UNIVERSIDAD DE VALPARAÍSO

FACULTAD DE CIENCIAS ECONÓMICAS Y ADMINISTRATIVAS

ESCUELA DE AUDITORÍA

"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"

TESIS PARA OPTAR AL TÍTULO DE CONTADOR PÚBLICO AUDITOR Y AL GRADO DE LICENCIADO EN SISTEMAS DE INFORMACIÓN FINANCIERA Y CONTROL DE GESTIÓN

TESISTA: ROCÍO ISABEL DÍAZ CÉSPEDES

PROFESOR GUÍA: ARTURO CORNEJO ARANDA

VALPARAÍSO, 2014

Agradezco a Dios por otorgarme la sabiduría, paciencia y demostrarme que en esta vida todo es posible.

A mí Madre, por su apoyo incondicional, por sus consejos y por enseñarme que el confiar en mis aptitudes es lo primordial para lograr el éxito.

A mí querida Mami, por su atención y la continua preocupación por mis estudios.

Le doy gracias a mí familia en general, por darme tantas instancias de alegrías y por su constante apoyo.

Finalmente, agradezco a todas aquellas personas importantes en mi vida que hicieron posible que este sueño se hiciera realidad.

TABLA DE CONTENIDOS

RESUMEN

A raíz de la necesidad de efectuar transacciones bancarias de forma rápida, sencilla y de cualquier lugar, las entidades bancarias han tenido que invertir en medios acorde a las nuevas tecnologías y necesidades de sus clientes, siendo un ejemplo la banca en línea. 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. Por lo tanto, es necesario contar con las medidas de seguridad y la aplicación de las técnicas de investigación de fraudes para evitar este suceso y otros similares.

Bajo este contexto, se analizaron 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 con alcance de sintetización, el 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 con estrecha relación en transacciones electrónicas sobre temas de fraudes electrónicos, elementos de seguridad, transacciones electrónicas y técnicas de investigación de auditoría forense, se procedió a concluir en base a los objetivos establecidos.

Para finalizar, los resultados indican que la institución bancaria utiliza, tanto la mayoría de las técnicas de investigación de auditoría forense indagadas, como los elementos de seguridad descritos en la teoría 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, considerándose a nivel de la banca nacional, como aquella entidad en que constantemente se encuentra invirtiendo en nuevas tecnologías con el fin de dar una mayor seguridad y tranquilidad a sus clientes al realizar transacciones electrónicas.

CAPÍTULO I: MARCO TEÓRICO

ANTECEDENTES GENERALES

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 electrónicas 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, nacen nuevos fraudes, especialmente los de tipos electrónicos que amenazan la seguridad de los bancos del país afectando principalmente a sus clientes, por ello estas entidades deben buscar nuevas herramientas, como por ejemplo el anti-phishing, la encriptación de datos o técnicas de investigación de auditoría forense, entre otras, para prevenir y combatir esos fraudes en particular.

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.

Es necesario el conocimiento y desarrollo de esta auditoría para comenzar a combatir y erradicar los actos de corrupción, tanto en el sector público como el privado que perjudiquen el interés de la sociedad.

Causas y origen de la auditoría forense

La auditoría forense surge a raíz de la unión de diversos factores adversos de origen social y contable que favorece los actos de corrupción, fraude y lavado de dinero, afectando tanto a personas, empresas y gobiernos, generando como consecuencia daño a su imagen. El origen de este tipo de auditoría se remonta hacia muchos años atrás, relacionándose con la creación del *Código de Hammurabi*, el cual da a entender en sus fragmentos del 100 al 126 el concepto básico de la auditoría forense "el demostrar con documentación contable un fraude o mentira", indicando además cálculos de ganancias y pérdidas de los negocios siendo necesario la ayuda de un contador, condenando así el fraude o mentira del que negaba haber recibido el pago haciéndole pagar hasta seis veces el monto.

Existen muchos tratados e historiadores de la contabilidad, pero no de la auditoría forense, ya que además en un momento determinado los tribunales no se enfocaban en la búsqueda de evidencia para demostrar la culpabilidad de las personas, razón por la cual existe un vacío enorme en la auditoria forense. Es por ello, que esta rama de la auditoría repuntó en los años 30; época en la cual el crimen organizado prosperó, ganando millones de dólares utilizando prácticas criminales. Este pequeño repunte fue provocado por el arresto de Alphonse Gabriel Capone, más conocido como "*Al Capone*", quien lavaba dinero y permitía vivir como magnates a sus jefes; para encarcelar a "*Al Capone*", el contador del Departamento de Impuestos utilizó la Ley de Impuestos para inculparlo, por lo que recopiló evidencia encontrándose con cuentas de un negocio que lavaba y planchaba el dinero y libros de pagos comprobándose que el volumen de las ventas superaba la capacidad teórica del negocio de los lavadores, por lo que el volumen de ventas real no coincidían con el volumen de ventas declarado. El contador al demostrar el fraude en el pago de impuestos desmanteló la organización.

Aún con este tipo de crímenes de la época, la auditoría forense tuvo su gran impulso entre los años 70 y 80 surgiendo como herramienta para suministrar pruebas a los fiscales, como por ejemplo el caso *Watergate* en 1972 que inició el análisis del fraude en los estados financieros. (Becerra, Cárdenas; 2007).

Características de la auditoría forense

Jorge Badillo (2008) clasifica las características principales de la auditoría forense de acuerdo a su:

- Propósito: Prevenir y detectar el fraude financiero.

- Alcance: Corresponde al período que cubre el fraude financiero sujeto a investigación.

- Orientación: Puede ser retrospectiva en relación al fraude financiero auditado; y prospectiva en cuanto a recomendar la implementación de los controles preventivos, detectivos y correctivos necesarios para evitar futuros fraudes financieros.

- Normatividad: Las normas de auditoría financiera e interna que son aplicables como: normas de investigación, legislación penal, disposiciones normativas relacionadas con los fraudes financieros, entre otras.

- Enfoque: La auditoría puede ser preventiva y/o detectiva para combatir la corrupción financiera, ya sea pública o privada.

- Auditor a cargo: La realizará un contador público, abogado u otro profesional calificado.

- Equipo de apoyo: Será un equipo multidisciplinado compuesto por: abogados, auditores informáticos, investigadores públicos o privados, criminalistas, agentes de oficinas del gobierno, miembros de inteligencia y especialistas de diferentes campos de acuerdo a las necesidades de la investigación.

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:

- Identificar, demostrar y sustentar el fraude o ilícito realizado.
- Prevenir y reducir el fraude, a través de la implementación de las recomendaciones de fortalecimiento de control interno propuestas por el auditor.
- Participar en el desarrollo de los diferentes programas de prevención de pérdidas y fraudes.
- Participar en la evaluación de sistemas y estructuras de control interno.
- Recopilar evidencias necesarias aplicando diversas técnicas de investigación.
- 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.

Técnicas de investigación

La aplicación de diversas técnicas de investigación concede al auditor forense el conocimiento y experiencia necesaria para desarrollar diferentes habilidades, a fin de establecer indicadores pertinentes de fraude y obtener evidencias suficientes para sustentar las pruebas. (Fontán; 2002).

Entre las técnicas de investigación se encuentran:

- Técnicas de verificación ocular: Conformada por la observación, revisión analítica, comparación y rastreo del desarrollo de procesos, procedimientos y actividades.

- Técnica de verificación verbal: Consiste en obtener información oral de la entidad a través de entrevistas, encuestas o cuestionarios realizados a empleados o terceros.

- Técnica de verificación escrita: Corresponde a analizar, conciliar y confirmar la información lógica otorgada por funcionarios internos o externos con el fin de identificar que sea válida, verdadera, idónea y auténtica en relación a las operaciones sujetas a comprobación.

- Técnica de verificación documental: Consiste en obtener de la entidad documentación escrita para soportar las afirmaciones, análisis, procesos o estudios realizados por los auditores, con el fin de comprobar que los documentos justifican o sustentan una operación o transacción.

- Técnica de verificación física: Consiste en inspeccionar la manera en cómo los responsables desarrollan y documentan los procesos o procedimientos de la ejecución de las actividades.

- Técnica de verificación informática: El crecimiento tecnológico e informático es cada día más rápido, lo que da lugar al aumento de delitos y fraudes informáticos, por lo tanto, para que la evidencia digital sea aceptada por la justicia, se deberán aplicar técnicas forenses muchos más rigurosas para asegurar la confidencialidad, confiabilidad e integridad absoluta de los datos obtenidos. De acuerdo a ello, las técnicas más utilizadas son: observación y análisis de datos, revisión selectiva, conciliaciones, comparaciones y el rastreo en sistemas de comunicación electrónica.

Normativa relacionada a la auditoría forense

Actualmente para la auditoría forense no existe un cuerpo definido de principios y normativas aplicables, sin embargo este tipo de auditoría se debe apoyar en las Normas de Auditoría Generalmente Aceptadas (NAGAS) y de manera especial en normas referidas al control, prevención, detección y divulgación de fraudes, tales como las Declaraciones de Normas de Auditoría o Statements on Auditing Standars (SAS).

- SAS N° 82 "Consideraciones sobre el Fraude en una Auditoría de Estados Financieros".

Esta norma entró en vigencia a partir del año 1997, proporcionando la orientación respecto de las responsabilidades del auditor independiente con respecto al fraude material. Requiere que aquellos auditores realicen una evaluación específica sobre el riesgo de uso incorrecto de los estados financieros en relación a 40 factores de riesgos específicos de fraudes los que incluyen a la administración, la industria y características operacionales; específicamente, se le solicita que realice averiguaciones sobre la administración con relación al riesgo de posible fraudes y que documente en los papeles de trabajo cualquier factor de riesgo identificados y la reacción del auditor ante esos factores de riesgo.

A raíz de los nuevos requerimientos, los auditores invertirían más tiempo en cuestiones de fraudes, ya que a los pasos de ejecución de la auditoría incluirán la determinación sobre cómo el cliente previene, impide y detecta el fraude, aumentando la verificación independiente, las observaciones físicas y el tamaño de las muestras; efectuando visitas no anunciadas y pruebas por sorpresa; realizando una revisión detallada de los asientos contables de cierre y aumentando las revisiones de los asientos de ajuste de fin del ejercicio.

La administración es la principal responsable sobre la prevención y detección del fraude en la entidad, detectándolos a través de los controles internos y porque otros empleados notan de los mismos o por los auditores internos. Por lo tanto, la administración debe asegurarse que sus controles contables y administrativos están

diseñados para limitar las oportunidades de fraude, ya que si no existen controles es más probable que existan incentivos para la ejecución del fraude y una oportunidad percibida de hacerlo. Si a su vez el auditor determina que un cliente ha cometido fraude financiero, deberá considerar el efecto posible del fraude e informar del mismo al encargado de administración del cliente y al comité de auditoría o al consejo de directores. (SAS 82; 1999).

- SAS 99 “Consideración del fraude en una intervención del Estado Financiero”.

Esta norma reemplaza la SAS N° 82 “Consideraciones sobre el Fraude en una Auditoría de Estados Financieros”, enmienda a la SAS N°1 “Consideración de normas y procedimientos de Auditoría” y SAS N°85 “Representaciones de la Gerencia”, entrando en vigencia en el año 2002. Aunque no modifica la responsabilidad del auditor para detectar fraudes significativos en una auditoría de estados financieros ni los requisitos de informar del auditor cuando haya evidencia de fraude, incorpora cambios significativos en los procedimientos y la documentación de una auditoria de estados financieros.

Menciona que la Gerencia es responsable de establecer un ambiente y controles adecuados, crear y mantener una cultura de honestidad y ética. Además, indica los puntos o divisiones referidas a las obligaciones y recomendaciones que debe seguir el auditor, en cuanto a la descripción de las características del fraude, la importancia de ejercer el escepticismo profesional, la importancia de debatir con el equipo de auditores sobre los riesgos de errores materiales debidas al fraude, el cómo obtener la información necesaria para identificar los riesgos de errores materiales debido al fraude, en la evaluación de los riesgos que se han identificado, dar una respuesta a los resultados de dicha evaluación, evaluar la evidencia de auditoría, comunicar sobre el fraude a la gerencia y/o comité de auditoría y documentar las consideraciones del auditor sobre el fraude. (SAS 99, 2003).

- NAGA 63, sección 240 “Responsabilidad del auditor de considerar el fraude en una auditoría de Estados Financieros”.

Esta norma trata sobre las responsabilidades del auditor en relación con el fraude en una auditoria de estados financieros. Aquellas representaciones incorrectas que en los estados financieros pueden surgir, ya sea por fraude o por error, siendo el factor que los distingue es si la acción subyacente que resulta en una representación incorrecta de los estados financieros es intencional o no. Al auditor le preocupa el fraude que resulta de una representación incorrecta significativa en los estados financieros, teniendo en consideración aquellas representaciones incorrectas, que del proceso de preparación y presentación de información financiera de la entidad, resultan en información financiera fraudulenta y aquellas representaciones incorrectas resultantes de la apropiación indebida de activos.

Adicionando, esta sección indica que la principal responsabilidad por prevenir y detectar el fraude corresponde tanto a los encargados del Gobierno Corporativo de la entidad como también a la administración. Es de gran importancia que la administración dé énfasis en la prevención de fraude, que pueda reducir las oportunidades para que ocurra un fraude y en la disuasión de ellos, persuadiendo a las personas a no cometer fraudes debido a la probabilidad de detección y castigo. En cuanto a la supervisión por parte del Gobierno Corporativo incluye considerar el potencial para hacer caso omiso de los controles y otra influencia inapropiada sobre el proceso de preparación y presentación de información financiera.

Relacionado con las responsabilidades del auditor, aquel auditor que realiza una auditoría de acuerdo a las NAGAS es responsable por obtener una seguridad razonable que los estados financieros en su conjunto están libres de representaciones incorrectas significativas, causadas por fraude o por error. El riesgo de no detectar una representación incorrecta significativa resultante de un fraude, es mayor al riesgo de no detectar una representación incorrecta significativa resultante de un error, debido a que el fraude puede involucrar esquemas sofisticados y cuidadosamente organizados, diseñados para ocultarlos, como por ejemplos falsificación o la entrega intencionada de representaciones incorrectas al auditor. La capacidad del auditor para detectar un fraude

depende de diversos factores, tales como la destreza del perpetrador, la frecuencia y el alcance de la manipulación, el tamaño de los montos individuales manipulados y la posición jerárquica de esos individuos involucrados. (NAGA 63; 2012).

Los principales objetivos del auditor son:

A. Identificar y evaluar los riesgos de las representaciones incorrectas significativas de los estados financieros debido a fraude,

B. Obtener suficiente y apropiada evidencia de auditoría respecto de los riesgos evaluados de representaciones incorrectas significativas debido a fraude, mediante el diseño e implementación de respuestas apropiadas, y

C. Responder apropiadamente a fraude o sospechas de fraude identificados durante la auditoría.

- Ley Sarbanes-Oxley

La ley Sarbanes-Oxley (también denominada "Ley SOX") fue propuesta por el senador Paul S. Sarbanes y el diputado Michael G. Oxley; de ahí su nombre. Fue aprobada en el gobierno de George W. Bush en Julio del 2002, surgiendo principalmente para responder a diversos escándalos financieros que afectaron a empresas estadounidenses, como lo es el caso Enron durante el año 2001 y principios del 2002, con el fin de proteger a los accionistas que cotizan en la Bolsa de Valores de los Estados Unidos, a través de la estructuración de un marco de requerimientos aumentando el nivel de confiabilidad de la información financiera proporcionada por las empresas.

La ley se agrupa en seis grandes áreas que afectan a todas las sociedades cotizadas en los mercados americanos, los cuales se mencionan a continuación:

1. Mejorar la calidad de la información pública y los detalles de la misma: La información presentada debe estar certificada por los directivos de la sociedad,

legitimando su responsabilidad y corrección en relación a los informes trimestrales y anuales, que los estados financieros no contengan omisiones o errores, de ser así, comunicar a los auditores y al Comité de Auditoría sobre estos hallazgos y que controlen la información enviada al mercado. Al realizar la evaluación del control interno este debe estar valorado, documentado y certificado por la dirección de la sociedad y auditado por el auditor de cuentas, quien opinará sobre la eficiencia de aquel control a la fecha de cierre de los estados financieros. Aquellos cambios de información, que tengan impactos significativos, tanto en las diversas operaciones de la sociedad o en los estados financieros, deben ser informados de forma rápida y efectiva.

2. Reforzar las responsabilidades del gobierno corporativo de las sociedades: Se incrementarán las comunicaciones directas entre el auditor y el Comité de Auditoría sobre temas relacionado con políticas contables significativas o tratamientos contables alternativos. En cuanto a los Comités de Auditoría deberán ser responsables directos al momento de designar, retribuir y supervisar al auditor, establecerán un sistema que recogerá denuncias anónimas y cada miembro debe ser consejero independiente. Los gobiernos deben contar, por obligación, con expertos financieros en el comité de auditoría e informar quienes poseen experiencia.

3. Mejorar la conducta y comportamiento éticos exigibles: Será ilegal cualquier acción de cualquier consejero o directivo que se encuentre destinada a influir de forma fraudulenta, confundir o manipular intencionadamente al auditor. Se debe cumplir obligadamente el código de ética por los ejecutivos del área financiera, cualquier incumplimiento a dicho código debe ser informada públicamente. Frente a esto, se dará una protección especial a los que realicen denuncias anónimas de conductas ilícitas.

4. Incremento de la supervisión a las actuaciones en los mercados cotizados: A través de la creación de un organismo público de supervisión, Public Company Acounting Oversight Board (PCAOB), teniendo la capacidad de supervisar y establecer los estándares de auditoría, controles de calidad y normas de éticas. La

compañía que quiera auditar sociedades cotizadas en mercados americanos, deberá estar inscrita en el PCAOB. Además, éste desplegará programas de supervisión de la labor que cumplan las auditoras para comprobar su efectivo cumplimiento, de acuerdo a los estándares profesionales. Extensión de las responsabilidades para los abogados: tendrán la obligación de informar cualquier evidencia que exista sobre incumplimiento a las leyes.

5. Aumento del régimen sancionador que se asocia a incumplimientos: Se extienden los plazos para perseguir un fraude cometido e/o identificado. Responsabilidades penales por manipular, alterar o destruir documentos que impidan una investigación oficial. Aumento significativo en las sanciones a los auditores por no facilitar información o cooperar con la investigación.

6. Aumento de las exigencias y presiones sobre la independencia efectiva de los auditores: Total prohibición para que el auditor de cuentas pueda prestar ciertos servicios a sus clientes. El socio firmante y el revisor deberán rotar cada 5 años. Se crean restricciones de importancia para que una entidad contrate personal del equipo de auditoría sin que esto pueda suponer un posible problema de independencia para la firma auditora.

La ley SOX se aplica a todas las empresas norteamericanas y extranjeras que cotizan en la bolsa de valores de Estados Unidos, incluyendo a la casa matriz, subsidiarias y sus afiliadas. Será aplicable a las empresas chilenas cuando ellas coticen en la bolsa de Estados Unidos y son subsidiarias o afiliadas de empresas que cotizan en aquella bolsa. (Díaz; 2005).

Enfoques de la auditoría forense

La auditoría forense, al ser una auditoría especializada, está compuesta por dos enfoques, siendo uno el preventivo y otro el detectivo:

- Auditoría forense preventiva

Está orientada a proporcionar aseguramiento o asesoría a diferentes organizaciones en cuanto a su capacidad para disuadir, evitar, detectar y reaccionar ante diferentes tipos de fraudes, desarrollándose programas de prevención y manejo de riesgos de fraudes, esquemas de alerta temprana de irregularidades, establecer un código de conducta y sistemas de administración de denuncias.

Este enfoque se considera proactivo, por cuanto conlleva a la toma de decisiones y acciones en el presente con el fin de evitar fraudes en el futuro. (Badillo; 2008).

- Auditoría forense detectiva

Está orientada a identificar la existencia de fraudes a través de una profunda investigación, logrando: determinar la cuantía del fraude; el impacto (en los sistemas y su daño económico); el tipo de fraude; los presuntos autores, cómplices y encubridores; y documentar los hechos o indicios de fraude. Generalmente, los resultados arrojados por el trabajo de este tipo de auditoría son considerados por la justicia, la que se encargará de analizar, juzgar y dictar la sentencia respectiva.

Este enfoque es reactivo, por cuanto implica tomar acciones y decisiones en el presente por fraudes que han sucedido en el pasado. (Badillo; 2008).

AUDITOR FORENSE

De acuerdo a Danilo Lugo en “Técnicas de Auditoría Forense” citado por José Luis Rojas (2012), el auditor forense corresponde a un auditor financiero con preparación técnica-forense, considerado como testigo importante frente a una Corte y capacitado en modalidades criminales, principalmente en delitos económicos y financieros.

Perfil del auditor forense

El auditor forense debe ser un profesional imparcial, con independencia en cuanto al proceso que es llevado a cabo, debe poseer la competencia y preparación de un experto en el área, con la experiencia necesaria para ser capaz de revisar los diversos hechos acontecidos y así proporcionar una opinión, que es utilizada para la toma de decisiones. Además, debe poseer múltiples habilidades y competencias en cuanto al conocimiento del negocio, comprendiendo el funcionamiento y la forma de planificar; adoptar una mente estratégica, obtener conocimiento avanzado en las tecnologías de información, adoptar técnicas innovadoras de auditoría para prevenir hechos delictuosos y desarrollar habilidades de investigación en relación a los tipos de fraudes y delitos que se pueden cometer en las entidades, principalmente en sus áreas vulnerables. En cuanto a las destrezas que el auditor forense adopta, se encuentra la agudeza, escepticismo profesional, análisis crítico, la profundidad de análisis, búsqueda de indicios, visualizador de riesgos y la capacidad de observar y explorar aquellas áreas de información valiosa para la entidad. (Instituto de Capacitación y Desarrollo en Fiscalización Superior; 2011).

Para Badillo (2008), el auditor forense debe ser un profesional altamente capacitado (conocedor de temas contables, de control interno, de finanzas, de tributación, de auditoría, de informática, sobre las técnicas de investigación; entre otras disciplinas). En relación a la formación como persona, debe ser objetivo, independiente, justo, honesto, analítico, planificador, inteligente, astuto, prudente y precavido. En cuanto a la experiencia y conocimiento, debe ser intuitivo, sospechar de todo y de todas las personas, debe identificar oportunamente cualquier indicio de fraude, siendo su trabajo guiado por el escepticismo profesional.

Riesgos y responsabilidades del auditor forense

Debido a la naturaleza de la auditoría forense, la cual se desarrolla bajo un estrecho vínculo con la justicia es de gran importancia distinguir el tipo de compromiso que debe asumir el auditor.

Es así que en una disputa judicial, siendo un conflicto potencial entre partes de las cuales se sospecha de algún ilícito o actividad ilegal que si se materializa se puede establecer fuera de la corte o puede llevarse a los procedimientos judiciales, existen varios involucrados que se relacionan con el trabajo del auditor forense. Por un lado se encuentra la parte que realiza las alegaciones o que tiene sospechas demostrando que se cometió algún hecho doloso o que haya sufrido una pérdida, mientras que por el otro lado está la parte contra quien se hace las alegaciones o se tienen las sospechas debiendo defenderse contra esas alegaciones o sospechas. Debido a ello, por el grado de compromiso entre las partes involucradas, la conclusión y el consejo que el auditor suministre producirán un impacto determinante en el resultado de una disputa, por lo que el auditor forense debe ser consciente de la responsabilidad al aceptar un compromiso de este tipo.

El auditor forense desarrolla su trabajo, normalmente en un ambiente emocionalmente cargado y conflictivo, por lo tanto debe tener en consideración la particularidad del ambiente y tratar a las partes involucradas con el respeto y dignidad correspondiente.

Antes de aceptar cualquier compromiso de auditoría forense, el auditor debe asegurarse de estar libre de cualquier conflicto de interés que podría dañar su juicio y objetividad, además de determinar si posee el conocimiento necesario para el campo de especialización relacionado al compromiso y si posee la experiencia suficiente para desarrollar este tipo de trabajo. Por otro lado, debe asegurarse de tener un claro entendimiento del objetivo del trabajo y si las condiciones del mismo son aceptables, en el caso de que existieran reservas sobre la buena fe del cliente o la racionalidad de las demandas debe considerarse la posibilidad de declinar a ese compromiso. El acuerdo de compromiso entre el auditor forense y el cliente debe fijarse por escrito, siendo redactado

cuidadosamente, ya que puede ser usado en la corte y podría ser usado en contra del auditor exponiéndolo a una posición de riesgo que podría arruinar su credibilidad.

La planificación de la auditoría debe ser continuamente ajustada a los cambios en los compromisos asumidos, como también aquellos nuevos hechos que surjan. Los cambios en la naturaleza y dirección del trabajo deben ser comunicados inmediatamente a las personas que participan en él.

El auditor forense debe documentar adecuadamente la evidencia de su trabajo, a través de sus papeles de trabajo que explican los métodos usados, los análisis que se han efectuado, los hechos básicos, los datos coleccionados, la evidencia recaudada que debe ser apropiado y suficiente para apoyar la conclusión. (Antonio, Jardon, Martínez, Montiel, Velazquillo; p67; 2009).

Certificaciones del auditor forense

No existen programas de tipo universitario para la formación de auditores forenses, dado que la formación básica es la de contador profesional (contador público auditor). Sin embargo, existen programas de entrenamiento y conferencias organizadas por el Institute of Internal Auditors (Instituto de Auditores Internos) y la National Association of Accountants (Asociación Nacional de Contadores), ambos en Estados Unidos y con un marcado sello de tipo profesional.

The Institute of Internal Auditors no limita su membresía a solo los contadores públicos, sino que es abierta a todo profesional de las diferentes ramas del conocimiento. Las certificaciones que otorga (CIA, CGAP, CFSA y CCSA) son escogidas y alcanzadas por diversos profesionales. Actualmente en la auditoría interna, no es requisito que la máxima jerarquía de un departamento de auditoría interna de una entidad sea necesariamente un contador público, ya que muchos líderes son abogados, economistas, administradores, entre otros.

A nivel internacional, el auditor se puede acreditar como Examinador de Fraude Certificado ante la Association of Certified Fraud Examiners - ACFE (Asociación de

Examinadores de Fraude Certificados). La ACFE es la principal y mayor organización antifraude en el mundo, que proporciona los conocimientos y formación con el fin de disminuir los fraudes corporativos. El Examinador de Fraude Certificado de credencial es preferido a nivel mundial por las empresas y entidades gubernamentales, valorando la experiencia en todos los ámbitos de la prevención y detección del fraude.

Las certificaciones no constituyen licencias para la práctica profesional, sino constancias o evidencias sobre la calificación de los profesionales los cuales han pasado por todos los cursos que le permiten desempeñar su labor con la autoridad, que ha recibido el entrenamiento básico en el sistema judicial y técnico pericial forense y que conoce la responsabilidad legal de dar un testimonio para sustentar una prueba antes las autoridades. Los auditores forenses certificados se pueden especializar en actividades como la de auditor de fraudes, investigador o especialista en el soporte procesal. (Rozas; 2009).

EL FRAUDE

De acuerdo a la 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.

Alan Rozas (2009), en su publicación en la revista de la Facultad de Ciencias Contables, indica que el fraude se entiende como:

1. Las acciones impropias que resultan en una declaración incorrecta o falsa de los estados financieros y que hace daño a los accionistas o a los acreedores;

2. Las acciones impropias resultantes en la defraudación del público consumidor, como por ejemplo publicidad falsa;

3. Las malversaciones y desfalcos cometidos por los empleados contra los empleadores; y

4. Otras acciones impropias como lo es el soborno, comisión, violación de reglas de las agencias reguladoras y las fallas para mantener un sistema adecuado de control interno.

Tipos de Fraudes

El fraude se puede clasificar en dos principales categorías: informes financieros fraudulentos y malversación de activos. Además, hay otra forma similar de clasificar los fraudes, los cuales pueden ser en: fraude corporativo y el fraude laboral.

- Informes financieros fraudulentos

Este tipo de fraude corresponde a un error u omisión intencional en las cantidades o revelaciones con el fin de engañar a los usuarios. La mayoría de los casos de fraude de este tipo son errores intencionales de cantidades y no revelaciones. Las omisiones de cantidades son menos comunes, pero una empresa puede sobrevalorar los ingresos al omitir las cuentas por pagar y otros pasivos financieros.

Principalmente este tipo de casos de informes financieros fraudulentos comprenden la sobrestimación de activos e ingresos u omisión de pasivos financieros y gastos en un intento por sobrevalorar los ingresos. Las empresas también pueden sobrevalorar los ingresos cuando las entradas son altas, para crear una reserva de entradas que se pueden utilizar para incrementar los ingresos en períodos futuros, conociéndose esta práctica como manejo del ingreso. Este manejo es una forma de administración del ingreso en la cual los ingresos y los egresos se cambian entre períodos para reducir la variación de las entradas. Una técnica para el manejo de estos ingresos es disminuir el valor del inventario y de los demás activos de una compañía al momento de la adquisición generando entradas altas cuando se vendan posteriormente los activos.

Este tipo de acciones puede conllevar la distorsión grave y deliberada de los estados financieros, además de la aplicación de forma equivocada de los principios de contabilidad. (Rozas; p8; 2009).

- Malversación de activos

La malversación de activos es el fraude que involucra el robo de activos de una entidad. Muchas veces las cantidades que están involucradas no son materiales, pero la pérdida de los activos es una preocupación importante para la administración, siendo probable que la materialidad de la administración en relación al fraude sea mucho menor a la materialidad utilizado por el auditor con el fin de los estados financieros.

Este concepto de fraude se utiliza generalmente como referencia al robo que involucra a empleados y otras personas que se encuentran dentro de la organización. La

ACFE ha estimado que el promedio que la compañía pierde por fraude es el 16% de sus ingresos, pero gran parte de ellos involucra a partes externas, como lo es el robo de mercaderías en tiendas y engaño por parte de los proveedores.

La malversación de activos normalmente se comete a niveles inferiores en la jerarquía de la organización, no obstante, en algunos casos es la administración la que se encuentra relacionada con el robo de los activos de la entidad, esto es por el grado de autoridad y control que tienen sobre ellos, generando como consecuencia un robo de cantidades importantes. (Rozas; p9; 2009).

- Fraude corporativo

Es aquel que se realiza con el fin de distorsionar la información financiera realizada por parte o toda la alta gerencia para causar algún perjuicio a los usuarios de los estados financieros, principalmente a prestamistas, inversionistas, accionistas y/o estado. Comúnmente se le denomina como fraude de la administración o crimen de cuello blanco.

Una empresa deshonesta, de acuerdo a las irregularidades y fines que persiga, puede distorsionar los estados financieros generalmente en dos sentidos: aparentar fortaleza financiera o aparentar debilidad financiera. (Rozas; p9; 2009).

- Fraude laboral

El fraude laboral es la distorsión de la información financiera con el ánimo de causar perjuicio a la empresa. Uno o varios empleados distorsionan la información financiera para obtener algún beneficio de forma indebida de los recursos de la empresa, como por ejemplo: activos, efectivo, títulos de valores, bienes. A este tipo de fraude se le denomina comúnmente apropiación indebida de activos o crimen ocupacional. (Rozas; p9; 2009).

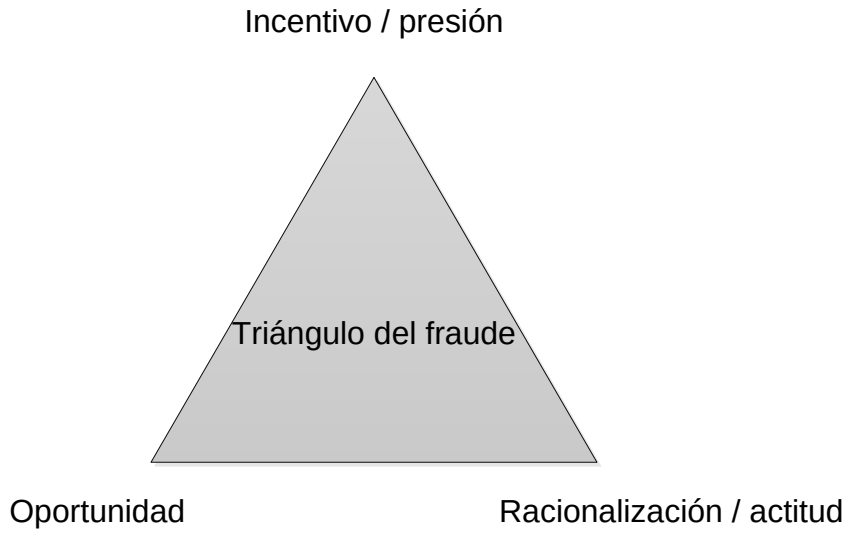
El triángulo del fraude

El triángulo del fraude es el marco conceptual más reconocido para comprender el concepto del fraude y los expertos han expuesto que para que el fraude se materialice deben existir tres elementos: incentivo o presión, oportunidad percibida y racionalización o actitud del comportamiento fraudulento.

De acuerdo al criminólogo Donal R. Cressey (1961), señala que los componentes del triángulo del fraude "surgen cuando una persona tiene altos estándares de moralidad, probablemente tiene dificultad de cuestionamiento moral cuando está cometiendo un fraude. Aquellos que no tienen principios, simplemente encuentran una excusa y se justifican a sí mismos diciendo que no hay nada de malo en lo que están haciendo" (citado por López, Sánchez; p.66; 2012).

A continuación, en la Figura 1: Triángulo del fraude, se muestran los elementos que conforman el triángulo del fraude.

Figura 1: Triángulo del fraude



Fuente: Elaboración propia, a partir de lo expuesto por Donal R. Cressey. 2014

Los elementos antes mencionados frecuentemente están presentes para que una persona común cometa fraude:

- Poder (incentivo o presión): La administración u otros empleados tienen un estímulo o trabajan bajo presión, lo que les da una razón para cometer fraudes. Ejemplos de ello son: alcanzar metas de desempeño, obtener bonos en función de resultados (aumentar las utilidades o rebajas de los costos). (Arens, Randal, Mark; 2007).

- Oportunidad: Existen circunstancias que facilitan la oportunidad de perpetrar un fraude. Esta oportunidad se presenta cuando alguien tiene acceso, conocimiento y tiempo para realizar acciones irregulares, como por ejemplo, la ausencia de controles, controles ineficaces o la capacidad de la administración para anular los controles. (Arens, Randal, Mark; 2007).

- Racionalización/ actitud: Aquellas personas capaces de racionalizar un acto fraudulento en total congruencia con su código de ética personal o que poseen una actitud, carácter o conjunto de valores que les permiten, consciente e intencionalmente, cometer un acto deshonesto, es decir, trata de justificar el fraude cometido. Como ejemplo alegar baja remuneración: convencerse de que no es un fraude, sino una compensación salarial; falta de reconocimiento en la organización: convencerse de que es una bonificación; fraude cometido por empleados y/o directivos: convencerse de que si otros cometen fraudes, él propio estaría justificado. (Badillo; 2008).

Método de prevención de los fraudes descritos

Las organizaciones deben establecer ciertas estrategias para prevenir la ocurrencia de fraudes, debiendo considerar:

- Un ambiente de control, lo que favorece la conciencia de control.

- Fijar metas y objetivos realistas para la organización.

- Establecer políticas escritas que describan las actividades prohibidas y las acciones a ejecutar al descubrir alguna violación.

- Instaurar y mantener políticas apropiadas de autorización para las transacciones.

- Desarrollar políticas, prácticas, procedimientos, informes y otros mecanismos para vigilar las actividades y salvaguardar los activos.

Consecuencias del fraude

Es relevante destacar los peligros que el fraude encierra, cualquiera que sea la organización o empresa en que se produce. Se puede creer que la única consecuencia del fraude fuese su repercusión económica, lo que tal vez sea cierto para determinadas empresas o sectores especialmente las de mayor dimensión.

A continuación, se enumeran algunas consecuencias que los fraudes generan, más allá de la simple evaluación económica o monetaria:

- Imagen: Las empresas objeto de fraudes significativos sufren un deterioro de su imagen, modificando su actitud y comportamiento habitual, respecto a su organización.

- Indisciplina: La disciplina se debilita, siendo difícil mantener actitudes exigentes, cuando no existe una política clara de lucha contra los defraudadores. Si el fraude importante no es radicalmente combatido, cada persona se considera con derecho a tratar de beneficiarse de las posibilidades que en beneficio propio le ofrece el desempeño de su trabajo.

- Pérdida de eficiencia: La eficiencia de la organización puede resentirse, puesto que los empleados estarán más atentos a buscar debilidades de control, que el desempeño y perfeccionamiento de sus tareas.

- Costos adicionales: Cuando no existe una política antifraude, cualquier fraude supondrá la realización de investigaciones, análisis, auditorías, demandas judiciales para tratar de resolver cada situación.

- Desmotivación: Los fraudes consentidos son una muestra del desinterés de la dirección hacia el trabajo de los empleados. Por ello, cuando los empleados perciben esa falta de atención hacia el trabajo que realizan, suelen interpretarse como que en su trabajo no es relevante que las cosas se hagan bien o se hagan mal, perdiendo interés y la ilusión que requieren el trabajo bien hecho.

- Tensiones internas: Se extienden a todo el ámbito de la empresa, especialmente cuando se hace partícipe de la mala imagen del defraudador, al colectivo de donde este procede generándose un clima que acentúa gran parte de los efectos ya comentados.

Estas consecuencias son muy graves que se den en una empresa, pues al no gozar de buena imagen, los efectos en ellas se manifiestan, muchas veces injustamente. (Avalos, Navarrete, Sánchez; 2012).

FRAUDES ELECTRÓNICOS EN EL SECTOR BANCARIO

Evolución de los bancos en Chile

Sin duda, la banca ha experimentado numerosos cambios desde la década de los 70', en la cual se observaba una oferta de productos muy limitada, una escasa competencia y una profesionalización casi inexistente, prácticamente no se utilizaba tecnología, limitándose a aplicaciones informáticas básicas. En 1973 se comienza a liberar el sistema, el cual se encontraba reprimido y desde 1975 se empieza a privatizar un gran número de bancos anteriormente estatales. Los acontecimientos más importantes de esta época son la liberación de las colocaciones de crédito, la reducción del encaje a los depósitos en moneda nacional, la liberación de las tasas de interés, entre otras.

Durante la década de los 80', luego de la crisis financiera de 1982 - 1984, hubo un incremento de la competencia, por parte de los profesionales de la tecnología hubo una mayor presencia, se aumentó la potencia computacional, se enfatizó en el procesamiento en *batch centralizado,* o sea, en el procesamiento de un gran volumen de datos a un tipo de documentos, el manejo transaccional de carteras masivas y la aparición de los primeros cajeros automáticos.

En el año 1986 se desarrolla la reforma de la ley de bancos, siendo intervenidos 14 bancos y 8 sociedades financieras; de todo este conjunto sólo 8 se liquidaron. A su vez, ocurrió un gran número de fusiones y términos de giro, disminuyendo a 40 instituciones de las 63 existentes. A raíz de estos acontecimientos, surgieron por una parte grandes bancos, los que concentraron importantes porciones de participación de mercado y por otro lado, bancos de nicho con altos niveles de especialización en determinados segmentos de negocios. Además, se observó una caída de los precios de los productos financieros, producto de la reactivación de las economías al rebajar las líneas de financiamiento y de los efectos producidos por la competencia, dejando como consecuencia el aumento de la eficiencia operacional a través de la automatización de procesos y de una gestión más eficiente, obligando así a la banca a estar cada vez más automatizada y bajo recursos informáticos.

En la década de los 90’ se identificaron grandes cambios destacándose el alto crecimiento e incremento de la eficiencia, la consolidación y concentración del mercado y la integración internacional y aumento de la participación extranjera en la propiedad.

Hoy en día, en el negocio financiero no solo participan bancos e instituciones financieras debido al constante ingreso de nuevos actores a este negocio, principalmente en el sector del financiamiento a operaciones de consumo por parte de empresas del sector retail, se han impuesto mayores exigencias para los bancos. Adicionando a ello, la industria se concentra en las ofertas de servicios de valor agregado y en la administración del conocimiento de los clientes, lo que va acompañado de herramientas de desarrollo, equipos de gran rendimiento y de la utilización de bases de datos para el tratamiento de los perfiles de clientes y segmentación de la cartera, destacando además, la banca por internet, medios telefónicos y la red de cajeros automáticos; también conocidos como “canales no presenciales”.

Estos nuevos desafíos son excelentes oportunidades para utilizar canales no presenciales, permitiendo el ahorro de los costos de atención en sucursales y una mayor personalización de los productos y servicios. (Traverso; 2008).

Del banco tradicional a la banca electrónica

De acuerdo a Mallory Malesky (2013) se puede definir al banco tradicional como aquella sucursal 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. (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, Vásquez; 2005; p.3).

El servicio online que ofrecen la mayoría de los bancos tanto a personas naturales como jurídicas resulta muy útil, permitiendo consultar sus cuentas corrientes, cartolas históricas, cobro de cheques, depósitos de ahorro, inversiones y todo sin la necesidad de acercarse a una oficina bancaria.

La banca en línea presenta ventajas y desventajas que deben ser consideradas al momento de ofrecer servicios por internet. (Leal; 2012).

Las ventajas que pueden ser consideradas de esta herramienta son:

1. El ahorro significativo de tiempo y recursos para el banco que puede o deben repercutir en el cliente.

2. La comodidad de operar desde la casa: El cliente tiene acceso desde su computadora a los servicios que ofrece su banco las 24 horas del día, sin ajustarse a horarios.

3. La rapidez: A través de la banca online se pueden realizar transacciones en pocos minutos, sin la necesidad de realizar filas ni esperar turnos.

4. La versatilidad y capacidad de personalización del servicio: El cliente posee en su computador su propia sucursal bancaria, permitiéndole acceder y obtener información de los servicios que desee.

5. La amplia accesibilidad y cobertura de los servicios del banco: El cliente se puede contactar con su banco desde localidades donde el mismo no cuente con oficinas físicas e incluso desde el extranjero.

A su vez, es necesario mencionar las desventajas del sistema online, considerando:

1. La seguridad de las operaciones en línea: Es un elemento que se ha convertido en uno de los mayores impedimentos para que un gran número de usuarios de la banca decida utilizar los servicios por internet.

2. La inseguridad de la privacidad de los datos personales en internet.

3. La falta de velocidad de las conexiones a la red: La lentitud en las conexiones derivadas de las deficiencias en la infraestructura de red disponible.

4. El trato impersonal, ya que si es necesario resolver problemas con las cuentas de los clientes o consultas generales no hay más opción que dirigirse a una sucursal.

Transacciones electrónicas

Los servicios que ofrece una institución bancaria son diversos y cada día están al alcance de más personas. Mediante las transacciones electrónicas, el consumidor puede realizar operaciones bancarias sin la necesidad de ir físicamente a las instalaciones del banco. 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 internet.

- 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, transferir dinero de entre diferentes cuentas de bancos, utilizar tarjetas con chip, incluso realizar recargas para teléfonos celulares a cualquier hora del día durante todo el año, sin la necesidad de ir al banco. Están instalados tanto fuera de las sucursales de las instituciones bancarias como en centros comerciales.

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 POS (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).

- 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 accesar por medio de una computadora personal, la cual debe estar conectada a la red de internet pudiéndose realizar las siguientes operaciones:

1. Consulta de saldo y últimos movimientos de cuentas.

2. Transferencias bancarias.

3. Inversiones.

4. Solicitudes de chequeras.

5. Reportes de robos / extravío de tarjetas.

6. Pagos por transferencia electrónica (pagos de tarjetas de crédito).

7. Asesores y simuladores virtuales (cálculos de créditos, cálculo de inversiones).

8. Suspensión de pago de cheques.

9. Pagos de cuentas y recargas telefónicas. (Leal; 2012).

- Transacciones en CajaVecina

CajaVecina es un sistema de servicios financieros, el cual permite a las personas que residen en zonas alejadas de las grandes ciudades o comunas realizar una serie de transacciones bancarias, a través de terminales instalados en los almacenes y locales comerciales de cada comuna. En este sistema, utilizando las tarjetas de cajeros automáticos, se pueden realizar retiros de dinero de hasta un máximo de $200.000, depósitos en efectivo, transferencias entre cuentas del mismo banco, pagar cuentas de servicios y créditos de una manera más rápida, fácil y segura. Todas las operaciones se realizan con una conexión en línea con BancoEstado quedando efectiva de forma automática cada transacción que se realice, operando solo con dinero en efectivo o con transacciones electrónicas. (BancoEstado; 2010).

Fraudes electrónicos bancarios

La modernización y globalización de las operaciones financieras han provocado cambios positivos para los usuarios o consumidores de los servicios financieros, pero

también han traído diversas problemáticas, ya que la tecnología no sólo ha sido utilizada para buenas prácticas, sino que también por defraudadores, generando un incremento del riesgo en las entidades financieras contrarrestándose con los propios avances tecnológicos.

Julio Jolly y Osvaldo Lau (2013), define al 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".

Entre las formas de fraudes electrónicos más comunes en la actualidad se destacan los siguientes:

- Phishing

El 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.

El termino *phishing* proviene del inglés el que significa "pescar", teniendo gran similitud con la pesca, ya que se lanza un "cebo" y se espera a que alguien "pique".

Esta modalidad de estafa funciona a través de un mensaje electrónico, simulando proceder de una fuente fiable, intentando recoger los datos necesarios para estafar al usuario. Se trata en realidad de mensajes masivos, ya que los estafadores no saben específicamente el banco de la víctima, por lo tanto crean un mail con la apariencia corporativa del banco escogido y se envía masivamente. Algunos de esos mensajes llegarán a personas que pertenezcan a ese banco con indicaciones de que se han realizado cambios y por su seguridad debe introducir sus datos personales y códigos bancarios, por lo que debe hacer clic en el link indicado, re-direccionándolo a una página de gran similitud a la del banco habitual de la víctima, pero en verdad pertenece al

estafador, el cual solamente copia los datos que el usuario ingresa. (Recovery Labs; 2004).

- Pharming

El 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 denominada DNS (Domain Name System), 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. Comúnmente el atacante redirecciona el sitio web que está visitando el usuario a una página falsa mediante la implementación de códigos maliciosos, de esta forma, cuando se introduce un nombre de dominio accederá a la página web que el atacante haya especificado. (Recovery Labs; 2004).

- 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 el keylogger 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).

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).

- Fraudes en cajeros automáticos

El fenómeno de los cajeros automáticos 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 sólo para los clientes sino también para las entidades bancarias.

Los ataques a los cajeros automáticos se pueden clasificar en dos tipos: ataques a la infraestructura, tecnologías de información (TI), de los cajeros y redes que son empleadas para procesar transacciones y ataques físicos en cajeros automáticos. (Navajo; p165; 2011).

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.

El detener este tipo de fraudes es mucho más complejo, como no existe manipulación física del ATM en el momento de efectuar el fraude, la entidad bancaria si no dispone de herramientas necesarias, puede tardar mucho tiempo en identificar la causa del problema, dificultando la identificación del criminal.

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; p165; 2011).

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; p165; 2011).

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, siendo el miedo un factor importante que limita, en ocasiones, el uso de la banca electrónica por parte de los usuarios.

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.

Por lo tanto, es necesario incorporar medidas o elementos de seguridad que ayuden a los usuarios a incrementar la confianza en utilizar la banca electrónica con un grado mínimo de incertidumbre. (Leal; p26; 2012).

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

- Anti-phishing / Anti-pharming

Los métodos tradicionales para combatir el phishing y el 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 dé con algunas de ellas.

Como método de protección al sistema de nombres de dominio (DNS), los expertos recomiendan utilizar y verificar que el protocolo de conexión al sitio web sea seguro (HTTPS), el cual usa firmas digitales y cifrado de claves públicas (ambas técnicas

utilizadas para proteger documentos e información) permitiendo a los servidores web verificar los nombres de dominio de cada sitio y direcciones IP que correspondan. (Callegari; 2007).

- Tarjetas bancarias inteligentes

Con la incorporación de las tarjetas inteligentes, llamadas también “tarjetas con chip” o “tarjetas con microcircuito”, 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.

La tarjeta inteligente se puede describir como un dispositivo plástico que contiene un microprocesador o chip capaz de hacer diferentes cálculos, guardar información y manejar programas, los cuales se encuentran protegidos por dispositivos de avanzada seguridad.

Las transacciones con este tipo de tarjetas son mucho más sencillas y más seguras, debido a que la banda magnética no se desliza en un POS o terminal de punto de venta, sino que se introduce la tarjeta en una ranura destinada en el terminal para la lectura del chip.

Garantizar la seguridad de los pagos electrónicos es uno de los pilares fundamentales del sistema de medios de pago. Todas las tarjetas con chip cuentan con múltiples elementos de seguridad incorporados convirtiéndolas en un medio de pago seguro.

A diferencia de las tarjetas con banda magnética, las tarjetas con chip integrado no permiten que la información contenida en él se pueda trasladar a otro chip de similares características, evitando el riesgo de ser clonadas y disminuyendo los costos por fraudes con tarjetas. (Asbanc; 2013).

- Protocolo seguro de transferencia de hipertexto

El 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.

Este protocolo 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.

Https, utiliza códigos basado en SSL/TLS (protocolos para establecer comunicaciones seguras) 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; p167; 2013).

- Encriptamiento de datos

De acuerdo a José Echenique (2001), el encriptamiento o criptografía lo define como “el arte 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.

Debido a que el internet y diversas formas de comunicación electrónicas se han convertido en algo normal, la seguridad es un factor importante a considerar. Su propósito principal es asegurar la privacidad y mantener la información alejada del personal no autorizado.

LEY 19.233. “LEY DE DELITOS INFORMÁTICOS”

En 1993 entró en vigencia en Chile la Ley n° 19.223 sobre delitos informáticos. Cuerpo legal que consta de 4 artículos, a partir de los cuales se pueden clasificar en dos grandes figuras delictivas: sabotaje informático y espionaje informático.

El sabotaje informático, corresponde a conductas tipificadas que atiende al objeto que se afecta o atenta con la acción delictual. El atentado a los sistemas puede ser a través de su destrucción, inutilización, obstaculización o modificación.

Los artículos relacionados con lo mencionado son los artículos 1° y 3° de la ley:

Artículo 1°: “El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio máximo”.

Artículo 3°: “El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de la información, será castigado con presidio menor en su grado medio”.

En cuanto al espionaje informático, comprende aquellas figuras delictivas que atienden al modo operativo que se ejecuta y que pueden ser, delitos de apoderamiento indebido, uso indebido o conocimiento indebido de la información interceptando o accediendo al sistema de tratamiento de datos, como también comprende delitos de revelación indebida y difusión de datos contenidos en un sistema de tratamiento de la información, siendo los artículos aplicables el 2° y el 4°:

Artículo 2°: “El que con ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio”.

Artículo 4°: “El que maliciosamente revele o difunda los datos contenidos en un sistema de información sufrirá la pena de presidio menor en su grado medio. Si quien incurriere en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado”. (Ley 19.223; 1993).

RIESGOS ASOCIADOS AL SECTOR BANCARIO

La entidad bancaria identifica y analiza los distintos riesgos que existen en el negocio con el fin de lograr que existan las provisiones y el capital adecuado para enfrentarlos en caso de que éstos se materialicen.

Si bien los tipos de riesgos generados por las actividades de la banca electrónica no son nuevos, la forma específica en que cada uno de los riesgos se genera en cuanto a la magnitud de su efecto dentro de los bancos es nueva, tanto para los bancos como para sus supervisores.

Aquellos riesgos son múltiples y variados, encontrando al riesgo operacional, riesgo reputacional, riesgo legal y de contagio entre otros. Como por ejemplo, una violación de seguridad que permita el acceso no autorizado a la información de clientes se puede clasificar como riesgo operativo, pero también este evento expone al banco a un riesgo legal y a un riesgo de reputación. (Asociación de supervisores bancarios de las américas; 2009).

- Riesgo operacional

El Comité de Basilea II definió el riesgo operacional como “el riesgo de pérdidas que resultan de procesos internos fallidos o inadecuados, personas, sistemas o eventos externos. Incluye el riesgo legal, pero excluye el riesgo estratégico y el riesgo reputacional”.

Además, el comité define una serie de eventos relacionados con este riesgo, que periódicamente son considerados con una alta probabilidad de ocurrencia en pérdidas sustanciales. Estos eventos son:

A. Fraude interno: Errores intencionados en los informes, robos por parte de los empleados y utilización de información confidencial en beneficio del empleado.

B. Fraude externo: Robo, falsificación, circulación de cheques en descubierto y daños por intrusión en los sistemas informáticos.

C. Practicas con los clientes, productos y negocios: Abuso de confianza, abuso de información confidencial sobre el cliente, negociación fraudulenta en las cuentas del banco.

D. Daños a activos materiales: Terrorismo, vandalismo, terremotos y/o incendios.

E. Alteraciones en la actividad y fallos en los sistemas: Fallos en el hardware o software y/o problemas en las telecomunicaciones.

F. Ejecución, entrega y manejo de procesos: Errores en la introducción de los procesos. (Asociación de supervisores bancarios de las américas; p12; 2009).

- Riesgo reputacional

En la VI Reunión de Auditores Internos de Banca Central celebrada en Chile, se definió el riesgo operacional como “el riesgo de acciones y/o circunstancias que implican una publicidad adversa para la entidad por una situación degradada frente a la comunidad”.

Este riesgo se puede generar también cuando las acciones de un banco causan una pérdida de confianza importante por parte del público en la capacidad del banco de realizar funciones esenciales para la continuación de sus operaciones. El riesgo a la reputación puede ser el resultado de una deficiencia no esperada de los sistemas o productos, causando una reacción negativa en el público, por ejemplo: la violación de seguridad, ya sea por ataques externos o internos, puede disminuir la confianza del público en el banco o que se presenten problemas en las redes de comunicación que impiden a los clientes el acceso a sus fondos o información sobre las cuentas.

El riesgo reputacional no sólo puede ser significativo para un banco, sino para todo el sistema bancario, un ejemplo de ello puede ser que un banco mundial experimente un daño importante a su reputación relacionado con sus negocios en la banca electrónica, generando como consecuencia que la seguridad de los sistemas de los demás bancos también puede ser cuestionado. (Álvarez; p8; 2010).

- Riesgo legal

El riesgo legal surge de las violaciones o incumplimientos de las leyes, reglamentos o prácticas establecidas, o cuando los derechos y obligaciones legales de las partes de una transacción no se encuentren bien definidos. Muchas veces los derechos y obligaciones de las partes relacionadas que realizan actividades de la banca electrónica son poco precisos, generando incertidumbre en cuanto a la validez de los acuerdos suscritos por medios electrónicos surgiendo así el riesgo legal.

Aquellos bancos que se dedican a la banca electrónica y a las actividades de dinero electrónico pueden enfrentarse a riesgos relacionados con la divulgación a los clientes sobre la protección de la confidencialidad. Los clientes que no reciben información adecuada sobre sus derechos y obligaciones pueden iniciar acciones legales en contra del banco. Por lo tanto, el banco debe preocuparse principalmente de proteger los datos de los clientes y suscribir acuerdos rigurosos. (Comité de Basilea; 1998).

- Riesgo de contagio o riesgo sistémico

Debido a que el mundo actual se caracteriza por estar interconectado, las economías, las empresas y las personas viven en una interacción permanente, que muchas veces provoca que lo que ocurre a uno se transmite rápidamente a otros. Es por esto que se utiliza la palabra *contagio* para diversos temas.

El riesgo de contagio está relacionado con el efecto dominó causado por un banco sobre sus pares, debido a fallas en sus actuaciones, principalmente si incurre en una quiebra, o sea que el contagio bancario implica el riesgo de quiebra de una institución debido al colapso en otro banco.

El peligro de contagio de los problemas de una entidad a otra puede ocurrir por su vinculación directa o indirecta (mismas operaciones, mismos dueños, etc), pero además porque la entidad que ha sido afectada tenga un tamaño o una imagen que conlleve a perder la confianza en la misma, volviéndose en una pérdida de confianza en el sistema, convirtiéndose el riesgo en sistémico porque afecta a todo el sistema. (Álvarez; 2010).

CAPÍTULO II: ANTECEDENTES DE LA INVESTIGACIÓN

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 ACFE (Albarracín, 2013). En cuanto al análisis de los delitos informáticos, el 46,71% corresponde a la falsificación o estafa vía informática, refiriéndose con la introducción, borrado o supresión de datos o el 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; y el 10,18% 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).

Debido al rápido crecimiento tecnológico se genera como consecuencia el aumento de delitos y fraudes informáticos, siendo los bancos un objetivo atractivo. Ellos registran numerosas pérdidas a raíz de las propias vulnerabilidades existentes en sus sistemas informáticos, siendo aprovechadas por personas, que con o sin conocimiento del área, buscan conseguir información privilegiada y así obtener un ingreso extraordinario a su favor (Mendoza; 2012). Aquellas vulnerabilidades se pueden relacionar, por un lado, con el control interno de la entidad bancaria, como también lo puede ser la poca seguridad existente en las plataformas informáticas por el otro. 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 aquella rama de la auditoría denominada auditoría forense.

OBJETIVOS DE LA INVESTIGACIÓN

Objetivo general

Analizar los diferentes elementos de seguridad que permiten prevenir los distintos fraudes de tipo electrónico en las transacciones bancarias de la misma naturaleza, en relación con la auditoría forense.

Objetivos específicos

1. Comparar aquellas transacciones electrónicas que presentan un mayor riesgo de fraude con aquellas de menor riesgo.

2. Describir los elementos de seguridad utilizados para prevenir los fraudes electrónicos en las instituciones bancarias.

3. Identificar la relación entre los elementos de seguridad con los fraudes electrónicos bancarios.

4. Verificar la aplicación de técnicas de investigación de auditoría forense y de elementos de seguridad como método de prevención de fraudes de tipo electrónicos en una institución bancaria.

METODOLOGÍA DE LA INVESTIGACIÓN

La presente investigación se desarrolla bajo un paradigma cualitativo y con un alcance de sintetización. A continuación, se presentan las bases para materializar lo anteriormente señalado:

ETAPA I: RECOPILACIÓN DE LA INFORMACIÓN

La recopilación de información se basará en:

Bibliografía, libros relacionados al área de la auditoría, auditoría forense, leyes bancarias, Normas de Auditoría Generalmente Aceptadas (NAGAS) y Declaraciones de normas de auditoría (SAS).

Página web de la Superintendencia de Bancos e Instituciones Financieras (SBIF), base de datos EBSCO, documentos electrónicos y revistas relacionadas con las medidas de seguridad utilizadas por los bancos, fraudes electrónicos bancarios e información de auditoría forense.

ETAPA II: SISTEMATIZACIÓN DE LA INFORMACIÓN

Los criterios de orden de la información son los siguientes:

- Auditoría forense y sus técnicas de investigación.
- Tipos de fraudes electrónicos bancarios.
- Elementos de seguridad.

ETAPA III: ELECCIÓN DEL SUJETO DE INVESTIGACIÓN

El sujeto de investigación será BancoEstado, donde la indagación se realizará a aquellas personas que tengan una relación estrecha con las transacciones electrónicas. Para dicho efecto participará Sebastián Morales Lisboa especialista programador en aplicaciones bancarias, Agustín Bascoli Postigo asistente del departamento de seguridad de canales no presenciales y por último, Cristian Soto León jefe del departamento de seguridad de la información.

BancoEstado es una empresa 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.

ETAPA IV: APLICACIÓN DE LA TÉCNICA DE RECOGIDA DE DATOS

Ruta de investigación: Entrevista en profundidad.

- El contacto inicial se realizará por medio de un e-mail o llamado telefónico solicitando la realización de entrevistas a los sujetos de la investigación.

- Luego de la respuesta a la solicitud, se procederá a realizar la entrevista pertinente estructurada en base a temas que se deseen abordar que en este caso corresponde a las medidas de seguridad utilizadas para prevenir fraudes en las transacciones electrónicas bancarias.

- Temas a abordar en la entrevista: diversos fraudes electrónicos bancarios, medidas de seguridad utilizados para prevenir fraudes y aplicación de técnicas investigación para la detección de fraudes electrónicos.

- Una vez realizada la entrevista, se transcribirá para verificar y constatar que los entrevistados se encuentran conforme con lo que se publicará, enviándose vía e-mail la transcripción al entrevistado.

- Para terminar, se confeccionará un informe de entrevista final.

ETAPA V: CRITERIOS DE CALIDAD

El análisis de la información recopilada en las entrevistas incorporará criterios de credibilidad, confirmabilidad, transferibilidad y fiabilidad.

La credibilidad de las entrevistas en profundidad se logrará una vez que los entrevistados estén de acuerdo con la transcripción final, según las entrevistas realizadas.

La confirmabilidad se presentará al incorporar las tres personas que ocupan los distintos cargos al interior de la entidad y que forman parte de la investigación.

La transferibilidad estará dada al describir el contexto en particular de la entrevista en conjunto con las características de los entrevistados.

La fiabilidad se entregará a partir de la descripción a realizar respecto de la ideología del alumno tesista: Rocío Isabel Díaz Céspedes, para optar al título de Contador Público y Auditor y al grado de Licenciado en Sistemas de Información Financiera y Control de Gestión.

ETAPA VI: TABULACIÓN DE RESULTADOS

Corresponde a las categorías de análisis a presentar según lo indicado en la siguiente tabla:

Categoría	Subcategoría	Su-subcategoría
Banca Electrónica	Transacciones electrónicas	Transacciones en cajeros automáticos
		Transacciones en banca en línea
		Transacciones en CajaVecina
	Fraudes electrónicos	Phishing
		Pharming
		Fraudes relacionados con banca en línea (keylogger y spyware)
		Fraudes en cajeros automáticos (ataques a las infraestructuras TI y Skimming)
	Elementos de seguridad	Anti-phishing / Anti-pharming
		Tarjetas bancarias inteligentes
		Protocolo seguro de transferencias de hipertexto
		Encriptación de datos
	Riesgos asociados	Operacional
		Legal
		Reputacional
		De contagio
Auditoría forense	Técnicas de investigación	Verificación ocular
		Verificación verbal
		Verificación escrita
		Verificación documental
		Verificación física
		Verificación informática

Tabla 1: Categorías de análisis, elaboración propia. 2014.

ETAPA VII: ANÁLISIS DE RESULTADOS

Consiste en el análisis de los resultados que se lograron a través de la entrevista en relación a las categorías de análisis mencionadas anteriormente en la Tabla 1: Categorías de análisis.

ETAPA VIII: DISCUSIÓN DE RESULTADOS

Corresponde a la comparación entre los resultados que se logran a través de las entrevistas realizadas a la institución bancaria y con la teoría que sustenta el problema de investigación.

ETAPA IX: CONCLUSIONES

Corresponde a la exposición de las conclusiones en base a los objetivos propuestos, los resultados obtenidos y la discusión de resultados que se lograron con la investigación.

CAPÍTULO III: 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 - 7 días, tanto para realizar traspasos de dinero, consultas de saldo y/o pago de servicios. Al momento de analizar cuáles son las transacciones que representan un mayor riesgo de fraude se encuentran aquellas	Transacciones en cajeros automáticos	En relación a la respuesta del asistente de canales no presenciales, se indica que aquellas transacciones que se ejecutan a través de los cajeros automáticos lideran las estadísticas como el medio más utilizado por sus clientes, ya 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 lo que evita el paso por caja. Además, el banco considera a este medio como uno de los que posee un

		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 significativa, 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 electrónica. Mientras que el segundo medio, se puede considerar 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 y no riesgoso por manejarse montos muy bajos, no aceptando pagos con cheques y realizándose giros y depósitos con cuentas de BancoEstado. Aquellas transacciones que se realizan por		menor riesgo de fraude, porque todos los cajeros BancoEstado poseen anti-skimming, sumando a ello, que los mismos clientes observan las características y el estado en que se encuentran los cajeros automáticos de las diferentes instituciones bancarias y resguardan el ingreso 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

		cajeros automáticos se consideran las de más menor riesgo de fraude, porque todos los cajeros del banco poseen anti-skimming, siendo más difícil el robo de información.		de servicios, solicitudes de créditos realizadas en cualquier momento, horario y lugar. Por este motivo, es 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 y software no deseados, siendo responsabilidad de este último el propio cliente de 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 giros y depósitos entre cuentas del BancoEstado y que cada personas que desee tener CajaVecina en su negocio debe cumplir con ciertos requisitos. Mientras que otro entrevistado da como respuesta que CajaVecina puede representar 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 constantemente es una tarea difícil y de mucho costo.
	Fraudes electrónicos	Aquel fraude electrónico ejecutado a través de internet y 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	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 de la institución que

		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 la clave de acceso por ejemplo, de igual forma son considerados unos de los fraudes más bajos al relacionarlos con el flujo de conexiones que tiene la página de la entidad, 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, ya que aquellos clientes afectados ascienden a 117 aproximadamente por mes, pero corresponde a aquellos que utilizan las tarjetas bancarias en ATM de otras instituciones, porque todos los de BancoEstado cuentan con anti-skimming, siendo casi imposible el robo de		es cliente, siendo como objetivo obtener los datos de acceso y así realizar transacciones libremente, como por ejemplo el giro 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 tenga conexión segura 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

		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. En cuanto al 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.		clientes mostrando páginas que simulan ser del banco solo para robar información personal. En relación a las veces que ocurre este 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 computador, debido a que estas trampas son instaladas directamente en los equipos siendo muy difíciles detectarlos, es por esto que el banco no tiene estadísticas sobre estos fraudes, siendo difícil determinar el número de casos que lo afectan.
			Fraudes en cajeros automáticos (ataques a las	El fraude en cajeros automáticos es considerado como el más común dentro del banco, al ejecutarse a través del skimming, ya que algunos usuarios

			infraestructuras TI y Skimming)	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 estos fraudes es de 117, pero esta cifra indica el número de clientes BancoEstado estafados al utilizar su tarjeta en otro cajero diferente al del banco, porque todos los ATM BancoEstado 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	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

		hipertexto y el encriptamiento de datos, a excepción de las tarjetas bancarias inteligentes, elemento que se está analizado para su posterior lanzamiento, 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 a su dispositivo móvil 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.		electrónicos, que si bien no se eliminan el cien por ciento, han cumplido el objetivo de disminuir su ocurrencia.
			Tarjetas bancarias inteligentes	El banco, recientemente está analizando la implementación de las tarjetas bancarias inteligentes como un complemento a la seguridad para sus clientes, ya que sería un elemento mucho más confiable, 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	BancoEstado 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

		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.		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 BancoEstado por el gran número de clientes y las dificultades de dar	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

		soluciones rápidas y eficientes a las problemáticas que se presenten, le genera una mala imagen. Mientras que el riesgo legal y el de contagio, son importantes, pero el banco los ha mitigado, no surgiendo problemas de ellos.		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 una institución que lidera el sector bancario en relación a la seguridad, número operaciones financieras y que cuenta 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, el cual a través de encuestas y entrevistas se confirmar el cumplimiento de la normativa	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

		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.		nuevos empleados) encuestas y la realización de reuniones, 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 información es computarizada.
			Verificación física	Esta técnica de verificación física (llevada al ámbito del medio electrónico), muy frecuentemente es aplicada para obtener indicadores sobre la existencia de fraudes electrónicos, dado que el banco debe

				asegurar que todo proceso se cumpla con lo estipulado y así evitar que ocurran dichos fraudes.
			Verificación informática	Para obtener evidencia de la ocurrencia de fraudes electrónicos, el banco aplica la técnica de verificación informática muy frecuentemente, ya que este medio es el utilizado para analizar los diferentes procesos que indican si hubo o no fraude, con el fin de dar una solución efectiva y disminuir la ocurrencia de ello.

Tabla 2: Análisis de resultados. Elaboración propia. 2014

CAPÍTULO IV: 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 BancoEstado 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 pueden considerar, 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 BancoEstado.

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). BancoEstado 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 a BancoEstado; a nivel

general, este se considera como unos 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 sólo aplica para aquellos usuarios que utilizan sus tarjetas en cajeros de otras instituciones bancarias dentro de RedBanc, ya que todos los de BancoEstado 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 sus sistemas de seguridad a 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 atención 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.

Al momento de analizar qué riesgo es el que genera más daño a la entidad bancaria, se da como respuesta que es el riesgo operacional, debido a que el banco debe contar con controles y protocolos muy estrictos al momento de ejecutar un programa informático con el fin de evitar cualquier robo de información por parte de sus empleados y/o por personas ajenas a la institución. A su vez, es necesario identificar la preocupación que generan los demás riesgos. En relación al riesgo reputacional están presente los

problemas que pueden tener con los clientes, ya que esto les generan una mala reputación como institución, tanto con ellos como con las demás instituciones bancarias, en donde son los clientes los que se deben sentir conformes con los servicios que entregan. En los casos de riesgo legal y de contagio, si bien son importantes, el banco los ha mitigado, no surgiendo problemas de ellos.

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 de BancoEstado 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 él 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 relacionada con la auditoría forense, utilizando de forma muy frecuentemente la técnica de verificación ocular, verificación física y la verificación informática; todas 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 BancoEstado son la 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 BancoEstado 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 CajaVecina 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 especializado 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.

BancoEstado 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 para 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 a BancoEstado como la institución que más invierte en seguridad en comparación a la banca nacional, ya que continuamente se encuentra inspeccionando sus sistemas ante vulnerabilidades e invirtiendo en nuevos, con el objeto de contar con tecnología de punta que vaya a la par con las nuevas formas de realizar fraudes electrónicos.

BIBLIOGRAFÍA

Libros

- 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*

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

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

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

Fuentes electrónicas

- 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

- Avalos, M; Navarrete, L; Sánchez, M. (2012). *Diseño de un sistema de auditoría inteligente para la mejora continua del capital intelectual de las empresas dedicadas a la auditoría externa, ubicadas en el Municipio de San Salvador.* Trabajo de graduación. Universidad Francisco Gavidia, San Salvador.

- 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.* Número*134, 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

- 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

- 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

- 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

- 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.

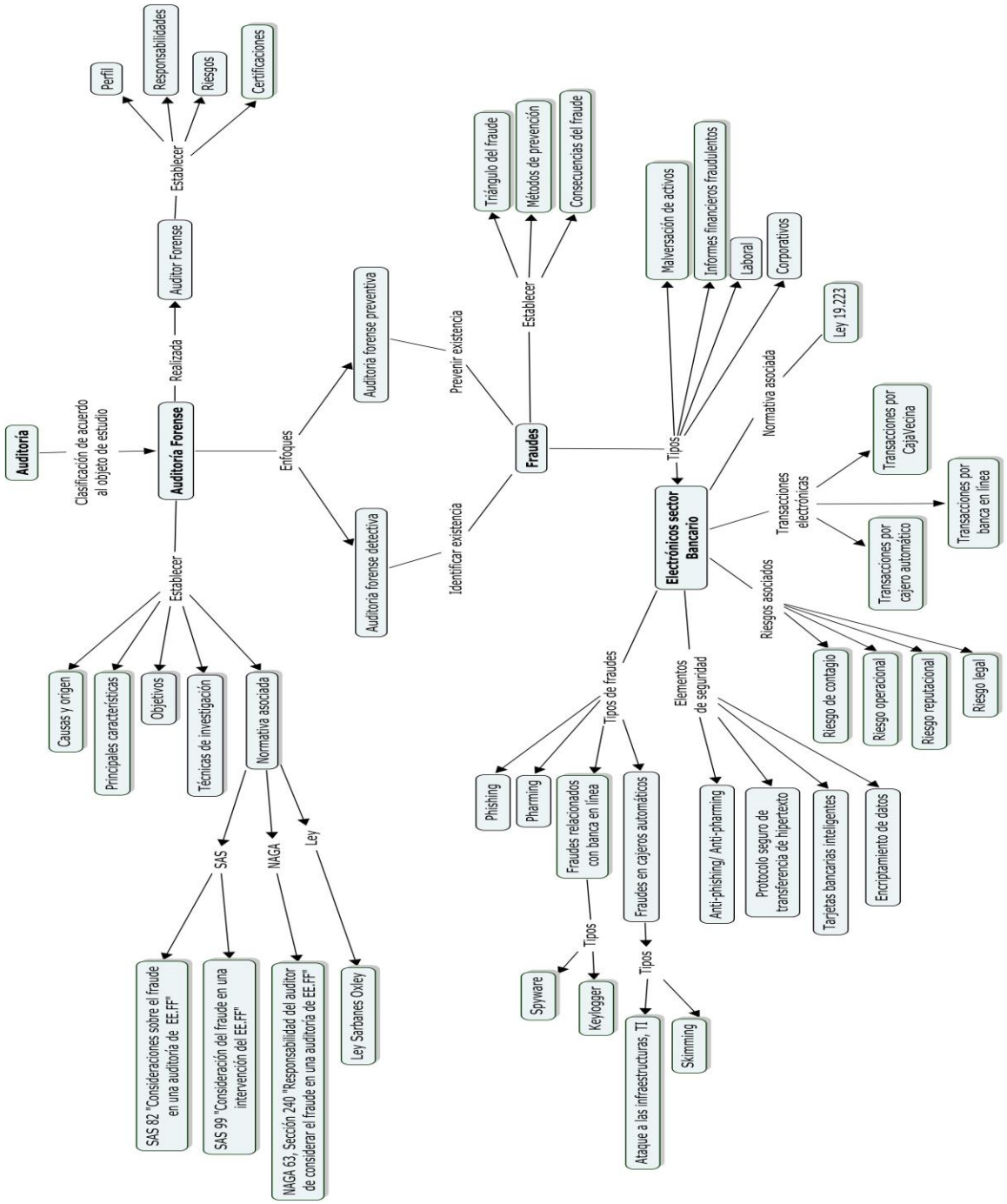
- Superintendencia de Bancos e Instituciones Financieras. (2012). *Evolución de los Medios de Pago.* Disponible en: http://www.sbif.cl/sbifweb/servlet/InfoFinanciera?indice=C.D.A&idContenido=12703

- Torres, E. 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

ANEXOS

ANEXO N°1: MAPA CONCEPTUAL DEL MARCO TEÓRICO



Mapa conceptual. Elaboración propia. 2014.

ANEXO N°2: CUMPLIMIENTO DE LOS OBJETIVOS ESPECÍFICOS

A continuación se indica cómo se cumplirán los objetivos específicos de esta investigación.

Objetivos específicos

1. Comparar aquellas transacciones electrónicas que poseen un mayor riesgo de fraude con aquellas de menor riesgo, mediante el análisis de la tabulación de resultados con la información recopilada en las entrevistas.

2. Describir los elementos de seguridad utilizados para prevenir los fraudes electrónicos en las instituciones bancarias, se realizará mediante la recopilación de información bibliográfica contenida en el marco teórico.

3. Identificar la relación entre los elementos de seguridad con los fraudes electrónicos bancarios, mediante el análisis de la información recopilada en las entrevistas.

4. Verificar la aplicación de técnicas de investigación de auditoría forense y de elementos de seguridad como método de prevención de fraudes de tipo electrónicos en una institución bancaria, mediante la realización de entrevistas en profundidad al personal de la entidad en estudio del área de fraudes electrónicos.

ANEXO N°3: TRANSCRIPCIÓN DE ENTREVISTAS

Entrevista N° 1: Especialista programador de aplicaciones bancarias en BancoEstado.

Transcripción de la entrevista:

Sebastián, buenas tardes, mi nombre es Rocío, la finalidad de esta entrevista es saber su visión interna sobre temas relacionados con las transacciones electrónicas, diversos fraudes de la misma naturaleza y elementos de seguridad utilizados por BancoEstado.

Señorita Rocío, muy buenas tardes. En primer lugar le agradezco la confianza de poder entrevistarme y tenga la tranquilidad de que colaboraré con todas las preguntas que usted necesita, para poder cumplir su objetivo que usted me está solicitando.

Sebastián:

1. En cuanto a las siguientes transacciones electrónicas: a) transacciones en cajeros automáticos; b) transacciones en banca electrónica y c) transacciones en CajaVecina

1.1 ¿Cuál es la más utilizada por BancoEstado?

Bueno, BancoEstado ofrece a sus clientes las distintas plataformas que usted me indicaba. Afortunadamente, tenemos como estadística que la plataforma de internet es la que más ocupan los usuarios, ya que pueden hacer un sinfín de transacciones, consultas, traspasos de dinero, conocido como transferencias, de una manera fácil, rápida y cómoda, piense usted de cualquier dispositivo conectado a internet puede hacer todas las transacciones sin la necesidad de ir al banco, de hacer fila y perder tiempo.

1.2 ¿Cuál representa un mayor y menor riesgo de fraude?, ¿por qué?

En este caso la plataforma de internet, como le comentaba, que es la más utilizada, es la que presenta un mayor riesgo de fraude, por qué, se debe básicamente a que hay mucha demanda en el sitio y los ladrones informáticos, hackers, denomínelos como quiera, no necesitan muchos conocimientos para poder utilizar trampas como ingeniería social, adivinar fácilmente su clave de acceso, solicitar por una forma no autorizada su clave de coordenadas, su digipass en el caso que existiera. Por lo tanto es la plataforma que más fraudes se realizan a diario.

La de menor importancia o la que tiene menos fraudes, podríamos decir que actualmente es la de los cajeros automáticos, ya que acá la gente está tomando más conciencia sobre los fraudes y las pillerías que se ocupan día a día, que quiero decir con esto, la gente está cuidando más el ingreso de la clave, se está fijando más en las características y en el estado físico que se encuentra el cajero y ya no ocupan estas plataformas para cargar el celular, para traspasar dinero, más que todo para sacar plata y muy pocas veces consultar el saldo. Por lo tanto podemos decir que el cajero automático se encuentra en la categoría de menor índice de fraudes.

2. De acuerdo a los siguientes fraudes electrónicos: a) phishing; b) pharming; c) fraudes relacionados con la banca en línea: spyware, keylogger y d) fraudes en cajeros automáticos: ataques a las infraestructuras, skimming*:* ¿cuáles son los más comunes dentro del banco?, ¿por qué?

En primer lugar tenemos que mencionar que todos los tipos de fraude que me ha mencionado tienen distintas finalidades, el phishing y el pharming, junto con los spyware y las banca en línea, son trampas que el usuario no visualiza hasta el momento en que se conecta a internet, a lo que voy no es una trampa que está instalada básicamente en su máquina, por lo tanto son las más difíciles que un usuario común y corriente puede detectar. No como lo es el Keylogger y los fraudes en cajeros automáticos que con eso el usuario está viendo en la plataforma y en la infraestructura que está ocupando si puede presentar algún defecto o algo que le llame la atención. Yendo a su pregunta yo le podría decir que el primer lugar lo lidera el phishing, que es la trampa visual que hace creer al usuario que está visitando la página oficial del banco, mientras todos los datos de acceso son enviados a un tercero. Es un tema que no deja de ser importante Rocío, ya que la cantidad de usuarios que se pueden ver afectados es tremendo. Imagine usted que es 15 minutos la demanda que tiene la página del banco es de unas 50 a 60 conexiones en línea, si un hackers realiza una página en donde aparenta ser BancoEstado utilizando el phishing, en promedio por una hora la cantidad de gente y de usuarios que vemos comprometidos sobrepasan los 100, por lo cual es un tema importante y no menor para el banco.

3. En cuanto a los elementos de seguridad que se nombran a continuación: a) anti-phishing/anti-pharming; b) tarjetas bancarias inteligentes; c) protocolo seguro de transferencia de hipertexto (https); d) encriptamiento de datos.

3.1 ¿Cuál de ellos ha utilizado el banco para prevenir los fraudes?

Todos los elementos que usted me indica los estamos utilizando con excepción de las tarjetas bancarias inteligentes. BancoEstado y como institución, reconocemos los índices de fraudes y nos ha llevado a emplear varios elementos de seguridad. Lamentablemente estamos un poco atrasados en lo que indica a tecnologías, por lo tanto las tarjetas bancarias inteligentes, es un complemento a la seguridad que recién el banco lo está analizando, para ver si es que lo lanzamos a nuestros usuarios.

3.2 ¿Piensa usted que los elementos de seguridad han cumplido el objetivo de prevenir los fraudes electrónicos? ¿Por qué?

Claramente que nos han ayudado a cumplirlos. Dentro de todos yo le podría indicar que la encriptación de datos y el protocolo de transferencia de hipertexto han sido los que más seguridad le dan a nuestros clientes. Sabemos que el uso de la tercera clave es un plus al momento de realizar transferencias no reconocidas. Usted me mencionaba dentro sus elementos de seguridad el antiphishing, el antipharming, las tarjetas bancarias inteligentes, protocolo de transferencia, pero yo le podría complementar que también en el banco ocupamos la tercera clave, ¿la tercera clave en qué consiste? Es un plus o complemento que le permite al usuario aceptar la transferencia que está realizando a través de otro dispositivo, por ejemplo usted va a realizar una transferencia por un monto no frecuente, pongamos que va a transferir en este caso 100.000 pesos a una persona por primera vez, BancoEstado y nuestro sistema reconoce que es algo que usted no está acostumbrado y pone en duda la operación que va a realizar, si usted tiene configurada la tercera clave le estaría llegando un mensaje de texto a su móvil, si es lo que lo tiene configurado, en donde le va a enviar una clave temporal, usted al confirmar esa clave en la página recién podrá realizar la transferencia. ¿Qué desventaja nos trae esto? Como usted sabe BancoEstado es el banco que muchos clientes chilenos tiene, ya que es un banco estatal, hay mucha gente la cual no sabe de tecnologías y no podemos pedirle que active su tercera clave y a la gente que se la pedimos es muy poca la que toma en cuenta las consideraciones y recibimos a llamados a diario en donde la gente nos pide que necesita activar la clave, un tema de última urgencia, y obviamente no podemos dar abasto a todas las llamadas que recibimos, pero la verdad yo le comento que sería bueno

que también usted considerara este complemento porque no es menor y cada vez lo vamos a solicitar más.

4. ¿Qué relación piensa usted que existe entre los fraudes electrónicos y los elementos de seguridad?

Bueno, básicamente creo que el uso de todos los elementos de seguridad que ofrece el banco puede ayudar a nuestros clientes a disminuir la tasa de los fraudes, pero tenemos que recordar que es el propio ser humano quien tiene el sentido común de seguridad al momento de realizar una transacción. Por ejemplo señorita Rocío, si yo le pregunto a usted, si un semáforo en verde le da seguridad en la vía pública, ¿Qué me diría? claramente yo sé que usted se va a sentir en la confianza de poder cruzar al otro extremo, mientras el semáforo este en verde, ya que usted tiene la autorización para hacer, en este caso, la transacción que es el cruce. Lamentablemente en el mundo tenemos factores externos que nos puede afectar, considere usted también que puede venir un vehículo, puede venir quizás que cosa, puede cambiar repentinamente la luz sin que usted lo tenía considerado y quizás podemos hablar de una tragedia en donde lamentablemente usted estaba con su confianza, pero el factor externo en este caso falló, es lo mismo que se habla en las relaciones con los fraudes y los elementos de seguridad, todo lo va a ayudar a que usted trabaje tranquilamente, pero siempre estamos expuesto por más seguro que nosotros hagamos sentir a los usuarios.

5. ¿Cuáles son las normativas de seguridad estándar que debe considerar un programador en vuestras aplicaciones?

BancoEstado siempre ha exigido a todas las áreas de desarrollo que cumplan una normativa básica de seguridad y de performance. Las áreas de desarrollo se dividen según la plataforma, tenemos áreas para el cajero automático, área para caja vecina, área para internet, área para transacciones, que son puntos distintos, y todos los problemas van a dar a cada área según corresponda. En el caso que nuestro software estuviese listo por instalarse en el banco y se encuentra alguna anomalía y no cumple la calidad que exige la institución estos no van a poder ser liberados, ya sea a un usuario, a un ejecutivo, a un agente, etc y tendremos que hacer todo el proceso de certificación nuevamente. Por ejemplo, yo le podría comentar de manera acotada que la normativa más básica de seguridad que nos pide el banco, es que todas las transacciones que se realicen por el

canal de internet vayan encriptadas con el estándar más seguridad… más reciente en seguridad y además tienen que ser en un tiempo muy corto, un usuario no puede estar realizando una transacción por más de 40 segundos, cuando ya el usuario pasa el tiempo permitido que en este caso es un minuto sin actividad en la página va automáticamente el sitio web le pedirá que inicie sesión de nuevo con su usuario y su clave y la transacción será abortada.

6. ¿En qué deberíamos tener más cuidado cuando estamos navegando por la red para no ser víctimas de ataques?

En primer lugar usted siempre tiene que tratar de ocupar su quipo personal o uno de confianza, las conexiones desde las maquinas desconocidas (cibercafé, el computador de un amigo, etc) pueden ocultar muchas veces las opciones de seguridad que están configuradas, sea en el sistema operativo o en el navegador de internet.

Cada vez usted quiera visitar el sitio web de BancoEstado debe escribir arriba en la barra de dirección manualmente la URL del banco, siempre tiene que empezar con "triple doble v" y antes de eso incorporar el protocolo de seguridad "HTTPS", ¿qué le ofrece ese protocolo a usted? Al estar bajo un protocolo seguro BancoEstado firma con empresas certificadoras un certificado de internet, lo que le indica que la página que usted está visitando es segura y no debiera tener problemas mayores. Además le recordamos que BancoEstado nunca les va a solicitar los datos de acceso bajo un correo electrónico, una llamada, una tarjeta con las claves de transferencias ni en ningún lugar, para que lo considere y lo tengan presente, ya que muchos de los fraudes son básicamente por ingeniería social, ¿qué significa? Ah! su fecha de nacimiento puede ser… no sé… 1990, probemos con esta fecha y así la gente va cayendo y lamentablemente el propio factor humano, como le decía anteriormente, el que tiene que estar atento a estos consejos y a estos riesgos.

7. Cuando se detecta alguna vulnerabilidad en sus sistemas, ¿existe algún flujo prioritario para superar el incidente?

Claramente que todas las vulnerabilidades son importantes. Como le comentaba existen varias áreas para el soporte informático según el canal en que se trabaje, por lo tanto cuando llega un problema todos estos son derivados por el área de soporte informático a los distintos equipos de desarrollo. Cada incidente viene con una prioridad

informada, en donde nosotros debemos cumplir los tiempos y las fechas límites de solución que el banco nos asigna según la prioridad. ¿En qué se diferencia una prioridad alta de una prioridad baja? por ejemplo, la prioridad alta son los casos más graves en donde la vulnerabilidad puede provocar un riesgo en cuanto a la seguridad del banco y de nuestros clientes y nosotros no lo podemos resolver dentro de las próximas horas para que esto quede solucionado, es aquí, cuando se dan estos casos, la gerencia de sistema toma la decisión drástica, por así decirlo, de bajar la plataforma de internet ¿qué significa esto? Que la pagina esta fuera de servicio y es donde todos los cliente empiezan a decir "oh se cayó la página del banco, no hay internet, no hay BancoEstado, etc." son puntos que podría decir que nos pasan muchas veces al año, podría asegurarle que son más de 20 veces, pero la ventaja es que algunas veces se cae por un minuto y la gente no se da cuenta, por lo tanto estamos por un lado salvados, ya que si tuviéramos muchas caídas y afectáramos a la gente estaríamos en problemas un poco mayores, pero creo que ahí nos escapamos un poco del foco de la conversación.

Entrevista N° 2: Jefe del departamento de seguridad de la información en BancoEstado.

Transcripción de la entrevista:

Cristian, buenas tardes, mi nombre es Rocío, la finalidad de esta entrevista es saber su visión interna sobre temas relacionados con las transacciones electrónicas, diversos fraudes de la misma naturaleza, elementos de seguridad utilizados por BancoEstado y conceptos relacionad con la auditoría forense.

Buenas tardes Rocío. Espero poder entregarle las respuestas necesarias para cumplir la finalidad que me menciona. Podemos comenzar en cualquier momento.

Cristian:

1. En cuanto a las siguientes transacciones electrónicas: a) transacciones en cajeros automáticos; b) transacciones en banca electrónica y c) transacciones en caja vecina

1.1 ¿Cuál es la más utilizada por BancoEstado?

Nuestro banco ofrece una variedad de productos y servicios a través de múltiples canales presenciales como también en sistemas automatizados, con la finalidad que nuestros clientes puedan disponer de ellos en el momento y lugar que lo deseen proporcionando una atención 24/7.

De acuerdo a nuestras estadísticas, el número de transacciones relacionadas con los diferentes canales que usted me menciona alcanzan las 1.050 anuales aproximadamente en su conjunto, representando algo más del 93% del total de las transacciones bancarias realizadas en el último año. Sin duda alguna, Rocío, el canal más utilizado por nuestros clientes al realizar sus transacciones es el de internet, ya que pueden realizar múltiples operaciones en cualquier momento y horario, como lo es el traspaso de fondos, consultas de saldo, pagos de productos y servicios, eehh ahorro, solicitudes de créditos, etcétera, demostrando que en el año 2013 se efectuaron un poco más de 360 millones de transacciones.

De acuerdo a nuestras estadísticas, el número de transacciones relacionadas con los diferentes canales que usted me menciona alcanzan las 1.050 anuales aproximadamente en su conjunto, representando algo más del 93% del total de las transacciones bancarias realizadas en el último año. Sin duda alguna, Rocío, el canal más utilizado por nuestros clientes al realizar sus transacciones es el de internet, ya que pueden realizar múltiples operaciones en cualquier momento y horario, como lo es el traspaso de fondos, consultas de saldo, pagos de productos y servicios, eehh ahorro, solicitudes de créditos, etcétera, demostrando que en el año 2013 se efectuaron un poco más de 360 millones de transacciones.

1.2 ¿Cuál representa un mayor y menor riesgo de fraude?, ¿por qué?

Podemos mencionar que las transacciones por internet son las que representan un mayor riesgo de fraude, debido a que es la de mayor uso por parte de los usuarios y por montos cuantiosos, aprovechándose de esto los hackers, quienes a través de la utilización de múltiples técnicas obtienen información de los usuarios, la clave secreta, el número de la cuenta bancaria, los dígitos de la tarjeta de coordenadas con la principal finalidad de utilizarla de forma fraudulenta.

Aquella de menor riesgo se puede indicar a las transacciones de CajaVecina porque si bien, es un canal que se encuentra en todo Chile y se realizan retiros de dinero, depósitos, pago de cuentas de servicios y créditos, sólo se manejan montos de dinero de hasta 200.000 mil pesos para efectuar retiros, no acepta cheques, los socios estratégicos (que es como nosotros llamamos a aquellas personas que tienen en sus negocios la CajaVecina) deben cumplir con ciertos requisitos para formar parte de esta red, como por

ejemplo el tener un buen comportamiento comercial y las operaciones que se realizan son con una sola conexión en línea siendo esta con BancoEstado.

2. De acuerdo a los siguientes fraudes electrónicos: a) phishing; b) pharming; c) fraudes relacionados con la banca en línea: spyware, keylogger y d) fraudes en cajeros automáticos: ataques a las infraestructuras, skimming*:* ¿cuáles son los más comunes dentro del banco?, ¿por qué?

Haber, esencialmente el phishing es líder en los fraudes electrónicos, seguido del pharming, el cual consiste en una estafa que utiliza mecanismos electrónicos, como un e-mail o una página web falsa, para robar información personal de un usuario. Estos ataques son posibles debido a la utilización de métodos de autentificación fáciles de descifrar, como por ejemplo una fácil combinación de usuario y clave. Dentro del mismo tipo de fraude, los relacionados con la banca en línea son poca ocurrencia, pero no deja de ser importante para el banco.

En cuanto a los fraudes de cajeros, también es un punto importante, principalmente el skimming, ya que algunos usuarios no se percatan que los cajeros están intervenidos con el fin de robar la información contenida en la banda magnética de su tarjeta. Afortunadamente, este tipo de delito ha ido disminuyendo, porque nuestros clientes se han informado y han tomado las medidas de seguridad adecuadas para evitar ser víctimas.

3. En cuanto a los elementos de seguridad que se nombran a continuación: a) anti-phishing/anti-pharming; b) tarjetas bancarias inteligentes; c) protocolo seguro de transferencia de hipertexto (https); d) encriptamiento de datos:

3.1 ¿Cuál de ellos ha utilizado el banco para prevenir los diversos fraudes electrónicos?

Bueno Rocío, el banco utiliza todos los elementos que me ha mencionado. Recientemente, para ser más precisos, el año pasado el banco inició la implementación de las tarjetas con chip en las tarjetas de crédito, el cual se caracteriza por ser un sistema mucho más confiable para nuestros clientes, porque no se han visto sistemas que vulneren masivamente los procesos ejecutados con este tipo de elementos.

Ah! como dato adicional, para que agregues a tu investigación Rocío, es la famosa tercera clave, la cual genera un nuevo nivel de autorización usando un procedimiento de validación en el que se hace llegar al cliente un mensaje de texto con la clave necesaria para autorizar la transacción que se está realizando por internet para concluir con el proceso.

3.2 ¿Piensa usted que los elementos de seguridad han cumplido el objetivo de prevenir los fraudes? ¿Por qué?

¡Sin duda alguna! Los elementos nos ayudan como institución financiera, a resguardar la información confidencial de cada uno de nuestros clientes y de las millones de transacciones que se realizan a diario de los numerosos hackers que se aprovechan de las deficiencias de los sistemas para obtener este tipo de información y utilizarla de forma inadecuada. O sea podemos concluir que se les hace mucho más complicado a este tipo de ladrones el hacer de las suyas en los diferentes canales utilizados en la realización de transacciones electrónicas, siendo la principal finalidad de los elementos de seguridad.

4. ¿Qué relación piensa usted que existe entre los fraudes electrónicos y los elementos de seguridad?

Pienso que se relacionan de forma directa, ya que los elementos de seguridad utilizados por el banco son de gran ayuda para prevenir los fraudes electrónicos, disminuyendo enormemente la tasa de ellos.

Como te mencionaba anteriormente no solo nos ayudan dichos elementos, sino también a los clientes. Hay que destacar el conocimiento que éstos han tenido y la postura que optan frente al fraude electrónico, preocupándose mucho más de los sitios bancarios por los cuales navegan, tomando en cuenta las diversas consideraciones que el banco les ha manifestado en cada oportunidad para realizar transacciones seguras.

5. ¿Por qué piensa usted que BancoEstado es el principal objetivo para realizar fraudes, esencialmente de tipo electrónico?

BancoEstado es la institución pública financiera más grande a nivel nacional y que por motivos obvios tiene la mayor cantidad de clientes. Bajo estas circunstancias, las necesidades de los ladrones informáticos se ven en aumento, ya que pueden llegar a una

cantidad no limitada de público. Dentro de nuestros clientes tenemos un amplios rango etario en dónde no muchos tienen conocimientos básicos sobre seguridad informática, la gran desventaja que deja la puerta abierta a los constantes ataques que recibimos. Sabemos cómo institución que dentro de todos nuestros canales de operación el electrónico es el más usado, tener un control absoluto de cada transacción es algo que se nos escapa de las manos, claramente estamos educando cada día más a nuestros clientes y capacitando a nuestros encargados de área tecnológica para saber enfrentar y prevenir los fraudes electrónicos.

6. Al sector bancario se asocian múltiples riesgos, como por ejemplo:

a) Riesgo operacional: es el riesgo de pérdida que resulta por errores intencionados de los empleados o personas externas, robo, abuso de confianza o fallas en el hardware o software.

b) Riesgo reputacional: es el riesgo que al realizar acciones o ataques internos o externos a la entidad, generen publicidad adversa al banco.

c) Riesgo legal: surge a raíz del incumplimiento de las leyes o reglamentos, como por ejemplo, que los contratos con los clientes no se definan adecuadamente, generando incertidumbre en cuanto a la validez de los mismos.

d) Riesgo de contagio: es el riesgo que las dificultades financieras de una entidad afecten a las otras entidades bancarias.

¿Cuál piensa usted que el que genera más daño a la entidad? ¿Por qué?

Dentro de todos los riesgos que me ha indicados, Rocío, permítame explicarle cómo nos afecta cada uno de ellos.

Riesgo operacional: sin duda que este tipo de riesgo es importantísimo, ya que se trabaja con información de todo Chile, de cada persona y todo tipo de transacción. Es por ello que el banco cuenta con controles y protocolos muy estrictos; toda transacción, programas informáticos son analizados y ejecutados de acuerdo a nuestra normativa de seguridad, con el fin de evitar que ocurra el robo de información privilegiada que es lo más importante para el banco.

Riesgo reputacional: para nosotros el tener problemas con clientes (problemas con las transacciones electrónicas, con las claves secretas, la mala gestión de los agentes)

nos genera una mala reputación, tanto con ellos como con las demás instituciones financieras, en donde nuestros clientes se deben sentir más conformes con el servicio que entregamos. BancoEstado siempre trata de compensar a nuestros clientes para que queden conformes con las soluciones que entregamos. Claramente tener una mala imagen nos cierra las posibilidades de llegar a más chilenos.

Riesgo legal: dentro de todos los riesgos mencionados en este estamos más tranquilo pues últimamente hemos mejorado nuestros protocolos de transparencia con nuestros clientes, claramente ellos también están más confiados en lo que nos corresponde ofrecerles según lo que contrataron.

Riesgo de contagio: BancoEstado lidera el sector bancario, tanto en seguridad como financieramente, dado que el número de clientes es muy elevado, por lo que cualquiera variación en el mercado o sector bursátil afecta tanto a nuestros competidores como a nosotros.

Bueno, resumiendo un poco y yendo a su pregunta le comento que todos los riesgos son muy dañinos, pero el que más daño nos produce es el operacional, por las razones mencionadas anteriormente.

7. *Se comenta al entrevistado en qué consiste la auditoría forense* - Desde su punto de vista, ¿qué importancia puede tener usar esta metodología en los servicios electrónicos del banco?

Es un tema más que importante para nuestra institución ya que nos aceleraría los procesos de investigación de fraudes. Claramente lo podríamos usar en grandes fraudes o estafas, creo que llevarlo a un problema en específico de un cliente nos demandaría más tiempo y costo que el reponer por nuestra parte los fondos que se vieron afectados. Más que usarlo en los servicios electrónicos yo lo emplearía en un nivel o situación crítica del banco, claramente sería un caos para quien la realice, recuerde que son muchos los movimientos de dinero dentro del banco, pero bueno, una por otra.

8. Para obtener información, indicadores o evidencia de la existencia de fraudes electrónicos. Indique y explique en qué grado han realizado las siguientes actividades:

Actividades	Muy frecuente	Frecuentemente	Poco frecuente
Observar, revisar y comparar diversos procedimientos o actividades.	X		
Realización de entrevistas, encuestas o cuestionarios a terceros o empleados.		X	
Analizar y confirmar de forma escrita la información otorgada por los empleados para identificar la validez de los registros y procesos.			X
Obtener documentación escrita para resguardar los procesos que justifican una operación o transacción.			X
Inspeccionar la forma en que se desarrolla y documentan los procesos de la ejecución de las actividades.	X		
Análisis de datos y rastreo de la información en los sistemas electrónicos.	X		

Explicación:

- Observar, revisar y comparar diversos procedimientos o actividades: *De forma muy frecuente se observan y se revisan las diversas actividades que realizan nuestros empleados al ejecutar los diversos procesos informáticos con el fin de que cumplan*

con la normativa de seguridad implementada por el banco, evitando que sufran "caídas" y que estas sean aprovechadas por personas ajenas a la institución.

- Realización de entrevistas, encuestas o cuestionarios a terceros o empleados: *Frecuentemente. Hemos realizado algunas encuestas o pequeñas reuniones, muchas veces no tan formales a los trabajadores, principalmente a aquellos que se han incorporado recientemente a la institución, siendo el fin averiguar si han cumplido las normativas de seguridad y calidad exigidas por el banco.*

- Analizar y confirmar de forma escrita la información otorgada por los empleados para identificar la validez de los registros y procesos: *mmm…. Esta actividad casi nunca se desarrolla de forma escrita, ya que todo es utilizado de forma computarizada, por lo tanto, estaría dentro de la aplicación poco frecuente.*

- Obtener documentación escrita para resguardar los procesos que justifican una operación o transacción: *La misma respuesta que la actividad anterior, Rocío, ya que todo es utilizado y manejado de forma computarizada.*

- Inspeccionar la forma en que se desarrolla y documentan los procesos de la ejecución de las actividades: *Muy frecuentemente, ya que no podemos confiar ciento por ciento de sólo observar o conversar sobre la aplicación de la normativa de seguridad, si no que debemos cerciorarnos de ello.*

- Análisis de datos y rastreo de la información en los sistemas electrónicos: *Muy frecuentemente se realiza esta actividad, ya que a través de ella se puede identificar y obtener evidencia si hubo o no fraude electrónico, analizando minuciosamente cada proceso que estuvo involucrado y dar una respuesta y solución lo más adecuada posible.*

9. ¿BancoEstado aplica en sus empleados algún tipo de seguridad para que no puedan acceder a información confidencial de sus clientes?

Sí. Siempre nos preocupamos por la confidencialidad de nuestros clientes, tenemos medidas y protocolos muy estrictos para que solo el personal autorizado pueda acceder a los datos. Frente a esto, no significa que no podamos sufrir algún tipo de ataque o robo de información para que después esta información se "venda" a otras empresas o instituciones. En el caso que detectemos actos fuera de la moral procedemos

con la desvinculación inmediata del trabajador y si es necesario podemos aplicar el peso de la ley según corresponda.

En resumen, podemos sentir la tranquilidad que es un acto por el que no hemos pasado.

Entrevista N° 3: Asistentes en el departamento de seguridad de canales no presenciales de BancoEstado.

Transcripción de la entrevista:

Agustín, buenas tardes, mi nombre es Rocío, la finalidad de esta entrevista es saber su visión interna sobre temas relacionados con las transacciones electrónicas, diversos fraudes de la misma naturaleza y elementos de seguridad utilizados por BancoEstado.

Buenas tardes Rocío.

1. En cuanto a las siguientes transacciones electrónicas: a) transacciones en cajeros automáticos; b) transacciones en banca electrónica y c) transacciones en caja vecina.

1.1. ¿Cuál es la más utilizada por sus clientes?

BancoEstado tiene estadísticas que revelan cuántas transacciones se realizan en los distintos canales. Las transacciones realizadas a través de cajeros automáticos (ATM) lideran la lista. Muchos de nuestros clientes utilizan este medio para realizar transacciones comunes de una manera más rápida evitando el paso por caja de sucursal. Recordemos que no todos los clientes tienen acceso y conocimientos básicos para usar la banca electrónica.

1.2. ¿Cuál representa un mayor riesgo de fraude y menor riesgo de fraude? ¿Por qué?

Caja Vecina presenta un mayor riesgo, ya que no tenemos un control específico de todos los terminales, algunos están en lugares muy alejados, por lo tanto verificarlos constantemente no es una tarea fácil.

En menor riesgo puedo decir que son los cajeros automáticos son más seguros que la plataforma de internet, esto se debe a que nosotros como institución no podemos verificar la seguridad que tiene cada usuario en su computadores, pueden estar infectados con spyware o un virus similar y eso no lo tenemos en conocimiento; en estos casos la responsabilidad del fraude recae en un 100% sobre el cliente.

2. De acuerdo a los siguientes fraudes electrónicos: a) phishing; b) pharming; c) fraudes relacionados con la banca en línea: spyware, keylogger y d) fraudes en cajeros automáticos: ataques a las infraestructuras, skimming*:* ¿cuáles son los más comunes dentro del banco?, ¿por qué?

Actualmente los más comunes son los skimming, porque el volumen de cajeros, incluidos los de otros bancos, es de un alto número y reciben un alto nivel de ataques. Además no toda la banca implementa medidas de seguridad en sus ATM.

3. En cuanto a los elementos de seguridad que se nombran a continuación: a) anti-phishing/anti-pharming; b) tarjetas bancarias inteligentes; c) protocolo seguro de transferencia de hipertexto (https); d) encriptamiento de datos.

3.1 ¿Cuál de ellos ha utilizado el banco para prevenir los fraude?

BancoEstado ha implementado en todas las alternativas iniciativas, con el objeto de disminuir los fraudes, a excepción de las Tarjetas Bancarias inteligentes.

3.2 ¿Piensa usted que los elementos de seguridad han cumplido el objetivo de prevenir los fraudes? ¿Por qué?

Creo que sí, ya que al comparar al día de hoy la cantidad de reclamos con la de unos años atrás estos han disminuido significativamente, sobre todo los fraudes a través de Internet.

4. ¿Qué relación piensa usted que existe entre los fraudes electrónicos y los elementos de seguridad?

La verdad es que considero que sin los fraudes electrónicos, BancoEstado no tendría la seguridad que tiene hoy en día. Aunque usted no lo crea, somos la institución más segura dentro del mercado. BancoEstado constantemente invierte en nuevas tecnologías para ofrecer a sus clientes la máxima seguridad y tranquilidad para que realicen sus transacciones electrónicas sin problemas.

5. ¿Qué diferencias, en cuanto a seguridad para sus clientes, tiene que destacar BancoEstado en comparación a otras instituciones bancarias?

Principalmente las medidas que ha implementado para evitar la clonación de tarjetas, mediante la instalación de anti-skimming en todas sus sucursales y ATM ubicados en ellos.

6. Al detectar el fraude electrónico y comenzar a dar una solución, ¿se prioriza la atención del fraude en cuanto a la magnitud de su monto? ¿Y qué procedimientos debe realizar para dar una solución?

No, BancoEstado no discrimina por los montos involucrados. Atiende a todos sus clientes de igual manera independiente del patrimonio que se vio afectado. El proceso de análisis establecido para este tipo de reclamo es estándar para todos nuestros clientes y en el mismo tiempo destinado para su resolución.

7. Indique el número de veces al mes en que ocurren los siguientes fraudes:

Fraudes electrónicos	**Veces al mes**
Phishing	*8*
Pharming	*4*
Fraudes relacionados con la banca en línea: Spyware.	*Al ser un problema netamente del usuario no podemos tener una estadística de los equipos infectados*
Fraudes relacionados con la banca en línea: Keylogger.	*Al ser un problema netamente del usuario no podemos tener una estadística de los equipos infectados*
Fraudes en cajeros automáticos: Ataques a las infraestructuras TI.	*El banco no cuenta con estadísticas relacionadas con este fraude.*

Fraudes en cajeros automáticos: Skimming	*117 (A clientes BancoEstado, no a los cajeros de nuestra institución.)*

8. ¿Cuál es su visión del nivel de seguridad existente en el banco? ¿otorga la seguridad necesaria para realizar transacciones seguras?

El nivel de seguridad del banco es de un alto nivel tecnológico que constantemente se está monitoreando, con el objeto de actualizarse e implementar nuevas iniciativas que vayan de la mano con los nuevos modus operandis utilizados por los defraudadores. En comparación con las demás instituciones bancarias, este nivel es de los más eficientes conforme a las mediciones otorgadas por la SBIF.

Cabe mencionar que BancoEstado es la institución financiera con la mayor cantidad de clientes operando y realizando transacciones en el mercado. Por lo cual al parecer es el banco con mayores índices de fraudes, pero porcentualmente esto no tiene coincidencia con la realidad.