RESUMEN.

A raíz de la necesidad de efectuar transacciones bancarias de forma rápida, sencilla y desde cualquier lugar, las entidades bancarias han tenido que invertir en medios acorde a las nuevas tecnologías y necesidades de sus clientes. A su vez, estas nuevas tecnologías traen consigo una gran problemática para los bancos: que se produzca el robo de información confidencial de cada cliente por no tener la protección adecuada en los sistemas informáticos. En este contexto, esta investigación busca analizar los elementos de seguridad que una institución bancaria utiliza para prevenir fraudes electrónicos en nexo con la auditoría forense. Para llevar a cabo este análisis se utilizó una metodología cualitativa la cual a través de la tabulación de resultados de la información obtenida de la teoría que sustenta esta investigación y de las entrevistas realizadas a personas partícipes de este contexto, se obtuvo como resultado que la institución bancaria utiliza, tanto las técnicas de investigación de auditoría forense, como distintos elementos de seguridad para prevenir los fraudes electrónicos, a excepción de uno de ellos, pero de forma adicional utiliza otros componentes de seguridad no investigados: la tercera clave y el anti-skimming.

Palabras Claves: TICs, Seguridad, Fraudes Electrónicos, Institución Bancaria.

ANÁLISIS DE LOS ELEMENTOS DE SEGURIDAD UTILIZADOS POR UNA INSTITUCIÓN BANCARIA PARA PREVENIR FRAUDES ELECTRÓNICOS EN TRANSACCIONES DE IGUAL NATURALEZA, EN RELACIÓN CON LA AUDITORÍA FORENSE

Rocío Díaz Céspedes [1]

ANALYSIS OF SECURITY ELEMENTS USED BY A BANK TO PREVENT PHISHING SCAMS IN TRANSACTIONS OF EQUAL NATURE IN RELATIONSHIP WITH FORENSIC AUDITING

ABSTRACT

Due to the necessity to make banking transactions in a quick, simple way from any place, banks have had the need to invest in resources according to the new technologies and their clients´ necessities .In its turn, these new technologies entail a major issue for the banks: the confidential information theft of each client because of not having the adequate protection on his/her information systems. In this context, this research tries to analyze the security elements, which a bank uses to prevent phishing scams in connection with forensic auditing. To carry out this analysis, a qualitative methodology was used. Thus, using the obtained information from the theory which sustains this investigation and the interviews made to people who form part of this context, the results were then tabulated and the finding was that the bank uses both: the investigation techniques of forensic auditing as well as different security elements to prevent phishing scams. With exception of one of them, which in addition it uses other security components that were not investigated here: the third clue and the anti-.skimming.

Key Words: TICs, Security, Phishing Scams, Bank

1 Alumna Tesista de la Carrera de Auditoría de la Universidad de Valparaíso, teniendo como profesor guía al Profesor Arturo Cornejo Aranda.

PROBLEMA DE LA INVESTIGACIÓN

A nivel global, el sector bancario obtiene pérdidas relacionadas con fraudes financieros de hasta US$3,5 billones anuales, de acuerdo a un estudio realizado por la Asociación de Examinadores de Fraude Certificados (ACFE en su sigla en inglés) (Albarracín, 2013). En cuanto al análisis de los delitos informáticos, el 46,71% corresponde a la falsificación o estafa vía informática, que dice relación con la introducción, borrado o supresión de datos o con interferir en los sistemas. El 43,11% son delitos contra la confidencialidad, la integridad y la disponibilidad de datos, siendo los más reiterados el acceso ilícito a sistemas informáticos; En menor escala el 10,18% de los delitos se relacionan con el contenido, como la producción, oferta y difusión de información por medio de un sistema informático (Recovery Labs; 2012). En Chile, las pérdidas causadas por los diferentes fraudes, incluidos los informáticos, superan los US$ 5 millones anuales, siendo el método más utilizados el phishing. (Muñoz; 2013).

El rápido crecimiento tecnológico genera como consecuencias el aumento de delitos y fraudes informáticos, siendo los bancos un objetivo atractivo. Ellos registran numerosas pérdidas a raíz de las propias debilidades existentes en sus sistemas informáticos, siendo aprovechadas por personas, que con o sin conocimiento del área, buscan conseguir información privilegiada y así obtener ingresos extraordinarios a su favor (Mendoza; 2012). Aquellas debilidades se pueden relacionar, por un lado, con el control interno de la entidad bancaria, y por otro la poca seguridad existente en las plataformas informáticas. Por lo tanto, es necesario que las entidades bancarias incorporen las medidas de seguridad adecuadas para prevenir y reducir el número de fraudes en las transacciones electrónicas, ayudándose además, con la denominada auditoría forense.

La finalidad de esta investigación es realizar un análisis de las distintas medidas de seguridad que permiten a una entidad bancaria prevenir los fraudes en sus transacciones electrónicas, relacionándose en alguna medida, con la auditoría forense.

MARCO TEÓRICO

ANTECEDENTES GENERALES

El fraude no discrimina en su ocurrencia, aun cuando existan controles antifraudes que pueden disminuir la probabilidad y el impacto potencial del mismo, no hay entidad que sea inmune a esta amenaza. Según lo señalado por la Asociación de Examinadores de Fraudes Certificados ACFE (2014) en su informe a las naciones en materia de fraudes y abuso laboral, los porcentajes de fraudes de acuerdo a cada sector industrial, y en el sector bancario y servicios financieros en particular son los más elevados. En Chile, a raíz del rápido progreso de la tecnología, las entidades bancarias han ampliado su gama de servicios para satisfacer las nuevas necesidades de sus clientes, con la finalidad de realizar transacciones de una forma más fácil, cómoda y segura. Es así como las estadísticas de la Superintendencia de Bancos e Instituciones Financieras (SBIF) demuestra que el medio más utilizado por los clientes, en el último período para realizar transacciones electrónicas, es la banca en línea. Por lo tanto, al conocer el aumento del número de éstas transacciones en los diferentes medios, aparecen nuevos fraudes, especialmente los de tipos electrónicos que amenazan la seguridad de los bancos del país.

LA AUDITORÍA FORENSE

Según la Comisión Técnica Especial de Ética Pública, probidad administrativa y transparencia CEPAT (2005), la auditoría forense es una rama de la auditoría orientada a participar y contribuir en la investigación de diversos fraudes, en actos conscientes y voluntarios en los cuales se eluden las normas legales, o se usurpa lo que por derecho corresponde a otros sujetos, mediante mecanismos fraudulentos para obtener ventajas económicas o un beneficio ilícito.

Objetivos de la auditoría forense

La CEPAT, en la XV Asamblea General de la OLACEFS (2005), menciona los principales objetivos de la auditoría forense, siendo los siguientes:

1.- Identificar, demostrar y sustentar el fraude o ilícito realizado.

2.- Prevenir y reducir el fraude, a través de la implementación de las recomendaciones de fortalecimiento de control interno propuestas por el auditor.

3.- Participar en el desarrollo de los diferentes programas de prevención de pérdidas y fraudes.

4.- Participar en la evaluación de sistemas y estructuras de control interno.

5.- Recopilar evidencias necesarias aplicando diversas técnicas de investigación.

6.- Colocar a disposición de los diversos órganos del Ministerio Público y de la Función Judicial la evidencia para ser investigada con el fin de determinar el tipo de delito y establecer la sanción.

EL FRAUDE

De acuerdo a la Asociación de Examinadores de Fraude Certificados (ACFE), define al fraude como aquellas actividades o acciones realizadas con el propósito de enriquecimiento personal a través del uso inapropiado o la sustracción de recursos o activos de una organización por parte de una persona. (ACFE, 2014)

FRAUDES ELECTRÓNICOS EN EL SECTOR BANCARIO

Del banco tradicional a la banca electrónica

De acuerdo a Mallory Malesky (2013) se puede definir al banco tradicional como aquella entidad bancaria que ofrece una completa variedad de servicios para el cliente, contando con el personal capacitado como lo son los cajeros y agentes de crédito. Mientras tanto, Darío Moreno explica que la banca electrónica corresponde a un conjunto de herramientas electrónicas como el internet, cajeros automáticos y otras redes de comunicación, que ofrece a sus clientes un fácil, rápido y cómodo acceso a sus cuentas, permitiendo que realicen una gama de operaciones bancarias, como si estuviesen en una oficina real. (Moreno citado por Leal; 2012)

El banco tradicional ha cedido el paso a las diversas formas de uso del internet. “La forma más común que han adoptado las instituciones financieras es aquella relacionada con asumir un menor grado de compromiso por parte de la empresa y que consiste en complementar la atención del cliente a través de los servicios ofrecidos en una página web. Una segunda forma es la adoptada por aquellos bancos que han creado a través de internet una alternativa distinta para prestar sus servicios, ofreciendo condiciones y productos diferentes para los clientes y otorgando intereses privilegiados a lo común que ofrecen los bancos tradicionales. Por último, la tercera forma es la adoptada por las instituciones bancarias que han asumido un mayor compromiso con mencionado canal y por lo tanto un mayor

riesgo, desarrollando una oferta específica y diferenciada a través de internet." (Torres y Vásquez; 2005; p.3)

Transacciones electrónicas

Los servicios que ofrece una institución bancaria son diversos y cada día están al alcance de más personas. Los servicios, generalmente, están a disposición del cliente las 24 horas del día y los 365 días del año. Los servicios van desde la realización de transacciones en cajeros automáticos hasta transacciones utilizando el internet.

1.- Transacciones en cajeros automáticos

Los cajeros automáticos, originalmente llamados ATM (Automatic Teller Machines o máquina de cajero automático) son dispositivos electrónicos que permiten a los clientes de un banco hacer retiro de dinero y ver sus estados de cuentas, depositar efectivo o cheques, transferir dinero de entre diferentes cuentas de bancos, utilizar tarjetas con chip o, incluso realizar recargas para teléfonos celulares a cualquier hora del día durante todo el año, sin la necesidad de concurrir al banco. Para realizar las diversas transacciones se utiliza una tarjeta de débito o de crédito y un código de identificación individual y personalizado conocido como PIN. La tarjeta se introduce en una ranura denominada lector de tarjetas P.O.S. (Point Of Sale o punto de venta), el cual la captura y lee la información del cliente contenida en la banda magnética o chip según sea el caso, enviándose los datos a una computadora central y ejecutando la transacción que se desea. El mecanismo que da el efectivo se llama ojo electrónico; tiene incorporado un sensor que cuenta cada billete una vez que se solicita la cantidad deseada. El conteo y los datos de las transacciones son grabados en un diario electrónico denominado Log. (Guillermo; 2008)

2.- Transacciones en banca en línea

La banca en línea, es un sistema que utiliza tecnología computarizada y electrónica, sustituye los cheques y otras transacciones efectuadas por medio de documentos de papel. Este servicio se encuentra a disposición de las personas en todo momento. Se puede acceder por medios computacionales conectados a la red de internet pudiéndose realizar las siguientes operaciones:

- Consulta de saldo y últimos movimientos de cuentas.
- Transferencias bancarias, Inversiones.
- Solicitudes de chequeras.

- Reportes de robos / extravío de tarjetas.
- Pagos por transferencias electrónicas
- Asesores y simuladores virtuales (cálculos de créditos, cálculo de inversiones)
- Suspensión de pago de cheques
- Pagos de cuentas y recargas telefónicas (Leal; 2012)

Fraudes electrónicos bancarios

Julio Jolly y Osvaldo Lau, definen el fraude electrónico como "cualquier actividad por la cual, una persona toma acciones mediante la utilización de equipos o recursos informáticos para obtener ventaja sobre otra persona o entidad a través de falsedades, engaños u omisión de la verdad". (Jolly y Lau, 2013). Entre las formas de fraudes electrónicos más comunes en la actualidad se destacan los siguientes:

Phishing: "es una técnica de captación ilícita de datos personales y de cuentas bancarias, a través de la suplantación de sitios de internet. Son principalmente correos electrónicos engañosos y páginas web fraudulentas que aparentan ser instituciones de confianza, como bancos e instituciones financieras, pero en realidad están diseñadas para estafar al destinatario y conseguir la entrega de información confidencial." (Recovery Labs; 2004;1)

Pharming: "se basa en el mismo principio del phishing en cuanto en hacer creer al usuario que está en una web distinta a la que realmente está, pero es una estafa con un mayor grado de dificultad. Este mecanismo consiste en manipular direcciones de una base de datos, la cual es utilizada para traducir los nombres de dominio (fácilmente recordables) en números de protocolo de internet (dirección IP) que es la forma en que la información se pueden encontrar en internet, para engañar al usuario y cometer fraude". (Recovery Labs; 2004;1)

Fraudes relacionados con la banca en línea

1. Keyloggers: Es un software o hardware que permite identificar lo que escribe o selecciona una persona en su teclado, permitiendo la captura de los datos de acceso del usuario. En el caso del software, captura todo lo que

escribe el usuario y se envía a una dirección de correo electrónico del estafador; son programas que se instalan y funcionan sin que el usuario se percate de ello. En el caso del hardware, corresponden a dispositivos que se conectan al computador y graban en una memoria interna el texto escrito por el usuario. (ASOBANCARIA, 2009; 1)

2. Spyware: El spyware o programas espías son aplicaciones que recopilan información sobre una persona u organización sin su consentimiento ni conocimiento. Generalmente se instalan cuando se acepta la instalación de otras aplicaciones relacionadas con ello. El tipo de información que pueden recopilar estos programas es muy diversa, como por ejemplo: nombre y contraseña del correo electrónico del usuario, dirección IP y DNS del equipo, los hábitos de navegación o datos bancarios que el usuario utiliza para realizar sus transacciones. (Recovery Labs, 2004; 1).

Fraudes en cajeros automáticos

El fenómeno de los cajeros automáticos o ATMs (Automated Teller Machine) ha tenido un rápido crecimiento desde que surgieron, alcanzando cifras de hasta 2 millones de unidades en el mundo, con grandes ventajas tanto para el consumidor como para la entidad bancaria, aunque su seguridad siempre ha sido un problema de difícil solución. Debido a la valiosa información que manejan estos dispositivos y a la propia gestión y almacenamiento de dinero en efectivo, son elementos bastantes atractivos para los defraudadores, generando un incremento de los ataques a redes de cajeros automáticos de manera organizada y sofisticada convirtiéndose en un gran problema, provocando importantes pérdidas de dinero, no solo para los clientes sino también para las entidades bancarias.

Los ataques a los cajeros automáticos se pueden clasificar en:

1.- Ataque a las infraestructuras, TI: Los criminales se han dado cuenta que resulta más rentable explotar las vulnerabilidades de la infraestructura TI del cajero, ya sea infectando al ATM con algún software maliciosos, pudiendo tomar el control remoto del cajero o incluso obtener dinero en efectivo directamente del mismo o también aprovechando alguna vulnerabilidad del software.

“Los cajeros automáticos emplean, la mayoría de ellos, como sistema operativo Microsoft Windows para su funcionamiento común y utilizan redes IP como

mecanismo de comunicación, lo que genera un aumento del riesgo de seguridad asociado a las debilidades existentes en este tipo de sistemas abiertos, quedando dispuestos a infectarse con software maliciosos." (Navajo, 2011; 165)

2.- Skimming: Se denomina Skimming "al robo de información de tarjetas de crédito utilizadas en el momento de la transacción, con la finalidad de reproducir o clonar la tarjeta de crédito o débito para su utilización fraudulenta posterior. El objetivo de este método es capturar la información que se encuentra codificada en la banca magnética en el reverso de cada tarjeta, a través de un lector de tarjetas modificado conocido como un dispositivo duplicado. Estos dispositivos son diseñados para ser colocados en la abertura del lector de tarjetas del cajero automático, fabricando además, paneles falsos que cubren toda la superficie del frente del lector de tarjetas, con el fin de mimetizarlos y dar a conocer que son parte del cajero automático". (Navajo, 2011; 165)

Elementos de seguridad

Las entidades bancarias, en relación a su esfuerzo por ofrecer un mejor servicio a sus clientes, ajustan sus sistemas de seguridad a la actualidad de los riesgos. Es "así como las entidades bancarias cuentan con plataformas tecnológicas que permitan garantizar la seguridad de las transacciones efectuadas por sus clientes, sin embargo, se reconoce que existen muchas instituciones financieras que carecen de esta tecnología necesaria para prevenir intrusos y para asegurar parte de su información." (Leal, 2012; 26)

Dentro de los elementos de seguridad, se encuentran los siguientes:

• Anti-phishing / Anti-pharming son aquellos relacionados con la utilización de software especializado y protección a DNS. El software suele ser utilizado en los servidores de grandes compañías para proteger a sus usuarios y empleados de posibles ataques de pharming o phishing. Se caracteriza por actualizar de forma constante una base de datos de páginas web fraudulentas, a través de un análisis de comportamientos malintencionados con el fin de ser bloqueadas cuando se contacte con algunas de ellas. (Callegari; 2007)

• Tarjetas bancarias inteligentes, llamadas también "tarjetas con chip" o "tarjetas con microcircuito", con este tipo de tarjetas se ha creado una plataforma de nueva generación que permitirá llevar servicios y nuevos productos a los

clientes del sistema financiero de una forma más efectiva, eficiente y segura. Las transacciones con este tipo de tarjetas son mucho más sencillas y más seguras, debido a que la banda magnética se introduce con la tarjeta en una ranura destinada en el terminal para la lectura del chip. (Asbanc; 2013)

• Protocolo seguro de transferencia de hipertexto, más conocido como "HTTPS" (HiperText transfer protocol), es un protocolo de aplicación que se encuentra destinado a la transferencia segura de datos. Es empleado mayoritariamente por las entidades bancarias, tiendas en línea y cualquier tipo de servicio que requiera el envío de datos personales o contraseñas, como puede ser alguna transacción electrónica en donde es indispensable que el usuario disponga de sus datos para completar la transacción, utiliza códigos para crear un canal de comunicación de información codificado. De este modo, se consigue que la información importante para el usuario, como por ejemplo los datos de acceso, no sean utilizados por algún defraudador que haya conseguido interceptar la transferencia de datos, ya que lo único que obtendrá sean valores imposibles de descifrar. (Domingos; 2013: p167)

• Encriptamiento de datos o criptografía es la técnica de proteger la información transformándola con un determinado algoritmo dentro de un formato para que no pueda ser leída normalmente. En palabras más simples, consiste en la transformación de datos a una forma en que no sea posible leerla por cualquier persona, a menos que cuente con las claves para desencriptarlos. (Echenique, 2001)

METODOLOGÍA DE LA INVESTIGACIÓN

La presente investigación se desarrolla bajo un paradigma cualitativo y con un alcance de sintetización. Se ejecuta a través de la realización de entrevistas a personal que tenga estrecha relación con las transacciones electrónicas, con temas diversos de fraudes electrónicos bancarios, medidas de seguridad para disminuir los riesgos de fraudes y aplicación de técnicas investigación para la detección de fraudes electrónicos. El sujeto de investigación corresponde a un banco con presencia nacional, autónoma del estado, con personalidad jurídica y patrimonio propio, sometida a fiscalización de la SBIF y creada con el objetivo de otorgar acceso al crédito y el resguardo del dinero a sectores productivos y al público en general, además de favorecer el desarrollo de las actividades económicas nacionales a través de la prestación de servicios y productos financieros.

ANÁLISIS DE RESULTADOS

A continuación se presentan los respectivos análisis de los resultados que se obtuvieron de las entrevistas efectuadas, tabulados de acuerdo a las categorías de análisis establecidas.

Categoría	Subcategoría	Conclusiones	Su-subcategoría	Conclusiones
Banca Electrónica	Transacciones electrónicas	Las transacciones electrónicas efectuadas a través del cajero automático y por la banca en línea son las más utilizadas por los clientes de la institución bancaria, realizándose, en este último, un poco más de 360 millones de transacciones en el año 2013, debido a que son medios que están a disposición las 24 horas del día, los 7 días de la semana, tanto para realizar traspasos de dinero, consultas de saldo y/o pago de servicios. Al momento de analizar cuáles son las transacciones que representa un mayor riesgo de fraude se encuentran aquellas que se efectúan a través de la banca en línea y por CajaVecina. El primer medio se considera riesgoso por ser uno de mayor demanda y por manejar grandes montos de dinero e información importante, siendo un objetivo privilegiado para los hackers, que a través del uso de múltiples técnicas obtienen la clave secreta de los clientes, las combinaciones de la clave de coordenadas siendo elementos esenciales para efectuar cualquier tipo de transacciones electrónicas. Mientras que el segundo medio, se considera riesgoso y no riesgoso, riesgoso porque no hay un control físico de cada uno de los terminales de CajaVecina al ubicarse la mayoría de ellos en lugares muy lejanos, pero se considera no riesgoso, al manejarse montos bajos, no aceptando pagos con cheques y realizándose giros y depósitos solamente con el Banco. Y aquellas transacciones que se realizan por cajeros automáticos, se consideran las de más bajo riesgo de fraude, principalmente, porque todos los cajeros del banco poseen anti-skimming, siendo más difícil el robo de información.	Transacciones en cajeros automáticos	En relación a la respuesta del asistente de canales no presenciales, indica que aquellas transacciones que se ejecutan a través de los cajeros automáticos lideran las estadísticas como el medio más utilizado por sus clientes, debido a que muchos de ellos no tienen acceso ni nociones básicas para utilizar la banca en línea y siendo el cajero automático el de más fácil acceso para realizar transacciones comunes de manera más rápida evita así, el paso por caja. Además, el banco considera a este medio como uno de los que posee un menor riesgo de fraude debido a que todos los cajeros del Banco poseen anti-skimming, sumado a ello, que los mismos clientes observan las características y el estado físico en que se encuentran los cajeros automáticos de las diferentes instituciones bancarias, como también, resguardando el ingresó de la clave secreta para comenzar a ejecutar la transacción.

			Transacciones en banca en línea	Dos de los entrevistados indican que las transacciones realizadas por este medio son muy numerosas, efectuándose un poco más de 360 millones de transacciones durante el año 2013, relacionadas con el traspaso de fondos entre clientes del mismo banco o con otras instituciones bancarias, consultas de saldos, pago de servicios, solicitudes de créditos, realizadas en cualquier momento, horario y lugar. Por este motivo, que las transacciones realizadas por la banca electrónica están más propensas a que ocurran fraudes de tipo electrónicos, porque al ser la más demandada por sus clientes y de acuerdo a los montos que se manejan, los hackers usando un sinfín de técnicas, pueden obtener información confidencial de cada persona como su clave secreta, las combinaciones de la clave de coordenadas o infectar los computadores con spyware, siendo responsabilidad del propio cliente tomar los resguardos correspondientes.

			Transacciones en CajaVecina	Se observan dos puntos de vista en relación a las transacciones en CajaVecina. Por un lado, se indica que las transacciones realizadas por este medio representan un menor riesgo de fraude, debido al monto de dinero que se maneja, cuyo giro máximo es por $200.000, no acepta el pago o depósitos por cheques, solamente se hacen giros y depósitos en cuentas del Banco y que cada personas que desee tener CajaVecina en su negocio debe cumplir con ciertos requisitos. Mientras que por el otro lado, se da como respuesta que la CajaVecina es que la representa un mayor riesgo de fraude, principalmente porque no hay un control específico de todos los terminales, ya que muchos de ellos se encuentran en lugares muy alejados y verificarlos física y constantemente es una tarea difícil.

	Fraudes electrónicos	El fraude electrónico, ejecutado a través de internet, que lidera las estadísticas del Banco es el phishing cuya ocurrencia es de aproximadamente 8 veces en un mes, seguido del pharming siendo el número de casos aproximado 4 veces al mes. Son las trampas visuales más comunes, ya que hacen creer al usuario que se encuentra en la página del Banco o que los correos electrónicos que reciben son de él, con el fin de obtener información confidencial de cada cliente, como lo es la clave de acceso. Pero de igual forma son considerados unos de los fraudes más bajos al relacionarlos con el flujo de conexiones que tiene la página del Banco, por cada 15 minutos existen cerca de 50 a 60 conexiones. En cuanto a los fraudes en cajeros automáticos, esencialmente a través del uso del skimming, se realiza una distinción, porque aquellos clientes que son afectados por este tipo de fraude ascienden a 117 aproximadamente por mes, pero son aquellos usuarios que utilizan sus tarjetas bancarias en cajeros de otras instituciones bancarias, ya que todos los del Banco cuentan con anti-skimming, siendo casi imposible el robo de información. En cuanto a los fraudes electrónicos spyware, keylogger y ataques a la infraestructura de los cajeros automáticos TI, no se obtuvo información, ya que son fraudes relacionados únicamente con las deficiencias de seguridad del usuario en su equipo computacional, para los dos primeros casos. Para el tercero el Banco no cuenta con información ni estadísticas. Al momento de detectar la ocurrencia de algunos de los fraudes mencionados y comenzar a solucionarlos, la entidad bancaria da respuesta a todos sus clientes de igual manera independiente del monto que se encuentra involucrado y del tipo de cliente que sea para el banco.	Phishing	Es uno de los fraudes que lidera las estadísticas en el Banco en cuanto a las trampas visuales, ya que hace creer al usuario que ha recibido un correo electrónico del Banco del cual es usuario, con el fin de obtener los datos de acceso y realizar transacciones libremente, como por ejemplo el giro total de los fondos. El número de veces que ocurre este fraude es de aproximadamente 8 veces en el mes teniendo en consideración que en 15 minutos hay cerca de 50 a 60 conexiones en línea. El bajo número de casos de phishing se debe a que de alguna forma los clientes toman las medidas de seguridad para evitar cualquier tipo de fraude, por ejemplo, verifican que la página web sea la del banco o no dan respuestas a correos electrónicos que pidan información personal, pero de igual forma este tema no deja de ser una preocupación para la institución bancaria.

			Pharming	Junto con el Phishing, son las trampas visuales más comunes que ocurren dentro del Banco, engañando a los clientes mostrando páginas del banco que son falsas solo para robar información personal de ellos. Pero en relación a las veces que ocurra este tipo de fraude durante un mes es muy bajo, tan así que solo ocurre aproximadamente 4 veces al mes.
			Fraudes relacionados con banca en línea (keylogger y spyware)	En relación al spyware y los keylogger, que se encuentran dentro de este ítem, son fraudes relacionados únicamente con las deficiencias de seguridad que el usuario tiene en su equipo computacional, debido a que estas trampas son instaladas directamente en los equipos, siendo muy difíciles detectarlos, por esto el banco no tiene estadísticas sobre estos fraudes, siendo difícil determinar el número de casos que afectan al banco.

			Fraudes en cajeros automáticos (ataques a las infraestructuras TI y Skimming)	El fraude en cajeros automáticos es considerado como el más común dentro del Banco, el cual es ejecutado a través del uso del skimming, ya que algunos usuarios no se percatan que los cajeros automáticos han sido intervenidos con el fin de robar información contenida en la banda magnética de las tarjetas bancarias. El número de veces al mes que ocurren fraudes por el uso del skimming es de 117, pero esta cifra indica el número de clientes del Banco estafados al utilizar su tarjeta en otro cajero diferente al del banco, debido a que los ATM Banco contienen un anti-skimming. En cuanto al número de veces que ocurren ataques a la infraestructura TI, o sea infectar al cajero automático con algún virus, no se puede determinar, ya que el banco no cuenta con las estadísticas asociado a dicho fraude, considerándose el menos común.

	Elementos de seguridad	El banco utiliza como elemento de seguridad para prevenir fraudes electrónicos el anti-phishing/anti-pharming, el protocolo seguro de transferencia de hipertexto y el encriptamiento de datos, a excepción de las tarjetas bancarias inteligentes, elemento que se está analizado para su posterior lanzamiento a sus usuarios, todos los demás elementos ayudan al banco a resguardar la información confidencial de cada uno de los clientes y de las numerosas transacciones que se realizan. De forma adicional, el Banco informa de otros dos elementos utilizados para los mencionados fines, el uso de la tercera clave y el anti-skimming, cuya característica del primero, es permitirle al usuario validar la transacción que está efectuando por internet a través del ingreso de una clave secreta temporal enviada al dispositivo móvil del cliente para concluir con la operación; el segundo elemento es utilizado en los cajeros automáticos, el cual codifica la información contenida en la banda magnética de las tarjetas bancarias con el fin de evitar su clonación y robo de información. La institución bancaria constantemente invierte en nuevas tecnologías, referidas a seguridad de información, monitoreando las diversas actividades con el objeto de actualizarse e implementar nuevos elementos de seguridad que estén a la par con las nuevas modalidades utilizadas por los ladrones informáticos. El Banco es considerado como la entidad más segura en comparación de sus pares.	Anti-phishing / Anti-pharming	Todos los entrevistados concuerdan que el anti-phishing y el anti-pharming son utilizados por el Banco como alternativa para prevenir los fraudes electrónicos, que si bien no se eliminan el cien por ciento, han cumplido el objetivo de disminuir el riesgo de ocurrencia.

			Tarjetas bancarias inteligentes	El Banco, recientemente está analizando la implementación de las tarjetas bancarias inteligentes como complemento a la seguridad de sus clientes, ya que sería un elemento mucho más confiable porque serían menos vulnerables que las tarjetas con bandas magnéticas, por lo tanto no es un elemento utilizado por la institución bancaria
			Protocolo seguro de transferencias de hipertexto	El Banco si hace uso de este tipo de elemento de seguridad a través de la firma de un contrato con una empresa certificadora, siendo el fin demostrar a sus clientes que la página que visitan es segura, que corresponde al Banco y que no tendrán problemas al efectuar alguna transacción, por lo tanto otorga una mayor seguridad a sus clientes, cumpliendo con el objeto de prevenir los fraudes electrónicos
			Encriptación de datos	Este elemento también es utilizado por el Banco, por la razón que da más seguridad al resguardar la información confidencial de cada cliente y de las múltiples transacciones que se generan, cumpliendo con el objetivo de prevenir la ocurrencia de fraude electrónico, ya que en relación a otros períodos de tiempo, estos han disminuidos significativamente.

	Riesgos asociados	Los riesgos que más preocupan a la institución bancaria son, por un lado el riesgo operacional debido a que debe contar con controles y protocolos muy estrictos al ejecutar algún programa informático con el fin de evitar cualquier robo de información por parte de sus empleados o por personas ajenas a la institución y el riesgo reputacional, por el otro, en donde el Banco se caracteriza por tener una mala reputación, lo que ocurre especialmente, por el gran número de clientes que tiene, dificultando dar soluciones rápidas y eficientes a las problemáticas que se presenten. Mientras que el riesgo legal y el de contagio, son importantes, pero el banco los ha mitigado, no surgiendo problemas de ellos.	Operacional	De acuerdo a la entrevista planteada, se concluye que el riesgo operacional es el que más daño produce a la entidad, ya que la institución financiera debe contar con controles y protocolos muy estrictos, siendo analizado cada programa informático y ejecutado de acuerdo a la normativa de seguridad implementada por el Banco, con el fin de evitar cualquier robo de información, tanto por sus empleados como por personas externas a la institución.
			Legal	El entrevistado indica que la institución bancaria ha mejorado su protocolo de transparencia de información, lo que genera que sus clientes se sientan confiados en cuanto al servicio que van a recibir y que este sea de acuerdo al servicio contratado.
			Reputacional	El riesgo reputacional está siempre presente en la institución bancaria, porque al contar con un gran número de clientes, las deficiencias de gestión de los agentes, los problemas al realizar transacciones electrónicas o problemas con sus claves secretas, genera descontento en los usuarios creando una mala reputación al banco, este último con el fin de dar más confianza y hacer sentir más conformes a los clientes, les trata de otorgar soluciones rápidas y eficientes ante cualquier anormalidad.

			De contagio	Al ser un banco que lidera el sector bancario en relación a la seguridad, el número operaciones financieras y que cuente con una gran cantidad de clientes, cualquier acción de grandes magnitudes afectaría las actividades de sus competidores.
Auditoría forense	Técnicas de investigación	Aquellas técnicas utilizadas de forma muy frecuentemente son: las de verificación ocular, física e informática, todas tomadas en cuenta desde el punto de vista electrónico, en las que la institución bancaria observa las diferentes actividades de sus empleados, inspeccionar y analizar que todo proceso y programa informático se realice de acuerdo a la normativa de seguridad implementada por el Banco. En cuanto a la técnica de verificación verbal la aplica frecuentemente, aplicándose con mayor énfasis a los nuevos trabajadores, encuestas y entrevistas para confirmar el cumplimiento de la normativa de seguridad y calidad de información que exige el Banco. Finalmente, aquellas que menos frecuentemente realiza el Banco son la de verificación escrita y documental, por la razón que toda la información se hace y se obtiene de forma computarizada.	Verificación ocular	La institución bancaria, muy frecuentemente aplica la técnica de verificación ocular para obtener algún indicio de fraude electrónico, preocupándose de observar las diferentes actividades que realizan sus empleados, revisando, principalmente, que los procesos electrónicos se ejecuten de acuerdo a su normativa de seguridad.
			Verificación verbal	Se concluye que la técnica de verificación verbal es utilizada frecuentemente por parte del Banco para conseguir indicadores de fraudes electrónicos aplicándose a sus trabajadores, con mayor énfasis a los nuevos empleados, encuestas y la realización de reuniones y siendo el fin confirmar que se cumplan las normativas y calidad que la institución exige.

			Verificación escrita	El banco aplica la verificación escrita de forma poco frecuente para obtener información de la existencia de fraude, por la razón que toda la información se hace y se obtiene de forma computarizada.
			Verificación documental	Se obtiene la misma respuesta que al consultar por la actividad anterior. La institución aplica de forma poco frecuente la verificación documental, por el hecho que toda la información es computarizada.

Tabla 2: Análisis de resultados. Elaboración propia. 2014

DISCUSIÓN DE RESULTADOS

Al momento de efectuar la presente investigación se puede ratificar que la información contenida en el marco teórico concuerda con la información obtenida a través de la recopilación de datos.

La banca electrónica, como se plantea en el marco teórico, se compone de numerosas herramientas para efectuar transacciones de tipo electrónico, es por ello que el Banco ofrece a sus clientes medios como el cajero automático, la banca en línea y la CajaVecina. Los más utilizados por sus clientes son el cajero automático y la banca en línea realizándose, en este último, un poco más de 360 millones de transacciones durante el año 2013, ya que son medios que están a disposición las 24 horas del día por toda la semana, tanto para realizar traspasos de dinero, consultas de saldo y/o pago de servicios. Las transacciones que se efectúan por cajero automático representan el medio con menor índice de fraudes electrónicos, ya que todos ellos poseen anti-skimming dificultando el robo de información, mientras que las transacciones realizadas por banca en línea (al ser el canal más demandado), son de un alto riesgo de fraude ya que los hackers utilizan diversas técnicas para obtener sus claves secretas y combinaciones de la tarjeta de coordenadas. En cuanto a las transacciones por CajaVecina, estas se consideran, por una parte, las de mayor riesgo de fraude al no contar con un control físico específico en cada uno de los terminales de este medio al encontrarse la mayoría de ellos en lugares muy alejados, pero por otra parte lo consideran como el de menor riesgo, ya que los montos que se manejan son bajos, no aceptando pago con cheques y solo se hacen giros y depósitos para clientes del Banco.

Dentro de este tipo de banca, se aprecia la existencia de fraudes electrónicos, siendo los más comunes, de acuerdo al marco teórico, el phishing, el pharming, los fraudes relacionados con la banca en línea (keyloggers y spyware) y los fraudes en cajeros automáticos (ataques a las infraestructura TI y skimming). El Banco identifica los diversos fraudes electrónicos que lo afectan, aquel que lidera las estadísticas en cuanto a trampas visuales es el phishing, con aproximadamente 8 casos en un mes, seguido del pharming con 4 casos al mes, los cuales hacen creer al cliente que la página web que visitan o los correos electrónicos recibidos corresponden al Banco; a nivel general, este se considera como uno de los fraudes de menor ocurrencia. Al momento de consultar por los fraudes en cajeros automáticos, esencialmente a través del uso del skimming, se realiza una distinción, porque aquellos clientes que se ven afectados por este tipo de fraude ascienden a 117 aproximadamente por mes, pero solo aplica para aquellos usuarios que utilizan

sus tarjetas en cajeros de otras instituciones bancarias dentro de RedBanc, ya que todos los del Banco cuentan con anti-skimming, siendo casi imposible el robo de información. En cuanto a los fraudes electrónicos como spyware, keylogger y ataques a la infraestructura de los cajeros automáticos TI, no se obtuvo información, ya que son fraudes relacionados únicamente con las deficiencias de seguridad del usuario en su equipo computacional, para los dos primeros casos; en cuanto al tercero, el banco no cuenta con información ni estadísticas.

Para prevenir la ocurrencia de los fraudes mencionados, las entidades bancarias deben ajustar permanentemente sus sistemas de seguridad a las exigencias de la actualidad, contando con plataformas tecnológicas que garanticen la seguridad de las transacciones efectuadas por sus clientes y que ofrezcan un mejor servicio. Es así como el Banco utiliza elementos de seguridad para resguardar la información confidencial de cada uno de sus clientes y de las numerosas transacciones que se realizan: entre ellas se encuentra el anti-phishing/anti-pharming, el protocolo seguro de transferencia de hipertexto y el encriptamiento de datos, con excepción de las tarjetas bancarias inteligentes, el que se encuentra en observación para su posterior lanzamiento a sus usuarios. De forma adicional, el banco informa de otros dos elementos para resguardar la seguridad del cliente: el uso de la tercera clave y el anti-skimming; la primera permite al usuario validar la transacción que está efectuando por internet a través del ingreso de una clave secreta temporal enviada a su dispositivo móvil y la segunda es utilizada en los cajeros automáticos, cuya función es codificar la información contenida en la banda magnética de las tarjetas con el fin de evitar su clonación y robo de información.

En relación a lo planteado en el marco teórico, al ser la auditoría forense aquella rama que orienta a participar y contribuir en la investigación de diversos fraudes, la importancia de utilizarla en los servicios electrónicos del Banco es que aceleraría los procesos de investigación de grandes fraudes, ya que llevarlos a un problema en específico con un cliente demandaría mayores costos y tiempo, siendo más conveniente realizar una auditoria forense a aquellas situaciones y transacciones más críticas para el Banco, debido a que son muchos los movimientos de dinero que se efectúan diariamente.

Si bien la aplicación de diversas técnicas de investigación concede al auditor forense el conocimiento y la experiencia para obtener indicadores de fraudes, según lo expuesto en el marco teórico esta entidad bancaria aplica técnicas de investigación relacionadas con la auditoría forense, utilizando de forma muy frecuente, las técnicas de; verificación ocular, verificación física y la verificación

informática. Todas estas tomadas en cuenta desde el punto de vista electrónico, en donde la institución bancaria observa a sus empleados, inspecciona y analiza minuciosamente que todo proceso y programa informático se realice de acuerdo a la normativa vigente de seguridad adoptada por el Banco, con el fin de evitar fallas en los sistemas y tener una plataforma estable. En cuanto a la técnica de verificación verbal, esta se aplica frecuentemente realizando encuestas y entrevistas a los nuevos trabajadores para confirmar el cumplimiento de la normativa de seguridad y calidad de información que exige el Banco. Finalmente, aquellas que menos efectúa el Banco son las de verificación escrita y documental, por la razón que toda la información se hace y se obtiene a través de procesos informáticos.

CONCLUSIONES

Luego de efectuar los respectivos análisis y discusiones de los resultados obtenidos, es posible exponer las conclusiones que dan cumplimiento a los objetivos planteados en la investigación.

Al comparar aquellas transacciones electrónicas que presentan un mayor y menor riesgo de fraude para el Banco se observa que aquellas efectuadas por la banca en línea lideran los índices de riesgo. Mientras que las transacciones por cajeros automáticos son la que presentan el menor índice de fraude, esto último gracias a que todos los cajeros de la institución tienen tecnología anti-skimming, lo que dificulta el robo de información por parte de terceros. Sin ir más lejos, también están en la lista las transacciones que se ejecutan por Caja Vecina, las cuales son consideradas como las de mayor y menor riesgo según el punto de vista que se trate. Por una parte, se consideran las de mayor riesgo por la sencilla razón de que no hay un control físico permanente en los terminales de este canal y, por otro son consideradas las de menor riesgo por las características específicas que se presentaron.

En base a la comparación anterior, se puede señalar que los bancos deben ir ajustando sus sistemas de seguridad en relación al avance de la tecnología, implementando diversos elementos de seguridad para otorgar un mejor servicio a sus clientes y que les ayude a prevenir los fraudes electrónicos. Para ello, las instituciones bancarias utilizan: (a) anti-phishing/anti-pharming cuya principal característica es combatir el phishing y pharming, respectivamente, a través de la utilización de software especializados y con la protección a los sistemas de nombres de dominio (DNS), los que bloquean páginas web fraudulentas y verifican que los nombres de dominio de cada sitio web concuerden con sus direcciones IP ya registradas; (b) las tarjetas bancarias inteligentes, que al contener un microchip no es posible el traspaso de información de manera estándar a otro chip evitando así el ser clonadas; (c) el protocolo seguro de transferencia de hipertexto más conocido como “HTTPS”, el cual protege la información que se encuentra en las página web, creando canales de comunicación seguros entre el usuario y la web del banco; y por último, (d) la encriptación de datos, que consiste en la codificación de datos a una forma en que es imposible leerla por cualquier persona, a menos que cuente con conocimientos especiales y certificados de seguridad propios del banco para poder desencriptarlos.

La existencia de todos estos elementos de seguridad se relacionan completamente

con los fraudes electrónicos, ya que ayudan tanto a que las instituciones bancarias disminuyan los índices de fraudes, como a que los clientes confíen más en los medios electrónicos que ofrecen los bancos al momento de realizar transacciones por cualquier medio, sin preocuparse de ser víctima de un posible fraude.

El Banco aplica los elementos de seguridad antes expuestos, siendo la única excepción la tarjeta bancaria inteligente. Pero, de forma adicional a esos componentes, utiliza otros dos elementos de seguridad no definidos en esta investigación: el anti-skimming y la tercera clave. El primer elemento tiene la característica de codificar la información contenida en la banda magnética de las tarjetas bancarias con el fin de evitar su clonación y a la vez el robo de información, mientras que en el segundo la particularidad, es validar la transacción que el cliente efectúa por internet a través del ingreso de una clave secreta temporal que es enviada a su teléfono celular la que permite finalizar la transacción web. Junto a ello, la institución usa técnicas de investigación de auditoría forense para obtener conocimientos de la existencia de fraudes pero no las aplica bajo ese nombre en específico, sino más bien como procedimientos de control para verificar que los procesos y programas informáticos se desarrollen de acuerdo a la normativa vigente de seguridad implementada, con el fin de evitar fallas en los sistemas y que los datos tratados por los programas no sean usados por defraudadores.

En el marco de lo expuesto, se puede considerar al Banco como una institución que invierte en seguridad, ya que continuamente se encuentra inspeccionando sus sistemas ante vulnerabilidades e invirtiendo en ellos con el objeto de tener tecnología reciente que vaya a la par con las nuevas formas para realizar fraudes electrónicos.

BIBLIOGRAFÍA

- Arens, A; Randal, E; Mark, B. (2007). Auditoría. Un enfoque integral. Decimoprimera edición. México. Prentice-Hall.
- Auditing Standars Board. (1997). Statements on Auditing Standars N° 82. Consideraciones sobre el Fraude en una Auditoría de Estados Financieros.
- Auditing Standars Board. (2002). Statements on Auditing Standars N° 99. Consideración del fraude en una intervención del Estado Financiero.
- ACFE. (2014). Report to nations on occupational fraud and abuse. Disponible en: http://www.acfe.com/rttn/docs/2014-report-to-nations.pdf
- Albarracín, P. (2013). La batalla de la analítica contra el fraude bancario. Disponible en: http://tecno.americaeconomia.com/noticias/la-batalla-de-la-analitica-contra-el-fraude-bancario
- Álvarez, F. (2010). Fraudes Bancarios. Impacto en el resto de las Entidades del Sistema Financiero. Mitigación del Riesgo y Sanciones Aplicadas. Disponible en: http://www.felaban.com/archivos_actividades_congresos/11.pdf
- Antonio, I; Jardon, C; Martínez, M; Montiel, A; Velazquillo, M. (2009). Auditoría forense. Informe final que para obtener el título de contador público. Escuela Superior de Comercio y Administración. Instituto Politécnico Nacional- México D.F. Disponible en: http://tesis.bnct.ipn.mx/dspace/bitstream/123456789/4547/1/AUDITFORENSE.pdf
- ASBANC. (2013). Las tarjetas con chip: Mayor seguridad para las transacciones. Disponible en: http://www.asbanc.pe/ContenidoFileServer/ASBANC%20SEMANAL%20N%C2%BA78_20130913030409566.pdf
- ASOBANCARIA. (2009). Modalidades del fraude bancario y recomendaciones para su prevención. Disponible en: http://www.asobancaria.com/portal/pls/portal/docs/1/776080.PDF
- Asociación de supervisores bancarios de las Américas. (2009). Riesgo operacional en instituciones bancarias. Disponible en: http://www.ccsbso.org/sites/default/files/g6_es.pdf

- Badillo, J. (2008). Auditoría forense, más que una especialidad profesional una misión: prevenir y detector el fraude financiero. Disponible en: https://na.theiia.org/translations/Spanish%20Documents/Auditoria_Forense_Una_Misi%C3%B3n_JBadillo_Mayo08%2814023%29.pdf

- BancoEstado. (2010) ¿Qué es CajaVecina? Disponible en: http://www.bancoestado.cl/CDCBF770095146CD8DE974DEB97B9BDA/E72F5C5AFFA341C995EC39427259E51C/articulo/14135.asp

- Becerra, A; Cárdenas, L. Rol del contador auditor, en la aplicación de la justicia. Disponible en: https://docs.google.com/document/d/1KEV3XzAlN0XJGjWc4livNMfIKtNhv0rWvyM66fEv3UM/edit?hl=es

- Borrajo, M. (2002). La auditoría interna y externa. Partida doble. Número134, pág. 50 a 59. Disponible en: http://pdfs.wke.es/4/5/6/2/pd0000014562.pdf

- Callegari, O. (2007). Delitos informáticos: Pharming. Disponible en: http://www.rnds.com.ar/articulos/031/RNDS_176W.pdf

- Cepeda, G. (1997). Auditoría y control interno. Colombia. McGraw-Hill.

- Christiansen. A. (2014). Delitos informáticos se reducen 43% en últimos tres años en Chile. La Tercera. Disponible en: http://www.latercera.com/noticia/tendencias/2014/02/659-565552-9-delitos-informaticos-se-reducen-43-en-ultimos-tres-anos-en-chile.shtml

- Comisión técnica especial de ética pública, probidad administrativa y transparencia, CEPAT. (2005). La auditoría forense, herramienta de las EFS en la lucha contra la corrupción. San Salvador. Disponible en: http://www.contraloria.cl/NewPortal2/portal2/ShowProperty/BEA%20Repository/Sitios/Olacefs/Cepat/doc/PONENCIAS/Historico/Auditoria_Forense.pdf

- Comité de Basilea para la Supervisión Bancaria. (1998). Gestión de riesgos para la banca electrónica y actividades con dinero electrónico. Disponible en: http://pdf.edocr.com/e288a76a41d89b526784144297ed6df01bf55f92.pdf

- Díaz, J. (2005). La ley Sarbanes-Oxley y la Auditoría. Partida doble. número 169, pág. 104 a 109. Disponible en: http://pdfs.wke.es/5/3/4/4/pd0000015344.pdf

- Domingos, F. (2013). Comercio electrónico y pago mediante tarjeta de crédito en el ordenamiento jurídico español: una propuesta para su implementación en el ordenamiento jurídico de Guinea-Bissau. Tesis doctoral. Universidad Carlos III de Madrid. Disponible en: http://e-archivo.uc3m.es/bitstream/handle/10016/16963/Fernandinho_Domingos_Sanca_tesis.pdf?sequence=1

- Echenique, J. (2001). Auditoría en Informática. México. McGraw-Hill.

- Fontán, E. (2008). El impacto de la Auditoría Forense como técnica de prevención, detección y control del fraude. Disponible en: http://www.ideaf.org/archivos/ideaf_impacto_af_prev_det_cont_fraude.pdf

- Guillermo, P. (2008). Cómo funciona un cajero automático. Disponible en: http://codigopgt.wordpress.com/2008/03/05/como-funciona-un-cajero-automatico/

- Instituto de capacitación y desarrollo en Fiscalización Superior. (2011). Introducción a la auditoría forense. Disponible en: http://www.ofsnayarit.gob.mx/capacitacion/2011/material0328_1.pdf

- Jolly, J; Lau, O. (2013). Técnicas para la prevención de fraude electrónico en instituciones financieras. Panamá. Disponible en: http://www.felaban.com/archivos_actividades_congresos/CLAIN%202013%20-%20J.Jolly%20-%20O.pdf

- Leal, J. (2012). Impacto de la banca electrónica en el rendimiento y perfil de riesgo de la gestión bancaria de Banesco, Banco Universal. Universidad Centroccidental Lisandro Alvarado. Barquisimeto. Disponible en:

- López, W; Sánchez; J. (2012). El triángulo del fraude. Vol.17 (N°1), PP. 65-81. Puerto Rico.

- Mendoza, V. (2012). Los 5 fraudes más temidos por los bancos. Ciudad de México. México. Disponible en: http://www.cnnexpansion.com/mi-dinero/2012/06/20/los-5-fraudes-mas-temidos-por-los-bancos

- Ministerio de justicia. (1993). Ley 19223: Tipifica figuras penales relativas a la informática, Disponible en: http://www.leychile.cl/Navegar?idNorma=30590

- Montilla, O; Herrera, L. (2006). El deber ser de la auditoria. Estudios

gerenciales, 98, pp. 83-110, Business Source Complete, EBSCO.

- Morchio, D. (2013). Código malicioso: la nueva forma de realizar fraudes bancarios. Pulso. Disponible en: http://www.pulso.cl/noticia/empresa-mercado/empresa/2013/09/11-30054-9-codigo-malicioso-la-nueva-forma-de-realizar-fraudes-bancarios.shtml

- Muñoz, M. (2013). Estafas bancarias por internet: Los métodos más usados en Chile. Emol. Disponible en: http://www.emol.com/noticias/economia/2013/04/08/592283/conozca-los-metodos-mas-utilizados-por-los-estafadores-bancarios-de-internet-en-chile.html

- Norma de Auditoría Generalmente Aceptada. (2012). NAGA 63, sección 240. Responsabilidad del auditor de considerar el fraude en una auditoría de EE.FF.

- Navajo, R. (2011). Combatir el fraude en los cajeros automáticos. Revista dintel. Número 18. Disponible en: http://www.revistadintel.es/Revista/Numeros/Numero18/old/rnavajo.pdf

- Recovery Labs. (2012). Peritaje informático-estadísticas. Madrid. España. Disponible en: http://www.delitosinformaticos.info/peritaje_informatico/estadisticas.html

- Recovery Labs. (2012). Phishing: Fraude en internet. Madrid. España. Disponible en: http://www.recoverylabs.com/informes/Recovery_Labs_phishing.pdf

- Recovery Labs. (2012). Fraude en internet: del phishing al pharming. Madrid. España. Disponible en: http://www.recoverylabs.com/informes/Recovery_Labs_pharming.pdf

- Piattini, M; Del Peso, E. (1998). Auditoría informática: un enfoque práctico. México. Alfaomega.

- Rojas, J. (2012). Técnicas de Auditoría Forense. Paraguay. Disponible en: http://sitios.poder-judicial.go.cr/auditoria/documentos/XVI_CLAIPARAGUAY_2012/Jos%C3%A9%20Luis%20Rojas-T%C3%A9cnicas%20de%20Auditor%C3%ADa%20Forense.pdf

- Rozas, A. (2009). Auditoria Forense. Revista de la Facultad de Ciencias Contables. Vol.16 (N°32), PP. 73-101. Lima, Perú. Versión electrónica ISSN: 1609-8196.

- Superintendencia de Bancos e Instituciones Financieras. (2012). Evolución de los Medios de Pago. Disponible en: http://www.sbif.cl/sbifweb/servlet/InfoFinanciera?indice=C.D.A&idContenido=12703

- Torres, E. y Vásquez, A. (2005). Integrando los Beneficios para el Cliente de Servicios Bancarios: Banca tradicional Versus Banca en internet. Vol.23 Issue 31, p2-p26.25p. Business Source Complete, EBSCO.

- Traverso,j. (2008). Breve historia de los Bancos en Chile. Ebanking News. Disponible en: http://www.ebanking.cl/columnas/breve-historia-de-los-bancos-en-chile-003