Universidad de Valparaíso

Facultad de ciencias económicas y administrativas

Escuela de Auditoria

Evaluación del riesgo operacional en el departamento de Prevención de fraude de Banco Ripley, Contact Center Ripley, Sucursal Valparaíso.

Tesis para optar al título de contador público auditor y el grado de licenciado en sistemas de información financiera y control de gestión.

Profesor cátedra : Carlos Murat Ibaceta

Profesor Guía : Guillermo P. Rebolledo

Alumna : Fabiola Martina Yáñez Guerrero

Valparaíso, 10 de Junio de 2008.

ÍNDICE **páginas**

Resumen

El riesgo operacional afecta como un todo a las organizaciones, sin discriminar tamaño o el tiempo que lleve desempeñándose en sus actividades. El no considerar el riesgo operacional puede afectar gravemente a los objetivos que esperan cumplir las entidades, ya sea una empresa prestadora de servicios, manufactureras, vendedoras al por menor, etc. La disciplina que considera el riesgo operacional es la administración del riesgo operacional, el que tiene como finalidad identificar, evaluar y aplicar políticas que sean capaces de minimizar dicho riesgo. Esto no se podría llevar a cabo si no se ejecutan controles adecuados por parte de la administración para que las actividades se cumplan y no se desvíen de su curso, y así, se lleven a cabo los objetivos esperados, sobre todo los objetivos operacionales para los que se ejerce el control interno en la organización. El riesgo operacional se puede controlar pero no eliminar, por lo tanto, se debe considerar un margen en que el riesgo puede reflejarse en las actividades diarias de los trabajadores, pero esto no quiere decir que se desvíe del curso normal de los objetivos de la entidad.

El problema que se pretende investigar en el presente proyecto de tesis es evaluar el riesgo operacional en el departamento de prevención de fraude de Banco Ripley, Contact Center Ripley, sucursal Valparaíso. Lo que se busca es identificar información de aquellos riesgos operacionales más significativos identificados por la administración del riesgo operacional y tecnológico de banco Ripley, junto a su respectivo control y el que se supervisará para luego realizar una apreciación real con respecto al cumplimiento de los objetivos estipulados para dicho departamento.

Problema

En toda organización se corre un alto riesgo de que no se puedan llevar a cabo los objetivos propuestos, debido a que en algunas ocasiones las organizaciones se enfrentan a inconvenientes como por ejemplo, fallas en los sistemas computacionales, problemas en el ambiente interno y externo de la empresa, el inadecuado desempeño de las personas en sus labores diarias, entre otras, lo que no permite un correcto funcionamiento en el logro de sus objetivos. El riesgo que se involucra tras los inconvenientes mencionados anteriormente es el llamado “riesgo operacional”, un riesgo que por definición contempla todos los inconvenientes mencionados anteriormente y afecta a la organización como un todo, ya que va directamente a los objetivos que las entidades buscan cumplir.

La probabilidad de que algo ocurra siempre ha existido, por ejemplo, la caída del sistema en el trabajo durante un determinado proceso o que el clima impida que trabajadores puedan ejecutar su trabajo, por lo tanto, debe existir una disciplina encargada de administrar y aplicar procedimientos que se anticipen de cierta forma a hechos que puedan provocar desviaciones en las directrices y que ayuden en el cumplimiento de los objetivos. En el departamento de prevención de fraude de banco Ripley, Contact Center Ripley, sucursal Valparaíso, se busca cumplir sus objetivos a través de la administración del riesgo operacional, la cual, ayuda a reducir dicho riesgo.

Para la administración es difícil identificar y evaluar todos los riesgos operacionales, por lo tanto debe establecer adecuados controles que permitan el idóneo desempeño de todas las actividades y a las vez, saber que siempre existe una pequeña posibilidad de que fallas o inconvenientes pueden intervenir, por lo que deben considerar un margen de error aceptable de que no siempre todos los objetivos se cumplirán y se llevarán a cabo eficiente y eficazmente.

El presente proyecto de tesis se basará en una evaluación del riesgo operacional en el departamento de prevención de fraude de banco Ripley, Contact Center Ripley, sucursal Valparaíso. Se realizará una investigación que aporte información de los riesgos operacionales más significativos identificados por dicho departamento, junto al control que lo minimiza, para luego supervisar lo recopilado y realizar una apreciación real con

respecto al cumplimiento de los controles y objetivos estipulados para este departamento entre el 17 de marzo al 27 de mayo de 2008.

Formulación del problema

- ¿Cuáles son los objetivos que pretende cumplir el departamento de prevención de fraude de banco Ripley, Contact Center Ripley, sucursal Valparaíso?
- ¿Qué se esta haciendo en el departamento de prevención de fraude de Banco Ripley, Contact Center Ripley, sucursal Valparaíso, para minimizar el riesgo operacional?
- ¿Cuáles son los riesgos más significativos identificados por la administración que podrían afectar el cumplimiento de los objetivos establecidos por el departamento de prevención de fraude de Banco Ripley, Contact Center Ripley, sucursal Valparaíso?
- Los trabajadores del departamento de prevención de fraude de Banco Ripley, Contact Center Ripley, sucursal Valparaíso, ¿Tendrán conocimiento de los objetivos que deben alcanzar?
- ¿Se realiza el adecuado control en la gestión de minimizar el riesgo operacional dentro del departamento de prevención de fraude de Banco Ripley, Contact Center Ripley, sucursal Valparaíso?
- ¿Qué conclusiones se podrán obtener de la investigación y recopilación de información durante el 17 de marzo y 27 de Mayo de 2008 en relación al cumplimiento de los objetivos y los controles que minimizan el riesgo operacional en el departamento de prevención de fraude de Banco Ripley, Contact Center Ripley, sucursal Valparaíso?

Objetivos Generales

- Evaluar el riesgo operacional en el departamento de prevención de fraude del Banco Ripley, Contact Center Ripley, sucursal Valparaíso, relacionado a los objetivos y controles establecidos para dicho departamento.

Objetivos específicos

- Describir los objetivos, riesgos operacionales más significativos identificados por la administración del riesgo operacional de Banco Ripley y los controles establecidos para minimizar dichos riesgos, además de las actividades y labores que deben desempeñar los ejecutivos del departamento de prevención de fraude de Banco Ripley, Contact Center Ripley, sucursal Valparaíso.
- Identificar el conocimiento que poseen los ejecutivos del departamento de prevención de fraude de Banco Ripley, Contact Center Ripley, sucursal Valparaíso en cuanto a la ejecución de sus actividades de control para el cumplimiento de los objetivos estipulados para dicho departamento.
- Comparar la información entregada por la administración y la obtenida del conocimiento y actividades realizadas por lo ejecutivos del departamento de prevención de fraude de Banco Ripley, Contact Center Ripley, Sucursal Valparaíso para aplicación de pruebas de cumplimiento.
- Obtener conclusiones con respecto a los controles aplicados para minimizar los riesgos operacionales identificados por la administración como más significativos en el departamento de prevención de fraude de Banco Ripley, Contact Center Ripley, sucursal Valparaíso.
- Conocer la situación real que sucede entre los riesgos operacionales identificados como más significativos por la administración y el cumplimiento del los objetivos y controles establecidos para el departamento de prevención de fraude de Banco Ripley, Contact Center Ripley, Sucursal Valparaíso.

Marco teórico

1. Control Interno

Dentro de todas las organizaciones, independiente de su tamaño, siempre se ha buscado la forma de controlarla de la mejor manera posible. El control interno se implementa con el fin de detectar, dentro de un plazo deseado, cualquier desviación respecto a los objetivos de rentabilidad establecidos por la empresa y de limitar sus imprevistos. Dichos controles permiten a la dirección hacer frente a los rápidos cambios competitivos del entorno económico, así como a las prioridades cambiantes de los clientes y adaptar su estructura para asegurar el crecimiento futuro. Defliese y col. (2001).

En las organizaciones, el control interno fomenta la eficiencia, reduce el riesgo de pérdidas de valor de los activos y ayuda a garantizar la fiabilidad de los estados financieros y el cumplimiento de las leyes y normas. Coopers & Librand (1997).

La utilidad que nos entrega la implementación de un adecuado control interno es la consecución de los objetivos estipulados para cualquier organización, por lo que cada vez se busca disponer de mejores sistemas de control interno, ya que es considerado como una solución a numerosos inconvenientes.

El control interno se define, según Coopers & Librand (1997), de la siguiente manera:

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 los objetivos dentro de las siguientes categorías:

I. Eficiencia y eficacia de las operaciones
II. Fiabilidad de la información financiera y,
III. Cumplimiento de las leyes y normas aplicables.

La definición anteriormente señalada correspondiente a Coopers & Librand (1997), contiene ciertos conceptos fundamentales que se explican a continuación:

a) El control interno es un proceso: El control interno constituye una serie de acciones que se extienden por todas las actividades de una entidad. Estos procesos se llevan a cabo dentro de las unidades de funciones de la organización y entre las mismas, se coordinan en función de los procesos de gestión básicos de planificación, ejecución y supervisión. La incorporación de controles puede influir directamente en la capacidad de la entidad de conseguir sus objetivos.

b) El control interno lo llevan a cabo las personas: Son las personas quienes establecen los objetivos de la entidad e implementan los mecanismos de control. El control interno tiene en cuenta que las personas no siempre comprenden, se comunican o realizan sus cometidos de una manera uniforme. Cada individuo trae consigo un historial y unos conocimientos técnicos únicos y sus necesidades y prioridades difieren de las de los demás.

c) El control interno solo puede aportar un grado de seguridad razonable: El control interno, por muy bien implementado que esté, solamente puede aportar un grado de seguridad razonable a la dirección y al consejo de la administración acerca de la consecución de los objetivos de la entidad, las posibilidades de conseguir tales objetivos se ven afectadas por las limitaciones que son inherentes a todos los sistemas de control interno. Estas incluyen ciertos hechos que son innegables:

- Las opiniones en que se basa la administración pueden ser erróneas.
- Los empleados encargados de establecer controles deben considerar el costo-beneficio de la aplicación de ellos.
- Se pueden producir problemas en el funcionamiento de sistemas por fallas humanas, aunque se trate de simples errores o equivocaciones.
- Además, los controles pueden se evadidos por dos o más personas coludidas que se lo proponen, pudiendo ser trabajadores de altos mandos, como de la alta dirección o ejecutivos de diferentes o mismas áreas.

Los puntos mencionados anteriormente son considerados, entre otros, algunos de los riesgos a los que está afecta cualquier organización y que a través del control interno se busca la forma de mitigarlos.

d) <u>El control interno esta pensado en facilitar la consecución de objetivos de una o más de las diferentes categorías:</u> Cada entidad tiene una misión, la cual determina sus objetivos y las estrategias necesarias para alcanzarlos. Los objetivos pueden establecerse para la organización como conjunto o dirigirse a determinadas actividades dentro de la misma.

Los objetivos pueden estar claramente identificados o estar implícitos. Los objetivos específicos se derivan de la estrategia global de la entidad. Los objetivos globales de la empresa están relacionados e integrados en objetivos más específicos establecidos, para las diversas actividades tales como ventas, producción e ingeniería, asegurándose de que son coherentes entre sí.

Dentro de la definición indicada por Coopers & Librand (1997), podemos indicar los siguientes objetivos según su clasificación:

I. *Objetivos relacionados con las operaciones:*

Se refieren a la eficacia y eficiencia de las operaciones de la entidad, incluyendo los objetivos de rendimiento y rentabilidad y la salvaguarda de los recursos contra posibles pérdidas. Estos objetivos varían en función a la elección de la dirección respecto a estructura y rendimiento

II. *Objetivos relacionados con la información financiera:*

Se refiere a la preparación de estados financieros fiables y a la prevención de la falsificación de la información financiera pública. A menudo, estos objetivos están condicionados por requerimientos externos.

III. *Objetivos relacionados al cumplimiento:*

Estos objetivos se refieren al cumplimiento de las leyes y normas a las que está sujeta la entidad. Dependen de factores externos tales como la reglamentación en materia de medio ambiente entre otros, y tienden a ser parecidos en todas las entidades, en algunos casos, o en todo un sector, entre otros.

Esta clasificación nos permite considerar diferentes aspectos en el control interno ya que estas son diferentes, pero que a su vez, se encuentran entrelazadas (un objetivo

determinado dentro de alguna entidad puede pertenecer a más de una categoría), las cuales tiene diferentes necesidades y pueden quedar bajo la responsabilidad directa de diferentes ejecutivos.

De un sistema de control interno se puede esperar que proporcione un grado de seguridad razonable con respecto a la consecución de los objetivos correspondientes a la fiabilidad de la información financiera y el cumplimiento de las leyes y normas aplicables ya que estos están basados en gran parte de normas impuestas por terceros, ajenos a la entidad y solo depende de cómo se realizan las actividades bajo el control de ella. Sin embargo, la realización de los objetivos operacionales no siempre esta bajo el control de la organización. El control interno no es capaz de prevenir las opiniones o decisiones erróneas, o los hechos externos, que pueden evitar que se alcancen las metas operativas esperadas, ya que estos no están basados en pautas externas y todo se puede desviar de lo planeado. Entonces, para tales objetivos, el sistema de control interno solamente puede entregar un nivel razonable de seguridad de que la administración o el alto mando de la entidad estén informados puntualmente del grado de avance en la consecución de dichos objetivos operacionales. Coopers & Librand (1997).

2. Objetivos operacionales

Como definición podemos indicar según Defliese y col. (2001), que es la obtención de un grado de seguridad razonable de que las operaciones se llevan a cabo tal como fueron autorizadas. Exige evidencia independiente de que las autorizaciones son dadas por personas que actúan dentro de su esfera de autoridad y que las operaciones se ajustan a los términos de las autorizaciones.

Estos objetivos están relacionados con la consecución del objetivo social, que es la razón de ser de una entidad. Incluye objetivos específicos, dirigidos a la mejora de la eficacia y eficiencia en el camino a la consecución de dicho fin, Coopers & Librand (1997). Los objetivos relacionados con las operaciones tienen que irradiar el entorno empresarial, industrial y económico en que se despliega la entidad, ya que es necesario que se adapten y asegurarse que los objetivos están asentados en la realidad y en las exigencias del mercado y están enunciados en términos que permitan que el rendimiento de ellos se evalúe adecuadamente.

El inconveniente está en que no existen pautas externas para guiarse en el cumplimiento de los objetivos operacionales ya que cualquier eventualidad podría cambiar todo lo planeado, como por ejemplo: acontecimientos climáticos, cambio de gobiernos, catástrofes en instalaciones, etc., las cuales no se pueden controlar. Incluso puede ser que se tengan considerados eventuales acontecimientos en el proceso de establecer los objetivos operacionales y se cree un plan de contingencia por si ocurrieran.

Sin embargo, un plan de este tipo únicamente amortigua el impacto que produciría un eventual acontecimiento externo, generando un riesgo, por lo que no garantiza la consecución de los objetivos. Por lo tanto, la meta del control interno en esta área fundamentalmente se centra en el desarrollo de objetivos y metas coherentes en toda la organización, además, la presentación en el adecuado tiempo a la administración o altos mandos con respecto a la información respectiva al rendimiento y expectativas de la entidad.

"Aun que no se pueda garantizar el éxito, la dirección debe tener la seguridad razonable de que de se le advertirá en el caso de que exista peligro de que no vayan a conseguirse los objetivos". Coopers & Librand (1997).

3. El riesgo.

El riesgo es inherente en los negocios. Los riesgos afectan la habilidad de cada entidad para sobrevivir, competir con éxito dentro de un sector, mantener una posición financiera fuerte y una imagen pública positiva así como la calidad global de sus productos, servicios y empleados. Defliese y col. (2001).

De acuerdo a la definición indicada por Coopers & Librand (1997), se entiende que el control interno es fundamental para llevar a cabo los objetivos organizacionales, pero a su vez nos dice que nos proporciona un grado de seguridad razonable, esto quiere decir, que no nos afirma en un cien por ciento el logro de los objetivos, debido a que las entidades son sistemas que interactúan con otros sistemas y que están inmersos en un mundo donde ocurren cosas que no es posible predecir.

"La incertidumbre existe siempre que no se sabe lo que ocurrirá en el futuro. El riesgo es la incertidumbre que "importa" porque incide en el bienestar de la gente… Toda situación riesgosa es incierta, pero puede existir incertidumbre sin riesgo" (Bodie ,1998).

Por lo tanto, dentro de las organizaciones es muy importante considerar el riesgo en las diferentes categorías en relación al cumplimiento de los objetivos, con mayor razón, en la implementación de los controles internos que nos ayudarán a la consecución de los objetivos operacionales, los cuales son complejos de definir ya que no se conocen las variables externas a las cuales se podría ver enfrentadas las entidades.

Los riesgos pueden surgir tanto de fuentes internas como externas. Los riesgos podrían provocar la falla de un proyecto sin alcanzar sus objetivos, la falta de satisfacción por parte del cliente, una publicidad poco favorable o la amenaza de la salud pública, una mala administración, problemas con la cultura organizacional, fallas en los sistemas computacionales, fraude, deficiencias en los controles internos. La lista es casi infinita. Fragoso, J.C. (2002).

Así, el riesgo se puede clasificar dependiendo del elemento al que se le identificará el riesgo, ejemplos:

- Riesgo de crédito
- Riesgo de liquidez
- Riesgo de mercado
- Riesgo de tasa de interés
- Riesgo legal
- Riesgo de tipo de cambio
- Riesgo operacional
- Riesgo de insolvencia
- Etc.

4. El riesgo operacional

Este riesgo tiene su justificación en la pérdida derivada significativas en la integridad o confianza del sistema. Las consideraciones de seguridad son importantes, en la medida en que los bancos pueden ser sujetos a ataques externos o internos sobre sus sistemas o productos. El riesgo operacional puede también surgir de un mal uso del cliente, de un diseño inadecuado o de un sistema de banca electrónica mal implantado. Revista BCC (2005)

Se refiere a las pérdidas potenciales resultantes de sistemas inadecuados, fallas administrativas, controles defectuosos, fraude, o error humano, Jorion (1999). Otras definiciones como la que indica Basilea II (2004), dice que son las pérdidas monetarias como resultado de fallos o de falta de adecuación de los procesos internos, de las personas, de los sistemas o por eventos externos. La definición de riesgo operacional dada por el documento Basilea II, es la guía para que cada banco adopte su propia definición de lo que entiende como riesgo operacional.

También podemos indicar según Van Greuning y col. (2003), que el riesgo operacional proviene de los procesos internos en la producción de servicios. Se podría definir como los errores producidos en los procedimientos de la institución, o a la falta de estos procedimientos adecuados. Este riesgo surge de la ineficacia de los controles internos, de la capacidad e integridad del personal, de la tecnología de información y de todos los procesos operativos.

Las áreas con mayor riesgo operacional en las entidades y que además se perciben como críticos son los siguientes tipos de riesgo son: la gestión de procesos, el control de fraude externo y las interrupciones en el negocio y fallos de los sistemas. Revista BBC (2005).

Además el tamaño de la entidad influye en la medida del riesgo operacional, ya que si las entidades son de un tamaño mayor, muestran un posicionamiento peor en la situación de Riesgo Operacional aunque una mayor madurez en su percepción del Mapa de Riesgo Operacional (mayor afinidad a la realidad). En estas entidades, a pesar de que

las pérdidas potenciales pueden ser muy altas, son las que presentan menores salvaguardas. Comité de supervisión bancaria de Basilea (2004).

Los pilares del riesgo operacional son los siguientes:

a. Continuidad operacional del negocio.
b. Calidad en los procesos.
c. Seguridad de la información.

El riesgo operacional es muy heterogéneo, se asocia a errores humanos, mecánicos, informáticos y de control, como se definió anteriormente.

Para poder minimizar el efecto del riesgo operacional es necesario medirlo, pero a diferencia de otros tipos de riesgos como el de crédito o de mercado, el riesgo operacional es más difícil de cuantificar, pues este riesgo puede estar constituido por diversos elementos que pudieran tener su causa, por ejemplo, en el simple error al introducir un dato en el sistema informático, en situaciones impredecibles como la aparición de un virus informático en el sistema, o en situaciones más complejas como un incorrecto proceso administrativo o en la conducta indisciplinada de un empleado que no respete ni cumpla las normas y procedimientos establecidos en su institución.

Una manera de clasificar el riesgo operacional consiste en seguir el criterio de su causa, que puede estar constituida por:

a. Sucesos inesperados ajenos al control de la entidad: Entre estos riesgos se encuentra desastres naturales, ausencia en el suministro eléctrico, interrupción en las telecomunicaciones, virus informáticos, incendios, robos, y otros. Estos errores se pueden minimizar mediante planes de contingencia, planes contra catástrofes probados en condiciones normales, correcta salvaguarda de al menos tres generaciones de la información financiera, actualización constante de antivirus, etc.

b. Errores humanos: Son causados por negligencia del personal de la entidad, distracciones, ausencia de interés o motivación. Estos errores se pueden minimizar mediante la capacitación y actualización continua del personal, mejoramiento del proceso de la acción de revisión en el sistema de control interno.

c. Operadores indisciplinados: A diferencia del caso anterior, los errores humanos eran voluntarios, pero en este caso se trata de empleados sin escrúpulos, generalmente representados por individuos que no acatan las normas establecidas y que, por tanto, pudieran también estar involucrados en acciones inescrupulosas, realizando operaciones no autorizadas que pueden ocasionar pérdidas para la entidad, pudiendo ser incluso considerables. Este riesgo se puede reducir al establecer adecuados controles internos, mediante el conocimiento por la más alta dirección acerca de los riesgos que enfrenta la institución y de los elementos de control que debe contener el sistema de control interno para cada operación, además de realizar una eficiente auditoria interna. Castellón Novo (2004).

Aún cuando no es posible tener un medio ambiente totalmente libre de riesgos, es posible eludir, reducir, eliminar o transferir ciertos riesgos. Esto se puede conseguir a través de la administración del riesgo operacional.

5. Administración del riesgo operacional.

La administración del riesgo operacional nos ayuda en la identificación del riesgo operacional. Según algunas definiciones como la de Fragoso, J C. (2002), podemos decir que “es un proceso lógico y sistemático que puede ser utilizado cuando se toman decisiones para mejorar la efectividad y eficiencia”. Otras definiciones como Tinoco y Hernández (1996) indica que es “la aplicación sistemática de políticas, procedimientos y practicas de gestión a la tarea de identificar, analizar, evaluar, tratar y controlar los riesgos”, En fin, es una disciplina que ayuda a las organizaciones a gestionar el riesgo operacional todo el tiempo, que busca minimizarlo y definir que nivel de riesgos es el aceptable.

Al enlazar la información explicada anteriormente, nos damos cuenta que la administración del riesgo operacional apoya a la organización en la identificación de dicho riesgo, para que su presencia no impacte fuertemente sobre los objetivos establecidos por la organización. Pero nos falta algo muy importante que debe estar para que lo anteriormente dicho se cumpla, la adecuada aplicación de un buen control interno.

Administrar el riesgo significa pensar en el futuro. Cuando se administra el riesgo tratamos de identificar y estar preparados para lo que pueda suceder, se trata de tomar acciones destinadas a eludir y reducir la exposición a los costos u otros efectos de aquellos eventos que ocurran, en lugar de reaccionar después de que un evento ya ha ocurrido e incurrir en los costos que implican recuperar una situación, por lo que se debe evaluar los riesgos, para su identificación y medición.

6. Evaluación de riesgos

Todas las entidades deben hacer frente a una serie de riesgos, independiente de su dimensión, estructura, naturaleza o sector al que pertenezcan, de todas formas encontraremos riesgos en todo los niveles de su organización. Los riesgos afectan la destreza de cada entidad para sobrevivir, luchar con éxito dentro de su sector, conservar una posición financiera fuerte y una imagen pública positiva así como la calidad global de sus productos, servicios y empleados. No existe ninguna forma práctica de reducir el riesgo a cero. De hecho, el riesgo es inherente a los negocios. La dirección debe determinar cual es el nivel de riesgo que se considera admisible y esforzarse para mantenerlo dentro de los límites marcados. Coopers & Librand (1997).

La evaluación de riesgos consiste en la identificación y análisis de los factores que podrían afectar la consecución de los objetivos, y en base a dicho análisis, determinar la forma en que los riesgos deben ser gestionados.

El establecimiento de objetivos es una situación previa a la evaluación de los riesgos. La dirección debe fijar primero los objetivos antes de identificar los riesgos que pueden tener un gran impacto sobre su consecución y tomar las medidas oportunas. Por tanto, el establecimiento de los objetivos es una fase clave de los procesos de gestión. Si bien no constituye un componente del control interno, es un requisito previo que permite garantizar el funcionamiento del mismo. Coopers & Librand (1997).

7. Actividades de control

Las actividades de control son las normas y procedimientos que constituyen las acciones necesarias para implementar las políticas, que pretenden asegurar que se cumplen las directrices que la dirección ha establecido con el fin de controlar los riesgos. Las actividades de control pueden dividirse en tres categorías, según el tipo de objetivo de la entidad con el que están relacionadas: operaciones, la fiabilidad de la información financiera o el cumplimiento de la legislación aplicable.

Aunque algunos tipos de control están relacionados solamente con un área específica, con frecuencia afecta a diversas áreas. Dependiendo de la circunstancias, una determinada actividad de control puede ayudar a alcanzar los objetivos de la entidad que corresponden a diversas categorías. De este modo, los controles operacionales también pueden contribuir a la fiabilidad de la información financiera, como los controles sobre fiabilidad de la información financiera pueden contribuir al cumplimiento de la legislación aplicable, y así, sucesivamente. Las actividades de control tienden también a asegurar que se toman las medidas necesarias para afrontar los riesgos que ponen en peligro la consecución de los objetivos de la entidad. Coopers & Librand (1997).

8. Integración de las actividades del control con la evaluación de riesgos

Según Defliese y col. (2001), de forma paralela a la evaluación de riesgos, la dirección debería establecer y aplicar el plan de acción necesario para afrontarlos. Una vez identificadas, estas acciones también serán útiles para definir las operaciones de control que se emplearán para garantizar su ejecución de forma correcta y por el tiempo deseado.

Las actividades de control forman una parte esencial del proceso mediante el cual una empresa intenta lograr sus objetivos de explotación. Las actividades de control no son un fin en sí mismas ni tampoco deben existir simplemente porque parece que “es lo que hay que hacer”. La dirección o administración debe tomar las medidas para asegurar que se alcanzan los objetivos esperados.

Las actividades de control sirven como mecanismos para asegurar el cumplimiento de los objetivos. Tales actividades podrían incluir tanto el seguimiento del desarrollo de las ventas, como ejemplo, comparándolo con el calendario previsto como las medidas adoptadas para garantizar la exactitud de la información obtenida. En este sentido es un elemento de integrado en el proceso de la gestión. Coopers & Librand (1997).

9. Principios para minimizar el riesgo operacional

Los principios fundamentales para minimizar el riesgo operacional son:

a) Interiorización y compromiso por parte del Consejo de Administración en la aprobación y supervisión del marco de minimización de riesgo operacional.
b) El Consejo de Administración debe asegurar una auditoria interna efectiva e integral del marco de minimización del riesgo operacional efectuada por personal calificado e independiente del área de riesgo operacional.
c) La alta dirección debe ser responsable de la aplicación del marco de minimización del riesgo operacional aprobado por el Consejo de Administración.
d) Las instituciones financieras deberán identificar y evaluar el riesgo operacional inherente a todos sus productos, actividades, procesos y sistemas.
e) Las instituciones financieras deberán implantar un proceso de control continuo de los perfiles de riesgo y de la exposición a pérdidas por riesgo operacional.
f) Las instituciones financieras deberán tener políticas, procesos y procedimientos para reducir los riesgos operacionales como, por ejemplo:

- Controles operacionales diseñados para monitorear los riesgos identificados por la entidad.

- Segregación de funciones y delimitación de responsabilidades que eliminen conflictos de interés potenciales.

- Prácticas internas para el control del riesgo operacional como, por

ejemplo, la observancia de los límites de riesgo, el control de acceso y el uso de los activos y archivos de la entidad.

- Algunos de los riesgos operacionales tienen una baja probabilidad de ocurrir, sin embargo, tienen un gran impacto financiero.

- El riesgo operacional aparece de forma frecuente en nuevos productos o actividades, nuevos mercados o negocios geográficamente lejos de las sedes centrales de las instituciones financieras.

- Las instituciones financieras deben ver las diferentes herramientas para reducir el impacto del riesgo operacional como complementarias no sustitutivas de los controles.

- La inversión en tecnología de procesamiento y de seguridad de los sistemas es importante para reducir el impacto por riesgo operacional.

- Las entidades financieras deberán promover el desarrollo de las prácticas adecuadas para la minimización y supervisión del riesgo operacional asociado a sus actividades de subcontratación.

- La alta dirección deberá asegurar que las expectativas y obligaciones de los proveedores y de la entidad sean claramente definidas, entendidas y cumplidas para evitar potenciales deficiencias en el servicio.

g) Las entidades financieras deberán promover la elaboración de planes de contingencia y de continuidad del negocio para asegurar la capacidad de operar y minimizar las pérdidas en caso de una alteración grave del negocio.
h) Los organismos supervisores deberán exigir que las entidades, independientemente de su tamaño, posean un marco efectivo de identificación, evaluación, seguimiento, control y reducción de riesgo operacional como parte de un enfoque de gestión integral de riesgos.
i) Los supervisores deberán realizar de forma regular, directa o indirecta, una evaluación de las políticas, procedimientos y prácticas relacionados con el riesgo operacional.

j) Las entidades deberán proporcionar suficiente información al mercado para que los participantes puedan evaluar su enfoque de gestión de riesgo operacional.

Para reducir el riesgo operacional existen controles y procedimientos de vigilancia de las transacciones y posiciones y de su documentación. Los auditores internos y externos deben revisar periódicamente el cumplimiento de los procedimientos.

Una entidad bancaria con un sistema de control interno adecuado podrá hacer frente al riesgo y evitar caídas de resultados o situaciones no deseadas.

El control interno puede ayudar a que una entidad consiga sus objetivos de rentabilidad y rendimiento, tal como a prevenir la pérdida de recursos y a obtener información financiera fiable. También, puede reforzar la confianza en que la empresa cumpla con las leyes y normas aplicables, evitando efectos perjudiciales para su reputación y otras consecuencias. En resumen, puede ayudar a que una entidad logre sus propósitos, evite riesgos y sorpresas. Castellón Novo (2004).

10. Principios para la disminución y supervisión del riesgo operacional.

En el documento “Sound Practices for the Management and Supervision of Operational Risk”, publicado por el Comité de Basilea en julio de 2002, se definen los principios para una efectiva gestión y supervisión del riesgo operacional:

Principio 1:

El Consejo de Administración deberá tener conocimiento de los principales aspectos relativos al riesgo operacional que soporta la entidad, el cual será tratado como un tipo de riesgo diferente que requiere ser gestionado. También deberá aprobar y revisar periódicamente el marco de gestión del riesgo operacional en la entidad. Dicho marco debe proporcionar una definición sobre qué es el riesgo operacional para toda la organización y establecer los principios para su identificación, evaluación, seguimiento, control y reducción.

Principio 2:

> El Consejo de Administración deberá garantizar que el marco de gestión del riesgo operacional esté sujeto a una efectiva y exhaustiva revisión interna por parte del personal competente, funcionalmente independiente y con una formación adecuada. La función de auditoria interna no deberá ser directamente responsable de la gestión activa del riesgo operacional.

Las entidades deben poseer una cobertura de auditoria interna que verifique que las políticas y procedimientos operativos están efectivamente implantados. El Consejo ya sea de forma directa o indirectamente, debe garantizar que el alcance y la frecuencia de las revisiones de auditoria se apliquen a los riesgos incurridos. El área de auditoria interna deberá validar periódicamente que el marco de gestión del riesgo operacional está siendo implantado de forma efectiva en toda la organización.

En la medida en que el área de auditoria interna esté involucrada en la supervisión del marco de gestión del riesgo operacional, el Consejo deberá garantizar la independencia de la función de auditoria. Esta independencia podrá verse afectada si la función de auditoria está directamente involucrada en el proceso de gestión del riesgo operacional.

La función de auditoria interna puede aportar información relevante al área encargada de gestionar este riesgo, pero en ningún caso debe tener responsabilidades en la gestión del riesgo operacional. Sin embargo, el Comité de Basilea reconoce que el área de auditoria en algunas entidades (especialmente las entidades pequeñas y medianas) puede tener la responsabilidad inicial del desarrollo del plan de gestión del riesgo operacional. Cuando ello suceda, las entidades deberán tratar de transferir lo antes posible las responsabilidades de la gestión diaria del riesgo operacional a otras áreas. El Comité de Basilea ha definido las mejores prácticas en referencia a la organización interna de las entidades frente al riesgo operacional, y fomenta la utilización de metodologías avanzadas, desarrolladas internamente, de forma similar a lo sucedido en la gestión de los riesgos de crédito y de mercado, todo ello con una óptica global de integración y convergencia entre capital económico y regulatorio. Comité de supervisión Bancaria de Basilea (2004).

Metodología

Para elaborar el problema de investigación y así cumplir con alcanzar los objetivos propuestos en este proyecto, la metodología será de la siguiente manera:

1. Recopilación de información

En una primera parte se realizará a través de fuentes que se detallan a continuación:

a. Necesariamente se debe obtener conocimiento de Banco Ripley y del departamento de prevención de fraude de Banco Ripley, sucursal Valparaíso, objetivos, tiempo de funcionamiento, el por qué de su existencia, actividades y funciones de las analistas de fraude, todo esto obtenido de fuente directa, o sea por personas o desde el lugar de los hechos. También se solicitará a la administración del riesgo operacional de Banco Ripley indique aquellos riesgos operacionales más significativos junto con el control que lo minimiza.

b. Revistas, libros, apuntes, noticias, documentos, etc., todo lo que entregue (por medio impreso), información que incremente el conocimiento sobre el tema de riesgo operacional, la gestión del riesgo operacional y de control interno.

2. Población y muestra

El departamento de prevención de fraude de Banco Ripley, sucursal Valparaíso, está constituido por cuatro trabajadores:

- Tres analistas de fraude.
- Un supervisor del departamento.

Para el desarrollo del plan de investigación, se tomará el cien por ciento de la población y no una muestra, debido a que es pequeño el número de integrantes y se puede trabajar sin inconvenientes.

3. Técnicas de recolección de información

Para recopilar información se utilizará los siguientes instrumentos:

- Cuestionario: Será confeccionado de acuerdo a la información obtenida para que sea respondido por los analistas de dicho departamento. Estará compuesto de preguntas cerradas, para detectar conocimientos específicos sin necesidad de fundamentar. Las respuestas serán de SI y NO. Busca la identificación de controles y detectar el conocimiento de los trabajadores sobre las actividades de control.
- Entrevista: Servirá para aclarar incertidumbres y conversar con los analistas en caso que se tengan dudas con las respuestas entregadas en el cuestionario y ver la existencia de algún control compensatorio en caso de no existir uno principal. Esta entrevista se realizará al supervisor del área para identificar controles e indagar sobre las actividades que deben realizar los analistas y conocer sus funciones como supervisor.
- Documentación: Se solicitará a la administración del riesgo operacional de banco Ripley documentación e información. Esta información debe contener políticas de control o procedimientos internos relativos a la gestión del trabajo que se ejecuta en dicho departamento, además de información de programas informáticos y otros que tengan relación a lo solicitado.

4. Aplicación de pruebas de cumplimiento

Las pruebas de cumplimiento son procedimientos de auditoria diseñados para obtener seguridad razonable de aquellos controles internos en los cuales se depositó confianza y que los procedimientos de control se están realizando como se establecieron.

Se aplicará con la finalidad de probar que lo dicho por la administración de banco Ripley mediante protocolos y procedimientos es verdadero.

Tipos de pruebas de cumplimiento que se aplicarán:

i. *Observación:* Ver a los trabajadores desempeñando su trabajo durante una hora a cada uno. Este tiempo es considerado como prudente, ya que se pretende presenciar la actualización de cada una de las reglas que alertan en el sistema y si es posible ver ejecutar bloqueos de tarjetas de crédito, cualquiera sea el motivo de este.

ii. *Indagación:* Consiste en hacer preguntas específicas a los ejecutivos las que se realizarán de manera informal.

Las preguntas se relacionan con los riesgos indicados por la administración del riesgo operacional de Banco Ripley y otras por si existen dudas en alguna actividad.

iii. *Examen de evidencia*: Se realizará una inspección de registros y otros documentos para buscar pruebas de que un control ha sido aplicado debidamente. Se aclara que no será posible obtener copia de dicha información para respaldo de nuestro trabajo, ya que por políticas de la empresa no es autorizado, pero por tratarse de un trabajo de auditoria, se deja evidencia escrita de la existencia de ella para respaldo del procedimiento realizado.

5. Análisis y conclusiones del proyecto de tesis.

La información entrega por la administración del riesgo operacional de Banco Ripley en relación a los riesgos operacionales más significativos con su respectivo control indicado que lo mitigue, será relacionada junto con la información obtenida mediante las pruebas de cumplimiento aplicadas, concluyendo en correlación al logro de los objetivos y controles establecidos para el departamento de prevención de fraude de Banco Ripley, Contact Center Ripley, sucursal Valparaíso.

La información se analizará mediante la siguiente tabla:

Riesgo operacional Identificado como más significativo.	Control que lo mitiga	Puntos de atención	Se realiza		Descripción / comentario
			SI	NO	

Con esta relación o cruce de información se pretende indicar la situación real del departamento de prevención de fraude de Banco Ripley, Contact Center Ripley, sucursal Valparaíso. Todo esto relacionando la información de los riesgos operacionales más significativos para dicho departamento y el respectivo control que lo minimiza considerando los puntos de atención levantados en la investigación con su respectivo comentario.

6. Redacción y revisión del informe del proyecto de tesis

Se procederá a la redacción del informe para luego realizar una revisión a faltas de ortografías u otros puntos que tuvieran algunos inconvenientes y necesiten modificación.

Breve reseña de Banco Ripley.

Banco Ripley existe gracias a la tenacidad y visión empresarial de los fundadores de las empresas Ripley. Abrió sus puertas por primera vez al público el día 17 de mayo del año 2002, en la sucursal 21 de Mayo ubicada en Mall del Centro. El 8 de agosto del mismo año se inauguró con la participación de las más altas autoridades de la casa matriz ubicada en calle Huérfanos #1060.

Banco Ripley ha nacido para satisfacer las necesidades financieras de la clase media chilena, teniendo como estrategia la excelencia en el servicio y la rapidez de atención, basados en el uso de tecnología de punta.

Dicho banco se ha desarrollado en base a una estructura gerencial experimentada y profesional obteniendo un resultado que es propio de un equipo humano que con esfuerzo y dedicación ha logrado marcar un hito, por el nivel de desarrollo alcanzado en menos de seis años de experiencia, lo que ha permitido una gestión eficiente.

Banco Ripley se define como un banco de nicho orientado principalmente a las personas de ingresos medios, el cual se encuentra preparado para otorgar a sus clientes la mayoría de los productos bancarios tradicionales. El pool de productos disponibles en Banco Ripley está compuesto entre otros por créditos de consumo, créditos automotrices, crédito hipotecario y tarjetas de crédito Mastercard. En cuanto a pasivos, se dispone de depósitos a plazo en pesos y UF. Además el banco tiene créditos comerciales y factoring.

Breve reseña del departamento de prevención de fraude de Banco Ripley, Contact Center Ripley, sucursal Valparaíso.

El departamento de prevención de fraude de Banco Ripley, Contac Center Ripley, sucursal Valparaíso, fue creado en Agosto del año 2006, hace casi dos años comenzando desde cero.

Para el funcionamiento de las actividades de dicho departamento, Banco Ripley contrató los servicios del Contac Center Ripley Valparaíso. Se instalaron los elementos necesarios para el comienzo del desempeño de las actividades del departamento y además, Banco Ripley adquirió el sistema Sentinel Prevention a la empresa se sistemas operativos Smartsoft para el monitoreo constante de las transacciones realizadas con la tarjeta de débito y crédito de Banco Ripley.

El departamento se ha creado con la finalidad de cumplir el objetivo estipulado por el Banco Ripley de prevenir en forma eficaz y eficiente la prevención de fraudes con las tarjetas de crédito y débito entregadas por dicho banco.

En el tiempo que lleva en funcionamiento el departamento de prevención de fraude de Banco Ripley, gracias a su ayuda, se han detectado más de cien fraudes a los clientes, permitiendo un ahorro significativo al detectar tempranamente el fraude. Además vale destacar que gracias a su apoyo se has bajado a niveles mínimos el fraude interno.

El departamento de prevención de fraude de Banco Ripley, Contac Center Ripley, sucursal Valparaíso, cuenta con cinco integrantes (un supervisor del área y cuatro analistas de fraude, uno de ellos encontrándose durante el período de ejecución del presente proyecto con licencia médica cuyo motivo es pre-natal y post-natal), cuyos analistas desempeñan sus labores en turnos durante las 24 horas a través de un sistema informático llamado Sentinel Prevention, el cual será explicado más adelante.

Información solicitada a la administración para obtener el conocimiento de las actividades a realizar en el área.

Según la información indicada sobre las actividades que deben realizar los analistas de dicho departamento, y luego de su lectura es posible agruparlas en tres grupos que corresponden a los siguientes:

a) Recepción de llamados vía IVR, (llamada entrante línea 800), bloqueo de tarjeta de crédito Mastercard de Banco Ripley por solicitud de cliente, cuyo motivo de bloqueo puede ser robo, extravío o captura en cajero automático.

b) Monitoreo y seguimiento de transacciones a través de sistema Sentinel Prevention que son realizadas con la tarjeta Mastercard de Banco Ripley, independiente del lugar en donde se utilice la tarjeta.

c) Bloqueos de tarjeta de crédito Mastercard de Banco Ripley, por el desconocimiento de compra al detectar un posible fraude que cliente indique que no ha utilizado su tarjeta.

Cada uno de los grupos indicados anteriormente tiene un procedimiento a seguir, los cuales son los que se encuentran en evaluación para conocer el real cumplimiento de los controles estipulados.

A continuación se presenta información sobre la cual se ha obtenido información y conocimiento de las actividades que realizan los analistas de fraude y de los programas informáticos, entre otros entregados por el Jefe del departamento de prevención de fraude de Banco Ripley, el que se encuentra en sucursal de Santiago:

1. Procedimientos

<table>
<tr><td>NOMBRE</td><td colspan="3">PROCEDIMIENTO CONTAC CENTER 24X7</td><td>PP – OPTEC / GCOP / 5-3006 / V1.0</td></tr>
<tr><td>DOMINIO</td><td colspan="2">Gerencia de Gestión y Control Operacional</td><td>Clasificación de la Información</td><td>P</td></tr>
<tr><td rowspan="2">VIGENCIA</td><td>Fecha de Creación</td><td></td><td>Fecha última modificación</td><td></td></tr>
<tr><td>Desde</td><td></td><td>Hasta</td><td></td></tr>
<tr><td>OBJETIVOS</td><td colspan="4">Descripción del proceso de monitoreo y seguimiento de transacciones de clientes en el comercio por parte de la Unidad de Prevención de Fraudes del Contac Center 24 x 7 de Valparaíso.</td></tr>
<tr><td>ALCANCES</td><td colspan="4">Desde que el cliente utiliza su tarjeta en el comercio hasta que es contactado por parte de los analistas de prevención de fraude, y las acciones implementadas por ésta unidad al momento de contactar no a los clientes.</td></tr>
<tr><td>EXCEPCIONES</td><td colspan="4"></td></tr>
<tr><td>Solicitado por</td><td colspan="2">Jefe de Prevención de Fraude</td><td rowspan="4">Procedimientos Relacionados</td><td rowspan="4">1. Clientes No Ubicados en Contac Center (PP-OPTEC/GCOP/5-3005/V1.0)
2. Reclamos por TX Desconocidas Formalizadas en Sucursales (PP-OPTEC/GCOP/5-3007/V1.0)</td></tr>
<tr><td>Revisado por</td><td colspan="2"></td></tr>
<tr><td>Aprobado por</td><td colspan="2"></td></tr>
<tr><td>Redactado por</td><td colspan="2">Claudio Aguayo M.</td></tr>
<tr><td>Responsable</td><td colspan="4">Procedimiento a Efectuar.</td></tr>
<tr><td colspan="5">Todas las compras y movimientos efectuados en el comercio por los clientes de Banco Ripley, utilizando su tarjeta de crédito, quedan registrados a través de los diversos servidores de cada unidad (Redbanc y Transbank).

Todos estos servidores, tanto de Transbank como de Redbank alimentarán continuamente al servidor de FISA con la finalidad de llevar un registro de los movimientos diarios y en línea de los clientes de Banco Ripley al momento de utilizar su Tarjeta de Crédito en el comercio.

Además, el servicio del Contac Center permite entregar el servicio inbound, a través de la línea 800, donde los clientes pueden reportar los plásticos cuando estos son hurtados o extraviados por ellos, solicitando el bloqueo respectivo descrito en procedimiento de “Bloqueo de Plástico a través de Contac Center”.</td></tr>
<tr><td>ANALISTAS DE FRAUDE</td><td colspan="4">Al momento en que se efectúe el levantamiento de una de las alertas de Sentinel (Producto de la utilización de la Tarjeta por parte de los clientes en el comercio), el analista deberá ser cauto al momento de</td></tr>
</table>

	analizar y tomar la determinación de contactar o no al cliente. Actualmente, cada una de las alertar levantadas se encuentra clasificada de acuerdo a los siguientes criterios: 1. Montos asociados a cada una de las Transacciones. 2. Frecuencia de cada una de las Transacciones. 3. Comercios v/s monto en que se efectúan las transacciones. La combinación de éstos tres criterios determinarán y clasificaran las alertas en riesgosas y menos riesgosas. Un analista deberá tomar la determinación de contactar o descartar una transacción en base a los criterios antes descritos y la clasificación de riesgosa que la respectiva alerta tenga inmersa. En caso de tomar la determinación de posponer, deberá monitorear los movimientos de éste y ver si son reiterados, en intervalos de tiempo muy pequeños y los montos asociados a cada transacción. Cuando las alertas son reiteradas y de carácter riesgoso, el Analista de Fraude del Contac Center procederá a contactar telefónicamente al cliente. De no obtener respuesta a través de los teléfonos de contacto del cliente, procederá a recurrir a las alternativas que tiene a disposición de él para hacer efectivo el llamado telefónico, siendo estas: 1. Utilizar teléfonos de contactos (familiares) registrados en FISA. 2. Utilización de guías blancas para contactar a clientes. 3. Utilización de guía verdes para contactar a clientes. NOTA: Si no se logra contactar al titular del plástico y si a un familiar de éste, **NO se deberá entregar información** a éste último de la existencia del plástico. Sólo deberá indicar que es un contacto de carácter informativo para el cliente en contacto, y que se requiere dar la información al titular de la tarjeta. En caso que el cliente aún continúe inubicable, o se logre el contacto a través de los medios antes descritos el Analista deberá proceder según “Procedimiento de clientes no ubicados”, efectuando un bloqueo temporal del plástico del cliente de forma inmediata, sin importar el tipo de alerta levantada a través de Sentinel. En caso de lograr definitivamente el contacto con el cliente, no importando el medio a través del cual logro el contacto, el Analista deberá proceder de la siguiente manera: 1. Consultará a cliente por Transacciones por las cuales se levanto la Alerta de Sentinel, consultando montos y comercios en los cuales se efectuaron dichas transacciones. 2. En caso de reconocer las transacciones, procederá a registrar la información, descartando la alerta levantada y

	despidiéndose del cliente. 3. En caso de no reconocer las transacciones consultará a cliente si desea que se efectúe el bloqueo del plástico a través de Transbank. NOTA: Si el cliente no desea que se efectúe el bloqueo del plástico, procederá a validar la respuesta del cliente reiterando consulta de bloquear o no, de persistir la respuesta procederá a cerrar contacto telefónico registrando resolución del cliente y enviando información vía e-mail a Jefe de Prevención de Fraude con copia a Operaciones Tarjetas, indicando registro de llamada telefonica (Grabación) en caso que el cliente proceda a reportar algún reclamo formal a través de sucursales a futuro. 4. En caso de desear bloqueo del plástico, contacta telefónicamente a Operadores de Transbank y solicita el bloqueo del plástico. 5. Operador de Transbank procede a bloquear el plástico, informando fecha, hora y código de bloqueo al Analista de prevención de Fraude, finalizando llamada telefónica. 6. Comunica a cliente que se efectúo satisfactoriamente bloqueo del plástico comunicando código de bloqueo, fecha y hora en que éste se efectúo. 7. Solicita a cliente presentarse en sucursales a informar y reportar las Transacciones desconocidas para comenzar un proceso de investigación (regularización) a su caso, junto con solicitar la reposición de su plástico. 8. Finaliza contacto con cliente y procede a registrar llamado resultado de la gestión en Transbank. NOTA: AL momento de efectuar el cierre del contacto telefónico, deberá reiterar al cliente que deberá acercarse a sucursales a formalizar su reclamo, y que sólo se efectúo un cierre de la tarjeta, lo que no implica que se iniciará un proceso de investigación a las transacciones desconocidas reportadas vía telefónica. Dicha investigación se iniciará una vez formalizado el reclamo en sucursales. Por otro lado, una vez bloqueado un plástico de un cliente el Analista de Prevención de Fraude deberá inmediatamente cerrado el llamado telefónico con el cliente, informar vía e-mail del bloqueo del plástico a Operaciones Tarjetas (administrativo) con copia a Jefe de Prevención de Fraude. En dicho e-mail deberá enviar: 1. Nombre y Rut del cliente 2. Número de tarjeta del cliente. 3. Fecha y Hora del bloqueo. 4. Código de bloqueo de Transbank 5. Motivo del bloqueo. Adicionalmente, deberá llevar un registro en Excel con la misma

	información antes descrita, la cual deberá ser reportada diariamente por el Supervisor del Contac Center al Jefe de Prevención de Fraude con copia al Administrativo de Tarjetas de Crédito.
OPERACIONES TC	Recepciona e-mail por parte de los Analistas de Fraude informando bloqueo, temporal o permanente del plástico, efectuado a través de levantamiento de alertas del Contac Center. De haber procedido a bloquear permanentemente un plástico, el área de Operaciones Tarjetas efectuará el bloqueo del plástico en FISA de forma inmediata. La información reportada por los Analistas de Prevención de Fraude deberá ser guardada en carpetas personales como antecedentes, en espera de un reclamo o requerimiento formal del cliente en Sucursales. Es responsabilidad de cada unidad y de cada usuario mantener respaldada toda la información contenida en sus respectivos PC, en caso de fallas de los equipos o perdida total de éstos ante contingencias operativas.

<table>
<tr><td>Nombre</td><td colspan="3">CLIENTES NO UBICADOS EN CONTAC CENTER</td><td>PP- OPTEC / GCOP / 5-3005 / V1.0</td></tr>
<tr><td>DOMINIO</td><td colspan="2">Gerencia Gestión y Control Operacional – Prevención Fraude</td><td>Clasificación de la Información</td><td>P</td></tr>
<tr><td rowspan="2">VIGENCIA</td><td>Fecha de Creación</td><td></td><td>Fecha última modificación</td><td></td></tr>
<tr><td>Desde</td><td></td><td>Hasta</td><td></td></tr>
<tr><td>OBJETIVOS</td><td colspan="4">Describir flujo a efectuar para los clientes que no logran ser ubicados por los Analistas de Prevención de Fraude al momento de efectuado el levantamiento de una alerta de Sentinel.</td></tr>
<tr><td>ALCANCES</td><td colspan="4">Desde el levantamiento de una alerta y el contacto frustrado de éste por parte de los Analistas, hasta el contacto con éste a través de sucursal de origen o la unidad de actualización de datos.</td></tr>
<tr><td>EXCEPCIONES</td><td colspan="4"></td></tr>
<tr><td>Solicitado por</td><td>Jefe de Prevención de Fraude</td><td rowspan="4">Procedimientos Relacionados</td><td colspan="2" rowspan="4">1. Procedimiento Contac Center 24x7 (PP-OPTEC/GCOP/5-3006/V1.0)
2. Reclamos por TX Desconocidas Formalizadas en sucursales (PP-OPTEC/GCOP/5-3007/V1.0)</td></tr>
<tr><td>Revisado por</td><td></td></tr>
<tr><td>Aprobado por</td><td></td></tr>
<tr><td>Redactado por</td><td>Claudio Aguayo M.</td></tr>
<tr><td>Responsable</td><td colspan="4">Procedimiento a Efectuar.</td></tr>
<tr><td></td><td colspan="4"></td></tr>
<tr><td colspan="5">A.- Lograr contactar telefónicamente al cliente a través de teléfonos alternativos.</td></tr>
<tr><td>ANALISTAS DE FRAUDE</td><td colspan="4">De lograr finalmente el contacto con el cliente a través de las alternativas antes descritas, se procederá según “Procedimiento Contac Center 24x7”, con la única diferencia que la información a través de la cual se logró contactar exitosamente al cliente deberá ser registrada por cada uno de los analistas en una planilla Excel que deberá ser reportada diariamente a su Supervisor directo.</td></tr>
<tr><td>SUPERVISOR CONTAC CENTER</td><td colspan="4">Recepcionará diariamente la información entregada por todos los Analistas de Fraude, con los nuevos teléfonos de contacto del cliente con el cual se logro definitivamente el contacto. Esta información deberá ser derivada diariamente vía E-mail (Con Copia a Jefe de Prevención de Fraudes y Operaciones TC) a la Unidad de Actualización de Datos para que se proceda a contactar a los clientes y actualizar su información en el sistema FISA.</td></tr>
</table>

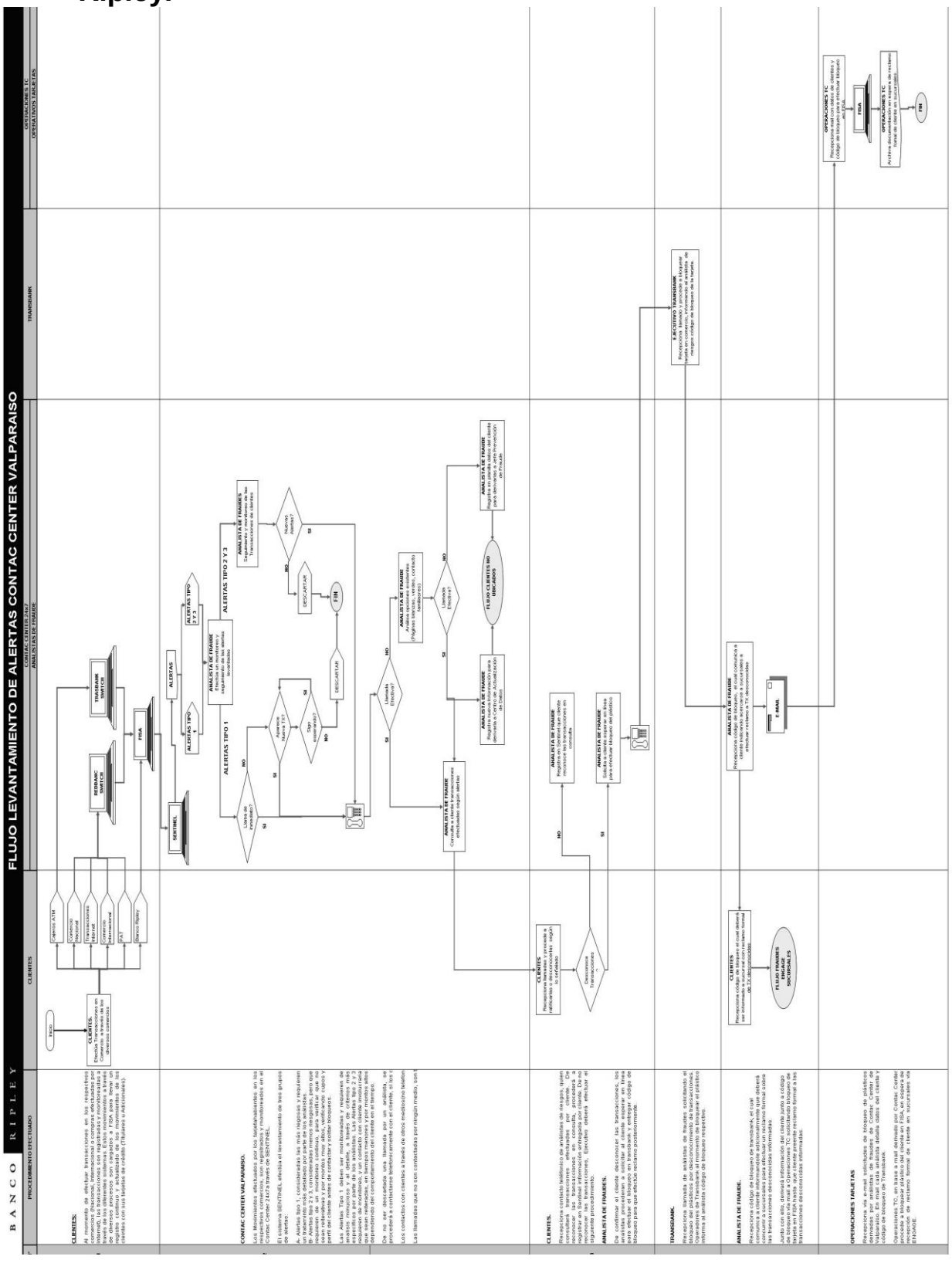
UNIDAD DE ACTUALIZACION DE DATOS	Recepcionan diariamente las planillas (Excel) derivadas por el Supervisor de la Unidad de Prevención de Fraudes del Contac Center, en la cual esta registrada la nueva información a través de la cual se logro el contacto del cliente. En base a dicha información, los Operadores de ésta unidad procederán a contactar a los clientes para proceder a la actualización de información de cada uno de ellos. Una vez contactado el cliente, se procederá a registrar la nueva información de contacto en FISA, en base a la confirmación de datos entregados y por el cliente. Una vez contactados todos los clientes informados en las planillas, y actualizada su información en FISA, se procederá a reportar dicha información (Vía E-mail con copia a Jefe de Prevención de Fraude y Operaciones TC) al Supervisor del área de Prevención de Fraudes del Contac Center con los resultados de la gestión realizada. La planilla en poder del Supervisor del Contac Center. con la información actualizada de los clientes, deberá ser enviada mensualmente vía E-mail al Jefe de Prevención de Fraude de Banco Ripley.
B.- No lograr el Contacto con el cliente.	
ANALISTAS DE FRAUDE	Cuando un cliente no logra ser ubicado a través de ninguno de los medios que tiene a su disposición, cada Analista deberá proceder de forma inmediata a efectuar un Bloqueo Temporal del Plástico del Cliente en FISA, de acuerdo a “Instructivo bloqueo temporal en FISA”. Una vez bloqueado el plástico, se procederá a informar de dicho bloqueo vía e-mail a Supervisor directo, Jefe de Prevención de Fraude y departamento de Operaciones Tarjetas. Adicionalmente, cada uno de los analistas deberán registrar en una planilla Excel, todos los bloqueos efectuados en el día, los que deberán ser informados a Supervisor directo al finalizar cada jornada o turno de trabajo. Dicha planilla deberá contener la información del cliente, y la sucursal de origen de cada uno de los plásticos.
SUPERVISOR CONTAC CENTER	Recepciona planillas derivadas por todos los Analistas de Fraude, con lo cual procederá a confeccionar una planilla única denominada “Planilla de Bloqueos Temporales”, la que deberá ser derivada diariamente a Jefe de Prevención de Fraude para gestionar la actualización de datos a través de sucursales de origen con Product Manager de Tarjetas.

JEFE DE PREVENCION DE FRAUDE	Recepciona planilla diaria de Supervisor de Contac Center, verificando que en ella se encuentre toda la información de los clientes y su respectiva sucursal de origen. De no encontrar observaciones, procederá a derivar vía e–mail planilla a Product Manager de Tarjetas de Crédito.
PRODUCT MANAGER BANCO RIPLEY	Recepciona diariamente planilla con bloqueo temporales de clientes no ubicados. En base a la información derivada, procederá a enviar vía e-mail la información de los clientes no ubicados a cada una de las sucursales de origen para que se gestione el contacto con los clientes en el menor tiempo posible. La información derivada es clasificada en dos grupos, una por cada sucursal de origen, que es derivada a cada uno de los Agentes de ella, y otra correspondiente a la sucursal 36, la cual asocia toda la información de Fuerza de Venta, que será derivada a los Supervisores respectivos. La gestión y actualización a través de Fuerza de Venta recaerá en el Product Manager, quien deberá gestionar por una rápida obtención de la información de los clientes para solicitar la posterior actualización y habilitación de los plásticos.
1.- Actualización de Datos en Sucursales.	
EJECUTIVOS SUCURSALES	Recepcionará planilla de clientes con bloqueo temporal inubicables, con los cual procederán a contactar y/o localizar a cada uno de los clientes, o bien, estar atentos para cuando ellos se acerquen a sucursales para consultar por el bloqueo de su plástico en el sistema. Al momento en que un cliente se acerca a Sucursal a consultar el bloqueo del plástico, el Ejecutivo deberá verificar causal de bloqueo en FISA (TX 8-810), o consultando a la unidad de Operaciones Tarjetas causales del bloqueo. Si identifica, o bien, la unidad de Operaciones Tarjetas informa que corresponde a un cliente no ubicado, procederá a informar a cliente la causal y a efectuar el siguiente procedimiento: 1. Corrobora la información del cliente registrada en FISA (Transacción 2-2). 2. De no coincidir la información, consultará a cliente nueva información (Teléfonos y nuevos domicilios de ser el caso). 3. Para actualizar los nuevos datos telefónicos, deberá llamar a los nuevos teléfonos informados, para validar la información. 4. De no lograr el contacto, informará a cliente que desbloqueo será efectuado una vez que se valide dicha información, consultando a cliente, en que momento puede ser contactado. 5. De lograr el contacto telefónico, actualizará la información del cliente e informará que será contactado en el instante en que se

	desbloqueará el plástico, plazo que no deberá sobrepasar en una hora. NOTA: AL momento de lograr el contacto, sólo se deberá consultar si el cliente reside en dicho lugar, no entregando a terceros mayor información del plástico del cliente. 6. Los nuevos teléfonos, una vez validados, deberán ser informados a la brevedad posible vía telefónica al Contac Center, para que se consulte por las transacciones y habilite nuevamente el plástico.
ANALISTAS DE PREVENCION DE FRAUDE	Recepciona nueva información del cliente ubicado a través de sucursales, con lo cual procederá a contactarlo para consultar por alertas levantadas en Sentinel y procediendo de acuerdo a respuesta entregada por cliente. En caso que los teléfonos entregados no correspondan, se procederá a informar a Ejecutivo que entrego la información, informando que no se procederá a desbloquear el plástico por no ser validad la nueva información entregada.
2.- Actualización de Datos por Supervisores.	
SUPERVISORES FFVV	Recepciona información de cliente no ubicados informados por Product manager de tarjetas de Crédito. En base a listado entregado, procederán a solicitar a Ejecutivos de Origen el ubicar y actualizar los datos de los clientes en forma urgente. Una vez que los clientes se logran ubicar y se obtienen sus nuevos datos de contacto, estos son reportados vía e-mail a la unidad de actualización de Datos, con copia al Product manager de tarjetas, para que se efectúe la validación de la información y posterior modificación de ésta en FISA.
UNIDAD DE ACTUALIZACIÓN DE DATOS.	Recepcionará la información actualizada del cliente que derivada por cada uno de los Supervisores de Fuerza de Venta. En base a los datos recopilados, procederá a contactar a clientes y actualizar la información en FISA. De no concordar la información reportada, deberá enviar mail de regreso a Supervisor, con copia a Product Manager de tarjetas, para que sea rectificada. Una vez actualizada la información en FISA, se solicitará vía e-mail a Supervisor de Contac Center para que se contacte y proceda a efectuar el contacto con el cliente para consultar por las transacciones y alerta levantadas y desbloquear posteriormente el plástico del cliente en FISA.

SUPERVISOR CONTAC CENTER.	Entrega información a Analistas de Prevención de Fraude para que contacten al cliente y consulten por las alertas pendientes. De reconocer las transacciones el cliente, procederá a desbloquear su plástico en FISA. De no reconocerlas se procederá según “Procedimiento Contac Center 24x7”.

2. Flujograma de levantamiento de alertas Contac Center Ripley.



3. Script

A través de estos script, los analistas de fraude saben de qué forma deben conversar con los clientes a los cuales es necesario llamar para consultar por transacciones sospechosas o con clientes que se comunican a la línea 800 de Banco Ripley.

Script – Banco Ripley

Nº	: 419-C
Área	: Prevención Fraude
Evento de aplicación	: Bloqueo de Tarjeta por Cliente
Emisor	: Departamento de Calidad
Fecha Creación	: 23/10/07
Fecha Inicio	: 23/10/07
Estado	: Vigente

Paso 1: Saludo y Presentación

Agente: Banco Ripley buenos días/ tardes, atiende _____.

Agente: ¿Con quién tengo el gusto de hablar?

Agente: ¿Sr. / Sra.____ en que puedo ayudar?

Paso 2: Validación de Datos

- Según el caso, titular o adicional.

Agente: Sr. / Sra._____, indíqueme su Rut por favor.

Agente: Sr. / Sra._____, su nombre completo es _____.

Paso 3: Entrevista

Agente: Sr./ Sra._____, ¿Cuál es motivo del bloqueo de su tarjeta bancaria?

Agente: ¿Dejó constancia en carabineros?

Agente: Sr. / Sra._____, ¿Dónde (país – ciudad) perdió su tarjeta?

Agente: ¿Usted también perdió su cédula de identidad?

Agente: Sr. / Sra. _____, procederé a realizar el bloqueo de su Tarjeta de crédito bancaria, me podría indicar por favor un número de contacto, para la devolución del llamado y entrega del código de bloqueo.

Paso 4: Despedida

Agente: Sr./ Sra._____,gracias por preferir Banco Ripley. Hasta luego.

Paso 5: Confirmar Teléfono

- Verificar teléfono en Fisa si es distinto y permite el contacto en llamada por código de bloqueo, registrar y gestionar con “actualización de datos”.

Script – Banco Ripley

Nº : 420-C
Área : Prevención Fraude
Evento de aplicación : Bloqueo de Tarjeta – Notificación de código de bloqueo
Emisor : Departamento de Calidad
Fecha Creación : 23/10/07
Fecha Inicio : 23/10/07
Estado : Vigente

Paso 1: Saludo y Presentación

Agente: Buenos días/tardes, quisiera comunicarme con el/la Sr. (a) _____ (nombre y apellido), por favor.

- **Si el Cliente se encuentra, iniciar paso 2.**
- Si no contesta, marcar el caso como No contesta el teléfono (reintentar siguiente número o en otro horario)
- En el caso de no tener contacto, registrar el motivo por el cual no pudo ser ubicado en sentinel, carpeta y bitácora.

Agente: Sr. / Sra._____, mi nombre es _____ (nombre y apellido) de Banco Ripley.

Paso 2: Entrevista

Agente: Sr. / Sra._____, el motivo de mi llamado es para informarle que su tarjeta de crédito MasterCard ha sido bloqueada. Tome nota por favor, el código de bloqueo es _____.

Agente: ¿Me podría repetir el código entregado para confirmar la información?

Agente: Sr. / Sra._____, con fecha _____ (mencionar día/mes/año) su tarjeta MasterCard, ha sido bloqueada por _____ (mencionar motivo), a las ____ (mencionar hora según AM o PM).

Agente: Sr./Sra._____con la información que acabo de señalar usted debe dirigirse a la sucursal más cercana de banco ripley, para solicitar el nuevo plástico de la tarjeta de crédito bancaria.

Paso 4: Verificar Operaciones en sistema

- **No existen operaciones**, si al momento de realizar el bloqueo, en el sistema no registran operaciones realizadas, iniciar paso 5 despedida.
- **Existen operaciones**, informar:

Agente: Sr./Sra._____, le indico que en nuestro sistema registra(n) la(s) siguiente(s) operación(s) el día_____ (mencionar monto, hora y comercio).

Agente: Sr. / Sra._____ cuando reciba su estado de cuenta en su domicilio, le sugiero dirigirse nuevamente a la sucursal para realizar un requerimiento por desconocimiento de compras.

Agente: Sr. / Sra._____, ¿Tiene alguna duda o consulta?
(Informar si lo solicita)

Paso 5: Despedida

Agente: Sr. / Sra. _____ que tenga muy buenas tardes (días). Hasta luego

Script – Banco Ripley

Nº : 28
Área : Prevención Fraude
Evento de aplicación : Posible Fraude
Emisor : Departamento de Calidad
Fecha : 13/07/06
Estado : Vigente

- Utilizar teléfono particular, laboral y/o celular de acuerdo a la hora en la cual se realizará la llamada para contactar al cliente.
- Si el cliente se encuentra, iniciar **caso 1**
- Si no se logra contactar al cliente en números telefónicos disponibles, utilizar paginas blancas y FISA Tx. 2-5 para establecer contacto con familiares u otros teléfonos registrados del cliente.
- Si el llamado es un contacto o familiar del cliente, iniciar **caso 2**
- Si el contacto con familiar o amistad y teléfono no es del cliente, iniciar **caso 3**
- Si no contesta, marcar el caso como No contesta el teléfono (reintentar siguiente número)
- En el caso de tener contacto en los teléfonos, registrar el motivo por el cual no pudo ser ubicado (tabla de causales de No Ubicación)

Caso 1 – Cliente Contactado

Paso 1: Saludo y Presentación

Agente: Buenos días/ tardes, quisiera comunicarme con el/ la Sr.(a)_____ (nombre y apellido cliente), por favor.
Agente: Mi nombre es (nombre y apellido) _____ de Banco Ripley.

Paso 2: Entrevista

Agente: Sr. / Sra._____, estamos verificando el uso de su tarjeta Mastercard de Banco Ripley, por este motivo deseamos confirmar transacciones que registran en nuestro sistema, tales como: (mencionar resumen o detalle de algunas transacciones)

- **Si el cliente requiere más información, entregar todos los antecedentes.**

- **Cliente reconoce transacciones**

Agente: Sr. / Sra._____, con la finalidad de resguardar su seguridad y prevención, hemos solicitado los antecedentes antes señalados ¿Sr. / Sra._____, tiene alguna duda o consulta? (Paso 3)

- **Cliente no reconoce transacciones**

Agente: ¿Entones Sr. / Sra._____, de acuerdo a lo que me informa, la(s) transacción(es) (mencionar comercio, hora, monto) no la(s) realizó usted?

- **Responde Sí** (Paso 3)

- **Responde No**

Agente: ¿Usted tiene su tarjeta en su poder?

- Registrar respuesta SI/NO.

Agente: Sr. / Sra._____, para su tranquilidad bloquearé su tarjeta en Transbank y le informaré su código de bloqueo, espere un momento por favor.
(Agente debe contactar a Transbank para el bloqueo de la tarjeta)

Agente: Su tarjeta fue bloqueada a las ____(mencionar hora según AM o PM) y el código es _____.

- **En caso que el cliente desee reclamar por transacciones**

Agente: Sr. / Sra._____, para la gestión y respuesta de su reclamo le sugiero que se dirija a su ejecutivo con su estado de cuenta y se formulará el reclamo correspondiente por desconocimiento de compras, en caso de ser necesario se investigará su situación. ¿Sr. / Sra._____, tiene alguna duda o consulta? (Paso 3)

Paso 3: Despedida

- **Informar según corresponda**

Agente: Sr. / Sra._____, gracias por su tiempo e información. Hasta luego.
Agente: Sr. / Sra._____, agradecemos su comprensión. Hasta luego.

Caso – 2

Paso 1: Saludo y Presentación

Agente: Buenos días/ tardes, quisiera comunicarme con el/ la Sr.(a)_____ (nombre y apellido contacto o familiar), por favor.
Agente: Mi nombre es (nombre y apellido) _____ de Banco Ripley.

Paso 2: Entrevista
Agente: Sr. / Sra._____, lo(a) estoy llamando con el fin de ubicar a Sr. / Sra._____, (nombre de cliente) ya que en los teléfonos de nuestros registros no hemos tenido contacto, por este motivo quisiera solicitar algún teléfono donde pueda comunicarme.

- **Si contacto indaga o solicita mayor información**

Agente: Sr. / Sra._____, estamos validando las compras realizadas por el /la Sr. / Sra._____.

- **No desea entregar información**

Agente: De igual forma, Sr./ Sra. _____ me puede contactar en el número_____, mi nombre es _____ (nombre y apellido) de Banco Ripley.

Paso 3: Despedida

Agente: Sr. / Sra._____, gracias por su tiempo e información. Hasta luego.

Caso – 3

Paso 1: Saludo y Presentación

Agente: Buenos días/ tardes, mi nombre es (nombre y apellido) _____ de Banco Ripley, estoy ubicando
a el/ la Sr.(a)_____ (nombre y apellido cliente)

Agente: ¿Con quien tengo el gusto de hablar?

Agente: Sr. / Sra._____, quisiera comunicarme con el/ la Sr. / Sra._____, me podría indicar en que horario puedo contactar al Sr./ Sra. _____, o si usted posee algún teléfono de contacto.

Paso 2: Entrevista

- **Si contacto indaga o solicita mayor información**

Agente: Sr. / Sra._____, por motivos de seguridad del cliente no estoy facultado para entregar mayor información, sin embargo el motivo de mi llamado es con la finalidad de verificar el uso de la tarjeta de crédito Mastercard.

- **VERIFICAR:**

- **Cliente tiene transacciones internacionales**

Agente: El/ la Sr. / Sra._____, se encuentra fuera del país?

- **Sí**

Agente: ¿En que país se encuentra el/ la Sr. / Sra._____, ?

- **Si el país es de donde se efectuó la transacción**

Agente: ¿El/ la Sr. / Sra._____, se localiza en _____ (mencionar país)? ¿Me podría indicar en que fecha viajó y cuando regresa?

- Registrar información

Agente: Sr. / Sra._____, de todas maneras solicitamos estos antecedentes como medida de seguridad.

- **No**

- **No esta en el país de la transacción o si la transacción de una región es distinta a la dirección del cliente**

Agente: Sr. / Sra._____, por favor informar al Sr. / Sra._____, (cliente) que procederé a bloquear temporalmente la tarjeta, además solicitó que me contacte lo antes posible para aclarar su situación, en el número _____, mi nombre es _____(nombre y apellido)

- **Si son transacciones de la región del cliente**

Agente: ¿Sr. / Sra._____, me podría indicar en que horario me puedo comunicar con el/la Sr./ Sra. _____?
De igual forma, me puede contactar en el número_____, mi nombre es _____ (nombre y apellido) de Banco Ripley.

- **Si contacto indaga o solicita mayor información**

Agente: Sr. / Sra._____, sólo deseo realizar algunas preguntas acerca de su tarjeta de crédito Mastercard Banco Ripley.

Paso 3: Despedida

Agente: Sr. / Sra._____, gracias por su tiempo e información. Hasta luego.

4. Sentinel Prevention

El supervisor del departamento de prevención de fraude de Banco Ripley, junto a los analistas de dicho departamento utilizan para el desempeño de las actividades de monitoreo y seguimiento de transacciones un sistema informático especial llamado Sentinel Prevention, el que se encuentra constantemente en línea con Redbanc y Transbank y se carga de todas las transacciones realizadas con la tarjeta Mastercard de Banco Ripley.

Sentinel Prevention permite la detección y seguimiento de fraudes para la sección emisora de una empresa de tarjetas de crédito, mediante el uso de la tecnología, para la detección y análisis de fraude conocida como regla de negocios, perfiles o indicadores.

a) *Generalidades:* Cada persona que utilice este sistema es identificado con un usuario, el cual es un analista del departamento para quien se establecen derechos y privilegios individualmente sobre cada una de las operaciones del sistema.

Una de las características principales es que permite el monitoreo y seguimiento de los casos sospechosos, por parte del departamento de prevención de fraude de Banco Ripley, sucursal Valparaíso, lo que brinda a la gerencia una visión en el ámbito general del comportamiento del fraude y la efectividad del seguimiento por parte de cada uno de los analistas.

b) *Características:*

- Interfase gráfica y amigable en sistemas Microsoft Windows 95 o superiores
- Manejo de la seguridad del sistema, por medio de claves de acceso a la base de datos, para cada usuario.
- Definición detallada de privilegios, para cada usuario, a las opciones utilizadas en el sistema.
- Ayuda en línea.
- Bilingüe (Inglés - Español).
- Totalmente operacional en redes (sistema multiusuario).

- Definición de reglas de negocios y perfiles para detectar actividad sospechosa de fraude en Tarjetahabientes.
- Ejecución automática de reglas de negocios e indicadores tanto para Comercios como para Tarjetahabientes.
- Revisión de actividad sospechosa de fraude, de lo general a lo específico.
- Determinación de las reglas de negocios o parámetros que permitieron detectar una actividad sospechosa de fraude.
- Medición del desempeño de reglas de negocios o indicadores establecidos para la determinación de actividad sospechosa de fraude.

c) *Beneficios:* Permite la detección de actividad sospechosa de fraude:

- Ejecución automática de reglas de negocios y perfiles, permitiendo que el personal de Seguridad invierta su tiempo en el análisis y seguimiento de los casos sospechosos.
- Permite el envío automático de correos electrónicos (email's), con el resultado de los distintos procesos a direcciones de correo predeterminadas.
- Permite a los departamentos de seguridad de las distintas entidades el acceso a la información, mediante la utilización de una interfaz Web, facilitando a cada entidad el monitoreo y seguimiento de la actividad sospechosa de fraude.
- Brinda la visión del comportamiento del fraude por Unidad Estratégica de Negocios, mostrando además, la efectividad en la prevención, detección y seguimiento de la actividad fraudulenta.
- Permite evaluar la efectividad de las reglas de negocios e indicadores en la detección del fraude, mediante la valoración del aporte brindado por cada regla.

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

Transacciones sospechosas: transacciones que, de acuerdo a perfiles de tarjetahabientes o indicadores establecidos, puede ser producto de un fraude.

e) *Ingreso al Sistema:* Para ingresar al sistema, se cuenta con un icono. Se puede activar presionando el botón izquierdo del ratón dos veces sobre él.
Al activarlo el sistema desplegará una ventana donde el usuario deberá registrarse con su clave de acceso. Esta ventana le pedirá los siguientes datos:

1. *Usuario*: Nombre con que el usuario se identifica en el sistema; usualmente se utiliza el primer nombre o las iniciales de la persona. Cada usuario tendrá diferentes privilegios en el sistema, es decir, pueden controlarse las opciones que utiliza y las aplicaciones que puede ejecutar. El administrador del sistema fijará los privilegios de estos usuarios desde la opción de menú Privilegio.

2. *Contraseña*: Código privado de cada usuario con el que tiene acceso a la base de datos, por razones de seguridad, el sistema presentará asteriscos en el espacio de captura cuando el usuario digita los caracteres de su contraseña. Al ingresar por primera vez al sistema, la contraseña de acceso al sistema será la misma que el usuario, por lo que el sistema le mostrará la pantalla de la opción Cambiar Password para que realice el cambio de su contraseña.

3. *DSN*: Espacio en que el usuario definirá la base de datos por utilizar, seleccionando la requerida entre la lista de Bases de Datos configuradas en la estación de trabajo. Este espacio cuenta con un botón tipo "combo" cuyo icono es una flecha hacia abajo. La función de este botón es desplegar en una lista las opciones que pueden seleccionarse, esta selección se realiza presionando el botón izquierdo del ratón con el cursor sobre la opción deseada.

5. Entrevista al supervisor del departamento de prevención de fraude.

Durante el desarrollo del presente proyecto de tesis se considera dentro de la metodología realizar una entrevista al supervisor para obtener mayor información con respecto a las actividades y funciones que los analistas de prevención de fraude deben ejercer junto a controles aplicados entre otras consultas y gestiones que él debe realizar en su cargo, pero por medidas tomadas por la administración de Contact Center Ripley se ha cambiado la directiva de la empresa y el área momentáneamente ha quedado sin supervisor por lo que durante el tiempo que se entrevistó a sus analistas estos realizaron sus actividades sin él, en espera que otra persona tomara el cargo.

Objetivos de Banco Ripley y del departamento de prevención de fraude.

Se procede a identificar los objetivos del Banco Ripley y del departamento de prevención de fraude de Banco Ripley, sucursal Valparaíso, indicados por el jefe de dicho departamento.

- OBJETIVO BANCO RIPLEY: *Prevenir en forma efectiva el fraude a que el Banco Ripley esta expuesto por el uso de las tarjetas de crédito y débito, de la manera más expedita, cuidando el patrimonio del banco y de los clientes.*

- OBJETIVOS DEL DEPARTAMENTO DE PREVENCIÓN DE FRAUDE DE BANCO RIPLEY, SUCURSAL VALPARAÍSO:
    1. *Prevenir el fraude interno (en el banco).*
    2. *Prevenir el fraude para los clientes.*

Existe relación entre el objetivo del Banco Ripley y el departamento de prevención de fraude, ya que la constitución de dicho departamento es con la finalidad de cubrir el objetivo del banco.

Riesgos operacionales más significativos y el respectivo control que lo mitiga.

Se ha solicitado a la administración del riesgo operacional de Banco Ripley que indique cuales son los riesgos más significativos para este departamento junto a la respectiva acción o control que lo minimiza. Todo esto para realizar una evaluación del riesgo operacional en mencionado departamento. La administración del riesgo operacional ha informado lo siguiente:

1. Colusión entre analistas y clientes para ignorar alertas y permitir el fraude sin bloquear tarjeta de crédito Mastercard de Banco Ripley.

   1.1 *En la revisión que reclaman los clientes se detecta la ausencia de actividad frente a un fraude y se determina quien y el porque no actuó.*

2. Ausencia de analista en el Contact Center Ripley, sucursal Valparaíso.

   2.1 *Ante la ausencia por problemas de accidentes o para llegar al Contact Center Ripley, sucursal Valparaíso, se puede buscar un remplazante de otro turno y si fuera imposible puede monitorear en Santiago por un tiempo corto.*

3. Analista no puede trabajar en Contact Center Ripley, sucursal Valparaíso, (desastre en el edificio o falla en la comunicación del sistema).

   3.1 *Se puede habilitar, en forma temporal, los puestos en Banco Ripley, sucursal en Santiago por un corto tiempo.*

Identificación del conocimiento que poseen los Analistas del departamento de prevención de fraude de Banco Ripley.

Para obtener el conocimiento que poseen los analistas de fraude de dicho departamento, se ha confeccionado un cuestionario de control interno (CCI), que señala los controles esperados, el cual también contempla diferentes procedimientos los que tendrán que ser contestados con respuestas cerradas de SI y NO. Además, de esta forma

se pretende documentar el sistema de control interno de las actividades que ejercen estos analistas.

Este cuestionario será respondido por los tres analistas de prevención de fraude que se encuentran durante la fecha del presente proyecto. Cada documento tendrá una identificación, analista Nº 1, analista Nº 2 y analista Nº 3. Este documento será de gran utilidad para preparar las pruebas de cumplimiento que se realizarán más adelante.

El cuestionario de control interno (CCI), deberá ser respondido con una “X” en la alternativa que seleccione el analista. A continuación, se adjuntan cuestionario de control interno con las respuestas entregadas por los analistas de dicho departamento:

Cuestionario de control interno (CCI)

Analista Nº 1	SI	NO
1. ¿Se realiza el correspondiente registro de los bloqueos efectuados o recibidos por el analista independiente de su motivo?	X	
2. Si el cliente reclama por fraude ¿Es posible verificar información en el sistema utilizado por el analista?	X	
3. Cada vez que se descarta una transacción ¿Se registra el debido comentario del por qué se descarta?	X	
4. ¿Es de acceso restringido la información y utilización de sistemas que ocupa el analista?	X	
5. ¿Existe monitoreo de sistema por parte del supervisor del área?		X
6. Si se ausenta un analista, ¿Siempre existe un reemplazante para el turno?		X
7. ¿Existe alguna secuencia correlativa que indique relación entre fraudes y bloqueos por desconocimiento de compra que indique algún cliente?		X
8. Caída del sistema IBM, Sentinel, etc. ¿Ha impedido trabajo del analista de fraude en el Contac Center Ripley, sucursal Valparaíso?	X	
9. Sistemas utilizados por analistas ¿Solicitan modificaciones de acceso, (cambio de password) cada cierto tiempo?	X	
10. Cuando el analista efectúa bloqueo de tarjeta de crédito Mastercard de Banco Ripley ¿Se registran los siguientes datos al momento de efectuarse el servicio?		
a) Nombre completo de cliente.	X	
b) RUT.	X	
c) Número de tarjeta de crédito.	X	

	d) Motivo del bloqueo.	X	
	e) Código de bloqueo.	X	
	f) Fecha y hora bloqueo.	X	
	g) Nombre del analista que ejecuta el bloqueo, ya sea bloqueo temporal o permanente.	X	
	h) Nombre del ejecutivo que bloquea en Transbank.		X
	i) Nombre del ejecutivo y sucursal a la que corresponde cliente.	X	
	j) Registro de envío de correo entregando información de bloqueo a supervisor y jefe de área.	X	
	k) Registro de monto ahorrado y monto de fraude en el momento de bloqueo de tarjeta de crédito.	X	
	l) Si el cliente tiene o no su tarjeta de crédito.	X	
11.	¿Existe algún registro de las llamadas tanto de salida como de entrada que son realizadas o recibidas para solicitar o realizar bloqueo de tarjeta de crédito?	X	
12.	¿Existen registros, bitácoras, etc., en que el analista pueda detallar su desempeño cada vez que realiza sus actividades?	X	
13.	¿Debe solicitar el analista autorización para practicar bloqueo temporal de tarjeta de crédito?		X

Cuestionario de control interno (CCI)

Analista Nº 2	SI	NO
1. ¿Se realiza el correspondiente registro de los bloqueos efectuados o recibidos por el analista independiente de su motivo?	X	
2. Si el cliente reclama por fraude ¿Es posible verificar información en el sistema utilizado por el analista?	X	
3. Cada vez que se descarta una transacción ¿Se registra el debido comentario del por qué se descarta?		X
4. ¿Es de acceso restringido la información y utilización de sistemas que ocupa el analista?	X	
5. ¿Existe monitoreo de sistema por parte del supervisor del área?		X
6. Si se ausenta un analista, ¿Siempre existe un remplazante para el turno?		X
7. ¿Existe alguna secuencia correlativa que indique relación entre fraudes y bloqueos por desconocimiento de compra que indique algún cliente?	X	
8. Caída del sistema IBM, Sentinel, etc. ¿Ha impedido trabajo del analista de fraude en el Contac Center Ripley, sucursal Valparaíso?	X	
9. Sistemas utilizados por analistas ¿Solicitan modificaciones de acceso, (cambio de password) cada cierto tiempo?	X	
10. Cuando el analista efectúa bloqueo de tarjeta de crédito Mastercard de Banco Ripley ¿Se registran los siguientes datos al momento de efectuarse el servicio?		
a) Nombre completo de cliente.	X	
b) RUT.	X	
c) Número de tarjeta de crédito.	X	

d) Motivo del bloqueo.	X	
e) Código de bloqueo.	X	
f) Fecha y hora bloqueo.	X	
g) Nombre del analista que ejecuta el bloqueo, ya sea bloqueo temporal o permanente.	X	
h) Nombre del ejecutivo que bloquea en Transbank.		X
i) Nombre del ejecutivo y sucursal a la que corresponde cliente.	X	
j) Registro de envío de correo entregando información de bloqueo a supervisor y jefe de área.	X	
k) Registro de monto ahorrado y monto de fraude en el momento de bloqueo de tarjeta de crédito.	X	
l) Si el cliente tiene o no su tarjeta de crédito.	X	
11. ¿Existe algún registro de las llamadas tanto de salida como de entrada que son realizadas o recibidas para solicitar o realizar bloqueo de tarjeta de crédito?	X	
12. ¿Existen registros, bitácoras, etc., en que el analista pueda detallar su desempeño cada vez que realiza sus actividades?	X	
13. ¿Debe solicitar el analista autorización para practicar bloqueo temporal de tarjeta de crédito?		X

Cuestionario de control interno (CCI)

Analista Nº 3	SI	NO
1. ¿Se realiza el correspondiente registro de los bloqueos efectuados o recibidos por el analista independiente de su motivo?	X	
2. Si el cliente reclama por fraude ¿Es posible verificar información en el sistema utilizado por el analista?	X	
3. Cada vez que se descarta una transacción ¿Se registra el debido comentario del por qué se descarta?		X
4. ¿Es de acceso restringido la información y utilización de sistemas que ocupa el analista?	X	
5. ¿Existe monitoreo de sistema por parte del supervisor del área?		X
6. Si se ausenta un analista, ¿Siempre existe un remplazante para el turno?		X
7. ¿Existe alguna secuencia correlativa que indique relación entre fraudes y bloqueos por desconocimiento de compra que indique algún cliente?	X	
8. Caída del sistema IBM, Sentinel, etc. ¿Ha impedido trabajo del analista de fraude en el Contac Center Ripley, sucursal Valparaíso?	X	
9. Sistemas utilizados por analistas ¿Solicitan modificaciones de acceso, (cambio de password) cada cierto tiempo?	X	
10. Cuando el analista efectúa bloqueo de tarjeta de crédito Mastercard de Banco Ripley ¿Se registran los siguientes datos al momento de efectuarse el servicio?		
a) Nombre completo de cliente.	X	
b) RUT.	X	
c) Número de tarjeta de crédito.	X	

d) Motivo del bloqueo.	X	
e) Código de bloqueo.	X	
f) Fecha y hora bloqueo.	X	
g) Nombre del analista que ejecuta el bloqueo, ya sea bloqueo temporal o permanente.	X	
h) Nombre del ejecutivo que bloquea en Transbank.	X	
i) Nombre del ejecutivo y sucursal a la que corresponde cliente.	X	
j) Registro de envío de correo entregando información de bloqueo a supervisor y jefe de área.	X	
k) Registro de monto ahorrado y monto de fraude en el momento de bloqueo de tarjeta de crédito.	X	
l) Si el cliente tiene o no su tarjeta de crédito.	X	
11. ¿Existe algún registro de las llamadas tanto de salida como de entrada que son realizadas o recibidas para solicitar o realizar bloqueo de tarjeta de crédito?	X	
12. ¿Existen registros, bitácoras, etc., en que el analista pueda detallar su desempeño cada vez que realiza sus actividades?	X	
13. ¿Debe solicitar el analista autorización para practicar bloqueo temporal de tarjeta de crédito?		X

Pruebas de cumplimiento.

Las pruebas de cumplimiento son procedimientos de auditoria diseñados para obtener seguridad razonable de los controles internos en los cuales se depositó confianza y que dichos controles se están realizando como corresponde.

Las pruebas de cumplimiento realizadas fueron sobre: Observación, indagación y examen de evidencia. Se recuerda que no se deja evidencia física del examen de la documentación, pero se constata en forma escrita la evidencia de su ejecución.

La información recopilada fue la siguiente:

Analista Nº 1

Observación:

- Se recepciona llamada solicitando bloqueo permanente de tarjeta Mastercard.
- Analista registra información de cliente en cuaderno personal exclusivo para el trabajo.
- Sigue script indicado para el bloqueo.
- Solicita información indicada como nombre completo, RUT, motivo del bloqueo, ciudad en que ocurrió, teléfono de contacto, entro otros antecedentes.
- Realiza llamado a Transbank solicitando bloqueo a través de número de tarjeta o RUT de cliente.
- Registra información entregada por ejecutivo que bloquea en transbank en cuaderno personal.
- Devuelve llamado telefónico a cliente para indicar código de bloqueo según script correspondiente al caso.
- Envía mail informando a supervisor, jefe del área y a los demás analistas el bloqueo efectuado
- Actualiza planillas manuales e informáticas respectivas según el motivo del bloqueo.
- Monitorea el sistema y actualiza cada tres a cinco minutos aproximadamente.
- Se contacta con algunos clientes por transacciones sospechosas confirmando operación.

- Registra comentario de descarte por transacción confirmada por cliente, pero no siempre escribe que intentó contactar a otro cliente y no contestaron.
- Analiza transacciones mediante pagos anteriores y registro histórico de otras transacciones que ha realizado el cliente para confirmar descarte sin necesidad de llamar a cliente.
- Analista revisa bitácora y contacta a cliente pendientes dejados por turno anterior.

Indagación:

- Ha tenido que remplazar urgente a analista que a faltado a su turno por caso fortuito o fuerza mayor, pero indica también que solo fue por disposición y no obligación.
- No se ha estipulado un lineamiento a seguir por si falta alguien en el turno.
- Nunca ha ocurrido colusión entre analistas y clientes, pero indica que dentro del Banco Ripley si.
- Caída de sistema al comienzo, en la creación de departamento, provocaba que no se pudiera trabajar, pero que ahora se ha regularizado y por lo general no sucede.
- Cámara registra quien entra y sale de módulo de trabajo.
- No identifica secuencia correlativa entre fraude y bloqueo, respondiendo que no en cuestionario de control interno, pero se consulta y responde que si existe correlación, por lo que indica que entendió mal la pregunta de dicho cuestionario.

Examen de evidencia:

- Se solicita que muestre secuencia correlativa que identifica fraude y bloqueo de un cliente determinado y lo busca sin inconvenientes observando que efectivamente existe.
- Planillas se encuentran actualizadas, tanto planillas manuales como informáticas.
- Bitácora se encuentra registrado con nombre y fecha en que analista trabaja. Se revisa el día de hoy y los demás y efectivamente se encuentran así.
- Cuaderno personal registra fecha y hora de trabajo, es dejado en módulo, siendo de uso exclusivo de trabajo.

Analista Nº 2

Observación:

- Identifica transacciones más sospechosas y son las primeras en intentar contactar a cliente.
- Se guía por script al contactar a cliente.
- Analista registra en cuaderno personal información de cliente que contacta.
- Ejecutivo solicita que cliente confirma transacción para que quede registro de ella en grabación
- Escribe comentario adecuado para el descarte de transacción que confirmó cliente.
- Casos pendientes en bitácora los revisa y llama a horario indicado por compañeros de trabajo.
- Actualiza reglas de sistema Sentinel de tres a cinco minutos aproximadamente.
- Cuando llama en ocasiones no escribe comentario indicando que no fue posible contactar a cliente.
- Analista busca en base de datos información de teléfonos alternativos para contactar a cliente a través de RUT o nombre completo en páginas blancas, DGC y RC Web. (sistemas solo para buscar información).
- Anota en cuaderno personal todos los datos de cliente por si sistema se desconecta (un resguardo para mantener nombre de cliente visible).

Indagación:

- Indica que nunca en el departamento a ocurrido algo como colusión o pérdida de información pero que en el banco si.
- Nunca ha remplazado a otro analista, indicando que no existe un procedimiento como medida para saber que hacer en tal caso.
- Se ha desconectado el sistema, el cual no ha permitido trabajar, pero son muy pocas las ocasiones en que a sucedido, por lo que cuando a ocurrido se en tomado las medidas del caso como llamar a IBM para solicitar ayuda y avisar a supervisor del área.
- Analista indica que no solicita el nombre de la persona que bloquea en Transbank porque código de bloqueo está compuesto por iniciales de nombre y apellido de quien bloquea.

Examen de evidencia:

- Se solicita planillas de bloqueos, las que se encuentran actualizadas tanto manuales como informáticas.
- Cuaderno personal es dejado en el trabajo, su uso es exclusivo para registro de información de clientes.
- Cuadratura diaria de sistema Sentinel se encuentra actualizado, tanto el día de ayer como los demás (esta cuadratura se realiza con un día de desfase).
- Bitácora registra fecha y hora, junto con el nombre del analista de turno, al igual que su cuaderno personal.

Analista Nº 3

Observación:

- Analista trabaja en planilla enviada mediante correo por el jefe de área y supervisor para que contacte a los clientes indicados en ella. Esta es una solicitud especial, no siempre se efectúa esta actividad.
- Monitorea sistema de vez en cuando, al parecer se le olvida por estar pendiente de cumplir con planilla solicitada.
- Casos pendientes dejados por compañeros en otros turnos son retomados y contactados en horario indicado.
- Registra información en cuaderno personal y en bitácora, con fecha y hora respectiva del turno en que se encuentra.

Indagación:

- Única persona que ha viajado a Santiago, pero porque en Contact Center Ripley instalaron un artefacto, por lo que no se podía trabajar en el edificio.
- Se consulta por colusión e indica que en departamento nunca ha ocurrido algo parecido pero que dentro del banco si ha ocurrido, siendo el departamento de prevención de fraude quien los detecta.
- Se consulta por comentarios e indica que no siempre se registran en Sentinel, pero que ocurre pocas veces dependiendo de la cantidad de trabajo que tenga el analista o por que las transacciones no son tan sospechosas que se quita de las demás reglas en base a información sin escribir comentario.
- Ha remplazado en forma urgente a otros analistas, pero por buena disposición. Indica que no existe un procedimiento a seguir en tal caso y que en una ocasión

supervisor anterior al actual no pudo contactar a ningún analista durante la madrugada que él se quedó monitoreando durante todo lo que quedaba de turno, sin conocer mucho el sistema.

- Cuaderno personal es dejado en lugar de trabajo, siendo de uso exclusivo para ello.
- Analista indica que supervisor del área no monitorea, como apoyo, sistema Sentinel Prevention, pero que para cualquier duda llama a jefe de área en Santiago y él también tiene acceso al sistema y monitorea transacciones.

Examen de evidencia:

- Planillas solicitadas se encuentran actualizadas
- Registro correspondiente en bitácora y cuaderno personal se encuentra con fecha y hora del turno en el cual se encuentra.

Análisis de información recopilada

La información recopilada es ingresada a la siguiente tabla para realizar un análisis de toda la información entregada por la administración y la adquirida por la aplicación de pruebas de cumplimiento y cuestionario de control interno.

El cuadro con la información ingresada es el siguiente:

Riesgo operacional Identificado como más significativo.	**Control que lo mitiga.**	**Puntos de atención.**	**¿Se realiza?**		**Descripción / comentario**
			SI	**NO**	
1. Colusión entre analista y cliente para ignorar y permitir el fraude sin bloquear tarjeta Mastercard de Banco Ripley.	En la revisión que reclaman los clientes se detecta la ausencia de actividad frente a un fraude y se determina quien y el porque no actuó.	Registro de bloqueos con todos los datos requeridos según procedimiento.	X		Registro es enviado en forma diaria junto con la cuadratura de transacciones de Sentinel.
		Registro de comentarios es siempre realizado por analista.		X	Se registra comentario, pero en algunos casos no se registra, porque analista no contactó a cliente o en otros depende de que transacción se trate.
		Al descartar una de las transacciones siempre el analista realiza el debido comentario.		X	En ocasiones analista no registra comentario debido a la poca importancia de la transacción, su monto o de la cantidad de trabajo que tenga el analista.
		Existe monitoreo por parte del supervisor		X	Jefe de área en Santiago, según indagaciones monitorea sistema.

Riesgo operacional Identificado como más significativo.	Control que lo mitiga	Puntos de atención	¿Se realiza?		Descripción / comentario
			SI	NO	
		Es de acceso restringido los sistemas utilizados por el analista.	X		Sistema solicita cambio de clave secreta cada cierto tiempo y se bloquea si no es utilizado por un lapso de período determinado.
		Existe secuencia correlativa entre fraudes y bloqueos.	X		Numero correlativo identifica fraude y bloqueo en Sentinel, el que no se puede modificar.
		Grabación de llamadas tanto realizadas como decepcionadas.	X		Analistas cuentan con sistema para grabar conversaciones, pero no da seguridad que se efectúe al cien por ciento de las llamadas..
		Registro adecuado en bitácora (información de respaldo)	X		Cada Analista registra fecha y hora en bitácora, junto a información que es relevante señalar para el siguiente turno.
		Los Bloqueos permanentes son comunicados mediante correo electrónico	X		Siempre se envía correo sea bloqueo por robo, extravío o captura en cajero automático.

Riesgo operacional Identificado como más significativo.	Control que lo mitiga	Puntos de atención	¿Se realiza?		Descripción / comentario
			SI	NO	
		Bloqueo temporal es comunicado a supervisor o jefe de área.		X	Es registrado en planilla correspondiente y en bitácora, pero se efectúa según criterio de analista dependiendo de la transacción y el monto de ella. Existe criterio en primera instancia que deben considerar. Si no hay contacto con cliente en 48 horas se bloquea según procedimiento de cliente no ubicadle, pero siempre es decisión del analista.
2. Ausencia de analista en Contact Center Ripley, sucursal Valparaíso.	Ante la ausencia por problemas de accidente o para llegar al trabajo se puede buscar un reemplazante de otro turno y si fuere imposible, se puede monitorear desde Santiago por un tiempo corto.	Siempre existe reemplazante para un turno.		X	Analista en ocasiones han reemplazado a compañeros, pero ha sido de buena disposición.

Riesgo operacional Identificado como más significativo.	Control que lo mitiga	Puntos de atención	¿Se realiza?		Descripción / comentario
			SI	NO	
		Existe un procedimiento a seguir en caso que falte un analista.		X	No siempre están dispuestos a reemplazar. Analistas se encuentran en su horario libre.
		Frecuentemente, falta algún analista.		X	Solo han sido casos fortuitos o de fuerza mayor. No ocurre con mucha frecuencia, pero cuando ha sido reemplazado, compañero ha devuelto el día trabajado. (Solo Compañerismo).
3. Analista no puede trabajar en Contact Center Ripley, sucursal Valparaíso (desastre en el edificio o falla en la comunicación).	Se puede habilitar en forma temporal los puestos en Banco Ripley Sucursal de Santiago por un tiempo corto.	Se ha habilitado en Santiago posición de trabajo.	X		Fue caso planeado, en Contact Center Ripley instalaron artefacto y no se podía trabajar en el edificio.
		Caída de sistema ha impedido trabajar a los analistas.	X		No por más de un turno completo, por lo que no ha sido necesario ir a Santiago.

Conclusión de los riesgos identificados por la administración.

Riesgo Nº 1

Colusión entre analista y cliente para ignorar alertas y permitir el fraude sin bloquea tarjeta de crédito Mastercard de Banco Ripley.

Considerado el más importante de los tres riegos indicados por la administración del riesgo operacional de Banco Ripley, cabe destacar que no existe una supervisión en cuanto al monitoreo de sistema por parte del supervisor del área, pero hasta el momento y como así lo comprobaron las pruebas de cumplimiento realizadas, los analistas ejecutan su trabajo tomando generalmente las medidas del caso para el adecuado monitoreo de transacciones y el registro de los bloqueos ya sea permanente o temporal. Se aclara que al ser turnos cubiertos por una persona, el supervisor debe apoyar la función de monitoreo indicando situaciones sospechosas y manteniendo contacto con su equipo para su motivación y dar a conocer resultados del desempeño de estos, ya que denota un fuerte cansancio e insatisfacción con la empresa por no ser considerados.

Es importante resaltar que el analista no siempre registra el comentario en sistema Sentinel, esto debido a que la transacción no es considerada riesgosa, el cliente ha realizado transacciones similares anteriormente o tiene comentario de confirmación por uso de tarjeta en mismo comercio.

Lo que se observó también, es que el analista al descartar transacciones sospechosas, deja registro en cuaderno personal de algunos antecedentes que indican que cliente ha realizado la operación y no es un fraude, como por ejemplo: pagos al día, fecha y lugar de apertura de tarjeta, entre otros datos, los que son considerados al momento de descartar y son registrados en comentario correspondiente. En cuanto al cuaderno personal de cada analista con los registros de clientes, son dejados en el lugar de trabajo y en caso de robo o pérdida de ellos existe una cámara de grabación hacia el módulo en caso que se necesite verificar las personas que entran y salen de el. No se conoce algún caso de colusión entre los analistas debido al mal uso de la información de los clientes.

El acceso a la información es restringido y los analistas lo tienen bastante claro. Ellos saben que sus claves son personales y que para ingresar y descartar transacciones su usuario es registrado en sistema, por lo que cada analista es responsable de anotar en bitácora fecha y hora del turno que corresponda y así identificar cualquier inconveniente como por ejemplo el descarte de una transacción sospechosa que pudiere ser fraude comprobado. Por indagación se sabe que entre los analistas se facilitan claves de acceso a Terminal en caso de emergencia cuando se encuentra bloqueado Terminal y IBM no pueda solucionar inconveniente. Aún así, el analista debe si o si trabajar con su clave de acceso a Sentinel Prevention, no existiendo hasta el momento caso de descarte de transacción con otro usuario, ni siquiera por urgencia. Teniendo acceso al Terminal, no debería tener problemas para ingresar con clave personal a Sentinel, como ha ocurrido hasta el momento.

Se realiza revisión de documentos y planillas informáticas las que se encuentran al día y completas. Los analistas tienen organizada cada actividad que deben realizar por turnos, la que no ha sido indicada por el jefe ni por el supervisor del área, lo que es importante de resaltar ya que el departamento cuenta con analistas que han alcanzado un alto grado de independencia pero en forma grupal, organizados, por lo que son capaces de tomar decisiones en equipo lo que demuestra un entorno de control adecuado (pero solo entre el equipo), con atributos individuales, valores éticos y profesionales que es difícil de alcanzar, sobre todo en áreas de prevención como lo es este departamento.

Conclusiones / acciones necesarias

- Se puede indicar que en cuanto al cumplimiento de los procedimientos del mencionado departamento, para este riesgo parecen ser adecuados, ya que son seguidos y cumplidos por cada uno de los analistas y los controles descritos en los procedimientos generalmente son aplicados en la realidad y en la manera debida.
- Una medida o acción necesaria es el monitoreo por parte del supervisor. Se indica que en este caso el supervisor del área ha sido asignado hace muy poco tiempo por lo que es importante la rápida capacitación para el apoyo del equipo.

Riesgo Nº 2

Ausencia de analista en Contact Center Ripley.

En ocasiones se ha buscado reemplazante para cubrir un turno. Por las indagaciones realizadas en una ocasión supervisor anterior al actual reemplazó a analista ya que nadie estaba con disponibilidad de hacerlo. Supervisor se intentó comunicar vía telefónica con analistas en búsqueda de reemplazante sin obtener buenos resultados. (Cabe destacar que era turno nocturno).

Por comentarios de analistas, si se ha reemplazado ha sido por buena disposición por lo que es difícil tomar la decisión de reemplazar ya que se encuentran en su horario libre.

Conclusiones / acciones necesarias

- En cuanto a procedimientos para buscar reemplazante, no existe ninguno, por lo que es aconsejable confeccionar el correspondiente procedimiento y no mantenerlo de palabra. Todo esto para tener claridad de que cuando no esté disponible un analista o un reemplazante se comience a monitorear rápidamente desde Santiago, y así, tomar las medidas correspondientes al caso.

Riesgo Nº 3

Analista no puede trabajar en Contact Center Ripley, sucursal Valparaíso (desastre en el edificio o falla en la comunicación)

En Santiago se ha habilitado anteriormente posición para que analista trabaje, pero nunca ha sido por consecuencia de desastre en el edifico o falla en la comunicación, sino que por instalación de artefacto en edificio.

Por indagaciones realizadas analistas indicaron que en ocasiones el sistema no envía información, por lo que no han podido trabajar, pero si han tomado las medida del

caso, como llamar a IBM para solicitar solución y pronta conexión al sistema y también informar al supervisor y jefe del área.

Indican los analistas que fallas de comunicación pueden ocurrir en cualquier momento, en este último tiempo no, pero ocurría con frecuencia cuando el departamento comenzó con sus funciones.

Conclusiones / acciones necesarias

- Por lo visto, fallas en la conexión si han ocurrido impidiendo el monitoreo del sistema y no se sabe con exactitud si han sido monitoreadas dichas transacciones desde Santiago.
- En cuanto a desastre en el edificio, si o si, se deben habilitar posiciones para analistas en Santiago, pero es importante que esta medida se documente al igual que procedimiento a seguir por inconvenientes en caída de sistema. Si esto ocurre durante el turno de noche o en cualquier turno, el analista solo informará a supervisor y llamará a IBM, pero si el problema persiste, mientras tanto en Santiago no se están monitoreando las transacciones, corriendo el riesgo de que ocurra un fraude durante el turno del analista, sin tener mayor claridad de lo que se puede hacer.

Resultados del presente proyecto de tesis.

Como resultados de la presente investigación, podemos apreciar, según la información recopilada, el primer riesgo indicado por la administración, hasta cierto punto se ve cubierto. Los dos últimos riesgos indicados por la administración de ninguna forma se encuentran cubiertos, por eso el motivo de recomendación en el punto anterior. Si bien es cierto, el principal riesgo y más importante corresponde a la colusión entre analistas, y que a su vez, se ve mitigado a través de los procedimientos, flujos y otros que se encuentran implementados para el área, nos encontramos con que el punto más alto en la pirámide de los componentes a nivel de entidad y que debería ser el más fuerte no existe, que es el monitoreo. De acuerdo al alto grado de presencia de fraude con que cuenta el departamento y que justamente el objetivo del área es prevenirlo, tanto en forma interna

como externa, es importante mantener minimizado al máximo los riesgos señalados por la entidad. Se debe contar con el supervisor que preste la ayuda necesaria, inclusive, para dar el corte en los otros dos riesgos que no se encuentran regulados formalmente y que según su función podría brindar el control que falta. Además, cabe destacar que por indagaciones realizadas, han existido otros supervisores pero que por no contar con la capacidad necesaria para utilizar de forma adecuada los sistemas con que cuenta el departamento, no han brindado de forma eficiente su función de monitoreo correspondiente.

De acuerdo a nuestra evaluación y análisis de la información podemos estimar que la situación actual en la que se encuentra el departamento de prevención de fraude de Banco Ripley, Contact Center Ripley, sucursal Valparaíso para la cobertura de cada riesgo indicado por la administración según el rango “alto riesgo operacional, moderado riesgo operacional y bajo riesgo operacional”, podemos estimar lo siguiente:

Riesgo Nº 1

Colusión entre analista y cliente para ignorar alertas y permitir el fraude sin bloquea tarjeta de crédito Mastercard de Banco Ripley.

“Moderado riesgo operacional”

Riesgo Nº 2

Ausencia de analista en Contact Center Ripley.

“Alto riesgo operacional”

Riesgo Nº 3

Analista no puede trabajar en Contact Center Ripley, sucursal Valparaíso (desastre en el edificio o falla en la comunicación)

“Alto riesgo operacional”

Bibliografía

1. BACA, Gómez Antonio (1997). “La Administración de Riesgos Financieros”. Articulo tomado de la revista Ejecutivos de Finanzas, publicación mensual, Año XXVI, No. 11, Noviembre, México.
2. BODIE, Zwi y Robert C. Merton (1999). Finanzas. Editorial Pretince Hall, México.
3. COOPERS & LYBRAND (1997). C.O.S.O report (Informe COSO). Ediciones Díaz de Santos S.A. Madrid. España.
4. DÍAZ, Tinoco Jaime y Fausto Hernández Trillo (1996). Futuros y opciones financieros. Edita Limusa, México.
5. DEFLIESE, JAENICKE, SULLIVAN, GNOSPELIUS (2001). Auditoria Mongomery. Editorial Limusa S.A. Quinta Reimpresión de la segunda edición. México.
6. FRAGOSO, J.C. (2002). “Análisis y Administración de Riesgos Financieros”. Exposición de la materia de Análisis de Riesgos, de la especialidad en Economía Financiera de la Universidad Veracruzana, Capítulo 13: Mercado de Derivados, Xalapa.
7. JORION, Philippe (1999). Valor en riesgo. Editorial Limusa, México.
8. KRUGMAN, R. Paul y Maurice Obstfeld (1995). Economía Internacional. 3ª Edición, Editorial McGraw-Hill, España.
9. LEVI, D. Maurice (1997). Finanzas Internacionales. 3ª Edición. Editorial McGraw-Hill. México.
10. LEWENT, Judy C., y A. John Kearney (1990). “Identifying, Measuring, and Hedging Currency Risk at Merck”. Continental Bank Journal of Applied Corporate Finance 2, pp.19-28; EE.UU.
11. PASCALE, Ricardo (1999). Decisiones Financieras. 3ª Edición, Ediciones Machi, Argentina.
12. RAIFFA, Howard. (1978). Análisis de la desición empresarial. Ediciones Deusto S.A. España.
13. RODRÍGUEZ, de Castro J. (1997). Introducción al Análisis de Productos Financieros derivados. 2ª Edición, Editorial Limusa, México.
14. VAN GREUNING, Hennie y Brajovic, Sonja (2003), “Analyzing and Managing Banking Risk”, The World Bank, Second edition.