



**FACULTAD CIENCIAS ECONÓMICAS Y ADMINISTRATIVAS
ESCUELA DE AUDITORÍA**

**AUDITORÍA A TRAVÉS DE LOS SISTEMAS DE INFORMACIÓN EN LAS
INSTITUCIONES BANCARIAS**

**Tesis para optar al Grado de Licenciado en Sistemas de Información Financiera y
Control de Gestión.**

Tesistas: Fernanda Andrea Soto Ruiz

Catalina Andrea Tapia Sobarzo

Profesor Guía: Dante Alvarado Estay

Valparaíso, 11 de Diciembre de 2017

Tabla de Contenido

PLANTEAMIENTO DEL PROBLEMA O FUNDAMENTACION DEL TEMA DE INTERES PROFESIONAL A DISCUTIR	4
MARCO TEORICO	5
ANTECEDENTES GENERALES	5
DEFINICIONES	6
1. AUDITORIA	6
1.1 AUDITORIA PREVENTIVA	7
1.2 AUDITORIA DETECTIVA	7
1.3 AUDITORIA INTERNA	8
1.4 AUDITORIA EXTERNA:	8
1.5 AUDITOR:	8
1.6 CARACTERÍSTICAS DEL AUDITOR:	9
1.6.1 FORMACIÓN TÉCNICA Y CAPACIDAD PROFESIONAL:	9
1.6.2 INDEPENDENCIA, INTEGRIDAD Y OBJETIVIDAD:	9
1.6.3 DILIGENCIA PROFESIONAL:	10
1.6.4 SECRETO PROFESIONAL:	10
2.0 SISTEMAS DE INFORMACIÓN	10
FIGURA N°1: CUADRO SISTEMAS DE INFORMACIÓN	11
2.0.1 SISTEMAS TRANSACCIONALES (TPS)	12
2.0.2 SISTEMAS DE INFORMACIÓN GENERAL (MIS)	12
2.0.3 SISTEMAS DE APOYO A LAS DECISIONES (DSS)	13
2.0.4 SISTEMAS PARA LA PLANIFICACIÓN DE LOS RECURSOS DE LA EMPRESA (ERP)	13
2.1 CONTROL INTERNO	14
FIGURA N°2: CUADRO CONTROL INTERNO	15
3.0 INSTITUCIONES BANCARIAS	15
3.1 SECTOR BANCARIO	16
3.2 FRAUDES EN EL SECTOR BANCARIO	16
3.3 ELEMENTOS DE SEGURIDAD	17
3.4 TIPOS DE FRAUDE:	19
OBJETIVOS GENERALES Y ESPECIFICOS	24
OBJETIVO GENERAL	24
	2

OBJETIVOS ESPECÍFICOS	24
METODOLOGIA DE LA INVESTIGACION	25
ETAPA I: RECOPIACION DE LA INFORMACION	25
ETAPA II: SISTEMATIZACION DE LA INFORMACION	26
ETAPA III: ELECCION DE SUJETO DE INVESTIGACION	26
ETAPA IV: APLICACIÓN DE LA TECNICA DE RECOGIDA DE DATOS	27
ETAPA V: CREDIBILIDAD, CONFIRMABILIDAD, TRANSFERENCIA Y FIABILIDAD	28
ETAPA VI: TABULACION DE RESULTADOS	29
TABLA N°1: TABULACIÓN DE RESULTADOS	29
ETAPA VII: ANALISIS DE RESULTADOS	29
TABLA N°2: ANÁLISIS DE RESULTADOS POR CATEGORÍAS	30
TABLA N°3: ANÁLISIS DE RESULTADOS POR SUB-CATEGORÍAS	32
TABLA N°4: ANÁLISIS DE RESULTADOS POR SU-SUBCATEGORÍAS	34
ETAPA VIII: DISCUSIÓN DE RESULTADOS	36
FIGURA N°3: REPRESENTACIÓN ÁRBOL ATLASTI	40
FIGURA N°4: REPRESENTACIÓN ÁRBOL ATLASTI	41
FIGURA N°5: REPRESENTACIÓN ÁRBOL ATLASTI	42
FIGURA N°6: REPRESENTACIÓN ÁRBOL ATLASTI	43
ETAPA IX: CONCLUSIONES	44
BIBLIOGRAFÍA	46
ANEXOS	50
ANEXO N°1: MAPA CONCEPTUAL	50
ANEXO N°2: TRANSCRIPCION ENTREVISTAS	51
2.1 ENTREVISTA N°1	51
2.2 Entrevista N°2	53
2.3 Entrevista N°3	56

PLANTEAMIENTO DEL PROBLEMA O FUNDAMENTACION DEL TEMA DE INTERES PROFESIONAL A DISCUTIR

Hoy en día, la auditoria se ha desarrollado con el fin de prevenir y estudiar hechos de corrupción y fraudes, los cuales son muy comunes en la actualidad.

Los fraudes en las instituciones bancarias en Chile son abordados a través de sistemas de información, los cuales pertenecen al control interno de una organización, es por ello que se decide investigar los sistemas de información utilizados para prevenir y detectar fraudes.

A través de los años se han implementado mayor tecnología en la prevención y detección en el sector bancario, alguno de ellos son la clave dinámica, la cual aprueba los pagos en línea y transferencias bancarias. Otro método es la tercera clave para mayor seguridad, dura únicamente cinco minutos, por lo que el cliente debe ingresarla inmediatamente, ya que de esta manera no hay forma de engaño.

Por consiguiente se realizará una comparación de sistemas de información entre dos entidades bancarias a nivel nacional e internacional, con el fin de verificar y evaluar sus métodos de prevención y detección a los fraudes que están expuestos día a día.

MARCO TEORICO

ANTECEDENTES GENERALES

Hoy en día debido al gran avance tecnológico, según las noticias a nivel mundial, en la actualidad, han nacido nuevos sistemas de información para resguardar a los clientes pertenecientes a entidades bancarias, con el fin de una mayor seguridad en sus transacciones. Es por ello que hay millones de personas que día a día forman parte de instituciones bancarias y confían en sus servicios.

Por lo anterior las instituciones bancarias deben actualizarse y buscar nuevos métodos y herramientas para hacer frente a las amenazas, fortaleciendo el control interno de la entidad mediante sistemas de información más modernos y actualizados.

El tema central de la investigación se fragmenta en tres conceptos claves, los cuales son auditoria, sistemas de información (SI) e instituciones bancarias, estos conceptos se analizarán en los escenarios de algunas instituciones bancarias, logrando determinar cómo actúa la auditoria a través de los sistemas de información en estas entidades.

DEFINICIONES

A continuación se presentan definiciones fundamentales para una mejor comprensión de la investigación abordada:

1. Auditoría
2. Sistemas de información
3. Instituciones Bancarias

1. AUDITORIA

La auditoría es un tema fundamental al momento de analizar la situación de una empresa, ya que se basa en diferentes métodos para la supervisión del control interno de una entidad, a continuación se da a conocer una definición, la cual consiste en:

La ley de Auditoría de Cuentas (LAC) y su reglamento definen la auditoria como “La actividad consistente en la revisión y verificación de las cuentas anuales, así como de otros estados financieros o documentos contables, elaborados con arreglo al marco normativo de información financiera que resulte de aplicación, siempre que aquella tenga por objeto la emisión de un informe sobre la fiabilidad de dichos documentos que puede tener efectos frente a terceros”. (La ley de Auditoría de Cuentas (LAC), 2015, Artículo 1.2)

Según La guía Internacional de Auditoria menciona que la Auditoria es:

Una Auditoría es el examen independiente de la información de cualquier entidad, ya sea lucrativa o no, no importando su tamaño o forma legal, cuando tal examen se lleva a cabo con objeto de expresar una opinión sobre dicha información.

El cumplimiento de los principios básicos requiere la aplicación de procedimientos de auditoría y pronunciamientos sobre dictamen, adecuados a las circunstancias particulares. (La guía Internacional de Auditoría, 1983, Principios básicos que rigen una Auditoría, P.2-3)

Existen varios conceptos y definiciones de Auditoría, pero se puede inferir que la Auditoría se refiere a una reconstrucción de hechos económicos de periodos anteriores, para entregar validez y emitir un diagnóstico.

A continuación se detallan los conceptos vinculados a la auditoría:

1.1 AUDITORIA PREVENTIVA

Según Arteaga indica que la auditoría preventiva “Ayuda a reconocer las áreas que tienen mayor riesgo a sufrir algún tipo de delito patrimonial, pues sus controles internos son rebasados por los propios miembros de la organización, quienes se aprovechan y sacan ventaja de las deficiencias de los controles. Además, se debe revisar permanentemente los procedimientos y controles”. (Arteaga, 2014)

1.2 AUDITORIA DETECTIVA

Según Arteaga indica que la auditoría detectiva “Identifica el origen, así como el impacto causado por el acto delictivo, proporcionando a la empresa información sobre los efectos directos e indirectos que ocasionó dicho acto, junto con los presuntos responsables. Todo con el fin de asesorar a la empresa a tomar las acciones legales para evitar la impunidad y generar transparencia”. (Arteaga, 2014)

1.3 AUDITORIA INTERNA

Según Bernal las funciones de la auditoria interna incluyen los siguientes aspectos:

- Revisión de operaciones para la verificación y exactitud de las políticas y procedimientos establecidos.
- Llevar un registro contable para tener en control los activos de la entidad.
- Evaluar la efectividad de las políticas y procedimientos.
- Evaluación de los cumplimientos de las estrategias. (Bernal, 2010)

1.4 AUDITORIA EXTERNA:

Según Bernal la auditoria externa es independiente y objetiva, se encarga de la revisión de los informes financieros que representen y transmitan eficiencia de la administración y efectividad para la toma de decisiones. (Bernal, 2010)

1.5 AUDITOR:

El auditor es un profesional experto en materias de control, el cual posee sólidos conocimientos técnicos y una formación integral, el cual es capaz de participar activamente en el diagnóstico, diseño, evaluación, construcción, mantención y evaluación de sistemas de información y control que se relacionan a la gestión administrativa de una organización. El auditor se encarga de la elaboración e interpretación de informes de gestión y es el responsable de la emisión de una opinión independiente respecto de los estados financieros, principios, políticas y normas profesionales vigentes, asegurando confiabilidad. (Gonzalez, 2009)

1.6 CARACTERÍSTICAS DEL AUDITOR:

1.6.1 FORMACIÓN TÉCNICA Y CAPACIDAD PROFESIONAL:

La auditoría debe llevarse a cabo por personas que tengan formación técnica y capacidad profesional como auditores y posean la autorización exigida legalmente.

El auditor debe poseer una adecuada formación y experiencia específica en el campo de la auditoría, el profesional debe llevar una actualización permanente de sus conocimientos, tanto en aspectos técnicos como generales de los diversos sectores de actividad.

Debe poseer experiencia profesional práctica necesaria para acceder al ejercicio de la profesión y esto lo logra mediante la ejecución de trabajos de auditoría bajo la supervisión y revisión de un auditor.

1.6.2 INDEPENDENCIA, INTEGRIDAD Y OBJETIVIDAD:

El auditor debe mantener durante su trabajo profesional una posición de absoluta independencia, integridad y objetividad. La independencia del auditor le permite actuar con libertad respecto a su juicio profesional, para lo cual debe encontrarse libre de cualquier predisposición que limite su imparcialidad en la consideración objetiva de los hechos, así como la formulación de sus conclusiones.

Su integridad es su rectitud intachable en el ejercicio profesional, es por ello que el auditor debe ser honesto y sincero al realizar su trabajo y al emitir su informe.

La objetividad del auditor implica una actitud imparcial en todas sus funciones, debe ser justo y no permitir ningún tipo de influencia o prejuicio.

1.6.3 DILIGENCIA PROFESIONAL:

El auditor debe actuar con la debida diligencia profesional al ejecutar su trabajo y al emitir su informe. Debe realizar una revisión crítica a cada nivel de supervisión del trabajo efectuado y del juicio emitido por todos los profesionales de su equipo de trabajo.

El auditor es el responsable del cumplimiento de las normas de auditoria establecidas y del cumplimiento de las mismas por parte de los profesionales del equipo de auditoria.

1.6.4 SECRETO PROFESIONAL:

El auditor tiene el deber de mantener la confiabilidad de la información obtenida concerniente al negocio de sus clientes. El auditor debe anotar en su informe cualquier negativa del cliente a mostrar toda la información necesaria para el desarrollo completo de la auditoria. Además el auditor debe garantizar el secreto profesional en las actuaciones de sus ayudantes y colaboradores. (n.d., 2009)

2.0 SISTEMAS DE INFORMACIÓN

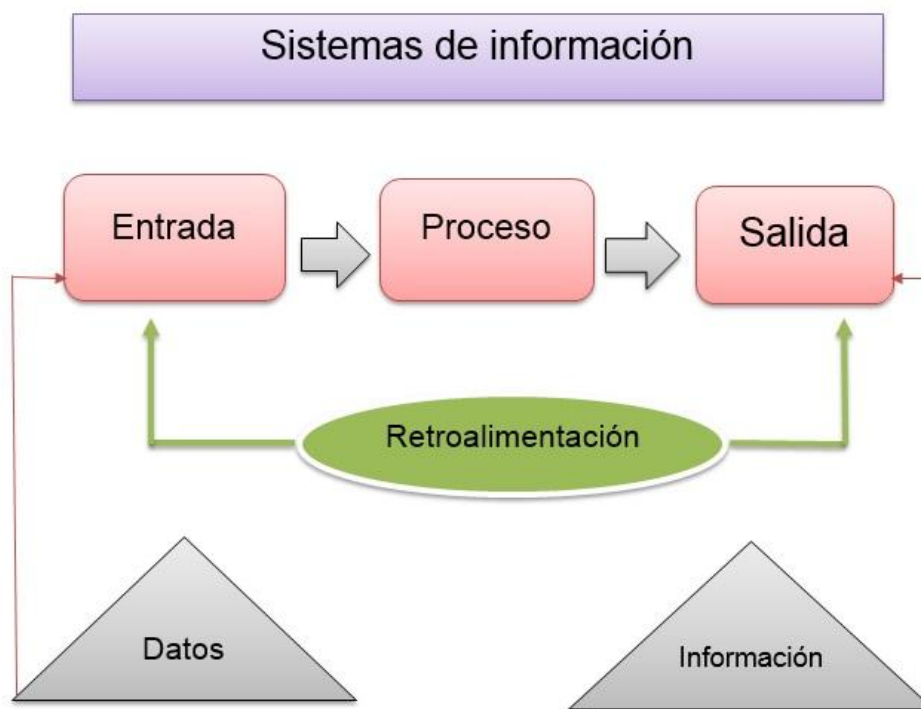
Los sistemas de información son muy útiles en la actualidad, debido al gran crecimiento de la tecnología, lo cual conlleva a tener más resguardos de la información privilegiada de una organización, algunas definiciones son las siguientes:

Se puede definir técnicamente como un conjunto de componentes interrelacionados que recolectan, procesan, almacenan y distribuyen información para apoyar la toma de decisiones y el control en una organización. (Laudon, Kenneth y Jane; 2012; p.15)

Por información entendemos los datos que se han moldeado en una forma significativa y útil para los seres humanos. (Laudon, Kenneth y Jane; 2012; p.15)

En contraste, los datos son secuencias de hechos en bruto que representan eventos, condiciones, valores o situaciones. Un dato puede ser una letra, un número, un signo ortográfico o cualquier símbolo y que representa una cantidad, una medida, una palabra o una descripción. Los datos se caracterizan por no contener ninguna información. (Laudon, Kenneth y Jane; 2012; 15)

FIGURA N°1: CUADRO SISTEMAS DE INFORMACIÓN



ELABORACIÓN PROPIA EN BASE A MARCO TEORICO.

Según Domínguez existen los siguientes tipos de sistemas de información:

2.0.1 SISTEMAS TRANSACCIONALES (TPS)

Según Domínguez un sistema transaccional controla el flujo de la seguridad y la consistencia de los datos involucrados.

Tiene la capacidad de corregir cualquier tipo de error que llegue a surgir durante una transacción almacenando la información obtenida antes de que dicho error surgiera.

Por consiguiente, es capaz de controlar y administrar múltiples transacciones, determinando las prioridades que hay entre éstas.

Sus características son las siguientes:

- A través de estas automatizaciones de tareas operativas de la organización de ha podido ahorrar un valioso tiempo en mano de obra.
- Son consideradas como el primer tipo de sistemas de información que llega a implementarse en las organizaciones. Este sistema sirve como apoyo en las tareas a nivel operativo de la organización.
- En los sistemas transaccionales son importantes las entradas y las salidas de información, y los procesos que llegan a realizarse suelen ser simples y poco sofisticados.
- Su prioridad es recolectar la información, es decir, a través de estos sistemas se cargan grandes bases de información para su explotación.

2.0.2 SISTEMAS DE INFORMACIÓN GENERAL (MIS)

Es un conjunto de sistemas de información que interactúan entre si y que a su vez proporcionan información a la administración acerca de las necesidades que se tienen en las operaciones, además ayudan a los directivos a tomar decisiones y resolver problemas.

Es conocido como una agrupación de la información extensa y coordinada de subsistemas relacionados que convierten los datos en información en una gran variedad de formas para mejorar la productividad con el estilo del administrador y sus características.

2.0.3 SISTEMAS DE APOYO A LAS DECISIONES (DSS)

Un sistema de soporte a decisiones suele ser implementado después de los sistemas transaccionales más importantes de una empresa, y prácticamente estos sistemas llegan a ser la plataforma principal en el manejo de su información.

La información generada por estos sistemas comúnmente sirve de apoyo a los mandos intermedios y a la alta administración para tomar sus decisiones.

En estos sistemas también se puede tomar en cuenta:

- la programación de la producción
- la compra de materiales
- el flujo de los fondos
- las proyecciones financieras
- el desarrollo de los modelos de simulación de negocios
- modelos de inventarios
- entre otros.

2.0.4 SISTEMAS PARA LA PLANIFICACIÓN DE LOS RECURSOS DE LA EMPRESA (ERP)

Se encarga de apoyar a los sistemas básicos funcionales de una empresa.

(Domínguez; 2012; p.35-37)

2.1 CONTROL INTERNO

Según Coopers y Lybrand, sostuvo que el control interno es un proceso efectuado por el consejo de administración, la dirección y el resto del personal de una entidad, diseñado con el objeto de proporcionar un grado de seguridad razonable en cuanto a la consecución de objetivos dentro de las siguientes categorías:

- Eficacia y eficiencia de las operaciones
- Fiabilidad de la información financiera
- Cumplimiento de las leyes y normas aplicables

De acuerdo a la definición anterior se puede inferir que el control interno se realiza de diferentes maneras en las organizaciones, pero siempre su propósito es el mismo, el cual consiste en la seguridad y resguardo de la información para la toma de decisiones de una entidad. (Coopers y Lybrand; 1997; p.22-25)

El control interno consta de cinco componentes relacionados entre sí que son inherentes al estilo de gestión de la empresa. Estos componentes están vinculados entre si y sirven como criterio para determinar si el sistema es eficaz. (Nuevos conceptos de control interno, Informe coso I; 1997; p.30-33)

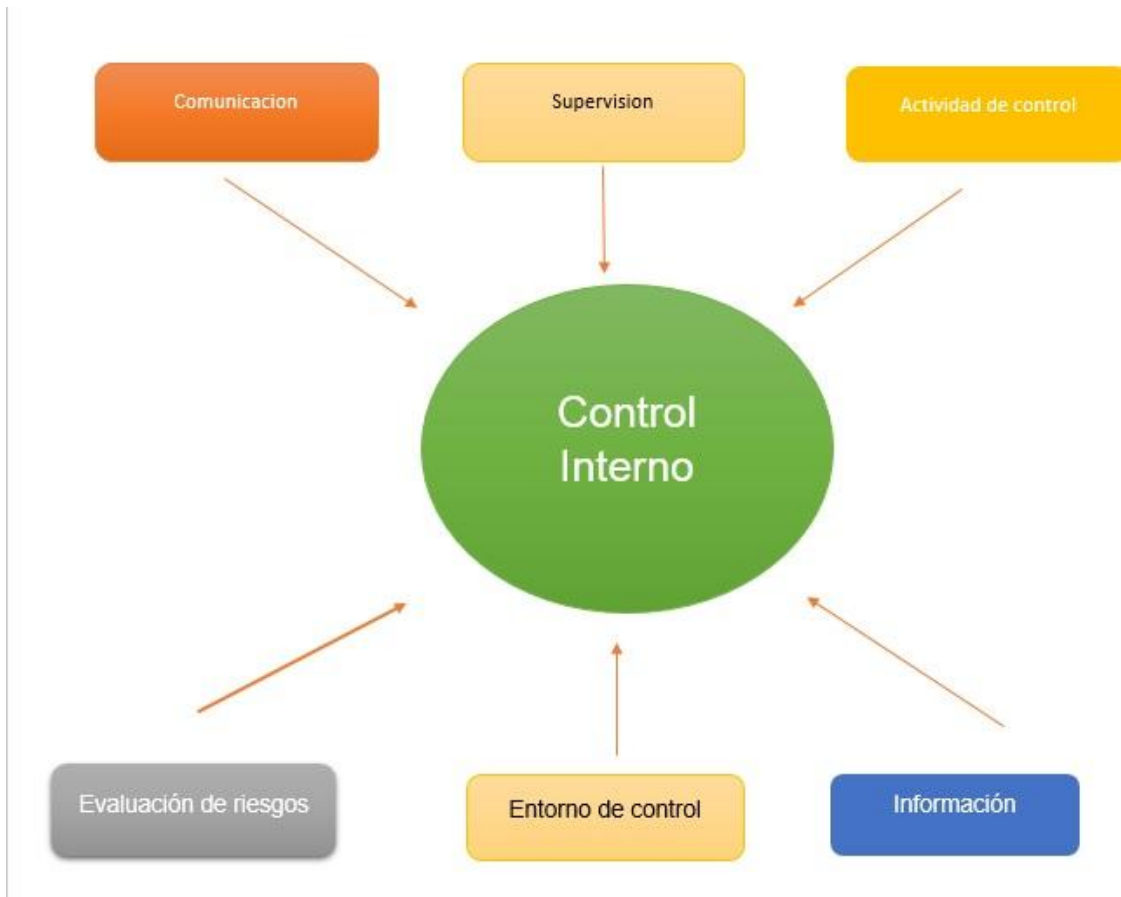
El entorno de control aporta el ambiente en el que las personas desarrollan sus actividades y cumplen con sus responsabilidades de control. Sirven como base de los otros componentes. (Nuevos conceptos de control interno, Informe coso I; 1997; p. 30-33)

Dentro de este entorno, los directivos evalúan los riesgos relacionados con el cumplimiento de determinados objetivos. Las actividades de control se establecen para ayudar asegurar que se pongan en práctica las directrices de la dirección

para hacer frente a dichos riesgos. (Nuevos conceptos de control interno, Informe coso I; 1997; p.30-33)

Mientras tanto, la información relevante se capta y se comunica por toda la organización. Todo este proceso es supervisado y modificado según las circunstancias. (Nuevos conceptos de control interno, Informe coso I; 1997; p.30-33)

FIGURA N°2: CUADRO CONTROL INTERNO



ELABORACIÓN PROPIA EN BASE A MARCO TEORICO.

3.0 INSTITUCIONES BANCARIAS

Según el Artículo 2 de la Ley 551, de la Superintendencia de Bancos e Instituciones Financieras de Chile, dice que este organismo tiene la facultad de fiscalización de las empresas cuyo giro consista en la emisión u operación de tarjetas de crédito o de cualquier otro sistema similar, siempre que dichos sistemas importen que el emisor u operador contraiga habitualmente obligaciones de dinero para con el público o ciertos sectores o grupos específicos de él. (Ley de Bancos e Instituciones Financieras de Chile N°551; 1997; p.2)

Por ende, este organismo es un ente fiscalizador del sector bancario. Para una mayor comprensión del tema será abordado el concepto de Banco, el cual se encuentra en el Artículo N°40 de la presente Ley.

Según el Artículo 40.- Banco es toda sociedad anónima especial que, autorizada en la forma prescrita por esta ley y con sujeción a la misma, se dedique a captar o recibir en forma habitual dinero o fondos del público, con el objeto de darlos en préstamo, descontar documentos, realizar inversiones, proceder a la intermediación financiera, hacer rentar estos dineros y, en general, realizar toda otra operación que la ley le permita. (Ley de Bancos e Instituciones Financieras de Chile N°551; 1997; p.28)

En esta investigación es abordada principalmente en instituciones bancarias, estas son diferenciadas nacionales e internacionales.

3.1 SECTOR BANCARIO

Se entiende como sector a un conjunto de clase o colectividad que representa caracteres particulares, que se encuentran en una zona o país determinado. Por ende, se puede concluir que el sector bancario, más conocido como la banca, se le denomina al conjunto de entidades financieras que operan dentro de la misma economía.

Además, el sistema bancario o financiero es un conjunto de instituciones, entidades financieras, cajas de ahorro y entidades de crédito que pretenden canalizar el ahorro de los prestamistas y dar seguridad a los movimientos de dinero y a los propios sistemas de pago.

3.2 FRAUDES EN EL SECTOR BANCARIO

A través de los años los fraudes en el sector bancario se han vuelto más comunes, según una noticia realizada el día 27 de Abril del presente año, **El año 2016, el Ministerio Público investigó 57.253 casos relacionados con fraudes relacionados con tarjetas bancarias. Claramente se trata de una de las formas de realizar aquel acto. Además, siguiendo con la noticia en el diario “La Tercera” el fiscal regional de la zona centro norte, Andrés Montes se refirió al tema asegurando que,** lo más difícil a la hora de perseguir este tipo de bandas es que, por un lado, la capacidad de encontrar a los sujetos es menor al 2% y que hay muchos casos en que las tarjetas son clonadas en Chile y utilizadas en el extranjero, lo que implica que **"el sistema es vulnerable y se deben mejorar las medidas de seguridad"**. (Noticia nacional de canal T13; 2017)

Por esta razón, las instituciones bancarias con el fin de resguardar la seguridad económica de sus usuarios hacen uso de medidas de prevención y detección de fraudes.

A continuación se detallan elementos de seguridad y tipos de fraudes que utiliza el sistema bancario:

3.3 ELEMENTOS DE SEGURIDAD

3.3.1 ANTI-PHISHING

Son campañas generadas por las instituciones bancarias, relacionadas con software especializado, en donde indican al usuario que no pedirán ningún tipo de clave o revelación de información confidencial. Suelen ser utilizados en servidores de grandes compañías para proteger a los usuarios y empleados por ataques de Pharming o Phishing. (Banco Chile, 2010)

3.3.2 TARJETAS BANCARIAS INTELIGENTES

Llamadas tarjetas con chip o tarjetas sin tacto, gracias a estas tarjetas se evita la clonación de las bandas magnéticas en donde se guarda toda la información bancaria del usuario, son más seguras y confiables, minimiza el fraude presencial y el mal uso de está. (Banco Santander, n.d.)

3.3.3 PROTOCOLO SEGURIDAD DE TRANSFERENCIA DE HIPERTEXTO

Es un protocolo de autorización de forma segura de datos, se utilizan códigos para crear un canal de comunicación de información codificada.

- 1) Súper clave: Es una tarjeta de coordenadas que contiene millones de posibles combinaciones. Se solicitará una

combinación única que no se repite nunca, para realizar las operaciones por Internet. (Banco Santander, n.d.)

- 2) Tercera clave: Al momento en que el cliente realiza una transacción que mueve fondos se le exige una clave dinámica privada y conocida solo por él. Pero, como existe la posibilidad que el cliente haya entregado – bajo engaño - sus claves a terceros, el banco analiza sistemáticamente las transacciones y si encuentra algún movimiento que parezca sospechoso y que no corresponde al historial del cliente, envía una tercera clave al celular o al correo del cliente para confirmar que esa transferencia sea verídica.

Para mayor seguridad, la tercera clave dura únicamente cinco minutos, por lo que el cliente debe ingresarla inmediatamente, ya que de esta manera no hay forma de engaño. Si alguien intenta realizar una transacción de manera fraudulenta, no podrá acceder a la tercera clave enviada al celular, impidiendo la consumación del fraude, y la clave caducará al cumplir su tiempo de vida. (Banco Estado, 2012).

3.3.4 DIGIPASS:

El DigiPass es hardware electrónico de alta seguridad, que genera una clave que te permite autorizar transacciones de forma segura en el portal privado de la banca en línea. Las claves que entrega el DigiPass duran un determinado período de tiempo, con el objetivo de resguardar la seguridad de cada transacción online. (Banco Chile, n.d.)

3.3.5 APLICACIONES MÓVILES:

Son aplicaciones que se descargan en celulares de usuarios los cuales cumplen la misma función que las páginas web, con la diferencia que esta de forma simple y amigable al usuario, en ellas podrás realizar operaciones como: Consulta saldos y movimientos, transferencias, envía dinero a través de cajeros automáticos, recarga celulares y paga tus cuentas, entre otros. (Banco Chile, n.d)

3.4 TIPOS DE FRAUDE:

3.4.1 ELECTRÓNICOS:

PHISHING

Phishing es un término utilizado en informática con el cual se denomina el uso de un tipo de ingeniería social, caracterizado por intentar adquirir información confidencial de forma fraudulenta, como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria. El estafador, mejor conocido como phisher se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico o algún sistema de mensajería instantánea. (Noticias de seguridad informática, 2017)

Es una estafa informática con la que se convence a una persona para que dé a sus estafadores, algún tipo de información bancaria relevante, como puede ser su clave de acceso a la banca electrónica o los datos de su tarjeta de crédito, este tipo de estafas, se convence a la víctima, por lo que en informática se conocen como técnicas de ingeniería social. Se realiza a partir de un correo electrónico no

deseado o spam, que supera el filtro de servicio de correo electrónico. (Banco BBVA, 2015).

PHARMING

Pharming es la explotación de una vulnerabilidad en el software de los servidores o en el de los equipos de los propios usuarios, que permite a un atacante re-direccionar un nombre de dominio a otra máquina distinta. De esta forma un usuario que introduzca un determinado nombre de dominio, que haya sido re-direccionado, en su explorador de internet, accederá a la página web que el atacante haya especificado para ese nombre de dominio. (Noticias de seguridad informática, 2017)

Este mecanismo consiste en conseguir direcciones de una base de datos de páginas visitas con mayor frecuencia por parte del usuario, la cual es utilizada para traducir nombres de dominio en números de protocolo de internet (dirección IP), con el fin de capturar datos confidenciales especialmente relacionados con la banca. (Banesco, 2017).

3.4.2 BANCA EN LÍNEA

KEY-LOGGERS

Es un programa que registra y graba la pulsación de teclas. La información recolectada será utilizada luego por la persona que lo haya instalado. Actualmente existen dispositivos de hardware o bien aplicaciones (software) que realizan estas tareas. (Seguridad de la Información, 2009)

Los Key-loggers físicos son pequeños dispositivos que se instalan entre nuestra computadora y el teclado. Son difíciles de identificar para un usuario inexperto pero si se presta atención es posible reconocerlos a simple vista. Tienen distintas capacidades de almacenamiento, son comprados en cualquier casa especializada y generalmente son instalados por empresas que desean controlar a ciertos empleados. Cabe aclarar que esta forma de actuar puede traer problemas legales a quien lo instala ya que registrar a un usuario mediante este accionar puede interpretarse como una violación a su privacidad. Es aquí donde cobra relevancia una política de seguridad clara, puesta por escrito y firmada por el usuario. (Seguridad de la Información, 2009)

Con respecto a las key-loggers por software, actualmente son los más comunes, muy utilizados por el malware orientado a robar datos confidenciales o privados del usuario. Como es de imaginar, la información obtenida es todo lo que el usuario ingrese en su teclado como por ejemplo documentos, nombres de usuarios, contraseñas, números de tarjetas, PIN es, etc. Esto explica el porqué de su gran éxito y utilización actual ya que como sabemos el malware, cada vez más orientado al delito, puede utilizar esta herramienta para proporcionar información sensible del usuario a un atacante. (Seguridad de la Información, 2009)

Fue uno de los primeros software o hardware detectados por la banca en línea en la década de los 90, estos permiten identificar lo que escribe o selecciona la persona en su teclado al entrar a páginas populares o al generar métodos de pago, permitiendo la captura de los datos de acceso del usuario. (Eleven Panths, 2013).

SPYWARE

El spyware es un software que recopila información de un ordenador y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del ordenador. (Más adelante, servicios y recursos para tener éxito en internet, 2017)

El término spyware también se utiliza más ampliamente para referirse a otros productos que no son estrictamente spyware. Estos productos, realizan diferentes funciones, como mostrar anuncios no solicitados (pop-up), recopilar información privada, redirigir solicitudes de páginas e instalar marcadores de teléfono. (Más adelante, servicios y recursos para tener éxito en internet, 2017)

Un spyware típico se auto instala en el sistema afectado de forma que se ejecuta cada vez que se pone en marcha el ordenador (utilizando CPU y memoria RAM, reduciendo la estabilidad del ordenador), y funciona todo el tiempo, controlando el uso que se hace de Internet y mostrando anuncios relacionados. (Más adelante, servicios y recursos para tener éxito en internet, 2017)

Son software maliciosos que se instalan con o sin tu autorización del usuario, espiando todas las operaciones e información confidencial. Se generan principalmente al ingresar a páginas falsas que aparecen en los buscadores de información y al descargar algún contenido de estos buscadores. (Banco Bci, n.d.).

3.4.3 CAJEROS AUTOMÁTICOS

ASALTO A INFRAESTRUCTURAS

Principalmente robo a cajeros automáticos, últimamente hay varias noticias sobre ellos como por ejemplo: uso de gas inflamable, bombas caseras, el robo de claves secretas mediante la tecnología, martillos o barras de hierro o simplemente llevarse el cajero. (Russia Beyond The Headlines, 2016).

SKIMMING

Consiste en la copia de la banda magnética de tu tarjeta, mediante un dispositivo de falsificación (skimmer) utilizado durante las transacciones. (Banco BCI, 2017).

Podrías encontrarlos en los cajeros automáticos, este dispositivo es insertado en la ranura de ingreso de tarjetas, haciendo pasar el dispositivo como parte del cajero. Además, en las tarjetas bancarias, estos dispositivos son utilizados, en ocasiones, cuando entregas tus tarjetas para efectuar un pago. (Banco BCI, 2017).

El skimming, una técnica delictiva que utiliza tecnología de avanzada, permite que el ladrón pueda robar claves personales de los cajeros sin la necesidad de estar presente; todo se hace a través de un dispositivo electrónico diseñado para este fin que permite capturar la información que hay en las bandas magnéticas de las tarjetas, incluyendo la clave, en el mismo momento en que el usuario teclea dicha clave. (mdzol, 2017)

En este caso, una vez que el usuario se va del cajero, el delincuente ingresa y carga los datos en un sistema con el que puede leerlos y posteriormente introducirlos en una tarjeta con una banda

magnética virgen. Digamos que es una especie de “tarjeta clon” de la original con la que se puede lograr la estafa. (mdzol, 2017)

Mediante un software especializado se realiza una clonación de tarjeta de crédito o débito, al momento de la transacción en un codificador de tarjetas o cajero automático, con la finalidad de acceder a los datos de la tarjeta y hacer uso de manera fraudulenta. (Banco BBVA, 2015).

OBJETIVOS GENERALES Y ESPECIFICOS

OBJETIVO GENERAL

Verificar los sistemas de información para detectar y prevenir fraudes a través de la auditoría en las instituciones bancarias.

OBJETIVOS ESPECÍFICOS

1. Identificar los sistemas de información que utilizan las instituciones bancarias para hacer frente a los fraudes.
2. Comparar los sistemas de información utilizados por las instituciones bancarias para la detección y prevención de los fraudes.
3. Verificar los procedimientos de la auditoría que están utilizando las instituciones bancarias.

METODOLOGIA DE LA INVESTIGACION

La presente investigación es elaborada bajo el carácter cualitativo con un alcance de sintetización, la cual se estructura de la siguiente manera:

ETAPA I: RECOPIACION DE LA INFORMACION

La recopilación de la información se basará en:

1.- La revisión de textos relacionados con auditoria, auditoria preventiva y detectiva y la labor del auditor:

- Los nuevos conceptos del control interno (Informe Coso) (1997)
- Auditoria forense: Prevención e Investigación de la Corrupción Financiera (2003)
- Sistemas de información gerencial (2012)

2.- Leyes y normativas:

- Ley General de Bancos e Instituciones Financieras emitidas por el Ministerio de Hacienda (1997)

3.- Tesis, noticias sobre las instituciones bancarias:

- Tesis: Análisis de los elementos de seguridad utilizados por una institución bancaria para prevenir fraudes electrónicos en

transacciones de igual naturaleza, en relación con la auditoria forense.

- Noticias relacionadas con el tema en la actualidad.

4.- Páginas web asociadas a auditoría, fraudes, sistemas de información e instituciones bancarias.

ETAPA II: SISTEMATIZACION DE LA INFORMACION

Los criterios de orden de la información son los siguientes:

- Auditoria
- Sistemas de información
- Instituciones bancarias

ETAPA III: ELECCION DE SUJETO DE INVESTIGACION

El sujeto de investigación será dos principales instituciones bancarias en el ámbito nacional e internacional. La entrevista se desarrollará a personas claves o con cargos de gerencia y/o jefatura (Auditores), en donde tengan la capacidad y condiciones de realizar y contestar la entrevista relacionada con la auditoria y los sistemas de información que utilizan dentro de la entidad bancaria.

Primera Institución, en la actualidad la entidad es una institución financiera líder, tanto por participación de mercado como por solidez patrimonial y rentabilidad. Las razones de este liderazgo están basadas en la especialización del negocio financiero, innovación en productos, cuidado de los riesgos, calidad de servicio hacia el cliente y una

activa participación en el mercado local, que se complementa con la red internacional que grupo Santander posee en todo el mundo.

Segunda Institución actualmente es un banco comercial que proporciona una completa gama de productos y servicios financieros una amplia base de clientes que incluye grandes corporaciones, pequeñas y medianas empresas y mercado de personas, a través de una gran red nacional de sucursales, cajeros automáticos y otros canales de distribución electrónicos.

ETAPA IV: APLICACIÓN DE LA TECNICA DE RECOGIDA DE DATOS

Ruta de investigación:

1. **Contacto inicial:** se coordinará una cita de entrevista con cada uno de los profesionales a través de llamados telefónicos y confirmación por correo electrónico.
2. **Entrevista en profundidad:** se desarrollará la entrevista a los profesionales de forma presencial en el lugar acordado anteriormente, en la cual se efectuarán preguntas relacionadas con nuestros resultados esperados conforma a la auditoria a través de los sistemas de información.
3. **Transcripción:** al finalizar la entrevista, se transcribirá en su totalidad.
4. **Revisión por parte del entrevistado:** la entrevista será enviada a los profesionales descritos anteriormente para esperar su aprobación para ser publicada posteriormente. Esta será enviada mediante correo electrónico.

5. **Informe entrevista final:** Preparar informe final en base a las entrevistas, para obtener una conclusión de la investigación realizada a las entidades bancarias en estudio.

ETAPA V: CREDIBILIDAD, CONFIRMABILIDAD, TRANSFERENCIA Y FIABILIDAD

La propuesta metodológica para la entrevista incorpora los criterios de credibilidad, confirmabilidad, transferencia y fiabilidad:

La credibilidad se realiza a través de las entrevistas desarrollas en profundidad, en la cual se espera la revisión por parte del entrevistado en cuanto a la transcripción final y su pronta confirmación.

La confirmabilidad se presentará al incorporar seis personas en total de ambas instituciones financieras los cuales son profesionales capaces de responder a la entrevista de la presente investigación.

La transferencia estará dada al describir el contexto y cada una de las entrevistas en particular, junto al desarrollo por parte de los sujetos.

La fiabilidad se entregará a partir de la presentación de la ideología de las alumnas en proceso de tesis: Fernanda Andrea Soto Ruiz y Catalina Andrea Tapia Sobarzo, que están optando al título de Contador Público y Auditor y al grado de Licenciado en Sistemas de Información Financiera y Control de Gestión.

ETAPA VI: TABULACION DE RESULTADOS

A continuación, se presenta la tabla N°1 en donde se encuentran las categorías y las subcategorías:

TABLA N°1: TABULACIÓN DE RESULTADOS

CATEGORÍAS	SUBCATEGORÍAS	SUB-SUBCATEGORÍAS
AUDITORIA	AUDITOR	RESPONSABILIDADES
	AUDITORIA PREVENTIVA	
	AUDITORIA DETECTIVA	
SISTEMAS DE INFORMACION	CONTROL INTERNO	
INSTITUCIONES BANCARIAS	SECTOR BANCARIO	TIPOS DE FRAUDE
	FRAUDES EN EL SECTOR BANCARIO	
		ELEMENTOS DE SEGURIDAD
Fuente: Elaboración Propia (2017)		

ETAPA VII: ANALISIS DE RESULTADOS

Corresponde al análisis de los resultados obtenidos a través de la entrevista realizada a los tres profesionales de las instituciones bancarias en relación a las categorías de la Tabla N°2 que lleva por nombre: Análisis de resultado

TABLA N°2: ANÁLISIS DE RESULTADOS POR CATEGORÍAS

CATEGORÍA	CONCLUSIONES
AUDITORÍA	La auditoría se utiliza para prevenir y fiscalizar eventuales fraudes que dañen el patrimonio como la imagen de la institución bancaria. Además, la auditoría se encarga de revisar que se cumplan las normativas del banco. En la actualidad, son menos los fraudes detectados hacia la institución como dentro de ella.
SISTEMA DE INFORMACIÓN	Hoy en día en las instituciones bancarias tienen mecanismos de control más rigurosos e innovadores, uno de estos es el lector de huellas para los cobros de cheques, mediante la captura de datos a través de la huella dactilar para la obtención de información y para la documentación de créditos de las distintas instituciones como por ejemplo AFP y SII. Estos mecanismos permiten tener mayor protección y control de datos e información referente a ingresos informado en Previred para validar la identidad del cliente y su vigencia de la cedula de identidad a través de este medio tecnológico. Por medio de las AFP se busca validar que los certificados entregados sean reales referente a los montos de pago de imposiciones, además de ser confirmado directamente con la superintendencia de AFP, se realizan verificaciones de domicilio tanto particular como comercial a través de empresas externas. Dentro de las instituciones bancarias cada funcionario posee un perfil y de acuerdo al cargo son las facultades y privilegios que el colaborador posee respecto al acceso de información, como mecanismo de control la institución crea usuarios para detectar que se consultó y quien lo consulto referente a cada cliente.

	Existe una ley que se encarga de prohibir la distribución de información a terceros, en caso de no cumplir con esto, el colaborador puede ser desvinculado de la entidad. Refiriéndose a lo anterior existen periódicamente cursos online obligatorios para la confirmar y recordar estos temas.
INSTITUCIONES BANCARIAS	Al descubrir un intento de fraude dentro de una institución bancaria se procede a ingresar el RUT para que no pueda operar en ninguna sucursal del banco a nivel nacional, y si es detectado se procede al cierre de su cuenta corriente si es que tuviese. En el caso que el fraude sea detectado dentro de la institución se realiza una investigación la cual puede arrojar sanciones para el involucrado y su cadena de control vulnerada, llegando incluso a la desvinculación de los funcionarios.

Fuente: Elaboración Propia (2017)

TABLA N°3: ANÁLISIS DE RESULTADOS POR SUB-CATEGORÍAS

SUBCATEGORÍA	CONCLUSIONES
AUDITOR FORENSE	El auditor previene y fiscaliza eventuales fraudes. También se encarga de revisar que se cumpla la normativa de la institución relacionados a los procesos, documentación solicitada, respaldos de documentación, acreditación y validación de estos.

	Además, verifica el cumplimiento de los procedimientos operativos, en cuanto a la confirmación correcta de la realización de los procesos y procedimientos comerciales los cuales deben cumplir las condiciones ingresadas en las propuestas de los clientes.
AUDITORIA PREVENTIVA	En la actualidad la auditoria preventiva es fundamental por lo que se debe revisar el canal de entrada del posible cliente a la institución. Se debe tener conocimiento fidedigno del cliente, validar su información y documentación con las herramientas tecnológicas que posee la institución. Se debe enviar toda la documentación a un área de prevención de fraudes, en donde se verifica con el empleador y a través de otras herramientas de autenticidad de los datos y la información. La auditoría preventiva dentro de la institución se realiza mediante controles internos recurrentes, aleatorios y a distancia respecto a cuses de productos, solicitando muestras a las oficinas y departamentos para velar por el fiel cumplimiento de las normas. Hoy en día existen cada vez más mecanismos preventivos dentro de las instituciones bancarias.
AUDITORIA DETECTIVA	Hoy en día son cada vez menos los fraudes detectados tanto hacia la institución como dentro de ella. En el caso que un fraude sea detectado se realiza una investigación la cual puede terminar en sanciones para el involucrado o incluso desvincularlo de la institución, ya que dentro de esta se crean usuarios que pueden detectar que se consultó y quien lo consulto, además a los funcionarios se les realizan permanentes capacitaciones. Para la detección de fraudes existen canales de apoyo disponibles y distintas áreas que trabajan en esto, porque las auditorias han detectado problemas en el ingreso de datos para la evaluación de un cliente refiriéndose a los ingresos y patrimonio.

	En el caso que se detecte un fraude a un cliente, se procede al bloqueo y posterior cierre de productos con el correspondiente envío de carta informativa por el motivo de cierre. Si el fraude es detectado por el cliente se procede al bloqueo de sus productos, cierre de estos y en algunos casos dependiendo del monto del fraude la cobranza a través de instancias legales.
CONTROL INTERNO	Un tipo de control interno dentro de la institución bancaria es realizar la revisión a la documentación de tesorería, arqueo de caja y bóveda. Además mensualmente se solicitan respaldo de operaciones realizadas para la verificación de algún error (fraude operativo, cheques, documentación falsa, entre otros). Si el departamento de control interno de la entidad detecta algún error se procede a una investigación respecto a la situación y posterior daño de la cadena de control interno.
SECTOR BANCARIO	Dentro del sector bancario existen organismos encargados de auditar, pero no son el resorte del banco propiamente tal. En el ambiente bancario cualquier tipo de fraude que es detectado ya sea por clientes o funcionarios involucra la realización de una investigación que pueda arrojar sanciones o la desvinculación.
FRAUDES	En la actualidad se ha cumplido con el objetivo de las instituciones bancarias con respecto a la disminución del porcentaje de fraudes, además del monto de riesgo involucrado. Uno de los fraudes más comunes es la entrega de documentación adulterada por parte de los clientes para acceder a mayores beneficios crediticios.

Fuente: Elaboración Propia (2017)

TABLA N°4: ANÁLISIS DE RESULTADOS POR SU-SUBCATEGORÍAS

SU-SUBCATEGORÍA	CONCLUSIONES
RESPONSABILIDAD	La responsabilidad del Auditor es prevenir y fiscalizar eventuales fraudes que dañen el patrimonio e imagen de la institución. Se encarga de la revisión del cumplimiento de la normativa del banco en cuanto a procesos, documentación y acreditación y/o validación de estos. El auditor forense forma parte del departamento de control de la institución, por el cual realizan controles en área comercial y operacional.
TIPOS DE FRAUDE	El tipo fraude más común en las instituciones bancarias es la entrega de documentación adulterada, que realizan para acreditar mayores ingresos a los reales y de esta forma llegar a montos más altos de créditos. Además esta adulteración de información se utiliza para la admisión como liquidaciones de remuneraciones falsas u otra información para acreditar ingresos mensuales, que pueden estar vencidos en su plazo como estado de situaciones mayores a un año al momento de evaluar. Otro tipo de fraude está relacionado con el área de operaciones, documentos mercantiles y adulteración de documentos en cobro, por esta razón es el área más vulnerable al momento de cometer un error, ya que diariamente se genera un gran número de transacciones.

ELEMENTOS DE SEGURIDAD	Como elementos de seguridad las instituciones bancarias cuentan como variados mecanismos como los siguientes: innovación tecnológica el cual permite tener mayor protección de datos mediante software que se encargan de leer la huella de dactilar para la verificación de identidad, vigencia de cedula de identidad y obtención fidedigna de ingresos del cliente a través del programa Previred, AFP y SII. Otro elemento de seguridad al momento de ser detectado el fraude se procede al bloqueo y cierre de productos del cliente. Como elemento de seguridad hacia los funcionarios de la institución bancaria es la permanente capacitación hacia ellos, además de canales de apoyos disponibles para su seguridad. Otro elemento de control es mediante la verificación de domicilios tanto particular como comercial por medio de empresas externas. Además en la actualidad se cuenta con un departamento que se encarga de la verificación de toda la información y documentación presentada por el cliente.
--------------------------------------	---

Fuente: Elaboración Propia (2017)

ETAPA VIII: DISCUSIÓN DE RESULTADOS

Al momento de realizar la presente investigación se puede confirmar que la información obtenida en el marco teórico concuerda en ciertos parámetros con la información recopilada mediante las entrevistas.

El contador auditor, como se plantea en la información recopilada mediante entrevistas, su principal responsabilidad es velar por el cumplimiento de la normativa de la institución bancaria, de forma que previene y fiscaliza eventuales fraudes dentro de las

entidades. Además, se encarga de detectar eventuales fraudes que puedan dañar la imagen de la institución. El auditor forma parte del departamento de control el cual verifica el cumplimiento de los procedimientos operacionales y comerciales. También, valida y verifica la documentación solicitada a los clientes, con el propósito de que la información entregada sea fidedigna y confiable.

Como se plantea en el marco teórico la auditoria preventiva ayuda a reconocer las áreas de la organización que presenta mayor riesgo a sufrir algún tipo de delito, ya que es muy común que los miembros de la entidad sacan ventajas de las deficiencias de los controles preventivos. En la recopilación de la entrevista se destaca que es fundamental revisar el canal de entrada del posible cliente, se debe tener conocimiento fidedigno, validar su información y documentación mediante controles tecnológicos. Dentro de las instituciones bancarias se realizan controles internos recurrentes y aleatorios, solicitando muestras a las oficinas y departamentos para velar por el fiel cumplimiento de las normas y políticas, evitando que los miembros de la institución saquen ventaja de la deficiencia de controles.

Referido a la auditoria detectiva el marco teórico indica que la empresa proporciona información sobre los efectos directos e indirectos que ocasionan los fraudes, en concordancia con la información capturada de las entrevistas realizadas a las instituciones bancarias que indican que hoy en día son cada vez menos los fraudes detectados dentro y fuera de la entidad. Al momento que el fraude es detectado se realiza una investigación la cual determina sanciones para los involucrados. Los funcionarios son permanentemente capacitados, estos poseen usuarios en los cuales se detecta que y quien consultó. Los procedimientos a seguir cuando se detecta un fraude a un cliente se procede a bloqueo y cierre de sus productos, además se le envía una carta por el motivo de cierre, en caso que el cliente sea el que comete el fraude se procede al cierre de sus productos y dependiendo del monto a la cobranza a través de instancias legales.

Según el marco teórico indica que la auditoria se encarga de analizar la situación de una entidad, ya que se basa en la supervisión del control interno dentro de una

organización, lo cual se relaciona con las respuestas de los entrevistados los cuales mencionan que la auditoria se encarga de prevenir y fiscalizar eventuales fraudes mediante el cumplimiento de las normativas dentro de las instituciones bancarias. Dentro de las entidades bancarias el control interno se realizan de diferentes maneras, pero su propósito siempre es el mismo el cual consiste en la seguridad y resguardo de la información, la cual entrega un grado de seguridad razonable en cuanto a la consecución de objetivos. En las entrevistas realizadas se determinan diferentes tipos de controles internos los cuales son revisión a la documentación de tesorería, arqueo de caja y bóveda. Además mensualmente se solicitan respaldo de operaciones realizadas para la verificación de algún error (fraude operativo, cheques, documentación falsa, entre otros). Si el departamento de control interno de la entidad detecta algún error se procede a una investigación respecto a la situación y posterior daño de la cadena de control interno.

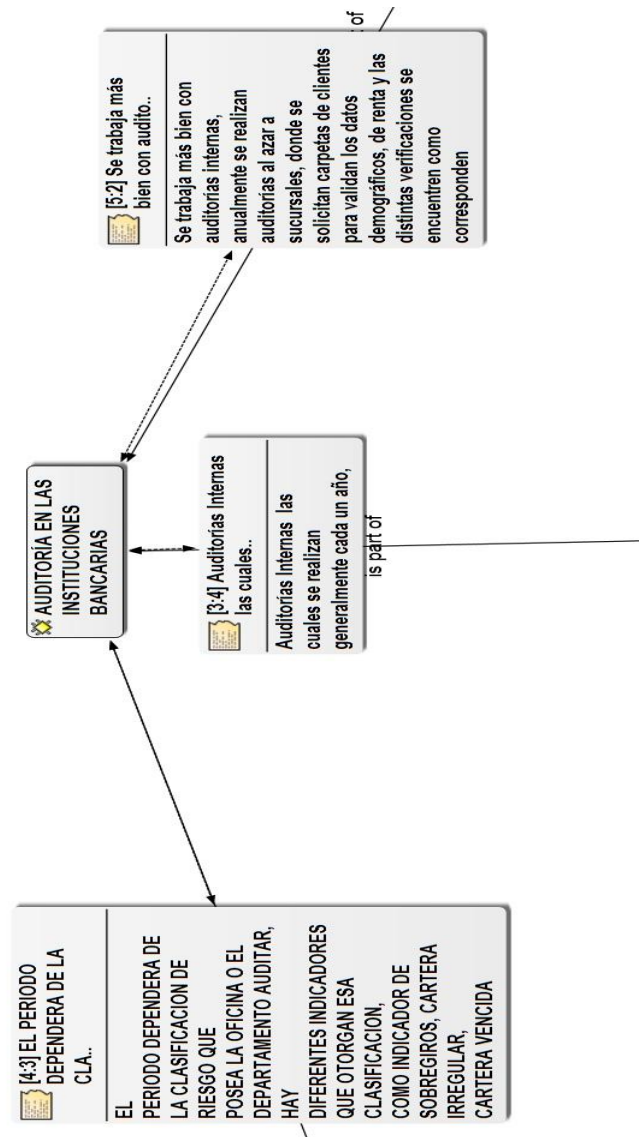
Según la investigación los sistemas de información son un conjunto de componentes interrelacionados que recolectan, procesan, almacenan y distribuyen información para apoyar la toma de decisiones y el control en una organización. En las entrevistas hacen referencia a los distintos tipos de mecanismos de control más rigurosos e innovadores los cuales son el lector de huellas, el cual permite tener mayor protección y control de datos e información referente a ingresos informados. Otro mecanismo de control se realiza por medio de la validación de información mediante Previred, SII y AFP, junto con su cedula de identidad. Además, la institución crea usuarios para detectar que se consultó y quien lo consulto referente a cada cliente. Actualmente existe una ley que se encarga de prohibir la distribución de información a terceros, en caso de no cumplir con esto, el colaborador puede ser desvinculado de la entidad.

Al realizar la entrevista se determina que no hay concordancia con los diferentes tipos de fraudes, debido que los entrevistados hacen relación a los fraudes internos de la organización y el marco teórico menciona los diferentes tipos de fraudes a los que están expuestos los clientes que poseen productos en alguna institución bancaria. Los fraudes propuestos en la entrevista son la entrega de documentación adulterada (liquidación de remuneraciones u otra información para acreditar ingresos mensuales) con el fin de optar a montos más altos de créditos. Otro tipo de fraude se relaciona con el área de

operaciones y adulteración de documentos mercantiles y de cobro, debido a que diariamente se genera un gran número de transacciones. Por otro lado el marco teórico menciona fraudes que están relacionados directamente a los clientes como los relacionados con la clonación de tarjetas bancarias.

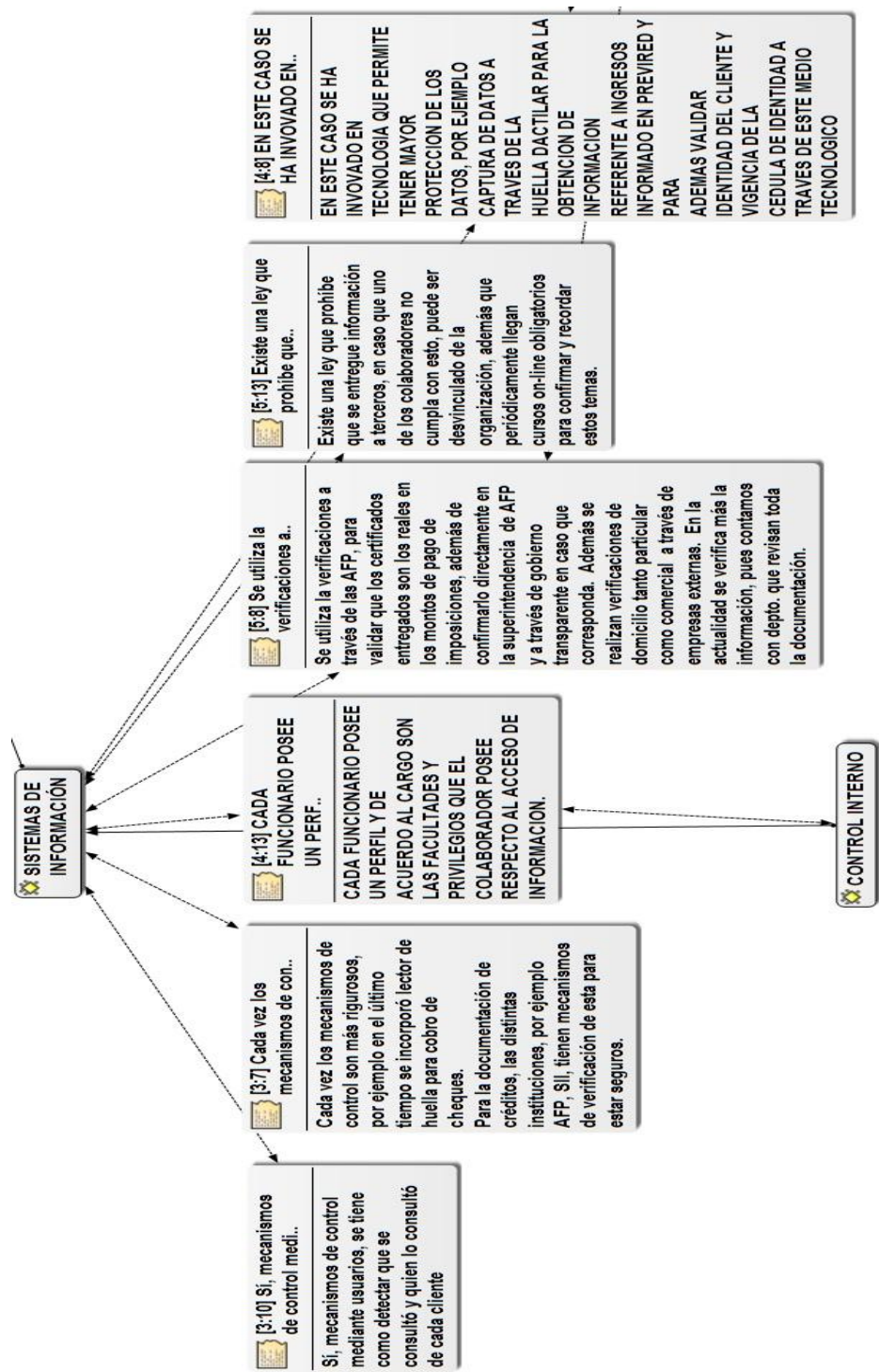
En cuanto a los elementos de seguridad en las instituciones bancarias no existe concordancia al momento de comparar el marco teórico frente a la entrevista. Debido que en la investigación menciona elementos de seguridad que ocurren de forma global a los clientes como por ejemplo el Anti-Phishing, tarjetas bancarias inteligentes, aplicaciones móviles y Digipass. Por otro lado los entrevistados dan a conocer mecanismos de seguridad destinados a la protección de la institución bancaria los cuales son la innovaciones tecnológicas mediante software, verificación por medio de huella dactilar y verificación de documentos a través de plataformas virtuales (Previred, SII y AFP). Otro elemento de control es mediante la verificación de domicilios tanto particular como comercial por medio de empresas externas.

FIGURA N°3: REPRESENTACIÓN ÁRBOL ATLASTI



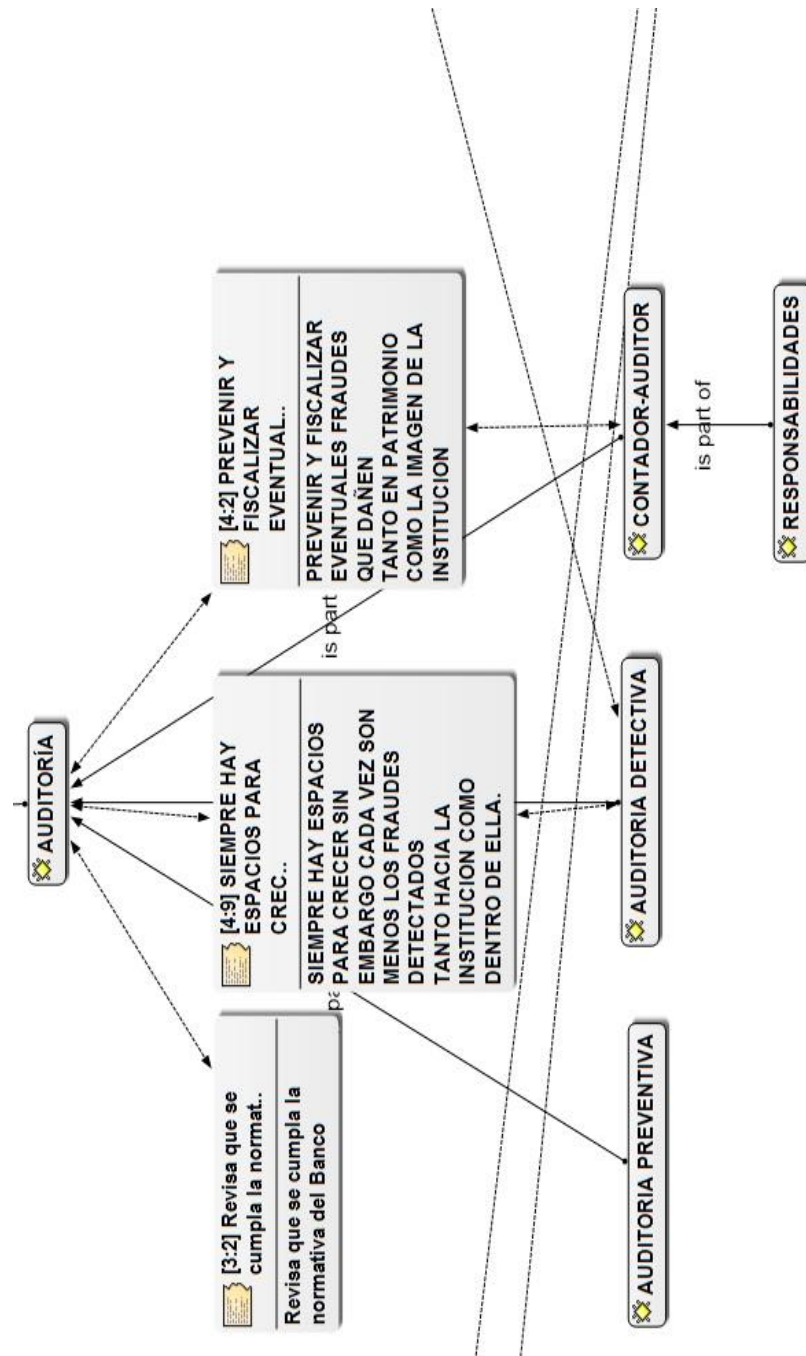
ELABORACIÓN PROPIA EN BASE A ENTREVISTAS REALIZADAS.

FIGURA N°4: REPRESENTACIÓN ÁRBOL ATLASTI



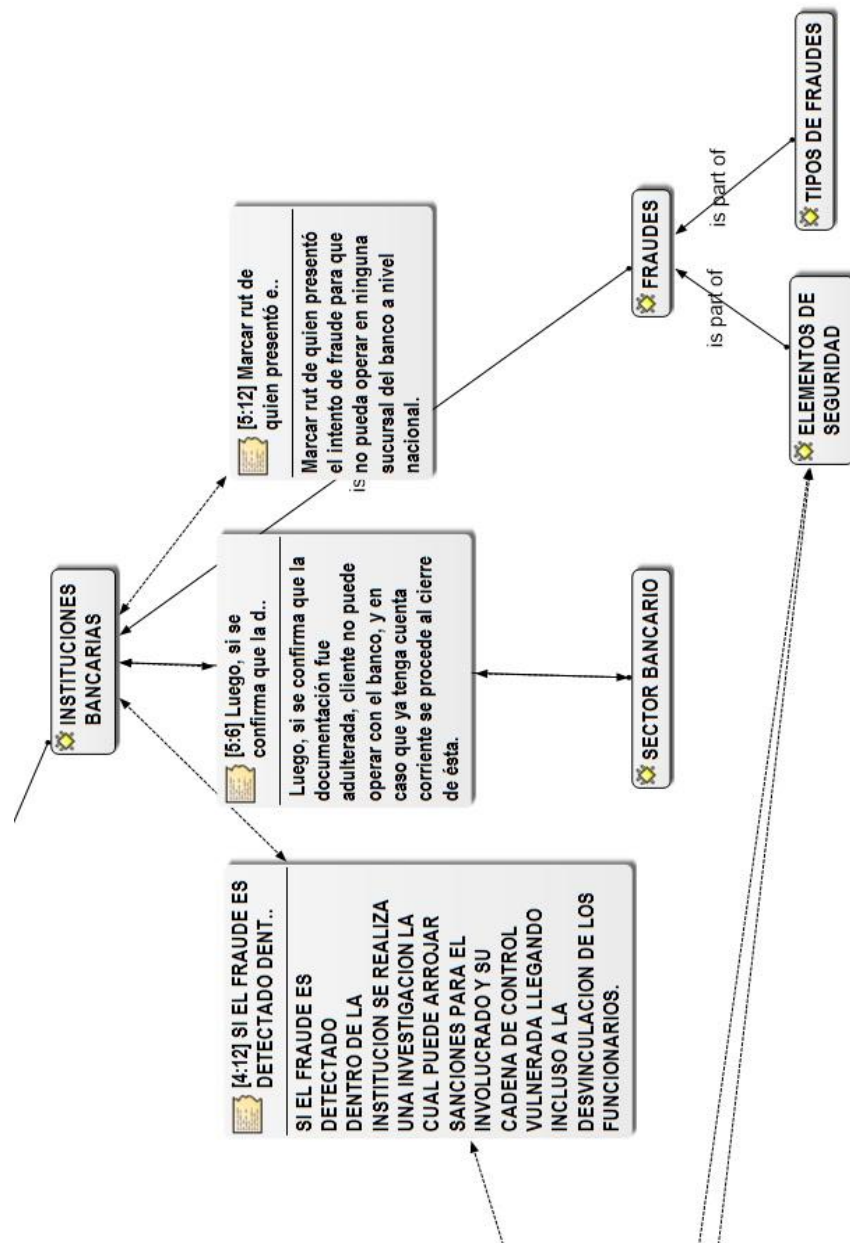
ELABORACIÓN PROPIA EN BASE A ENTREVISTAS REALIZADAS.

FIGURA N°5: REPRESENTACIÓN ÁRBOL ATLSTI



ELABORACIÓN PROPIA EN BASE A ENTREVISTAS REALIZADAS.

FIGURA N°6: REPRESENTACIÓN ÁRBOL ATLASTI



ELABORACIÓN PROPIA EN BASE A ENTREVISTAS REALIZADAS.

ETAPA IX: CONCLUSIONES

Es la comparación entre los objetivos planteados y los resultados obtenidos a través de la entrevista realizada a los profesionales en esta investigación

Al verificar los sistemas de información que son utilizados en las instituciones bancarias para hacer frente a los fraudes, se observa que ambas entidades poseen sistemas de información actualizados para detectar y prevenir hechos fraudulentos, como son la validación de certificados a través de AFP, verificaciones de domicilio particular y comercial, lector de huella para cobros de cheques, verificación de ingresos entregados mediante Previred y verificación de documentos mediante Servicio de Impuestos Internos. Ambas instituciones bancarias coinciden en que el objetivo de los sistemas de información ha contribuido a la prevención de fraudes ya que ha disminuido en el tiempo.

Al comparar los sistemas de información utilizados por las instituciones bancarias y los procedimientos a seguir cuando es detectado un fraude, se observa una gran similitud, ya que al momento que es detectado se procede a realizar una investigación y si el fraude es efectuado por un cliente se bloquean y cierran sus productos, en donde se envía una carta informativa de cierre. En el caso que el fraude es detectado dentro de la entidad, se arrojan sanciones para el involucrado y su cadena de control vulnerada, llegando incluso a la desvinculación de los funcionarios, además se le informa al área pertinente afectada y está a toda la red para evitar futuros fraudes. Ambas instituciones bancarias coinciden en que aplican sistemas de información para impedir acceso a información confidencial sobre clientes a sus colaboradores, ya que cada funcionario tiene un perfil y poseen mecanismos de control que ayudan a detectar que se consultó y quien consulto de cada cliente.

Las instituciones antes mencionadas, trabajan con auditorías internas y externas, las cuales solicitan documentación para verificar la información entregada y mensualmente se solicitan el envío de respaldos de operaciones realizadas. En una institución bancaria las auditorías internas se realizan por lo general en un año, mientras que en la otra institución bancaria el periodo de auditoria depende de la clasificación de riesgo que posea la oficina o el departamento auditar.

Los procedimientos de auditoria que utilizan las instituciones bancarias se aplican mediante el control interno de la entidad, al ser identificado un fraude se procede a realizar una investigación respecto al daño causado a la cadena de control interno, en una de las instituciones el principal daño se efectúa por el exceso de confianza, en ambas entidades el control interno se encarga de revisar los procesos en los cuales se pudo haber cometido el error y se debe enviar todo a un área de prevención de fraude que se encarga de verificar la autenticidad de la información.

Las instituciones bancarias mencionadas anteriormente coinciden que el fraude más común en la actualidad es la entrega de información adulterada por parte de clientes como por ejemplo la acreditación de ingresos mensuales, con el fin de llegar a montos más altos de créditos.

En lo expuesto, se puede considerar que ambas instituciones bancarias una internacional y la otra nacional, tienen bien definido sus procedimientos para la detección y prevención de los fraudes, ya que se deben actualizar regularmente debido a los avances tecnológicos, es por ello que se deben utilizar nuevos sistemas de información y revisiones constantes al control interno de la entidad, con el fin de combatir todos los fraudes. Periódicamente se deben efectuar capacitaciones a sus funcionarios con el propósito de estar preparados ante cualquier amenaza y de esta manera ir disminuyendo cada vez más los hechos fraudulentos.

BIBLIOGRAFÍA

1. Arteaga, D (2014). Auditoria. 20 abril 2017 (<https://veritasonline.com.mx/auditoria-forense-prevencion-y-deteccion/>)
2. Banco BBVA, (2015). Un ejemplo de phishing paso a paso. Obtenida el 15 julio 2015, de <https://www.bbva.com/es/un-ejemplo-de-phishing-paso-a-paso/>
3. Banco BBVA, (2015). Skimming: la estafa de clonación de tarjetas. Obtenida el 15 de julio 2017, de <https://www.bbva.com/es/skimming-la-estafa-la-clonacion-tarjetas/>
4. Banco Bci, (n.d.). Internet y móvil spyware. Obtenida el 29 de junio 2017, de <http://www.bci.cl/personas/seguridad/spyware.html>
5. Banco Chile. (2010). Alerta de Fraude. Obtenida el 5 julio 2017, <https://ww3.bancochile.cl/wps/wcm/connect/bchempresas/bancodechile/empresas/seguridad/alerta-phishing-banconexion+>
6. Banco Chile. (n.d.). ¿Qué es el digipass?. Obtenida el 10 de Julio 2017, de <http://ww3.bancochile.cl/wps/wcm/connect/personas/portal/seguridad/que-es-el-digipass>
7. Banco chile. (n.d.). Móvil. Obtenida el 10 de julio 2017, de <http://ww3.bancochile.cl/wps/wcm/connect/personas/portal/canales/movil/mi-banco>
8. Banco Santander. (n.d.). Clave secreta. Obtenida el 5 de Julio 2017, de <https://www.santander.cl/servicios/personas/superclave/index.asp>

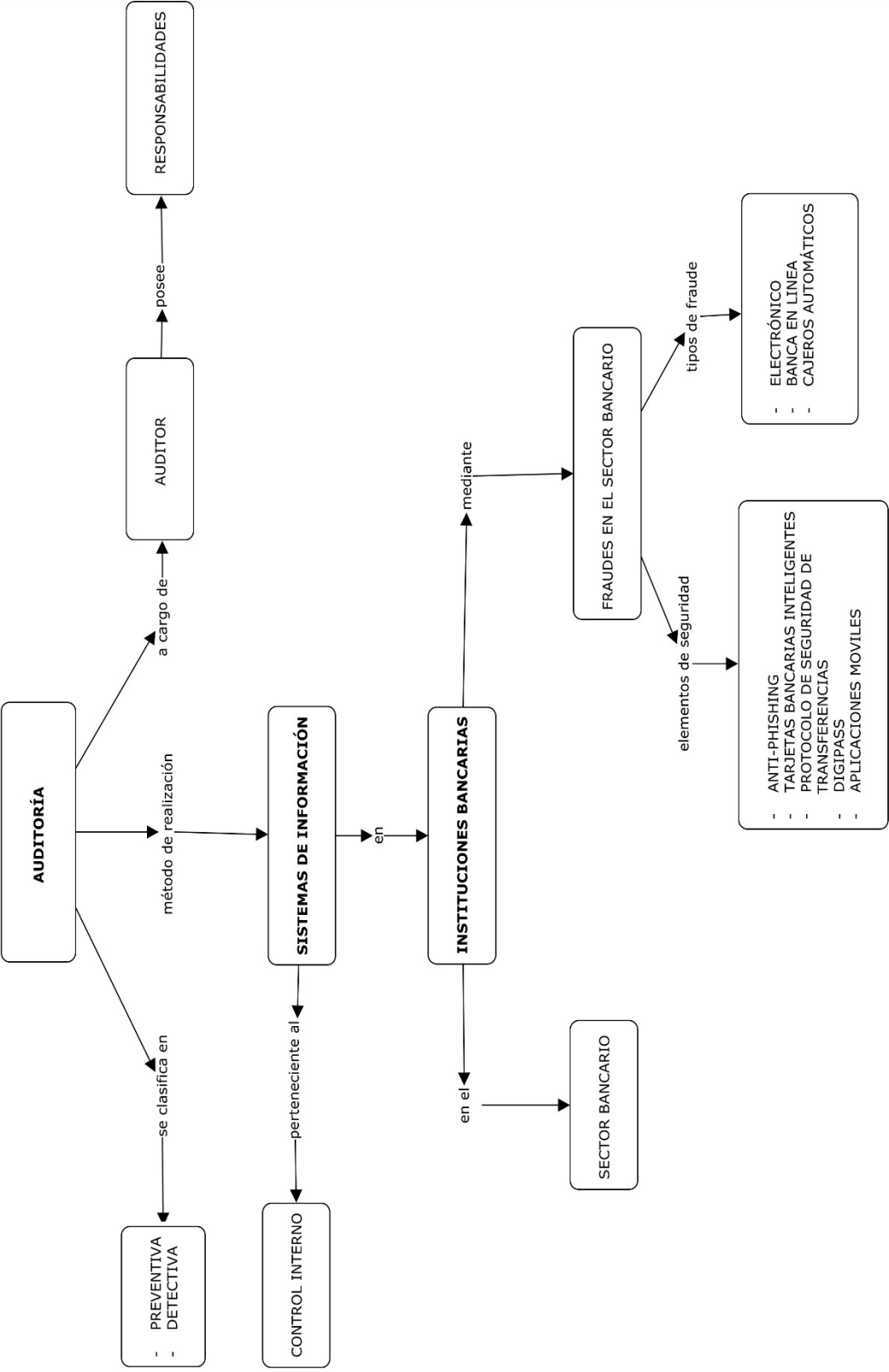
9. Banco Estado. (2012). Tercera clave. Obtenida el 5 de julio 2017, de <http://www.corporativo.bancoestado.cl/sala-de-prensa/noticias-bancoestado/noticias-2012/2015/09/04/tercera-clave-bancoestado-preocupado-por-la-seguridad-de-sus-clientes>
10. Banesco (2017). Banca por internet y banca móvil. Obtenida el 5 de Julio del 2017 de <http://www.banesco.com/seguridad/banca-por-internet-y-banca-movil/tipos-de-fraude-que-ocurren-en-la-banca-electronica>
11. Bernal, C. F. (2010). Rol y Funciones de la Auditoria Interna y Externa. *Actualidad empresarial*, 214.
12. Canal de Televisión Nacional T13 (23 de Abril 2017) Fraude con tarjetas bancarias”; Chile; 2017. Obtenido de <http://www.t13.cl/noticia/nacional/fraude-tarjetas-bancarias-fiscal-montes-critico-usuarios-paguen-cuando-sean-victimas>
13. Cano, miguel y Lugo, Danilo; “Auditoria Forense en la Investigación Criminal del Lavado de Dinero y Activos”; Ecoe Ediciones; Bogotá-Colombia; 2005; p. 16,20.
14. Coopers y lybrand; “Los nuevos conceptos del control interno”; Ediciones Díaz de Santos; 1997; p.22-28
15. Díaz Céspedes, Rocío (2014). *Análisis de los elementos de seguridad utilizados por una institución bancarias para prevenir fraudes electrónicos en transacciones de igual naturaleza, en relación con la auditoría forense*”.
16. Domínguez; “Análisis de sistemas de información”; Red Tercer Milenio; México; 2012; p.35-37

17. Escamilla, V.M. (20 de junio del 2017). Expansión en alianza con CNN. Obtenido de <http://expansion.mx/mi-dinero/2012/06/20/los-5-fraudes-mas-temidos-por-los-bancos>
18. Gonzalez, L. (31 de mayo de 2009). *La Contabilidad y la Etica del profesional* . Obtenido de <http://contaudito.blogspot.cl/2009/05/definicion-del-contador-auditor.html>
19. Laudon, Kenneth y Jane; “Sistemas de Información Gerencial”; Administración de La Empresa Digital; México; 2012; Capítulo I
20. Maldonado, Milton; “Auditoria Forense: Prevención e Investigación de la Corrupción Financiera”; Editora Luz de América; Quito-Ecuador; 2003; p.9.
21. Ministerio de Hacienda (13 de junio 2017) “Ley General de Bancos e Instituciones Financieras”; Chile; 1997. Obtenido de http://www.sbif.cl/sbifweb/internet/archivos/ley_551.pdf
22. n.d. (mayo de 2009). *Modelo Auditoria SG Seguridad y Salud Laboral en la Empresa* . Obtenido de http://www.cge.es/portalcge/novedades/2009/prl/pdf_auditoria/capitulo3_4_2.pdf
23. Blog Eleven Panths (2013) Keyloggers y protecciones. Obtenido el 5 de Julio 2017 de <http://blog.elevenpaths.com/2013/07/keyloggers-y-protecciones-de.html>
24. Diario Russia Beyond The Headlines (2016). Obtenido el 5 de Junio de https://es.rbth.com/pol%C3%ADtica-y-sociedad/sociedad/2016/05/31/4-consejos-practicos-de-criminales-rusos-para-robar-un-cajero-automatico_598883

25. Blog Dragonjar (2017) anti-phishing 11 de Diciembre 2017 de <https://www.dragonjar.org/anti-phishing>
26. Más adelante, servicios y recursos para tener éxito en internet (2017) , 11 de Diciembre 2017 de <http://www.masadelante.com/faqs/que-es-spyware>
27. Blog Seguridad de la información (2017), 11 de Diciembre 2017 de <http://www.segu-info.com.ar/malware/keylogger.htm>
28. Diario digital Argentino mdzol (2009), 11 de Diciembre 2017 de <http://www.mdzol.com/nota/100078-cuidado-llego-el-skimming-el-fraude-que-permite-duplicar-tarjetas-de-credito-y-debito/>
29. Blog Seguridad de la información (2017), 11 de Diciembre 2017 de <https://seguinfo.wordpress.com/2007/07/24/%C2%BFque-es-el-pharming/>
30. Coopers y lybrand; “Los nuevos conceptos del control interno”; Ediciones Díaz de Santos; 1997; p.30-33

ANEXOS

ANEXO N°1: MAPA CONCEPTUAL



FUENTES:
ELABORACIÓN PROPIA (2017)

ANEXO N°2: TRANSCRIPCION ENTREVISTAS

2.1 ENTREVISTA N°1

Objetivo: Identificar los sistemas de información utilizados en dos entidades bancarias en el ámbito nacional e internacional, para la prevención y detección de fraudes, a través de la auditoria forense.

Nombre (opcional) Carol Muñoz Santis

Cargo del profesional: Agente

1. ¿Cuál es el rol del contador auditor en esta institución bancaria?

Dentro del banco existe el área de control para la parte comercial, que verifica que se cumplan las condiciones ingresadas en las propuestas de los clientes. Además, se realiza controles al área de operaciones para confirmar la correcta realización de los procesos.

2. ¿La entidad bancaria trabaja principalmente con auditoria interna o externa? ¿Cada cuánto periodo son realizadas las auditorias?

Se trabaja más bien con auditorías internas, anualmente se realizan auditorías al azar a sucursales, donde se solicitan carpetas de clientes para validar los datos demográficos, de renta y las distintas verificaciones se encuentren como corresponden, además de realizar revisión a la documentación de tesorería, arqueos a las cajas y bóvedas. Además mensualmente solicitan enviar respaldos de operaciones realizadas.

3. Respecto a la ocurrencia de algún fraude ¿Cómo se aplica el control interno en la entidad?

Ante el curso de alguna operación, tanto el ejecutivo, como luego el agente debe verificar que los antecedentes y documentación que cliente presentó sea fidedigna, en el caso que se encuentre alguna incongruencia, se debe enviar todo a un área de prevención de fraude quien verificará con empleador y a través de otras

herramientas la autenticidad de la información. Luego, si se confirma que la documentación fue adulterada, cliente no puede operar con el banco, y en caso que ya tenga cuenta corriente se procede al cierre de ésta.

4. ¿Cuáles son los tipos de fraude más comunes dentro de las Institución bancaria? ¿Por qué?

El fraude más común es la entrega de documentación adulterada, que realizan para acreditar mayores ingresos a los reales y de esa forma llegar a montos más altos de crédito.

5. ¿Qué sistema de información utiliza en la actualidad el banco para prevenir y detectar fraudes dentro de la Institución Bancaria? ¿Siempre se ha utilizado los mismos SI?

Se utiliza las verificaciones a través de las AFP, para validar que los certificados entregados son los reales en los montos de pago de imposiciones, además de confirmarlo directamente en la superintendencia de AFP y a través de gobierno transparente en caso que corresponda. Además se realizan verificaciones de domicilio tanto particular como comercial a través de empresas externas. En la actualidad se verifica más la información, pues contamos con depto. que revisan toda la documentación.

6. En su opinión, ¿cree que se han cumplido los objetivos en cuanto a la prevención de fraudes?

Se ha cumplido el objetivo, pues ha disminuido el porcentaje de fraude además del monto de riesgo involucrado.

7. ¿Cómo previene y detecta el fraude la entidad bancaria?

La prevención es fundamental, por lo que se debe revisar el canal de entrada del posible cliente, tener conocimiento cabal del cliente (saber a lo que realmente se

dedica) validar la información y documentación con las herramientas mencionadas anteriormente.

8. ¿Cuáles son los procedimientos a seguir cuando estos son detectados?

Marcar rut de quien presentó el intento de fraude para que no pueda operar en ninguna sucursal del banco a nivel nacional. En caso que ya sea cliente se procede al bloqueo y posterior cierre de productos con el correspondiente envío de carta informativa del motivo del cierre.

9. La institución Bancaria con respecto a sus colaboradores ¿Aplica algún sistema de información, para impedir el acceso a información confidencial sobre sus clientes?

Existe una ley que prohíbe que se entregue información a terceros, en caso que uno de los colaboradores no cumpla con esto, puede ser desvinculado de la organización, además que periódicamente llegan cursos on-line obligatorios para confirmar y recordar estos temas.

2.2 Entrevista N°2

Objetivo: Identificar los sistemas de información utilizados en dos entidades bancarias en el ámbito nacional e internacional, para la prevención y detección de fraudes, a través de la auditoria forense.

Nombre (opcional): Marjorie Barrios Lizardi

Cargo del profesional: Jefe de Plataforma Empresas

1. ¿Cuál es el rol del contador auditor en esta institución bancaria?

Revisa que se cumpla la normativa del Banco en cuanto a los procesos, documentación solicitada, tanto los respaldos de esta documentación, acreditación y validación. Que los procedimientos tanto operativos como comerciales se cumplan en tiempo y forma.

- 2. ¿La entidad bancaria trabaja principalmente con auditoria interna o externa?
¿Cada cuánto periodo son realizadas las auditorias?**

Auditorías Internas las cuales se realizan generalmente cada un año, también existen organismos externos que nos auditan, pero no es resorte del Banco propiamente tal.

- 3. Respecto a la ocurrencia de algún fraude ¿Cómo se aplica el control interno en la entidad?**

El este control se revisan los procesos en los cuales se pudo haber cometido algún error, dependiendo del tipo de fraude, operativo, cheques, documentación falsa, blancas, etc

- 4. ¿Cuáles son los tipos de fraude más comunes dentro de las Institución bancaria? ¿Por qué?**

Generalmente los relacionados con área de operaciones, cheques, adulteración de documentos en cobro. Más que nada por el número de transacciones en el día en esta área es más fácil que se pueda cometer un error y es inmediato.

- 5. ¿Qué sistema de información utiliza en la actualidad el banco para prevenir y detectar fraudes dentro de la Institución Bancaria? ¿Siempre se ha utilizado los mismos SI?**

Cada vez los mecanismos de control son más rigurosos, por ejemplo en el último tiempo se incorporó lector de huella para cobro de cheques.

Para la documentación de créditos, las distintas instituciones, por ejemplo AFP, SII, tienen mecanismos de verificación de esta para estar seguros.

- 6. En su opinión, ¿cree que se han cumplido los objetivos en cuanto a la prevención de fraudes?**

Sí cada vez más.

- 7. ¿Cómo previene y detecta el fraude la entidad bancaria?**

Con los mecanismos utilizados anteriormente y las distintas áreas que trabajan en esto, además de todos los canales de apoyo disponibles.

Capacitaciones permanentes a los trabajadores.

- 8. ¿Cuáles son los procedimientos a seguir cuando estos son detectados?**

Se informa al área pertinente afectada y está a toda la red con el fin de aprender de la experiencia

- 9. La institución Bancaria con respecto a sus colaboradores ¿Aplica algún sistema de información, para impedir el acceso a información confidencial sobre sus clientes?**

Sí, mecanismos de control mediante usuarios, se tiene como detectar que se consultó y quien lo consultó de cada cliente

2.3 Entrevista N°3

Objetivo: Identificar los sistemas de información utilizados en dos entidades bancarias en el ámbito nacional e internacional, para la prevención y detección de fraudes, a través de la auditoria forense.

Nombre (opcional): _____

Cargo del profesional: EJECUTIVO DE CUENTAS BBPP

1. ¿Cuál es el rol del contador auditor en esta institución bancaria?

Prevenir y fiscalizar eventuales fraudes que dañen tanto en patrimonio como la imagen de la institución.

2. ¿La entidad bancaria trabaja principalmente con auditoria interna o externa? ¿Cada cuánto periodo son realizadas las auditorias?

Trabaja con ambas, el periodo dependerá de la clasificación de riesgo que posea la oficina o el departamento auditar, hay diferentes indicadores que otorgan esa clasificación, como indicador de sobregiros, cartera irregular, cartera vencida.

3. Respecto a la ocurrencia de algún fraude ¿Cómo se aplica el control interno en la entidad?

Se procede a realizar una investigación respecto a en qué situación se dañó la cadena de control interno. Habitualmente esta se daña por el exceso de confianza.

4. ¿Cuáles son los tipos de fraude más comunes dentro de las Institución bancaria? ¿Por qué?

Los que competen a mi área principalmente por parte de los clientes la adulteración de información en la admisión como liquidaciones de sueldo u otra información solicitada para acreditación de ingresos mensuales. Las auditorias han detectado además

problemas en el ingreso de datos para la evaluación de un cliente tanto lo referente a sus ingresos como a su patrimonio, estos problemas son principalmente que la documentación requerida no cumple la política de admisión utilizando datos que si bien son correctos pueden estar vencidos en su plazos como estados de situaciones mayores a un año al momento de evaluar.

5. ¿Qué sistema de información utiliza en la actualidad el banco para prevenir y detectar fraudes dentro de la Institución Bancaria? ¿Siempre se ha utilizado los mismos SI?

En este caso se ha innovado en tecnología que permite tener mayor protección de los datos, por ejemplo captura de datos a través de la huella dactilar para la obtención de información referente a ingresos informado en previred y para además validar identidad del cliente y vigencia de la cedula de identidad a través de este medio tecnológico.

6. En su opinión, ¿cree que se han cumplido los objetivos en cuanto a la prevención de fraudes?

Siempre hay espacios para crecer sin embargo cada vez son menos los fraudes detectados tanto hacia la institución como dentro de ella.

7. ¿Cómo previene y detecta el fraude la entidad bancaria?

Con controles internos recurrentes aleatorios y a distancia respecto a curses de productos, solicitando muestras a las oficinas y departamentos para velar por el fiel cumplimiento de las normas.

8. ¿Cuáles son los procedimientos a seguir cuando estos son detectados?

Si el fraude es efectuado por el cliente, se procede al bloqueo de sus productos, cierre de estos y en algunos casos dependiendo el monto del fraude la cobranza a través de instancias legales. si el fraude es detectado dentro de la institución se realiza una

investigación la cual puede arrojar sanciones para el involucrado y su cadena de control vulnerada llegando incluso a la desvinculación de los funcionarios.

9. La institución Bancaria con respecto a sus colaboradores ¿Aplica algún sistema de información, para impedir el acceso a información confidencial sobre sus clientes?

Cada funcionario posee un perfil y de acuerdo al cargo son las facultades y privilegios que el colaborador posee respecto al acceso de información.