia del departamento y por posibles aumentos de los requerimientos por desconocimientos de compra.

Cabe hacer mención que en los bancos donde realizan los llamados telefónicos los clientes agradecen la preocupación que manifiestan los analistas por saber si soy ellos los que están realizando las respectivas compras

Grafico Nº 3: Cantidad de llamados telefónicos que realizan por día los analistas de los distintos bancos por regla

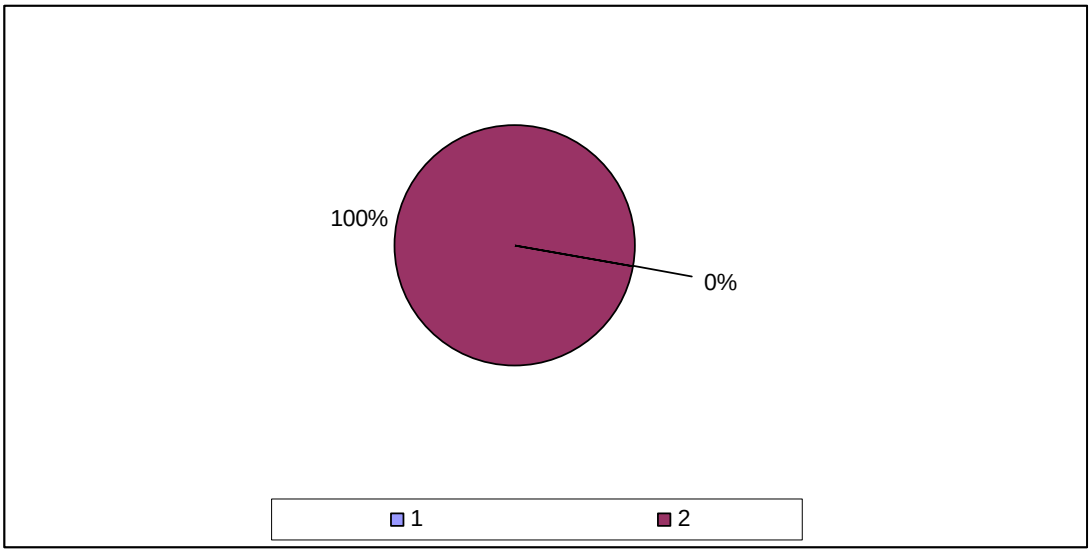


Fuente elaboración Propia, año 2009

Se puede apreciar que la mayor cantidad de llamados telefónicos son realizados tanto a primeras compras como a cambios de Pin, esto se debe principalmente al hecho que constantemente se esta incentivando la utilización de estas tarjetas a clientes nuevos y especialmente a los antiguos que nunca las han utilizado

Cabe hacer mención además que estas reglas fueron las que mas se repitieron a la hora de realizar la encuesta

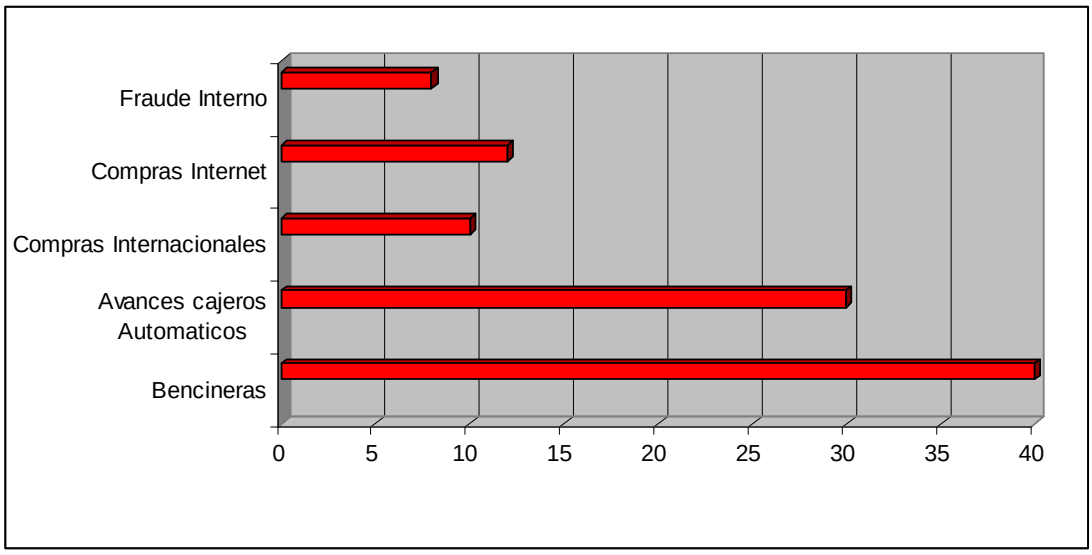
Grafico Nº 4: Conocimiento de la implantación del programa de seguridad de la información normas PCI Visa y Mastercard



Fuente elaboración Propia, año 2009

De todos los bancos chilenos que alcanza la muestra ninguno esta al tanto de las actuales normas de seguridad de la información que actualmente están aplicando Visa y Mastercard y que pronto esperan implantarlas acá en chile, al momento de efectuar la consulta las relacionaban con las actuales normas que rigen acá en chile las ISO 17.799. Un tema preocupante ya que según los datos recolectados si los bancos y comercios que trabajan con estas tarjetas de crédito no se acogen a estas normas se exponen a multas por falta de visa e incluso a que no sigan utilizando el producto tarjeta de crédito tema no menor sobre todo para los comercios que trabajan con este dinero plástico.

Grafico Nº 5: Comercios donde se ha registrado la mayor cantidad de fraudes con tarjetas de crédito bancarias durante el 2009.



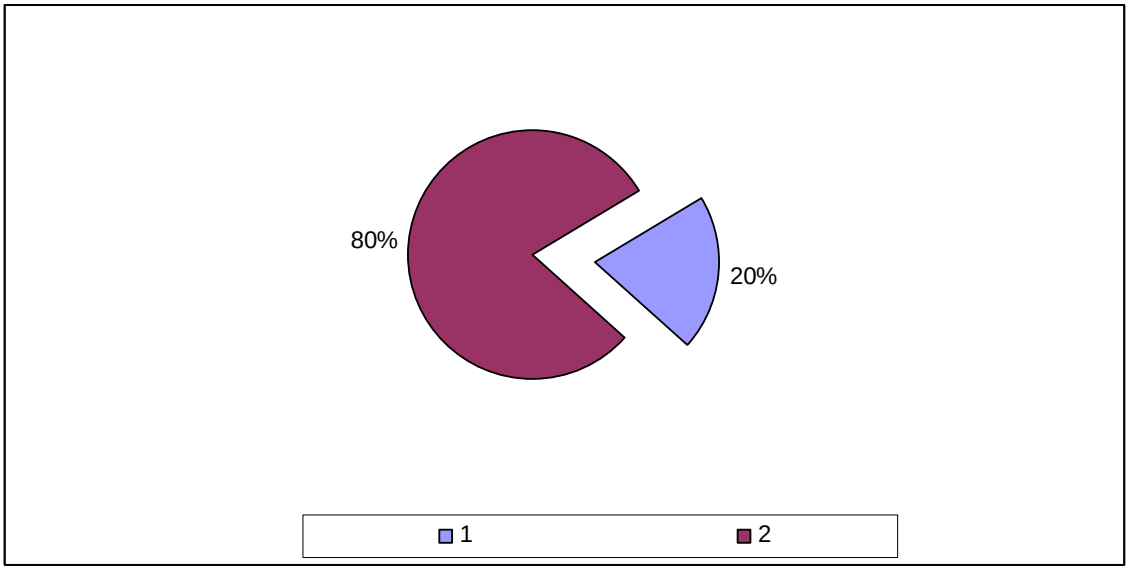
Fuente elaboración Propia, año 2009

Se puede apreciar de acuerdo a los resultados arrojados por la encuesta, que la mayor cantidad de fraudes que se cometen con estas tarjetas de crédito bancarias son precisamente en las bencineras donde todos los analistas concuerdan que no existe un control de los procedimientos propuestos ya que en muchas ocasiones ni siquiera piden la cedula de identidad para efectuar la compra e incluso en investigaciones posteriores han determinado una especie de colusión entre los delincuentes y los funcionarios de las bombas de bencina.

A partir de este grafico se puede establecer la importancia de incentivar políticas y procedimientos en estos tipos de comercios.

Otro porcentaje nada menor lo podemos apreciar en los cajeros automáticos con el caso ocurrido el año 2008 donde un ex funcionario de transbank robo una gran cantidad de datos de clientes para posteriormente efectuar diversos avances en efectivo desde los cajeros automáticos

Grafico Nº 6: Porcentaje de capacitaciones en terreno que realizan los distintos departamentos de prevención fraude en los comercios catalogados según la encuesta como más riesgosos



Fuente elaboración Propia, año 2009

Según lo recogido por la encuesta tan solo un 20% de los bancos encuestados realiza capacitaciones en terreno en los comercios catalogados como mas riesgosos el resto considera como una perdida de tiempo realizar este tipo de capacitaciones.

PROPUESTA

OBJETIVO

Esta propuesta esta dirigida a los respectivos departamentos de prevención de fraudes de los 6 bancos que alcanza la muestra, que trabajan con un departamento establecido físicamente.
Esta propuesta tiene como fin 2 objetivos:

1° Promover la implantación del actual programa de seguridad de la información diseñado por visa y mastercard y que actualmente a finales de este año debiese estar implementado en su totalidad en los países del extranjero.

2° Promover capacitaciones constantes sobre el uso, funcionamiento y validación de datos de las compras que realicen los clientes en los comercios catalogados como mas riesgosos y que de acuerdo a la encuesta se cometen la mayor cantidad de fraudes.

3° Promover la implementación del sistema de huella digital en conjunto con el uso de un chip electrónico insertado en la tarjeta de crédito y la presentación obligatoria de la cedula de identidad.

PRESENTACIÓN

Esta propuesta esta compuesta de 2 partes

1.- Entrega de toda la información referente a la pronta implantación del programa PCI acá en chile en los bancos y comercios asociados en cuanto al tema de seguridad de la información y datos de tarjeta habientes. De acuerdo a los investigado existen 12 estándares de seguridad de la información que debieran utilizar los bancos algo muy similar a lo que son hoy las normas ISO 17.799 pero con la salvedad de que sino se cumplen estas normas se exponen a elevadas multas por parte de las firmas Mastercard y Visa

2.- Clasificación de los comercios más riesgosos donde se cometen la mayor cantidad de fraudes con las TC determinados de acuerdo a la encuesta para efectuar las respectivas capacitaciones sobre uso funcionamiento y validación de las respectivas tarjetas de crédito. Según los funcionarios encuestados de los distintos departamentos de prevención de fraudes todos concuerdan que los mayores fraudes registrados durante el 2009 fueron los siguientes ordenados de acuerdo al grado de importancia:

1° Bencineras

2° Avances en cajeros Automáticos

3° Compras realizadas en páginas de Internet

4° Desconocimientos de compras realizadas en el ext erior

5° Personas que argumentan nunca haber solicitado l a tarjeta de crédito, llamados en definitiva fraudes internos.

CONCLUSIONES

De la ejecución del presente proyecto de tesis se pueden plantear las siguientes conclusiones.

Se puede decir que la gran parte de los bancos encuestados cuenta con un área de prevención de fraudes establecido físicamente (el 66% de ellos) el resto no lo tiene dado que ha nivel gerencial no existe el animo de inyectar recursos en este tipo de departamentos ya que no dejan ningún ingreso económico de por medio pero como opinión personal dejan una gran brecha de diferenciación con el resto de los bancos producto del nivel de satisfacción que día a día expresan miles de clientes contentos con el servicio ofrecido. Este resultado obtenido esta dentro de lo pretendido ya que se esperaba por la poca información que existe por parte de los bancos que el porcentaje de áreas de prevención fuese mucho menor.

En relación a la preparación académica de los analistas de fraudes se hace hincapié en que se trate de personas con una vasta experiencia en los temas de fraudes bancarios sin embargo de acuerdo a los porcentajes de analistas con una preparación de magíster o postgrados relacionados con sistemas de información se pudo determinar que solo 1 de los 42 funcionarios encuestados poseía este tipo de estudios el resto se trataba de gente recién egresada de carreras como ingieneria comercial y auditoria y de personas mayores de 45 años con algunos años de experiencia en estos temas.

Respecto a los comercios catalogados como más riesgosos la gran mayoría de los analistas coincide en que las bencineras son muy susceptibles de ser defraudadas por el escaso control que existe por parte de los funcionarios de esas empresas llamados comúnmente bomberos. Es en este comercio donde el presente proyecto de tesis hace mayor hincapié a la hora de proponer políticas y procedimientos tendientes a minimizar estos fraudes respaldando tales políticas en capacitaciones frecuentes sobre el uso y funcionamiento de la tarjeta de crédito también sin dejar de lado el tema de la privacidad de la información de los clientes catalogados como tarjeta habientes.

Otro tema nada menor es la poca información que manejan los bancos chilenos respecto al programa de seguridad de la información creado por visa y mastercard de acuerdo a los resultados el 100% de los bancos de la muestra desconoce tal programa tendiéndolo

a confundir con las normas ISO 17.799 que hablan de la seguridad de la información a nivel general.

Cabe destacar que debido al alto costo de implementación de un sistema de uso de huella digital y chip electrónico no es posible aun en chile poder llevarlo a cabo ya que los bancos no están dispuestos a desembolsar grandes sumas de dinero en este tipo de resguardos.

Para finalizar se puede decir que toda iniciativa que se haga para minimizar los riesgos de fraude con tarjetas de crédito nunca podrá llegar a un 100% de satisfacción ya que siempre va a estar presente en cierta medida un grado de riesgo, lo importante es tratar de minimizarlo de alguna forma a través de estos planteamientos.

BIBLIOGRAFIA

LIBROS:

Claudio P. Magliona Markovicth; Macarena López Medel.1999. Delincuencia y Fraude Informático. Derecho comparado y ley 19.223. Santiago, Chile. Editorial Jurídica de Chile. 273p.

Gustavo Eduardo Aboso; María Florencia Zapata 2006.Cibercriminalidad y Derecho Penal Buenos Aires Argentina.Editorial: Euros Editores. 221p.

Fermín Morales Prats (coordinador); Oscar Morales García 2002.Contenidos Ilícitos y Responsabilidad de los Prestadores de Servicios de Internet. España Editorial: Aranzadi. 267p.

Juan José Blossiers Hüme 2003. Criminalidad Informática Lima, Perú. Editorial: Portocarrero. 301p.

Raúl Durand Valladares 2002 Cyber-delito o Delitos de Ordenadores. Sistema bancario nacional. Lima, Perú Editorial: Raúl Durand Valladares. 259p.

Renato Javier Jijena Leiva 1992 Chile, la Protección Penal de la Intimidad y el Delito Informático. Santiago, Chile.Editorial Jurídica de Chile. 225p.

Ricardo M. Mata y Martín2002.Estafa Convencional, Estafa Informática y Robo en el Ámbito de los Medios Electrónicos de Pago. El Uso fraudulento de tarjetas y otros instrumentos de pago. España. Editorial: Aranzadi. 206p.

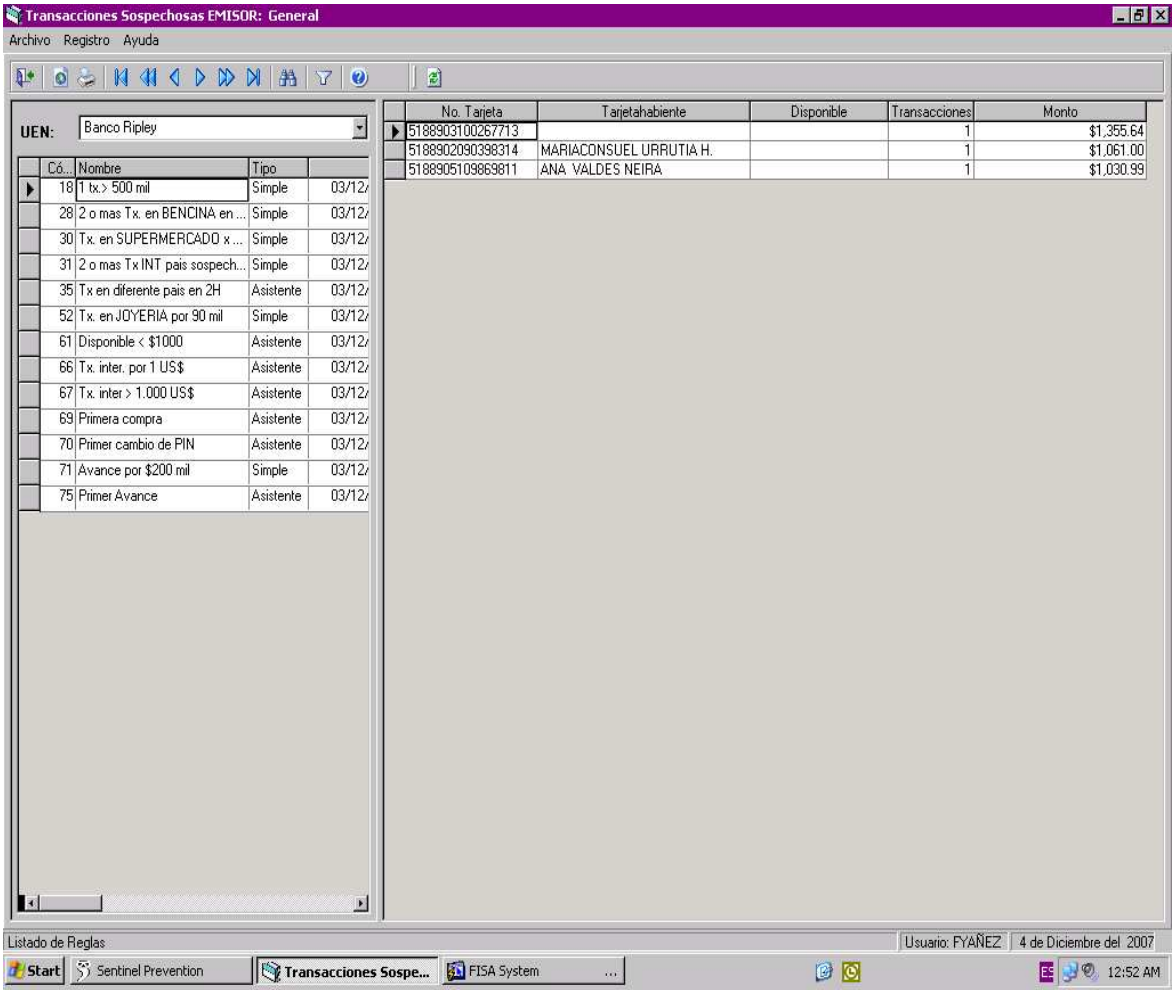
José Manuel Maza Martín.2002. Tarjetas Bancarias y Derecho Penal.Madrid, España Editorial: General del Poder Judicial.257p.

Angelo Benvenuto. 2003. El delito Informático y la función de Auditoria Informática Ley 19.223.Universidad de Concepción.XIV Conferencia académica permanente de investigación contable CAPIL (Temuco 2003).

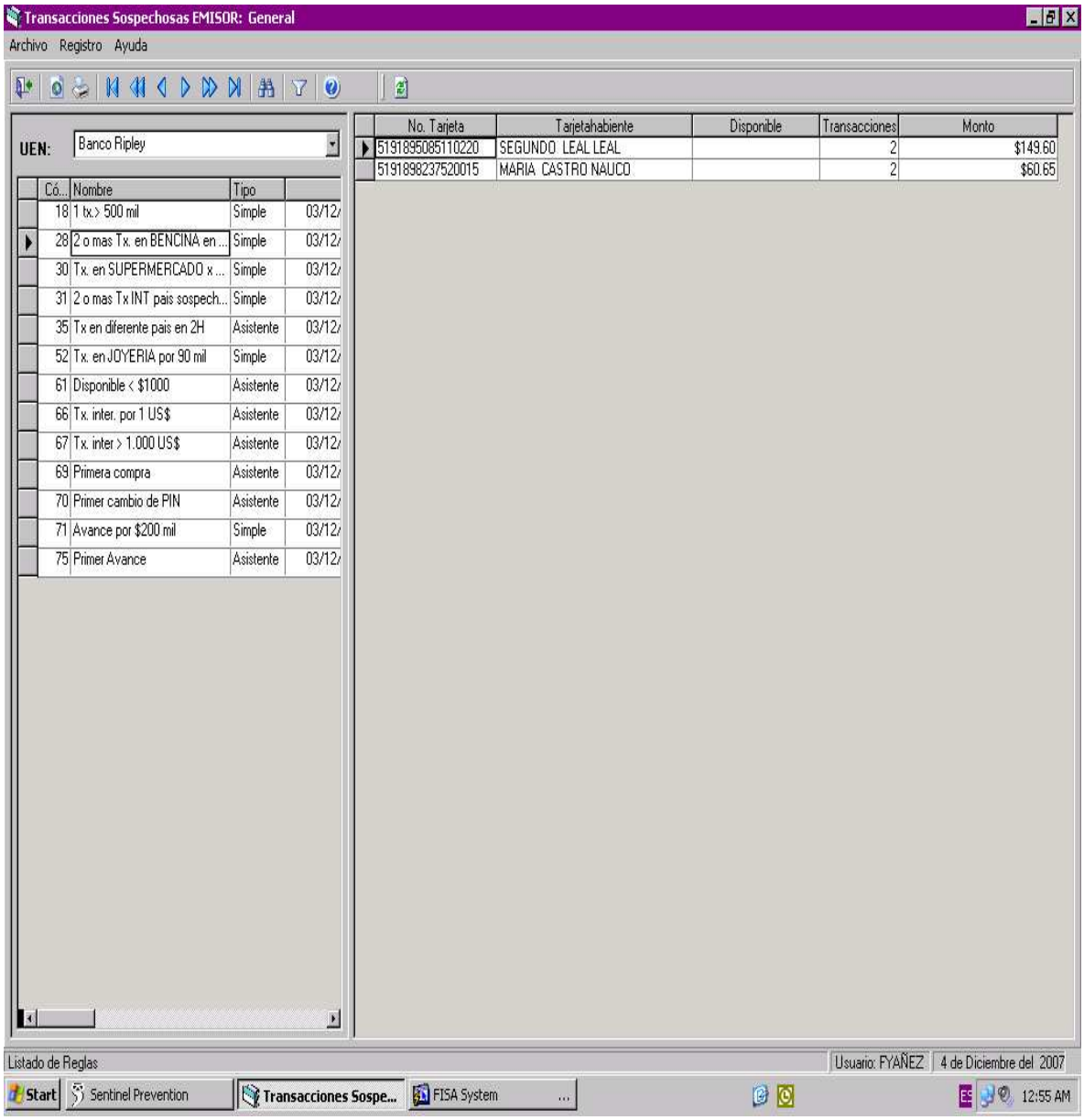
ANEXOS

Anexo Nº 1: Ejemplos de reglas del sistema sentinel más Riesgosas.

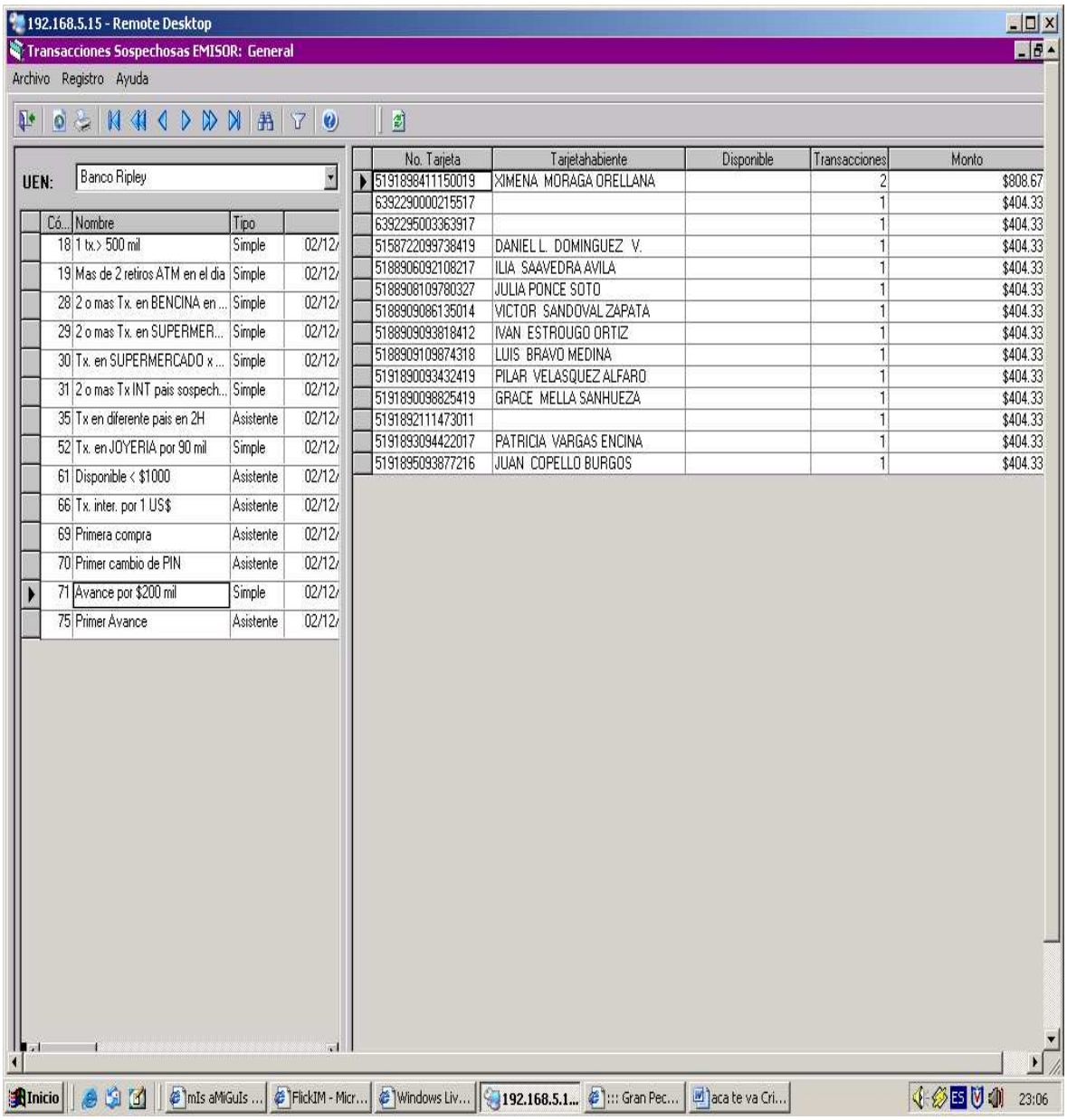
1.- Compras sobre 500 mil pesos



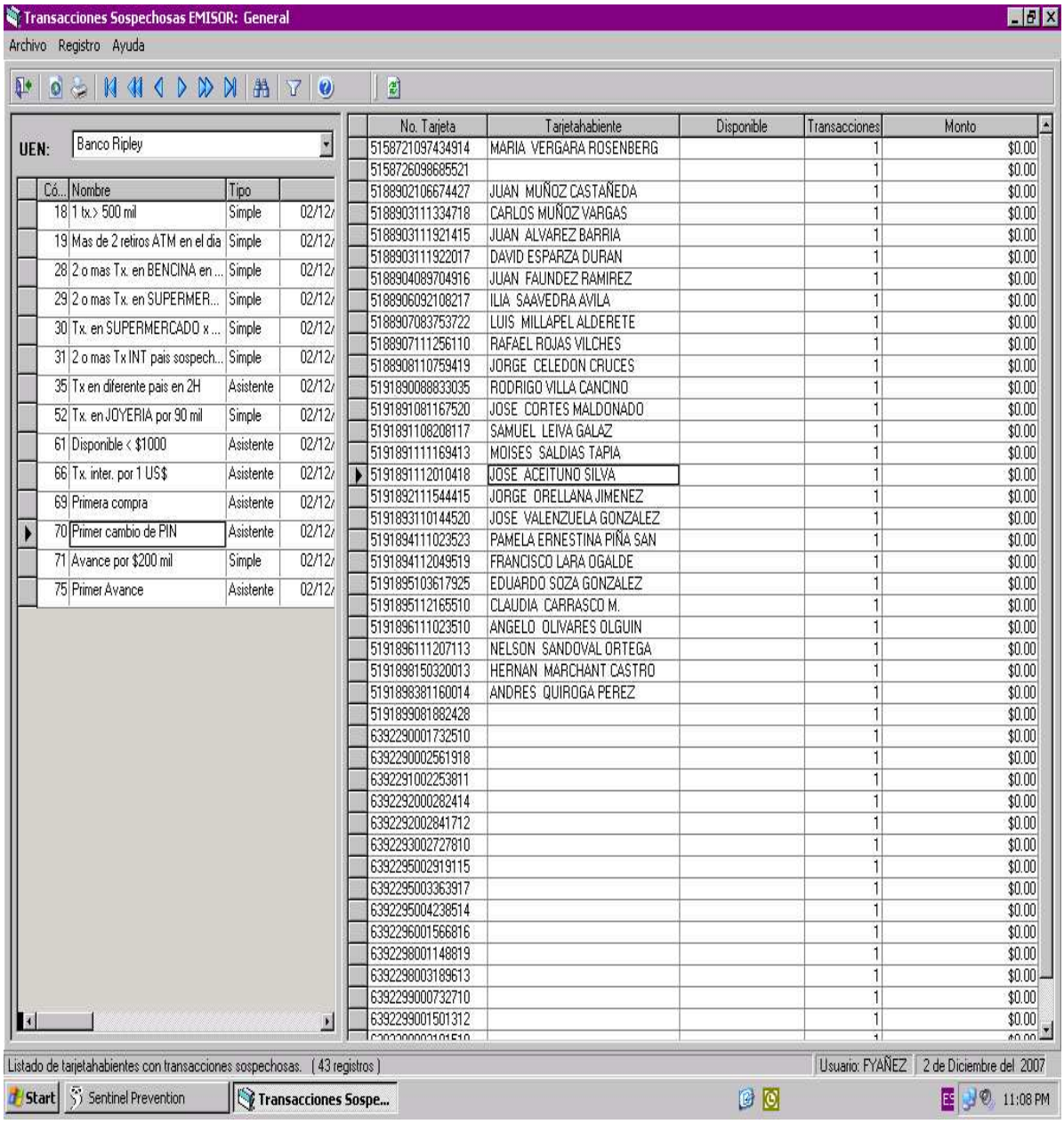
2.- Dos o más transacciones en bencinera durante el día



3.-Avances por 200 mil pesos Ingresados al sistema



4.-Primeros Cambios de Pin o Claves secretas que realizan los Clientes



Anexo Nº 2: Niveles de comercios

Tabla A: Conformidad con el estándar PCI de seguridad en los datos para comerciantes

Nivel del comerciante	Criterio de selección	Acciones de validación	Validado por
1	Cualquier comerciante - sin tener en cuenta el canal de aceptación - que procese más de 6.000.000 de transacciones de Visa al año Cualquier comerciante que haya sufrido un ataque o intrusión que haya resultado en que los datos de las cuentas se hayan visto comprometidos Cualquier comerciante identificado por cualquier asociación de tarjetas como de nivel 1	Auditoría anual de seguridad in situ y Escaneado trimestral de la red	Asesor independiente de seguridad o auditoría interna si está firmada por un directivo de la empresa Proveedor cualificado de escaneado independiente Los comerciantes de nivel 1 deberán haber validado su conformidad antes del 30 de Septiembre de 2004
2	Cualquier comerciante de comercio electrónico que procese entre 150.000 y 6.000.000 transacciones al año	Cuestionario anual de autoevaluación de la conformidad con el PCI y Escaneado trimestral de la red	Comerciante Proveedor cualificado de escaneado independiente Se requiere tener la validación en una fecha no posterior al 30 de Junio de 2005
3	Cualquier comerciante de comercio electrónico que procese entre 20.000 y 150.000 transacciones al año	Cuestionario anual de autoevaluación de la conformidad con el PCI y Escaneado trimestral de la red	Comerciante Proveedor cualificado de escaneado independiente Se requiere tener la validación en una fecha

			no posterior al 30 de Junio de 2005
4	Todos los demás comerciantes, sin tener en cuenta el canal de aceptación	Se recomienda el cuestionario anual de autoevaluación de la conformidad con el PCI y Se recomienda el escaneado anual de la Red	Comerciante Proveedor cualificado de escaneado independiente Nota: Mientras que la conformidad es obligatoria para los comerciantes del nivel 4, la validación es opcional, pero está muy recomendada

Tabla B: Conformidad con el CISP de Visa para los proveedores de servicios

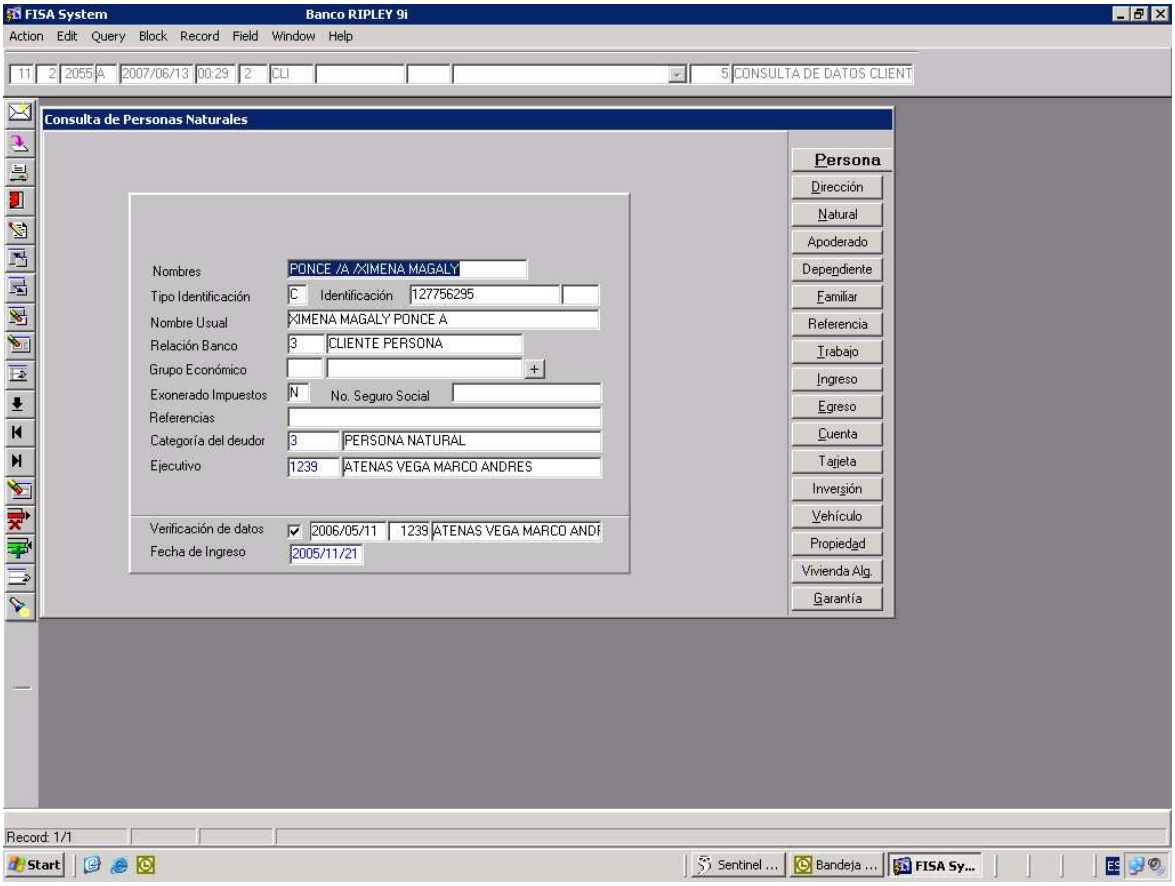
Nivel del comerciante	Criterio de selección	Acciones de validación	Validado por
1	Todos los procesadores de VisaNET (tanto miembros como no miembros) y todas las pasarelas de pago	Auditoría anual de seguridad in situ y Escaneado trimestral de la red	Asesor independiente de seguridad o auditoría interna si está firmada por un directivo de la empresa Proveedor cualificado de escaneado independiente

2	Cualquier proveedor de servicios que no se encuentre en el nivel 1 y almacene, procese o transmita anualmente más de 1.000.000 de cuentas/transacciones Visa	Auditoría anual de seguridad in situ y Escaneado trimestral de la red	Asesor independiente y cualificado de seguridad Proveedor cualificado de escaneado independiente
3	Cualquier proveedor de servicios que no se encuentre en el nivel 1 y almacene, procese o transmita anualmente menos de 1.000.000 de cuentas/transacciones Visa	Cuestionario anual de autoevaluación de la conformidad con el PCI y Escaneado trimestral de la red	Proveedor cualificado de escaneado independiente

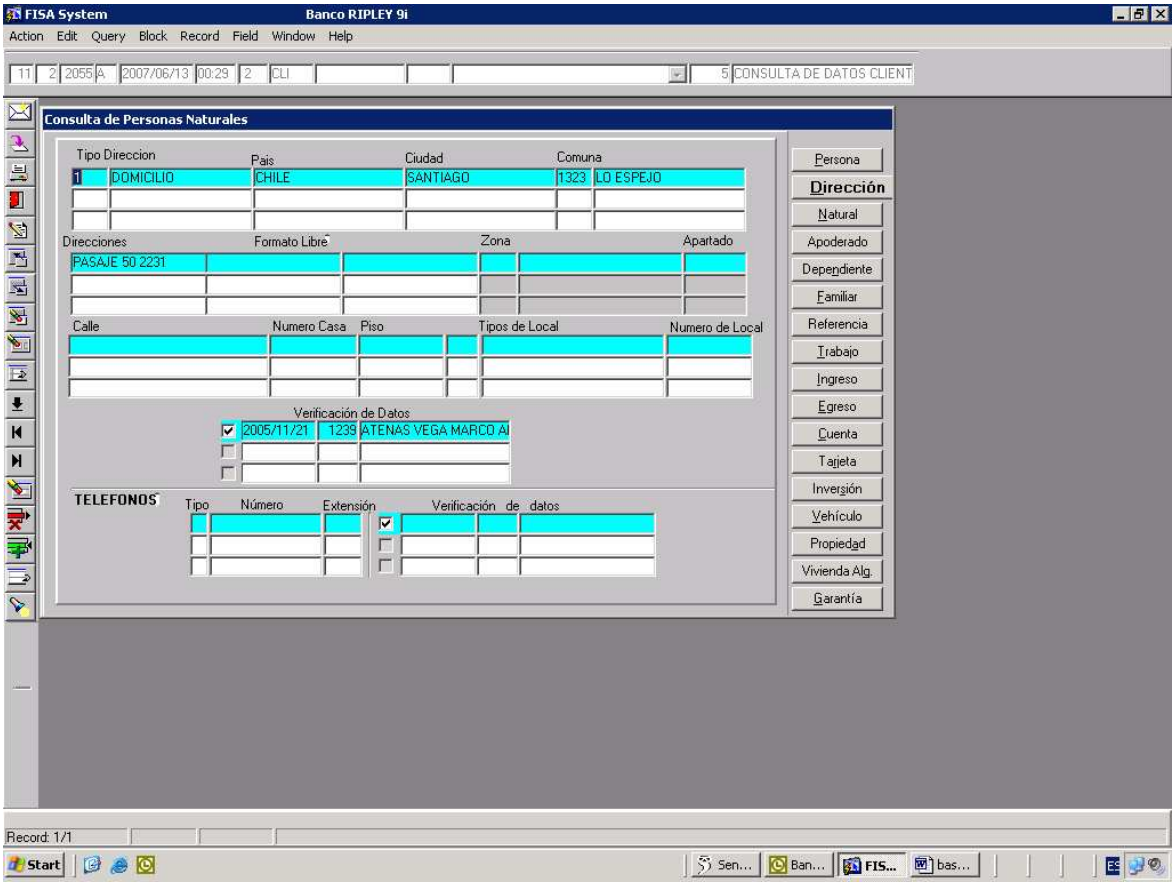
* Los niveles de comercios se basan en definiciones de Visa USA ** La PCI DSS requiere que todos los comercios realicen escaneos externos de red para conseguir el cumplimiento. Los receptores pueden requerir la emisión de informes de escaneos y/o cuestionarios de los comercios de nivel 4.

EJEMPLO DE BASE DE DATOS DE CLIENTE BANCO RIPLEY

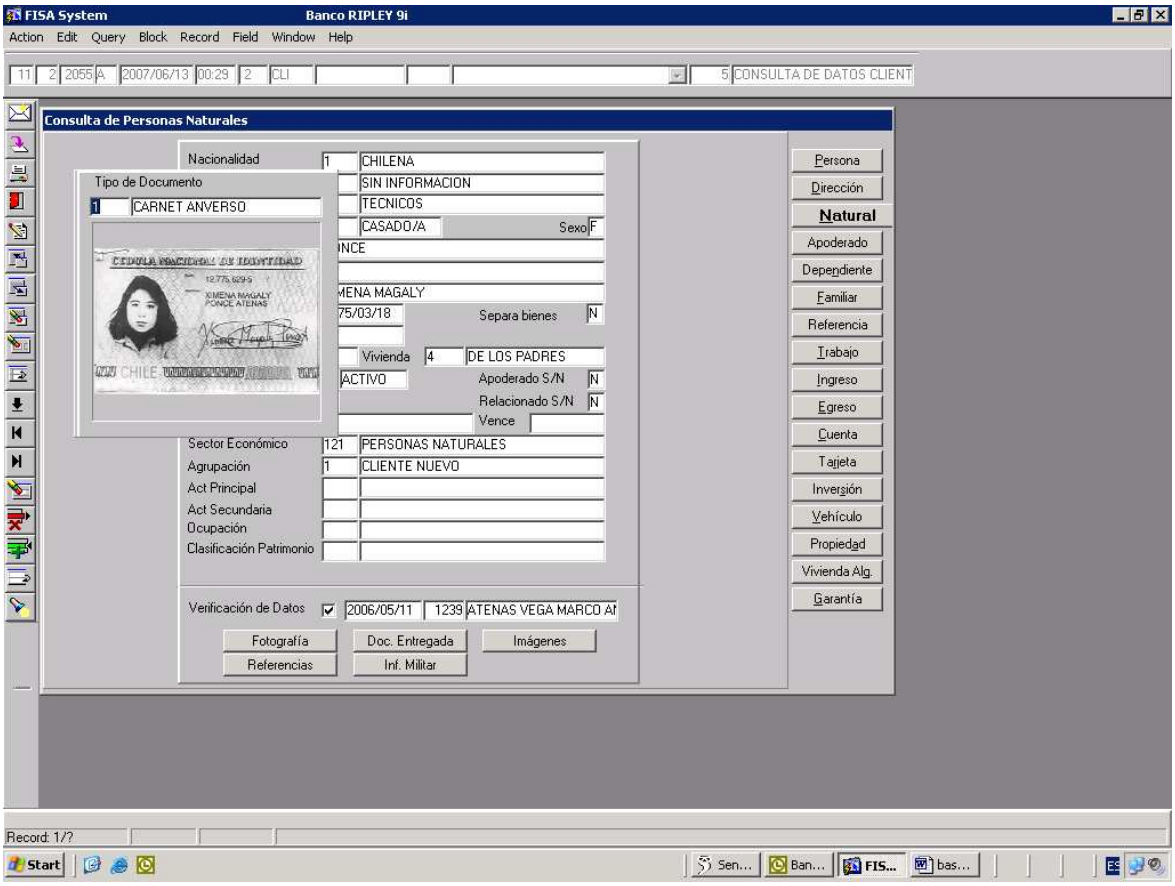
PERSONA: En este Ítems se incorpora todos los datos personales de los clientes del banco incluyendo la fecha de ingreso y su ejecutivo a cargo



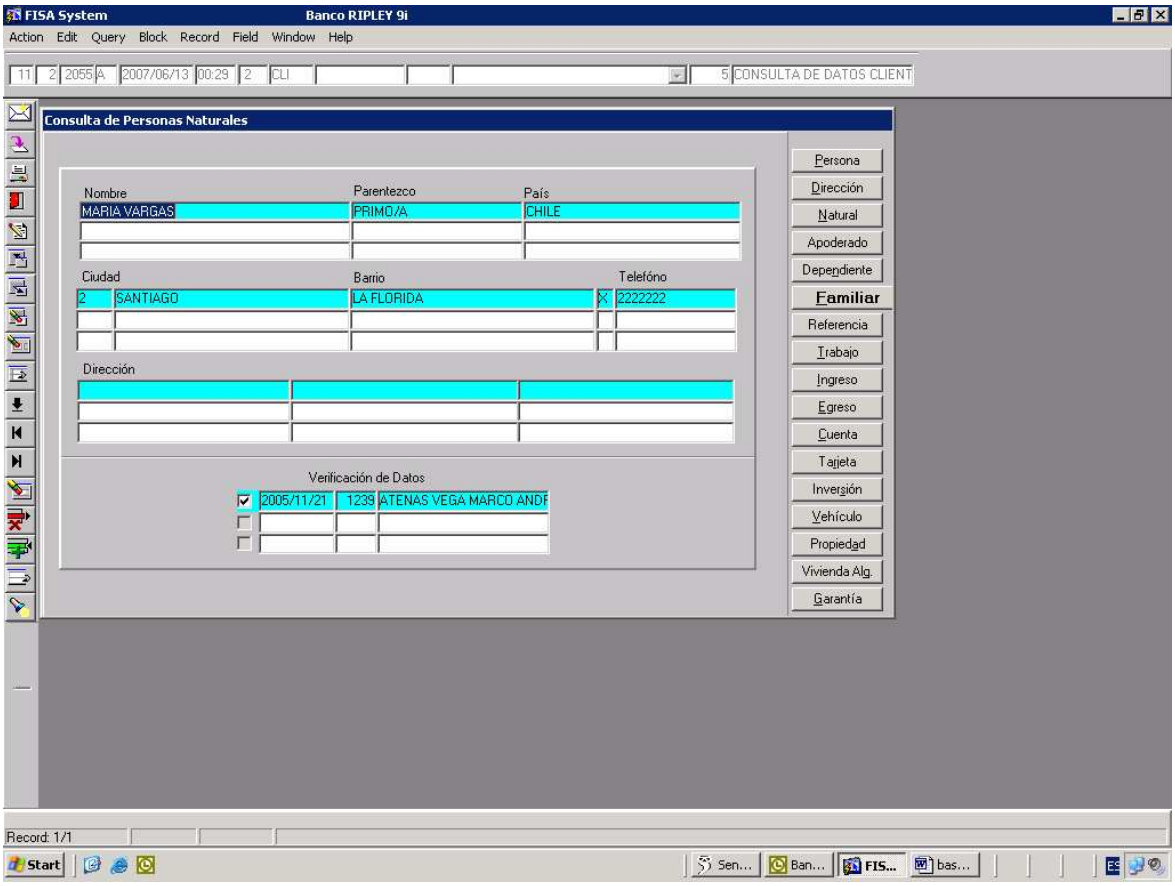
DIRECCIÓN: incorpora un detalle de la dirección completa del titular de la tarjeta con la oportuna confirmación de datos por parte de un ejecutivo a cargo



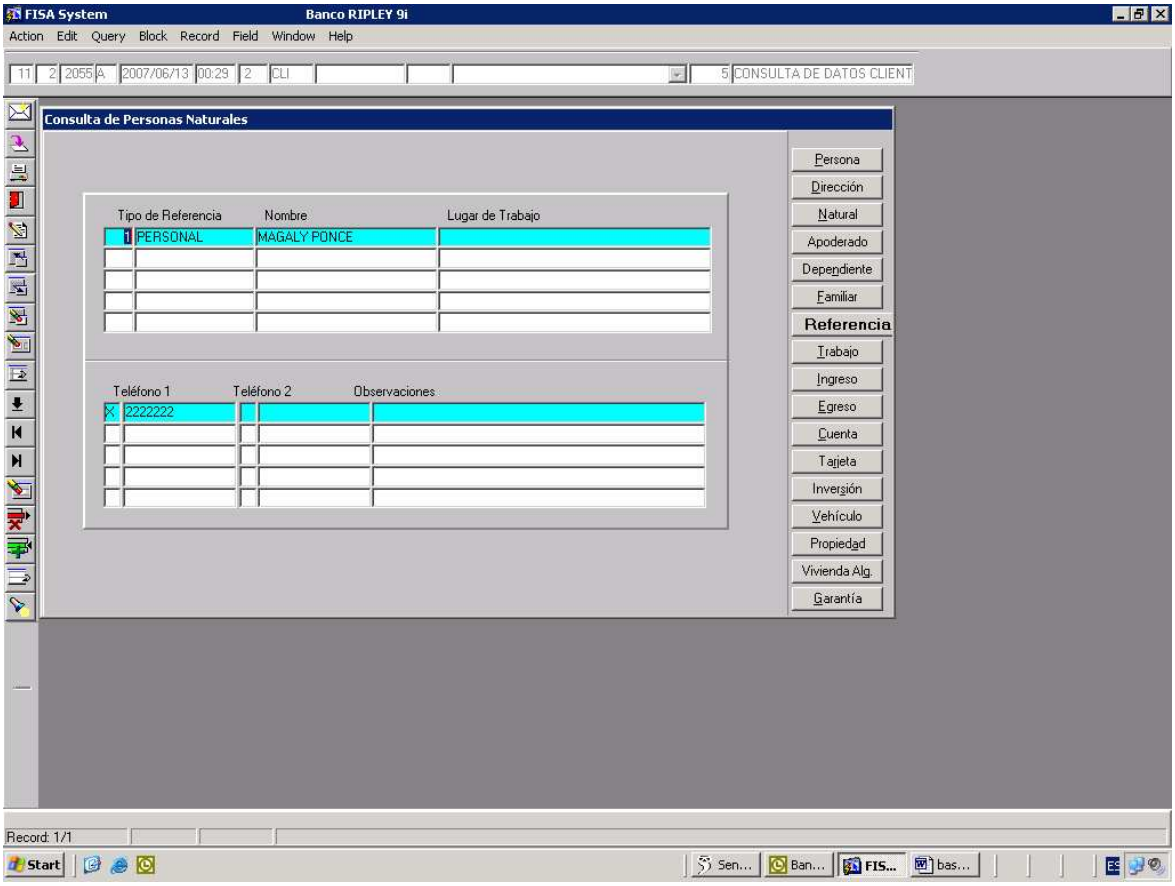
PERSONA NATURAL: se debe especificar antecedentes importantes como por ejemplo su nacionalidad, nivel de estudios, estado civil, hasta incluso un scanner de su cedula de identidad.



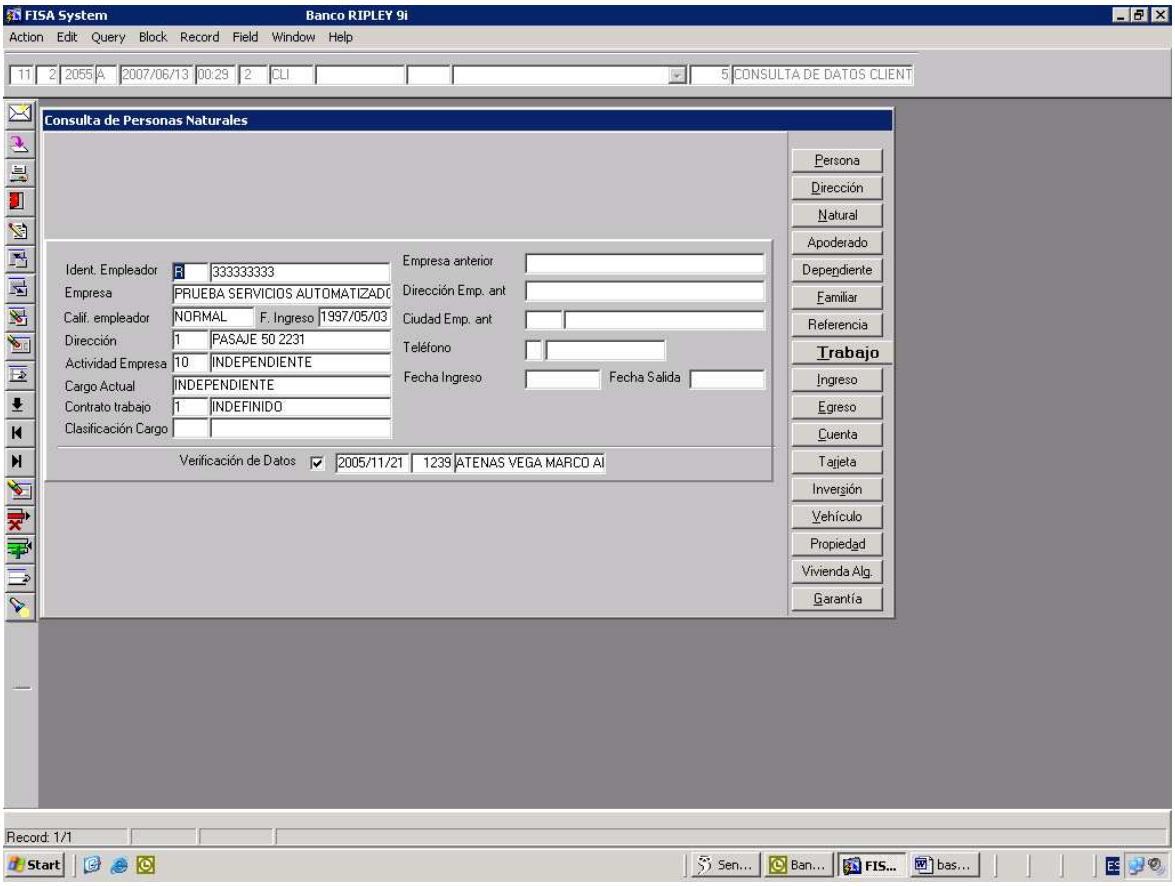
FAMILIAR: se incorpora el nombre de algún familiar directo en conjunto con un teléfono de contacto. Antecedentes primordiales a la hora de que no exista contacto con el titular de la tarjeta



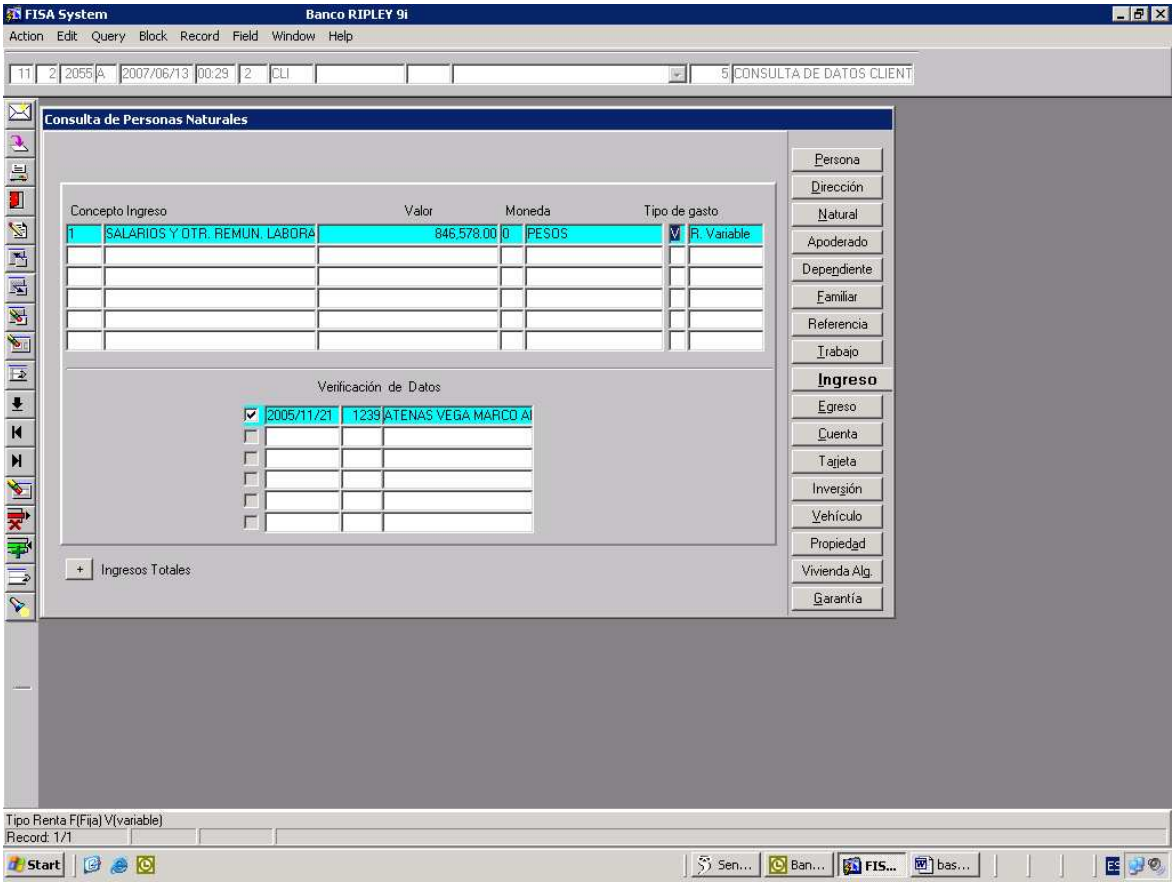
REFERENCIAS: Se incluyen individualización de cualquier tipo de referencia que indique el cliente en lo posible algún ejecutivo vigente del banco



TRABAJO: Esta sección incorpora todos los antecedentes laborales que informe el cliente como por ejemplo Rut empleador, nombre de la empresa, dirección, teléfonos, el cargo actual entre otros.



INGRESOS: esta sección se ocupa de registrar el respectivo ingreso promedio de los clientes de banco Ripley



Anexo Nº 4: Presentación de la encuesta.

Encuesta sobre los actuales sistemas de monitoreo y protocolo de trabajo de cada departamento de prevención fraude encuestado

Objetivo

Esta encuesta forma parte del trabajo tesis denominada "Propuesta para minimizar los fraudes cometidos con tarjetas de crédito bancarias" y esta dirigida a los funcionarios de cada departamento de Prevención fraude de cada banco que alcanza la muestra (6 bancos).

Esta encuesta tiene como objetivo obtener información acerca de la forma de trabajo de los distintos departamentos de prevención fraude que trabajan en el monitoreo de transacciones en línea con los tarjetas de crédito Visa y Mastercard. Teniendo también como objetivo identificar las razones por las cuales se cometen los principales fraudes en los comercios catalogados como mas riesgosos.

Presentación

Esta encuesta va a estar compuesta por 2 partes: Antecedentes Generales de los Encuestados y preguntas sobre los métodos y protocolos de trabajo aplicados

Se agradecerá completar esta encuesta con las preguntas formuladas, las que formaran parte de la evidencia del proyecto de investigación.
Sus respuestas serán de absoluta confidencialidad y utilizadas solo para efectos de este estudio de investigación.
Lea las instrucciones cuidadosamente, ya que existen preguntas en las que solo puede responder una opción, otras son de varias opciones y también se incluyen preguntas abiertas
Marque con una X la respuesta que a usted le parezca más adecuada.

Encuesta sobre los actuales sistemas de monitoreo utilizados por los bancos y el protocolo de trabajo de los analistas

ANTECEDENTES PERSONALES

Cargo Desempeñado:

Sexo:

- Masculino
- Femenino

Lugar de Nacimiento:

Estudios Realizados:

- Media Completa
- Universitaria Incompleta (Especifique):
- _____
- Universitaria Completa (Especifique):

  _____
- Postgrados (Especifique):

  _____

Tiempo de Antigüedad en el departamento:

Edad:

Estado Civil:

II PREGUNTAS:

Pregunta 1

a) Con relación al Sistema de monitoreo implementado ¿Ha sido este último objeto de modificaciones no deseadas, destrucción y/o inutilización de la totalidad o parte de sus procesos?

SI NO

b) ¿Hubo participación de auditores en el diseño, gestión y control de los procesos pertenecientes al Sistema de monitoreo?

SI NO

c) ¿Cuántos? (Indique cantidad): ____

Pregunta 2:

¿Cuantos Funcionarios trabajan en el departamento desempeñando las funciones de analistas de Fraude?

(Indique cantidad): ___

_____

Pregunta 3:

Con relación a las transacciones, cuantas operaciones catalogadas como sospechosas ingresan diariamente al sistema?

(Indique cantidad): ___

_____

Pregunta 4:

Usted conoce de otros sistemas de monitoreo de transacciones en línea?

SI NO

¿Cuántos? (Indique cantidad): ___

_____