



UNIVERSIDAD DEL BÍOBÍO
DIRECCIÓN DE GRADUADOS
MAGISTER EN DIRECCION DE EMPRESAS

Tesis para optar al Grado de Magíster en Dirección de Empresas.

“La Gestión del Riesgo Operacional: Diseño de sistema de administración de riesgo operacional y análisis de metodologías de estimación de capital regulatorio según Basilea III.”

Cristian Mauricio Muñoz Anziani.

Profesor Guía: Dr. Alex Medina Giacomozzi.

Marzo del 2014.

Agradecimientos

Creo firmemente que cada uno de mis logros, no son más que la sumatoria de los esfuerzos combinados de muchas personas, por lo cual entiendo plenamente la importancia de esos párrafos.

Quiero agradecer a mi familia, ya que con su amor han motivado mi vida y me han entregado la fuerza necesaria para enfrentar cualquier desafío con valentía, optimismo y alegría, son ellos quienes en gran parte guían mi actuar y por tanto este objetivo cumplido se los debo completamente a ellos.

Agradezco a mi padre Humberto y mi madre María Angélica, por los valores que me enseñaron desde pequeño, por su diaria preocupación y cuidado hacia mí y mis hermanos, y por entregarme tanto amor durante toda mi vida, solo espero ser digno de sus infinitos esfuerzos y sacrificios, y regalarme algún día la oportunidad de sacrificarme por ustedes.

Debo además, agradecer a mis dos hermanos, Jorge y Fernando, quienes son mi gran motor en la vida, su presencia y constante apoyo no solo me favorecen, sino que también me motivan a mejorar cada día. Sinceramente la presencia de ustedes es para mí, el motivo primordial de mi existencia y es mi gran sueño el ser un apoyo para ustedes el día que lo necesiten.

Por supuesto no puedo olvidar, ni dejar de agradecer a quienes completan este hermoso círculo de personas, mis abuelos, que son y serán un ejemplo de vida, a mis tíos y primos, personas de corazón grande y de alegría contagiosa, gracias a todos, pues como dije anteriormente este logro no es mío, es de ustedes.

Finalmente, quiero agradecer al profesor Sr. Alex Medina, quien guió esta tesis con gran profesionalismo, cualidad que personalmente me produce una gran admiración. Estimado profesor su experiencia, conocimientos, capacidad y humildad fueron de vital ayuda para el cierre de esta etapa.

Siento que por distintas circunstancias de la vida este fue un camino duro, un último esfuerzo digno mantener en mi memoria, pues en retrospectiva esta etapa que hoy culmina sacó lo mejor de mí, y me probó constantemente.

Soy un gran admirador de la fortaleza y la determinación, en consecuencia un camino difícil, no es más que una oportunidad de dar lo mejor de ti y crecer con aquello, por lo tanto hoy, mirando hacia atrás el camino recorrido, solo puedo decir muchas gracias.

Cristian Mauricio Muñoz Anziani.

Contenido

Agradecimientos	2
Introducción.....	6
PLANTEAMIENTO DEL PROBLEMA.....	7
Riesgo operacional	8
Objetivo Principal:.....	9
Objetivos Específicos:	9
CAPITULO I: MARCO TEORICO.....	10
Banco	10
Sistema Financiero chileno	12
Regulación.....	14
Comité Basilea	15
Basilea III	16
Capital Básico	17
Liquidez.....	17
Riesgo.....	18
Riesgo Crediticio	18
Riesgo Mercado	18
Capital económico	19
Capital regulatorio	19
Riesgo Operacional	20
Fuentes de riesgo operacional.....	20
Procesos Internos	20
Personas.....	21
Tecnología de Información	21
Eventos Externos.....	21
Conceptualización de las fuentes del riesgo operacional y sus eventos.....	22
Evolución del Riesgo Operacional.....	26
Métodos de Cuantificación de Riesgo Operacional	28
10 Principios gestión del Riesgo operacional.....	32
Ciclo de Riesgo Operacional.....	34
Sistema de Administración de Riesgo Operativo	35
Matriz de riesgo	36
Elementos para componer una Matriz de Riesgo.....	37
CAPITULO II: METODOLOGÍA	38
Tipo de investigación	38
1. Establecimiento de políticas de riesgo operacional:	38
2. Diseño de la estructura Organizacional del sistema de Administración R.O.....	39
3. Categorización y Codificación de los Eventos de Riesgo Operacional.	40
4. Diseño de la Base de Datos.....	44
5. Diseño de la Matriz de Riesgo Operacional.	46
6. Diseño de Controles.....	50
7. Monitoreo.....	51

Etapa cuantitativa.....	52
CAPITULO III. DISEÑO MODELO DE GESTION DE RIESGO OPERACIONAL	55
Etapa 1: Establecimiento de políticas de riesgo operacional.....	56
Etapa 2: Estructura Organizacional de Riesgo Operacional.	59
Etapa 3: Categorización y Codificación de los Eventos de Riesgo Operacional.	65
Etapa 4: Diseño de la Base de Datos.....	69
Etapa 5: Diseño de la Matriz de Riesgo Operacional.	76
Etapa 6: Diseño de Controles.....	86
Etapa 7: Sistema de Monitoreo.	92
CAPÍTULO IV: RESULTADOS APLICACIÓN DE METODOLOGÍAS.....	98
Método Indicador Básico	98
Metodologías de Medición Avanzada.....	107
CONCLUSIONES	114
BIBLIOGRAFÍA	118

Índice de Tablas

Tabla 1: Entidades bancarias en Chile. _____	13
Tabla 2: Factores Beta _____	29
Tabla 3: de categorías y tipos de eventos de pérdidas asociados a riesgo operacional _____	41
Tabla 4: Codificación de eventos. _____	43
Tabla 5: Niveles de Severidad _____	46
Tabla 6: Niveles de Severidad _____	47
Tabla 7: Rango Cualitativo de Frecuencia _____	48
Tabla 8: límites porcentuales de frecuencia. _____	48
Tabla 9: Puntaje de riesgos y categorías. _____	49
Tabla 10: Caracterización de frecuencias para simulación de Monte Carlo. _____	54
Tabla 11: Codificación de Evento de Riesgo Operacional _____	68
Tabla 12: Ejemplo planilla de registro de evento. _____	75
Tabla 13: Niveles de impacto y características. _____	77
Tabla 14: Niveles de Patrimonio e Ingreso. _____	79
Tabla 15: Niveles de Severidad _____	79
Tabla 16: Ejemplo rangos establecidos. _____	79
Tabla 17: categorías de probabilidad. _____	80
Tabla 18: límites porcentuales. _____	81
Tabla 19: Categoría por puntaje. _____	82
Tabla 20: grado de exposición. _____	84
Tabla 21: caracterización de los niveles de exposición. _____	85
Tabla 22: Categorías de Control _____	90
Tabla 23: Periodicidad en controles. _____	91
Tabla 24: Nivel de priorización. _____	92
Tabla 25: pesos relativos de impacto. _____	94
Tabla 26: pesos relativos de frecuencia. _____	95
Tabla 27: Pesos relativos por tipo de riesgo. _____	95
Tabla 28: Seguimiento de riesgos por evento individual _____	96
Tabla 29; Integración de riesgos por línea de negocios y tipo de evento. _____	97
Tabla 30: Estimación de capital económico por riesgo operacional metodología BIA en Millones de Pesos. _____	100
Tabla 31: Parámetros de simulación. _____	107
Tabla 32: Estadística descriptiva pérdidas. _____	108
Tabla 33: Banca Minorista Ejecución y entrega de Procesos _____	110

Introducción

Bajo el contexto de la supervisión bancaria, la industria a nivel mundial ha reconocido con el tiempo la relevancia del riesgo operacional y la necesidad imperativa de generar sistemas de gestión que permitan controlar este riesgo de la mejor manera posible.

En la actualidad el creciente desarrollo de la tecnología y la utilización de la misma para la gestión integral de los procesos operativos de cualquier negocio incluyendo las instituciones financieras han cobrado una enorme relevancia. El desarrollo y utilización de herramientas tecnológicas altamente automatizadas, la consolidación del comercio electrónico como una vía de acceso mucho más rápida y cómoda hacia el cliente, han en consecuencia aumentado la necesidad de generar procesos electrónicos integrales y como resultado de esto puede emerger una alta vulnerabilidad del negocio en torno a una eventual falla operativa.

Lo mencionado anteriormente ha conducido a un incremento en la importancia que se le otorga actualmente al riesgo operacional y a la administración del mismo, especialmente en el sector bancario, el cual claramente a través de los años ha incrementado el protagonismo de los procesos tecnológicos. Sumado a esto existe la posibilidad de ocurrencia de errores humanos, eventuales fraudes tanto de origen interno como externo, por lo cual es posible afirmar que una mala gestión de las operaciones cotidianas de una entidad bancaria puede inclusive llevar a la quiebra a la misma.

En respuesta a estos cambios el comité de Basilea, ha establecido principios y metodologías para estimar de manera adecuada los cargos de capital regulatorio destinado cubrir eventuales pérdidas derivadas del riesgo operacional.

Basilea III sucesora de las normativas Basilea I y II, procura mejorar en distintos campos a las mencionadas normativas anteriores, los principales cambios del documento que pretende entregar los futuros lineamientos regulatorios, se centran en un fortalecimiento del ratio de capital, la simplificación de la normativa facilitando la implementación y por último agrega ciertos componentes de gestión macroprudenciales del riesgo.

A mediano plazo en Chile se espera un eventual cambio en la ley general de bancos, la cual genere una transición formal de Basilea I y II, hacia Basilea III. En este contexto existe la necesidad de que Chile avance hacia Basilea III, por medio de un cambio de la ley general de bancos, de la cual se espera que esta otorgue la flexibilidad necesaria para enfrentar eventuales sucesos negativos.

Entendiendo esto Basilea III ciertamente enfoca criterios en los riesgos operativos entregando medidas que se relacionan con este riesgo, en ese sentido la nueva normativa presenta los pilares fundamentales para la correcta gestión del riesgo operacional.

PLANTEAMIENTO DEL PROBLEMA.

Señalar al sistema financiero contemporáneo como un elemento clave para cualquier economía a nivel mundial, es una afirmación en la que la mayoría de los expertos estaría de acuerdo. Las entidades bancarias actualmente son las principales encargadas de los procesos de intermediación crediticia, prestando servicios esenciales a clientes, pequeñas y medianas empresas, grandes corporaciones y entidades gubernamentales, convirtiéndose de este modo en entidades que influyen de manera directa en las economías de los países y del mundo.

Evitar posibles colapsos en el sistema bancario, requiere sin lugar a dudas, un constante monitoreo de los riesgos y un análisis acabado de los mismos con el objetivo de disminuir al máximo la probabilidad de enfrentar pérdidas y que eventualmente estas conlleven a profundas crisis, como la financiera del año 2008.

La adaptación hacia un mayor grado de regulación bancaria por medio de un marco regulador global para reforzar los bancos y sistemas bancarios conocido como Basilea, pretende eliminar, disminuir o en su defecto amortiguar las crisis de alto impacto, como la anteriormente mencionada, siendo el objetivo primordial de este comité regulador el de dictar los pilares fundamentales de la gestión del riesgo para las entidades bancarias a nivel global y de este modo mitigar las repercusiones negativas que estos eventos económicos desfavorables conllevan para la sociedad.

Esta búsqueda de estabilidad financiera está estrechamente vinculada a la mitigación de los distintos riesgos que afectan al sector de la banca, en donde el análisis integral de los mismos es considerado un estándar mínimo el cual deben cumplir las entidades del sector bancario de manera global.

En este contexto se considera que las entidades bancarias chilenas deberán adecuarse eventualmente a estas nuevas condiciones de mercado. Este cambio global del modo de gestionar el riesgo, impactará en cierto grado al sector bancario nacional, generando un nuevo entorno. Un ajuste adecuado por parte de los bancos hacia las nuevas normativas comprende bajo una primera etapa el adecuado entendimiento de la nueva normativa y la adaptación de las mismas a la organización, advertir el cómo realizar esta tarea y cuál es la mejor manera de lograr este objetivo se entiende como de por sí un desafío no menor.

El mundo de la gestión de los riesgos, hasta hace muy poco consideraba como estándares el control de los riesgos de crédito y riesgos de mercado, sin embargo y luego de diferentes estudios y análisis de situaciones ligadas a pérdidas económicas que no era posible atribuir a los riesgos mencionados, nace la noción de riesgo operacional, concepto que con el tiempo ha adquirido mayor relevancia, situándose hoy en día al mismo nivel que los riesgos de crédito y de mercado.

Riesgo operacional

El riesgo operacional se entiende como el riesgo de pérdida debido a la inadecuación o a falencias en los procesos, el personal y los sistemas internos o a causa de eventos externos. Se incluye en este concepto el riesgo legal, pero no el riesgo estratégico y el de reputación. Este tipo de riesgo posee el potencial de generar millonarias pérdidas y en algunos casos llevar a la quiebra a una entidad que maneje a la perfección los riesgos de crédito, de mercado o sistémicos, pero que deje de lado el cuidado del riesgo operacional.

El presente estudio se concentrará específicamente en el análisis del riesgo operacional, que corresponde al tipo de riesgo de menor madurez en términos de gestión y cuantificación por parte del sector financiero chileno.

Bajo el contexto de la gestión del riesgo operacional el comité de Basilea entrega documentos que presentan herramientas que ayudan a la administración del mismo. La integración de este conjunto de herramientas de características cualitativas y cuantitativas contempla el desarrollo de un sistema de administración de riesgo operacional.

Analizar cuáles son las características básicas para el adecuado diseño de un sistema de administración de riesgo operacional y cómo integrar estas mismas, con el objetivo de identificar, medir, controlar y monitorear el riesgo operacional comprende uno de los pilares fundamentales de esta investigación, la que además se enfocara en analizar las metodologías de estimación de capital regulatorio para cubrir este riesgo.

De acuerdo a lo indicado por el comité de Basilea la medición de las necesidades de capital para cubrir eventuales perdidas por riesgos operacionales puede realizarse por medio de distintas metodologías de cálculo, estas técnicas están divididas en dos grandes grupos de acuerdo a su nivel de complejidad.

De este modo que para efectos del estudio se analizaran la implementación de un método básico y un método de características avanzadas para la cuantificación de cargo de capital, evaluando las posibles diferencias.

Es posible señalar que la presente investigación se enfocara principalmente en la gestión del riesgo operativo, bajo el marco regulatorio que entrega Basilea II y III, en donde además se estudiaran distintos métodos de cuantificación que el ente regulador señala como adecuados para la correcta gestión del riesgo ya mencionado.

En donde el principal problema investigativo se centra en cómo generar un marco de gestión del riesgo operacional y además en cómo es posible medir o estimar los requisitos de capital regulatorio derivados de pérdidas que corresponden a riesgos operacionales.

Objetivo Principal:

- ✓ *Establecer una metodología para la elaboración de un sistema de administración de riesgo operacional en base a las directrices entregadas por el comité de Basilea y analizar los métodos de cuantificación para cargos de riesgo operacional y sus diferencias.*

Objetivos Específicos:

- ✓ *Diseñar un modelo de gestión de riesgo operativo para la banca chilena.*
- ✓ *Cuantificar los niveles de capital requeridos por medio de distintas metodologías presentadas por el comité de Basilea.*
- ✓ *Proponer un método óptimo de estimación de cargo por riesgo operacional.*

CAPITULO I: MARCO TEORICO

Banco

Para desarrollar este concepto clave para la investigación, en primera instancia se considera adecuado una definición más bien amplia que permita eventualmente deducir de forma intuitiva que es y cómo opera una entidad bancaria, para luego caracterizar el concepto al contexto de la legislación chilena.

Así un banco puede ser considerado como un “Establecimiento público de crédito, constituido en sociedad por acciones.” (Real Academia Española, 2001). En esta definición bastante general es posible vislumbrar dos elementos centrales que ayudan a entender cuál es la función de un banco y cómo opera el mismo.

El concepto de crédito se puede definir como un préstamo en dinero que el banco otorga a un cliente, con la obligación de que en el futuro, el cliente devolverá el monto solicitado en forma gradual o en un solo pago, más un interés agregado que beneficia al banco por todo el tiempo que no tuvo ese dinero, además se entiende que bajo el concepto de sociedad por acciones, un banco puede componerse por varias personas (accionistas) que aportan para crear un patrimonio.

De este modo se entiende que la operación fundamental de un banco comprende principalmente la otorgación de capital a quien se lo solicite obteniendo ganancias del diferencial que se presenta cuando quien solicita el dinero devuelve el monto solicitado más un interés.

Una definición un poco más acabada señala que “Las instituciones bancarias se conciben como aquellas organizaciones incluidas en el sector servicios, cuyo capital puede ser de origen privado o público, con autorización para recibir dinero en forma de depósitos, para concederlo en calidad de préstamos, descuentos o anticipos y para realizar cualquier otro tipo de operación o negocio previamente calificadas por las leyes del país, como de carácter financiero y/o bancario. (Morales, 2007)

Internándose en la realidad chilena, la Superintendencia de Bancos e Instituciones Financieras, organismo encargado de regular y normar a las instituciones bancarias en Chile, señala por medio del artículo 40 de la Ley General de Bancos, que:

“Banco es toda sociedad anónima especial que, autorizada en la forma prescrita por esta ley y con sujeción a la misma, se dedique a captar o recibir en forma habitual dinero o fondos del público, con el objeto de darlos en préstamo, descontar documentos, realizar inversiones, proceder a la intermediación financiera, hacer rentar estos dineros y, en general, realizar toda otra operación que la ley le permita.” (SBIF, 2011)

Además por medio del artículo 50, se determina que "El monto del capital pagado y reservas de un banco no podrá ser inferior al equivalente a 800 mil Unidades de Fomento". (SBIF, 2011) Sin embargo, en el artículo 51, expone que de no alcanzar el capital mínimo, la institución deberá mantener un patrimonio efectivo no inferior al 12% de sus activos ponderados por riesgo, proporción que se reducirá al 10% cuando tenga un patrimonio efectivo de 600.000 Unidades de Fomento.

Por último es importante mencionar que bajo la ley chilena es posible realizar únicamente cierto tipo de actividades por parte de un banco, estas operaciones son mencionadas en el artículo 69 de la ley general de bancos y complementadas por los artículos 70 y 73.

Sistema Financiero chileno

El actual sector bancario chileno comprende una totalidad de 24 entidades, de estas la gran mayoría pertenecen a la clasificación de “Bancos establecidos en Chile”, existe además un grupo de entidades bancarias clasificadas como los “Bancos Extranjeros” estos operan a una considerable menor escala que el grupo anterior y se caracterizan por representar intereses de inversionistas del país de origen del banco con Chile. Por último existe una tercera clasificación llamada “Banco Estatal”, que corresponde al Banco del Estado de Chile.

A continuación se presenta una tabla que agrupa a las distintas entidades agrupadas según el criterio entregado por la SBIF.

Tabla 1: Entidades bancarias en Chile.

<i>Bancos establecidos en Chile</i>	<i>Bancos Extranjeros</i>	<i>Banco Estatal</i>
<ul style="list-style-type: none"> ✓ Banco de Chile ✓ Banco Internacional ✓ Scotiabank Chile ✓ Banco de Crédito e Inversiones ✓ Corpbanca ✓ Banco Bice ✓ HSBC Bank (Chile) ✓ Banco Santander-Chile ✓ Banco Security ✓ Banco Falabella ✓ Deutsche Bank ✓ Banco Ripley ✓ Rabobank Chile ✓ Banco Consorcio ✓ Banco Penta ✓ Banco Paris ✓ Banco Bilbao Vizcaya Argentaria, Chile (BBVA) ✓ Banco Itaú Chile 	<ul style="list-style-type: none"> ✓ Banco do Brasil S.A. ✓ JP Morgan Chase Bank, N. A. ✓ Banco de la Nación Argentina ✓ The Bank of Tokyo-Mitsubishi UFJ, LTD ✓ DnBNor Bank Asa 	<ul style="list-style-type: none"> ✓ Banco del Estado de Chile.

Fuente: Elaboración propia a partir de SBIF.

Regulación

Según Rodríguez (2012) existen dos tipos de regulación financiera por un lado se presenta el término "regulación microprudencial" este hace referencia al continuo monitoreo de las instituciones de crédito para restringir el apetito inadecuado por el riesgo de la entidad, con el objetivo principal de resguardar a los usuarios, representados en sus clientes quienes pueden eventualmente resultar perjudicados producto de insolvencias de las entidades financieras, debido a una mala gestión de los riesgos.

Por otro lado se menciona un segundo concepto denominado regulación macroprudencial la cual tiene como principal tarea la de resguardar por la estabilidad integral del sistema financiero y del mecanismo de pagos, mediante la vigilancia de la solvencia general del conjunto de las correspondientes instituciones y el fomento de la confianza de los agentes económicos. Se entiende de los anteriores párrafos que el enfoque microprudencial atiende al comportamiento individual de la entidad y que además el enfoque macroprudencial realiza un monitoreo del conjunto de entidades que conforman el sistema financiero formando parte de un entorno que reacciona a los eventos tanto internos como externos lo que converge en la prevención del riesgo sistémico derivado de los comportamientos colectivos.

Lo que eventualmente conlleva especial un énfasis en controlar las interconexiones y exposiciones comunes entre entidades restringiendo la posibilidad de expansión de tensiones y dificultades a lo largo de dicho sistema. Un derivado importante de la regulación macroprudencial comprende las políticas "contra-cíclicas" para los requisitos de capital u otros elementos de la gestión bancaria que no hacen más que

Demandar patrimonio adicional a las entidades que conviven con ciertos tipos de en especial a las organizaciones denominadas "demasiado grandes para caer" cuya eventual mala gestión pudiese repercutir en importantes shocks para la economía en general.

En definitiva la regulación tiene como principal tarea la de reducir la concentración de riesgos; contar con vías para ajustar el suministro de liquidez según las circunstancias; proporcionar orientaciones acerca de los esquemas de retribución de los directivos bancarios; articular sistemas de garantía de los depósitos; establecer mecanismos para la resolución de insolvencias bancarias, entre otras.

Bajo el contexto chileno el organismo regulador por excelencia en lo que compete a los bancos e instituciones financieras corresponde a la superintendencia de bancos e instituciones financieras SBIF, esta institución autónoma posee una potestad jurídica y está directamente ligada al gobierno por medio del ministerio de hacienda. Tanto los bancos como cualquier organización que posea características de entidad financiera son supervisadas por el organismo mencionado y su acción y alcance como fiscalizador queda estipulado en el artículo 12 de la Ley General de Bancos señalando que: “Corresponderá al Superintendente velar porque las instituciones fiscalizadas cumplan con las leyes, reglamentos, estatutos y otras disposiciones que las rijan y ejercer la más amplia fiscalización sobre todas sus operaciones y negocios.”

Comité Basilea

Corresponde a una entidad establecida en 1974 por los gobernadores de los bancos centrales del Grupo de los Diez (G-10) producto de graves problemas bancarios ocurridos tanto en Europa como en los Estados Unidos, este comité tiene su principal sede en la ciudad de Basilea, Suiza de allí su nombre.

El comité de Basilea tiene como principal función, la de proporcionar un permanente foro de cooperación y discusión en torno a la regulación bancaria, estableciendo distintos métodos para mejorar la calidad en general de la supervisión bancaria, a través de intercambio de información entre supervisoras de distintos países, el mejoramiento de la efectividad de las técnicas para supervisar los bancos, el establecimiento de estándares mínimos de suficiencia de capital para operar de manera segura y la evaluación de la conveniencia de establecer estándares en otras áreas de importancia.

Es importante mencionar que los estándares y las recomendaciones sobre buenas prácticas emitidos por el comité no poseen fuerza legal, sin embargo ejercen una gran influencia para que las autoridades supervisoras de cada país adecuen a sus sistemas propios a la normativa internacional, logrando de este modo converger hacia estándares y enfoques de supervisión comunes entre diferentes naciones.

Basilea III

Sucesora de Basilea II, este conjunto de normas comprende los principales cambios en términos de la regulación bancaria como respuesta de los negativos efectos producidos por la crisis financiera internacional del año 2008. El marco regulador internacional para bancos o “Basilea III” es un conjunto integral de reformas elaborado por el Comité de Supervisión Bancaria de Basilea y su principal objetivo es fortalecer la regulación, supervisión y gestión de riesgos del sector bancario.

Dentro de este marco de acción las principales metas del comité persiguen los siguientes objetivos:

- ✓ Mejorar la capacidad del sector bancario para afrontar perturbaciones ocasionadas por tensiones financieras o económicas de cualquier tipo.
- ✓ Mejorar la gestión de riesgos y el buen gobierno en los bancos.
- ✓ Reforzar la transparencia y la divulgación de información de los bancos.

Estas reformas están dirigidas a:

- ✓ La regulación de los bancos a título individual (dimensión microprudencial), para aumentar la capacidad de reacción de cada institución en periodos de tensión.
- ✓ Los riesgos sistémicos (dimensión macroprudencial) que puedan acumularse en el sector bancario en su conjunto, así como la amplificación procíclica de dichos riesgos a lo largo del tiempo.

Estas dos dimensiones son complementarias, ya que aumentando la resistencia de cada banco se reduce el riesgo de alteraciones en el conjunto del sistema.

Cabe destacar que Basilea III en ningún caso reemplaza a los marcos anteriores (Basilea I y Basilea II), sino los complementa con un conjunto integral de medidas, algunas de las cuales corresponden a nuevos conceptos y herramientas. Los principales cambios llevados a cabo por la nueva normativa comprenden primordialmente simplificar la normativa antigua para hacerla más factible de ser implementada sin problemas, el fortalecimiento del ratio de capital el cual pasara de un 8% actual a un 10,5% para el año 2019 y por ultimo agrega ciertos componentes de gestión macroprudenciales del riesgo.

Capital Básico

En contexto de la ley chilena el concepto de capital básico es definido por la Ley General de Bancos, Según (SBIF, 2009) en su circular N° 3-479 el “capital básico” corresponde al importe neto que debe mostrarse en los estados financieros consolidados como “Patrimonio atribuible a tenedores patrimoniales” según lo indicado en el Compendio De Normas Contables. Al tratarse de un banco que no prepara estados financieros consolidados, el capital básico corresponderá a la suma de las cuentas que conforman el rubro del patrimonio en el Estado de Situación Financiera.

Otra definición más amplia entregada por la entidad indica al “capital básico” se definió como la suma del capital pagado y reservas, y otras cuentas patrimoniales conforme a las instrucciones de la Superintendencia de Bancos e Instituciones Financieras.

Liquidez

Ciertamente el concepto de liquidez hace alusión a la capacidad de atender las obligaciones de corto plazo, en términos financieros una entidad no es líquida cuando sus obligaciones de corto plazo no pueden ser cubiertas por activos convertibles en efectivo. En términos muy simplistas la liquidez se relaciona con la capacidad de pago de una empresa.

Según (Cano & Suárez, 2003) la liquidez se define como la capacidad de pago a corto plazo que tiene la empresa, o bien como la capacidad de convertir los activos e inversiones en dinero o instrumentos líquidos, lo que se conoce como tesorería.

En el contexto de la banca se entiende por riesgo de liquidez esencialmente al riesgo de fondeo, este evento puede ser definido como aquel en el que un banco, no posee la capacidad de cumplir de manera eficiente con los flujos de dinero que le son exigibles.

Bajo este contexto (Lopetegui, 1996) señala que la liquidez se relaciona con la capacidad de una empresa para hacer frente a:

- ✓ Reducciones en el nivel de depósitos u otros pasivos financieros.
- ✓ Aumento de activos no líquidos (préstamos)

Riesgo

El concepto de riesgo en líneas generales se relaciona con una posible contingencia que conlleve algún grado de perjuicio o daño. Bajo el punto de vista matemático se puede definir a este como la esperanza matemática de la pérdida es decir el valor esperado de sucesos dañinos asociados a una probabilidad de ocurrencia.

Bajo este marco es posible definir el riesgo como la combinación de la probabilidad de que se produzca un evento y sus consecuencias negativas. En el sector bancario, las consecuencias negativas son principalmente pérdidas generadas por incumplimiento de pagos, errores internos, externos y exposición a un entorno desfavorable, presentándose de este modo distintos tipos distintos de riesgos, los cuales están asociados a las operaciones bancarias.

En el mundo de la banca es concepto de riesgo se refiere a la posibilidad de pérdidas causadas por variaciones de los factores que afectan el valor de un activo. Por esa razón, es importante que se identifiquen, se midan, se controlen, y se haga un monitoreo continuo de los diversos tipos de riesgo a los que están expuestas las entidades en el devenir cotidiano de sus actividades. No obstante la gran cantidad de riesgos conocidos en finanzas, desde la perspectiva básica de los acuerdos de Basilea, todo riesgo financiero puede clasificarse en una de tres categorías: riesgo de mercado, riesgo crediticio o riesgo operacional Arbeláez et al. (2006).

Riesgo Crediticio

Es el principal riesgo del negocio bancario y corresponde a la medición de la valorización de las pérdidas inesperadas debido a incumplimientos y a fallos de las contrapartes y emisores. La cuantificación de este riesgo se puede realizar por medio de diferentes metodologías, método Basilea I, método estándar, y dos calificaciones internas (IRB básico y avanzado). El riesgo de crédito es en el que generalmente se presenta un mayor interés por parte de las entidades bancarias.

Riesgo Mercado

El riesgo de mercado se define como el riesgo de pérdida derivado de los cambios en el precio de mercado en los activos (tanto los registrados en el balance como los emergentes de su exposición fuera de balance). Los riesgos sujetos a estos requerimientos son:

1) Riesgo de tasa de interés: Aplica a las posiciones de compra-venta “trading” en títulos públicos y privados y que son valuadas a valor de mercado. Estas se ven afectadas por las variaciones de precio en el corto plazo, como producto de su venta o por diferencias de cotización. También incluye a derivados financieros mantenidos como cobertura o compensación. La respectiva autoridad de supervisión puede disponer que ciertas posiciones se valúen a precio de mercado, aunque la intención del banco no sea efectuar operaciones de compra-venta en el corto plazo.

2) Riesgo de moneda o de productos básicos “commodities”: Aplica a toda las operaciones del banco, ya sea que estén valuadas a valor de mercado o a valor libro (en este último caso puede aplicarse cierta discrecionalidad por parte del supervisor en aquellas posiciones estructuralmente registradas en moneda extranjera).

Capital económico

El capital económico se define como “los métodos o prácticas que permiten a los bancos la evaluación de manera consistente de sus riesgos y la asignación de capital para cubrir los efectos económicos de las actividades que implican la asunción de riesgos” (BCBS, 2009). Esta definición se enfoca en estandarizar las metodologías de cuantificación de capital necesario, para ser capaz de absorber las pérdidas inesperadas, asociadas al concepto de probabilidad de ocurrencia de distintos sucesos que se traducen eventualmente en mermas económicas.

En este contexto es posible realizar una definición de capital económico como la cantidad de capital que los propietarios de la organización consideran necesaria para que la institución pueda seguir funcionando con normalidad, aludiendo a la capacidad de cubrir eventuales pérdidas inesperadas.

De acuerdo a (Nucamendi & Solis Rosales, 2012) es posible categorizar al capital económico como una medida de riesgo y además señalan que ante una mayor dotación de capital económico, menor será la probabilidad de la entidad de caer en posibles incumplimientos

Capital regulatorio

El capital regulatorio si bien posee similitudes importantes con respecto al capital económico diverge en relación del origen de la estimación de requerimiento de capital, pues para el caso del capital regulatorio la estimación de capital mínimo viene dada por un agente externo de a la organización.

Así se considera al capital regulatorio como el nivel de capital mínimo exigido por el regulador y por capital económico el nivel de capital que elegirían los accionistas de un banco en ausencia de regulación. (Elizalde & Repullo, 2004).

El capital regulatorio y el capital económico no dependen de las mismas variables: el regulatorio (pero no el económico) depende del nivel de confianza exigido por el regulador, mientras que el económico (pero no el regulatorio) depende del margen de intermediación y del coste del capital bancario. Además, el capital regulatorio y el capital económico no reaccionan de la misma manera ante cambios en las variables que afectan a ambos, como son la probabilidad de impago, la pérdida en caso de impago y la correlación entre los impagos de distintos acreditados.

Riesgo Operacional

El comité de Supervisión Bancaria de Basilea define al riesgo operacional como “el riesgo de pérdida debido a la inadecuación o a fallos de los procesos, el personal y los sistemas internos o bien a causa de acontecimientos externos. Se incluye en este concepto el riesgo legal, pero no el riesgo estratégico y el de reputación”. (López, 2009).

Se puede mencionar en esta categoría, riesgos relacionados con sistemas informáticos y las telecomunicaciones, que pudiesen conducir a errores o fraudes de gran magnitud.

Este tipo de riesgo puede eventualmente generar millonarias pérdidas y en algunos casos llevar a la quiebra a una entidad que maneje a la perfección los riesgos de crédito, de mercado o sistémicos, pero que deje de lado el cuidado del riesgo operacional.

Uno de los principales problemas que conlleva este tipo de riesgo es considerar su cuantificación en relación al requisito de capital necesario para cubrirlo, aun así existen también distintos métodos de cálculo, el indicador básico, el estándar y la medición avanzada.

En el presente estudio se profundizara en relación a este riesgo en particular, analizando los distintos métodos de cuantificación y proponiendo uno en particular para el sistema bancario chileno.

Fuentes de riesgo operacional

Las fuentes de riesgo operacional hacen referencia a los agentes o factores que producen la existencia del riesgo operacional, estos a su vez pueden encontrarse tanto en el interior como en el exterior de la entidad y para el caso de los bancos son una parte primordial para la realización de las actividades de intermediación financiera. Se pueden clasificar las fuentes de riesgo operacional en: procesos internos, personas, tecnología y eventos externos.

Procesos Internos

Esta fuente considera la posibilidad de pérdidas asociadas a un mal diseño de los procesos críticos de la organización como por ejemplo, el establecimiento de políticas y procedimientos inadecuados e inclusive la inexistencia de estos mismos, producto de aquello se genera un desarrollo deficiente de las operaciones y servicios o la suspensión de los mismos. De acuerdo a esta definición es posible considerar entre otros a los riesgos asociados a fallas en modelos utilizados, errores en las transacciones, evaluación inadecuada de contratos o de la complejidad de los productos, operaciones y servicios, errores de información contable, pagos o liquidaciones inadecuadas, insuficiencia de recursos para el volumen de operaciones, inadecuada documentación de las transacciones e incumplimiento de plazos y presupuestos planeados entre otros.

Personas

Hace relación a la posibilidad de la generación de pérdidas financieras provocadas por negligencia, error humano, sabotaje, fraude, robo, paralizaciones, apropiación de información sensible, lavado de dinero, inapropiadas relaciones interpersonales y ambiente laboral desfavorable, falta de especificaciones claras en los términos de contratación de personal, entre otros factores. Es posible agregar además pérdidas vinculadas con insuficiencia de personal o personal con destrezas inadecuadas, entrenamiento o capacitación inadecuada y/o prácticas débiles de contratación.

Tecnología de Información

Abarca la posibilidad de pérdidas financieras derivadas del uso de inadecuados sistemas de información y tecnologías relacionadas, que eventualmente puedan afectar el desarrollo de las operaciones y servicios que realiza la institución al atentar contra la confidencialidad, integridad, disponibilidad y oportunidad de la información.

Se incluyen en este ítem los riesgos derivados a fallas en la seguridad y continuidad operativa de los sistemas de TI, a errores en el desarrollo e implementación de dichos sistemas y su compatibilidad e integración, problemas de calidad de información, inadecuada inversión en tecnología y fallas para alinear la TI con los objetivos de negocio entre otros. También se incluyen los riesgos por falla o interrupción de los sistemas, la recuperación inadecuada de desastres y/o la continuidad de los planes de negocio.

Eventos Externos

Posibilidad de pérdidas derivadas de la ocurrencia de eventos ajenos al control de la empresa que pueden alterar el desarrollo de sus actividades, afectando a los procesos internos, personas y tecnología de información. Entre otros factores, se podrán tomar en consideración los riesgos que implican las contingencias legales, fallas en servicios públicos, la ocurrencia de desastres naturales, atentados y actos delictivos, así como la falla en servicios críticos previstos por terceros. Otros riesgos asociados con eventos externos incluyen: el rápido paso de cambio en las leyes, regulaciones o guías, así como el riesgo político o del país.

Conceptualización de las fuentes del riesgo operacional y sus eventos

Para lograr una adecuada gestión de los riesgos operacionales no basta tan solo con realizar una clasificación de sus fuentes de origen, es fundamental la conceptualización de los distintos posibles eventos de manera que se permita identificarlos adecuadamente, para medirlos y valorarlos según corresponda con el objetivo de posibilitar la mitigación de los riesgos desglosados en diferentes eventos, así se presentan las diferentes definiciones de eventos que forman parte del riesgo operativo.

Evento de riesgo operacional:

Como base se define al evento como un incidente que se presenta en un proceso y cuya consecuencia es que el resultado final del mismo difiere de lo que se había planeado. Es debido a una falta de adecuación o de un fallo de los procesos, el personal y los sistemas internos o bien por acontecimientos externos

Procesos Internos:

- ✓ Incumplimiento de las políticas y procedimientos entregados por la institución.
- ✓ Incorrecta o inoportuna captura, ejecución y registro de una transacción.
- ✓ Errores operativos importantes
- ✓ Errores en pagos en caja y depósitos sobre préstamos de clientes

Recursos humanos:

- ✓ Negocios no autorizados.
- ✓ Abusos de información privilegiada
- ✓ Fraude
- ✓ Enfermedades y lesiones de los empleados
- ✓ Demandas de los empleados
- ✓ Conflictos derivados de remuneraciones, beneficios y terminaciones de contrato
- ✓ Problemas de reclutamiento o retención de personal calificado
- ✓ Asuntos legales

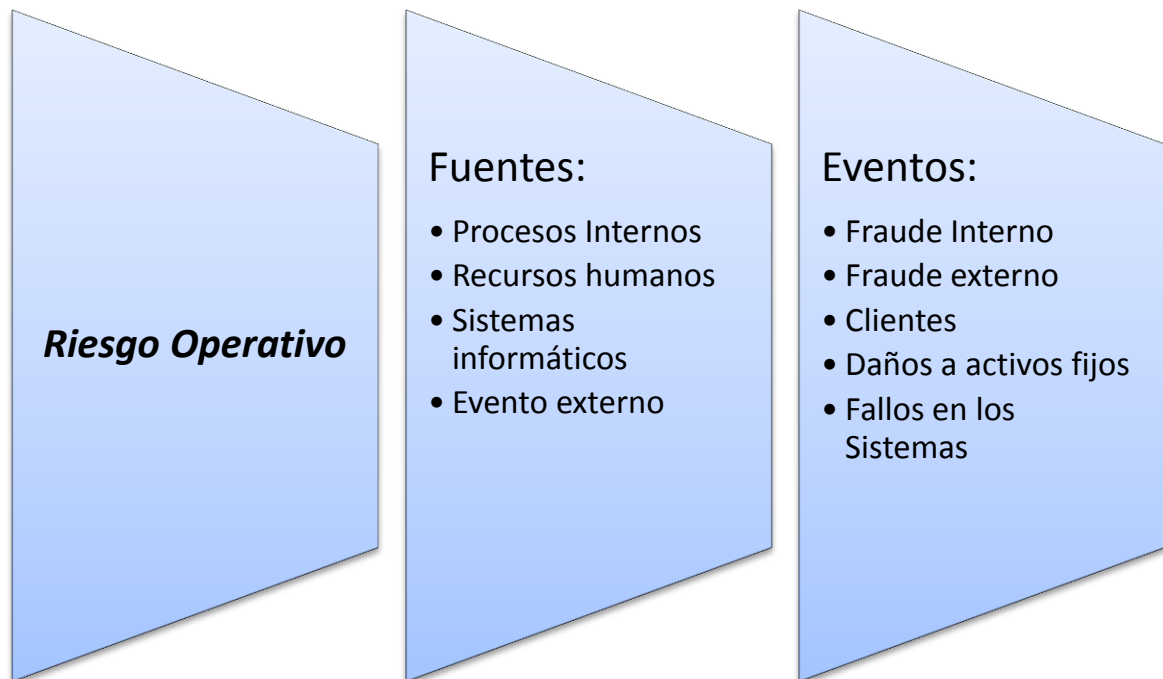
Sistemas informáticos:

- ✓ Fallas de hardware y/o software.
- ✓ Indisponibilidad de bases de datos o corrupción de las mismas
- ✓ Acceso de personal no autorizado a base de datos y sistemas
- ✓ Fallas de comunicación interna de los datos
- ✓ Interrupción o inconsecuencia de los sistemas
- ✓ Ataques de programas maliciosos en los sistemas computacionales

Evento externo:

- ✓ Fallas operacionales en proveedores de servicios de outsorsing.
- ✓ Control deficiente de pago de tributos e impuestos
- ✓ Incendios o desastres naturales
- ✓ Seguridad social y delincuencia
- ✓ Hurto robo

Figura N°1: Esquema riesgo operativo.



Fuente: Elaboración Propia.

A continuación se exponen las definiciones de los eventos “fallas” de mayor relevancia en términos de impacto y ocurrencia para una institución bancaria.

Fraude: Se define a un evento como fraude, cuando existe la intencionalidad de obtener un beneficio ilícito a través de mecanismos como el engaño, ocultación o simulación y este requisito es independiente de su origen interno o externo.

- **Fraude Interno:** acciones que de manera intencionada buscan defraudar o apropiarse de manera no debida activos de la entidad o incumplir normas o leyes en los cuales está implicado al menos, un empleado o administrador de la entidad.
- **Fraude externo:** Actos realizados por una persona externa a la entidad que busca defraudar, apropiarse indebidamente de activos de la misma o incumplir normas o leyes.

Clientes: fallas negligentes o involuntarias de las obligaciones frente a los clientes y que impiden satisfacer una obligación profesional frente a ellos.

Daños a activos fijos: pérdidas derivadas de daños o perjuicios a activos físicos de la entidad a causa de terrorismo, vandalismo, terremotos, incendios, inundaciones y desastres naturales en general.

Fallas tecnológicas: pérdidas procedidas de incidentes por fallas relacionadas con la tecnología ya sea esta de software hardware o telecomunicaciones.

Ejecución y administración de procesos: Pérdidas derivadas de la inadecuada ejecución y administración de los procesos.

Recurso Humano: corresponde al conjunto de personas vinculadas directa o indirectamente con la ejecución de los procesos de la entidad.

Vinculación directa corresponde a aquella basada en un contrato de trabajo en los términos de la legislación vigente, ya sea este celebrado por la misma entidad o un tercero.

Vinculación indirecta: se presenta cuando existen personas que tienen una relación jurídica de prestación de servicio con la entidad diferente a la que se origina con un contrato de trabajo.

Relaciones Laborales: se refiere a pérdidas ocasionadas sobre la gestión de recursos humanos comprendiendo todo su ciclo desde la fase de reclutamiento y selección hasta la salida del personal, traduciéndose estos como actos que son incompatibles con la legislación laboral, con los acuerdos internos de trabajo y en general la legislación vigente.

Diversidad y discriminación: hace relación a pérdidas derivadas de actos discriminatorios que generan pérdidas producto de demandas, juicios o instancias donde la empresa pueda llegar a reflejar pérdidas a consecuencia de acciones discriminatorias.

Seguridad en el puesto de trabajo: pérdidas emanadas de multas e indemnizaciones debido a incumplimientos en la normativa de seguridad laboral vigente y de las condiciones de seguridad e higiene en los lugares de trabajo.

Fallos en los Sistemas: inadecuado funcionamiento de cualquier sistema que afecte el correcto funcionamiento de los procesos internos. También se pueden considerar eventos derivados de interrupciones de servicios básicos, luz, agua, teléfono, etc.

Recepción, ejecución y mantenimiento de operaciones: conformados por pérdidas debido a errores en la introducción y mantenimiento de datos, así como la ejecución deficiente en los procesos de control, problemas en los procesos de presentación y resguardo de documentos.

Seguimiento y comunicación de informes: hace referencia a las pérdidas debido a errores involuntarios en el suministro de información obligatoria que se remita a clientes, inversores y órganos reguladores.

Gestión de cuentas de clientes: se refiere a pérdidas provocadas por la errónea ejecución o negligente tratamiento de instrucciones de clientes, estos errores pueden estar vinculados a procesos masivos o unitarios.

Contrapartes comerciales: Vinculado a eventos originados por incumplimiento involuntario de obligaciones contractuales con otras contrapartidas, agregando además a pérdidas ocasionadas por acuerdos directos entre partes o bajo la intervención de un tercero como mediador.

Evolución del Riesgo Operacional

Para el año 1989, el comité de supervisión bancaria de Basilea comenzó a notar cierta relación en torno a posibles riesgos derivados de sistemas informáticos y telecomunicaciones que para esa fecha evolucionaban de manera vertiginosa, además de riesgos vinculados a la falta de ética de algunos ejecutivos de las organizaciones. Estos elementos poseían un potencial de generar cuantiosas pérdidas e incluso llevar a la quiebra a las entidades que para ese tiempo no tenían las herramientas necesarias para mitigar dicho riesgo.

Ya para la década de los noventa se registraron numerosos casos, dentro de los más relevantes es posible nombrar al emblemático banco Daiwa del Japón que registro perdidas por USD \$ 1.1 billones, debido a un inescrupuloso ejecutivo quien logro esconder pérdida durante 11 años y como consecuencia produjo la quiebra de la entidad bancaria japonesa (Vizuite, s.f.)

Burneo et al. (2013) presenta emblemáticos casos que han tenido un alto impacto económico y además poseen una directa relación con el riesgo operativo, de los cuales se hace mención a los siguientes.

- ✓ WORLD TRADE CENTER: Daños a los activos físicos y la interrupción de las operaciones del negocio por los ataques del 11/09 significaron \$27 mil millones en pérdidas.
- ✓ ALLIED IRISH BANKS: Fraude interno y comportamiento criminal en negociaciones deshonestas ocasionaron pérdidas por \$690 millones.
- ✓ SUMIMOTO CORPORATION: Pérdidas totales de \$2,600 millones ocasionadas por negociaciones no autorizadas en 1996.
- ✓ ORANGE COUNTY: Negociaciones no autorizadas ocasionaron una pérdida de \$1,700 millones y su subsecuente quiebra en 1998.
- ✓ BARINGS BANK: La falta de supervisión permitió a Nick Lesson incurrir en pérdidas por \$1,200 millones que ocasionaron el colapso del Banco.
- ✓ DAIWA BANK: Pérdidas operativas de alrededor de \$1,000 millones.
- ✓ OTROS: Enron, World Com, Parmalat.

De esta manera quedó de manifiesto que no bastaba con únicamente gestionar de manera perfecta los riesgos de crédito y de mercado ya que existían otras variables y elementos para ese entonces no caracterizados que en algunos casos podían convertirse en la razón principal de una eventual quiebra de la organización.

Bajo este contexto el comité de supervisión bancaria de Basilea decide publicar en el año 1998 el primer documento que se ocupa específicamente del riesgo operacional (BCBS, 1998). En este documento se menciona que los riesgos operacionales más relevantes son consecuencia de deficiencias en los sistemas de control interno de las organizaciones derivados de la carencia de gobiernos corporativos eficientes que establecieran políticas de control adecuadas, con el fin de evitar cualquier tipo de pérdida por error, fraude o fallas en el desempeño tanto de los sistemas automatizados como también de los ejecutivos y personal humano de las instituciones.

Luego de identificar los principales factores que originan las pérdidas de este tipo de riesgo, surgió el problema de establecer los requerimientos de capital necesarios para cubrir este nuevo riesgo, destacando como mayor inconveniente la cuantificación del riesgo.

Según (Nucamendi & Solis Rosales, 2012) el primer intento del comité de supervisión bancaria de Basilea por cuantificar el requisito necesario para cubrir este riesgo se establece en el año 2001, en donde se estima que es necesario destinar el 20% del capital económico de un banco para cubrir las posibles pérdidas por riesgo operacional. En ese mismo año el BCBS publica un nuevo documento consultivo en donde se formaliza la definición del riesgo operacional la cual no incluye al riesgo sistémico, además en esta publicación se entregan las principales metodologías de cuantificación de cargos de capital para el riesgo operativo: los métodos indicador básico, estándar y avanzado .

El año siguiente, el comité de Basilea entregó un estudio en donde presenta una recopilación de datos sobre pérdidas derivadas de sistemas operacionales denominado “Loss Data Collection Exercise For Operational Risk”. La publicación comprendía la participación de 89 entidades financieras, en donde los resultados arrojaron un promedio de valor asignado por cobertura de este riesgo del 15% con valores extremos del 1 a 40%, como conclusión se determinó el valor objetivo correspondiente al 12%. A partir del año 2004 a través de Basilea II el capital requerido para la cobertura por riesgo operacional puede calcularse por los tres distintos métodos mencionados: el indicador básico, el estándar y el sistema de medición avanzada. (BCBS, 2004)

Es importante a su vez mencionar que la evolución del riesgo operacional se ha generado de la mano del crecimiento y propagación de los servicios de banca electrónica, el concepto de banca electrónica se puede definir de manera simple y general como “el conjunto de productos y procesos que permiten, mediante procedimientos informáticos, que el cliente pueda realizar una serie, cada vez más amplia, de transacciones bancarias sin necesidad de ir a la sucursal” (Tamames, Gallego, 1994).

En la actualidad es posible realizar dicha actividad con una variedad de dispositivos de acceso como computadoras, teléfonos móviles, tabletas electrónicas entre otros.

Particularmente para el caso chileno el sistema de banca en línea es altamente utilizado siendo el país de la región de América Latina en que los usuarios más utilizan los servicios online ofrecidos por los bancos, con un 34,8%, seguido de Brasil con un 30% y Argentina con un 24%. Este porcentaje aumenta considerablemente cuando se suma el uso de sitios financieros a los servicios utilizados, alcanzando un 46% en el caso de

Chile, esto según un estudio realizado a finales del año 2012 por la empresa Havas Digital, especializada en marketing digital. (Havas Digital, 2012)

Es incuestionable que la gestión del riesgo operacional con el tiempo ha alcanzado una importancia al nivel de los riesgos de mercado y crédito, la correcta gestión de este se ha hecho una necesidad para el sector industrial de la banca y la generación de sistemas de control de gestión en este ámbito son de gran relevancia hoy en día para la adecuada gestión de riesgos.

Métodos de Cuantificación de Riesgo Operacional

Como se menciona anteriormente existen diferentes metodologías que se pueden llevar a cabo con el fin de estimar los requerimientos para cubrir posibles pérdidas derivadas del riesgo operativo. A continuación se presentan las metodologías de cálculo de cada una de ellas. (BCBS, 2006)

A) Método del indicador básico

Los bancos deben cubrir el riesgo operativo con un capital equivalente a la media de los tres últimos años de un porcentaje fijo (α) de sus ingresos brutos anuales positivos.

$$KBIA = [\sum (GL\ 1\dots n * \alpha)] / n$$

KBIA = La exigencia de capital en el método estándar.

GL = Ingresos brutos anuales medios, cuando sean positivos, de los tres últimos años.

n = Número de años (últimos tres años), en que los resultados fueron positivos.

$\alpha=15\%$, parámetro establecido por el Comité, que relaciona el capital exigido al conjunto del sector con el nivel del indicador en el conjunto del sector.

B) Método estándar

Las actividades de los bancos se dividen en ocho líneas de negocio: finanzas corporativas, negociación y ventas, banca minorista, banca comercial, pagos y liquidación, servicios de agencia, administración de activos e intermediación minorista.

$$KTSA = \{(\sum \text{años } 1-3 \max[\sum (GI1-8 * \beta\ 1-8, 0)]\} / 3$$

KTSA=Exigencia de capital en el método estándar

GI1-8= Los ingresos brutos anuales de un año dado. Como se define el método del indicador básico, para cada una de las ocho líneas de negocio.

$\beta 1-8=$ Un porcentaje fijo, establecido por el Comité, que relaciona la cantidad de capital requerido con el ingreso bruto de cada una de las ocho líneas de negocio. 18

Los valores de los factores beta son los siguientes:

Tabla 2: Factores Beta

LINEA DE NEGOCIO	FACTORES BETA
<i>Finanzas corporativas</i>	18%
<i>Negociación y ventas</i>	18%
<i>Banca minorista</i>	12%
<i>Banca comercial</i>	15%
<i>Pagos y liquidación</i>	18%
<i>Servicios de agencia</i>	15%
<i>Administración de activos</i>	12%
<i>Intermediación minorista</i>	12%

Fuente: Elaboración propia a partir de Comité de supervisión bancaria

C) Los métodos de medición avanzada (AMA)

El requerimiento de capital regulador será igual a la medida de riesgo generada por el sistema interno del banco para el cálculo del riesgo operativo utilizando los criterios cuantitativos y cualitativos aplicables a los AMA.

Criterios cualitativos:

Contar con una unidad de gestión del riesgo operativo, encargada del diseño y aplicación del marco de gestión operativo del banco. El sistema de medición interna del riesgo operativo con que cuente la entidad deberá estar perfectamente integrado con los procesos habituales de gestión de riesgo del banco. Debe informarse en forma periódica a la dirección de las unidades de negocio, a la alta dirección, respecto de las exposiciones al riesgo operativo y del historial de pérdidas debidas a este riesgo. El sistema de gestión de riesgo operativo deberá estar bien documentado. Los auditores externos y/o internos deberán llevar a cabo exámenes periódicos de los procesos de gestión y sistemas de medición de este riesgo.

Criterios cuantitativos:

Considerando la continua evolución de los métodos analíticos para el tratamiento del riesgo operativo, el Comité no especifica un método para determinar cuantitativamente el nivel de capital requerido por riesgo operativo, usando AMA: No obstante lo anterior establece claras directrices al respecto (Sección 669 y anexo 7,). El banco debe ser capaz de demostrar que el método AMA que aplica, identifica adecuadamente eventos situados en las “colas” de la distribución de probabilidad, generadores de pérdidas graves.

De acuerdo a (López, 2009) bajo la cuantificación AMA no existen recomendaciones explícitas sobre metodologías particulares para la estimación de las pérdidas esperadas e inesperadas, lo cual se debe en gran parte a:

1. La idiosincrasia propia de cada institución y, por ende, a la mejor adecuación de ciertas técnicas, inclusive de desarrollo propio, por sobre otras.
2. La continua, incipiente y amplia investigación y desarrollo académico práctico sobre métodos avanzados de cuantificación del riesgo operacional.

Los métodos de medición avanzada exhibidos por el comité de Basilea son los siguientes:

- ✓ *Método de distribución de pérdidas (LDA).*
- ✓ *Método de cuadros de mando (MCM)*
- ✓ *Método de medición interna (IMA)*

De estos enfoques el que actualmente ha adquirido un mayor posicionamiento en la práctica corresponde al modelo loss distribution approach (LDA) representando un estándar en términos de estimaciones estadísticas de riesgo, según Jiménez et al. (2008). Esta técnica ostenta las características necesarias para cumplir de manera adecuada el objetivo de generar estimaciones efectivas de cálculo de capital económico para cubrir las eventuales pérdidas derivadas de la operación de una entidad financiera.

Dicho modelo se sustenta en una base de datos interna de pérdidas históricas, generadas por eventos de riesgo operacional, en donde las dos variables fundamentales a estudiar son la frecuencia y la severidad de dichas pérdidas. Según (Mora, 2010) estos datos históricos de eventos pueden originarse de diferentes fuentes

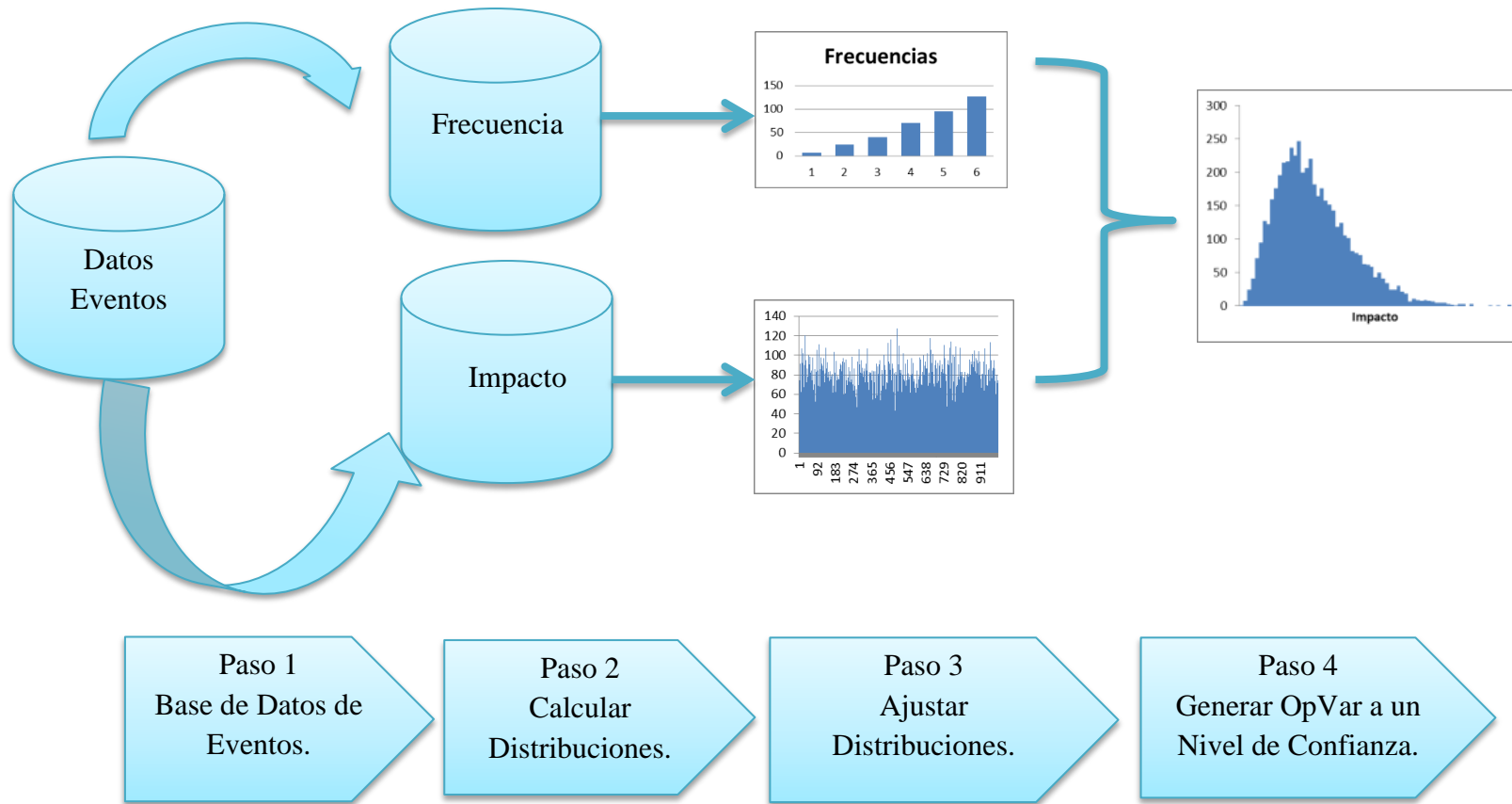
- ✓ *Datos internos*
- ✓ *Datos Externos*
- ✓ *Análisis de escenarios*
- ✓ *Entorno del negocio y factores de control interno.*

El objetivo principal del modelo LDA considera el estimar el nivel de riesgo operacional para una entidad, basándose en una particular distribución de pérdida la cual recopila datos de frecuencia y severidad a través de un sistema de registro interno, pudiendo ser esta información complementada con datos externos.

Estas pérdidas son clasificadas en una matriz según el tipo de evento y las líneas de negocio de la entidad (Jiménez, 2010), que en una primera instancia corresponden a las ocho líneas de negocios propuestas por Basilea, sin embargo la matriz puede ser adaptada a las necesidades de la entidad en el caso de que fuese necesario.

El modelo LDA se conforma por medio de la convolución, proceso que comprende la generación de una tercera función como producto de la combinación de dos funciones distintas. En el caso la función resultante es la de distribución de riesgo operacional, la misma se origina entre un proceso estocástico discreto asociado a la frecuencia y un proceso continuo asociado a la severidad o impacto de los eventos de riesgo. (Franco & Murillo, 2008)

Figura Nº 2: Esquema modelo LDA.



Fuente: Elaboración propia a partir de (Franco & Murillo, 2008).

10 Principios gestión del Riesgo operacional

El comité de supervisión bancaria de Basilea, con el afán de establecer las directrices en torno a la gestión del riesgo operacional, recoge en su documento “Buenas prácticas para la gestión y supervisión del riesgo operativo” (2003) una serie de principios para una gestión y supervisión eficaces del riesgo operativo para que estas sean utilizadas por los bancos y autoridades supervisoras al evaluar políticas y prácticas destinadas a gestionar este tipo de riesgos.

✓ *Desarrollo de un marco adecuado para la gestión del riesgo.*

Principio 1: el consejo de administración deberá conocer cuáles son los principales aspectos de los riesgos operativos para el banco, en tanto que categoría de riesgo diferenciada, y deberá aprobar y revisar periódicamente el marco que utiliza el banco para la gestión de este riesgo. Este marco deberá ofrecer una definición de riesgo operativo válida para toda la empresa y establecer los principios para definir, evaluar, seguir y controlar o mitigar este tipo de riesgos.

Principio 2: El consejo de administración deberá asegurar que el marco para la gestión del riesgo operativo en el banco esté sujeto a un proceso de auditoría interna eficaz e integral por parte de personal independiente, capacitado y competente. La función de auditoría interna no deberá ser directamente responsable de la gestión del riesgo operativo.

Principio 3: La alta gerencia deberá ser la responsable de poner en práctica el marco para la gestión del riesgo operativo aprobado por el consejo de administración. Dicho marco deberá ser aplicado de forma consistente en toda la organización bancaria y todas las categorías laborales deberán comprender sus responsabilidades al respecto. La alta gerencia también deberá ser responsable del desarrollo de políticas, procesos y procedimientos destinados a la gestión de estos riesgos para todos los productos, actividades, procesos y sistemas relevantes para el banco.

✓ *Gestión del riesgo: identificación, evaluación, seguimiento y cobertura/control.*

Principio 4: los bancos deberán identificar y evaluar el riesgo operativo inherente a todos sus productos, actividades, procesos y sistemas relevantes. Además, también deberán comprobar que antes de lanzar o presentar nuevos productos, actividades, procesos o sistemas, se evalúa adecuadamente su riesgo operativo inherente.

Principio 5: Los bancos deberán vigilar periódicamente los perfiles de riesgo operativo y las exposiciones sustanciales a pérdidas. La alta gerencia y el consejo de administración deberán recibir información pertinente de forma periódica que complemente la gestión activa del riesgo operativo.

Principio 6: Los bancos deberán contar con políticas, procesos y procedimientos para controlar y cubrir los riesgos operativos más relevantes. Además, deberán reexaminar periódicamente sus estrategias de control y reducción de riesgos y ajustar su perfil de riesgo operativo según corresponda, utilizando para ello las estrategias que mejor se adapten a su apetito por el riesgo y a su perfil de riesgo.

Principio 7: Los bancos deberán contar con planes de contingencia y de continuidad de la actividad, que aseguren su capacidad operativa continua y que reduzcan las pérdidas en caso de interrupción grave de la actividad.

✓ *La función de los supervisores.*

Principio 8: Los supervisores bancarios deberán exigir a todos los bancos, sea cual sea su tamaño, que mantengan un marco eficaz para identificar, evaluar, seguir y controlar o mitigar sus riesgos operativos más relevantes, como parte de su aproximación general a la gestión de riesgos.

Principio 9: Los supervisores deberán realizar, directa o indirectamente, una evaluación periódica independiente de las políticas, prácticas y procedimientos con los que cuentan los bancos para gestionar sus riesgos operativos. Además, deberán cerciorarse de que se han puesto en marcha los mecanismos necesarios para estar al tanto de cualquier novedad que se produzca en un banco.

✓ *La función de la divulgación de información.*

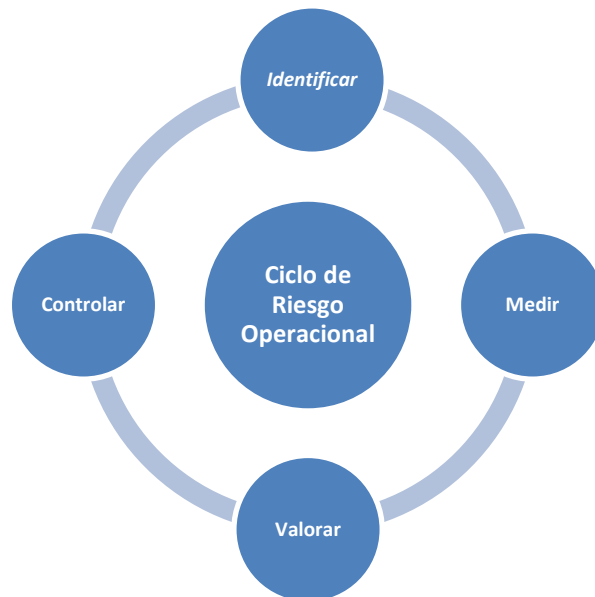
Principio 10: Los bancos deberán proporcionar información pública suficiente para que los partícipes del mercado puedan evaluar sus estrategias de gestión del riesgo operativo.

Ciclo de Riesgo Operacional

De acuerdo con García (2011) el ciclo de riesgo operativo considera cuatro etapas fundamentales.

- ✓ **Identificar:** averiguar e inventariar los riesgos operacionales a los que está expuesta la entidad a través de sus procesos
- ✓ **Medir:** utilizar una métrica cualitativa y/o cuantitativa para dimensionar cada riesgo identificado
- ✓ **Valorar** es establecer un juicio absoluto o relativo sobre la magnitud de cada riesgo
- ✓ **Controlar:** es poner en marcha medidas de mitigación y de seguimiento con el objetivo disminuir o anular la exposición al riesgo.

Figura N° 3: Ciclo de riesgo operacional.



Fuente: Elaboración propia a partir de (García, 2011)

Sistema de Administración de Riesgo Operativo

Conforme la gestión del riesgo operativo evolucionaba paralelamente se comenzaron a crear diferentes herramientas de gestión para la adecuada administración de este riesgo. Uno de los objetivos principales de la presente tesis es proponer un modelo adecuado a la realidad chilena que se encargue de gestionar de manera correcta los riesgos operacionales en el sistema bancario nacional.

Dicho esto se presenta como una excelente herramienta de gestión del riesgo operativo al modelo S.A.R.O. (sistema de administración del riesgo operacional) que es definido según (Giraldo, 2007) como el “conjunto de elementos tales como políticas, procedimientos, documentación, estructura organizacional, registro de eventos de riesgo operativo, órganos de control, plataforma tecnológica, divulgación de información y capacitación, mediante los cuales las entidades vigiladas identifican, miden, controlan y monitorean el riesgo operativo”.

(Bernal & Roncancio, 2009) señala que dicho sistema permite identificar, medir, controlar y monitorear eficazmente el riesgo operativo. Señalando además que previo a la implementación de este sistema es necesario que la entidad establezca políticas, objetivos, procedimientos y estructura para la administración del riesgo operativo en donde es esencial el adecuado alineamiento con los planes estratégicos de la institución.

Los requisitos mínimos para la confección de un adecuado sistema de administración de riesgo operativo comprenden elementos mínimos como

- ✓ Políticas
- ✓ Documentación
- ✓ Estructura organizacional
- ✓ Sistema de registro de eventos
- ✓ Organismos de control

Cada uno de estos elementos busca obtener una efectiva administración del riesgo operativo.

Matriz de riesgo

Para gestionar de buena manera el riesgo de una institución bancaria, es necesario recurrir al ciclo de administración del riesgo, para efectos de esta investigación se centrara en el ciclo del riesgo operativo. Por lo cual se hace imperativo realizar acciones de identificación, cuantificación, así como también actividades de control con el objetivo de mitigar o eliminar los riesgos.

Un instrumento que genera información relevante para el conocimiento de los riesgos corresponde a la matriz de riesgo, esta permite identificar el riesgo operativo, con los niveles de riesgo, en términos de su probabilidad de ocurrencia y además del posible impacto que produzca.

La matriz de riesgo es una herramienta de control y gestión utilizada para identificar los procesos más críticos de la organización, es decir las actividades relacionadas entre sí y agrupadas en virtud de la consecución de un objetivo común, el tipo y nivel de riesgo inherentes a estas actividades y los factores internos y externos que producen los riesgos. En general la matriz permite obtener señales y advertencias concluyentes sobre los controles existentes y su efectividad real respecto a los resultados esperados que una organización tiene (Idrobo, 2012).

Figura N° 4: Ejemplo Matriz de Riesgo

P R O B A P I L I D A D	5					
	4					
	3					
	2					
	1					
			1	2	3	4
IMPACTO						

Riesgos que necesitan monitorización.	
Riesgos que necesitan investigación.	
Riesgos que necesitan mitigación.	

Fuente: Elaboración Propia

Elementos para componer una Matriz de Riesgo.

Frecuencia: Es la probabilidad de que el riesgo se materialice, suponiendo que no estén establecidos los controles o la mitigación.

Severidad o Impacto: Es la consecuencia potencial del suceso, es decir en caso de materializarse el riesgo, cuál es la consecuencia en términos económicos, o bien, cuál es el efecto directo o indirecto sobre los accionistas o acciones de una organización.

Exposición al riesgo: Se define como el nivel de impacto del riesgo a la institución, considerando que ésta mantiene cierta posición y, por lo tanto, es vulnerable a lo que pueda suceder.

Estimación del riesgo: Para estimar el riesgo se debe definir a priori cuál es la frecuencia de que se materialice el riesgo, así como cuál es el impacto (severidad) que provoca sobre las actividades diarias del negocio a analizar.

Riesgo: Para efectos de la confección de la matriz el riesgo se considerara de la siguiente manera.

$$\text{Riesgo} = \text{Frecuencia} \times \text{Severidad}$$

CAPITULO II: METODOLOGÍA

Tipo de investigación

La investigación que se desarrolló supuso la implementación de técnicas tanto de carácter cualitativo como cuantitativo, el estudio cualitativo comprendió el diseño de un sistema de administración de riesgo operacional el cual tuvo como objetivo la esquematización de un sistema general que permitiera identificar, medir, controlar y monitorear eficazmente el riesgo operativo bajo las directrices de control dictadas por la normativa del comité de Basilea.

ETAPA CUALITATIVA.

Para el adecuado diseño del modelo fue necesaria la implementación de diferentes etapas que una vez constituidas conformarían el sistema integral de administración de riesgo operacional.

Las etapas más relevantes se explican a continuación:

1. Establecimiento de políticas de riesgo operacional:

Esta primera fase para el desarrollo del modelo, contempló la creación de políticas que se instauraron con el objetivo de enmarcar una estructura de administración adecuada y que confiera los lineamientos generales de la organización, en torno al riesgo operacional.

De este modo, se confeccionó un documento que entrega las principales directrices de comportamiento y de dirección relativas al riesgo operacional, así se fundaron los cimientos del sistema de administración de riesgo operacional, destacando que estos se basaron principalmente en documentos oficiales entregados por el comité de supervisión bancaria de Basilea en específico en base a la publicación del Banco de Pagos Internacionales “Buenas prácticas para la gestión y supervisión del riesgo operativo” (BCBS, 2003).

2. Diseño de la estructura Organizacional del sistema de Administración R.O.

El segundo paso para la creación del modelo requirió del diseño de estructura organizacional en el cual el sistema de administración de riesgo operacional descansara.

Es importante mencionar que para esta etapa el comité no exige requerimientos explícitos para su conformación aludiendo a su ordenación o forma, sin embargo el objetivo de la creación de una estructura organizativa de riesgo operativo debe centrarse en el cumplimiento de los requisitos tanto cualitativos como cuantitativos, que la entidad reguladora considera fundamentales.

La estructura organizacional obtenida para el modelo se desarrolló principalmente bajo la premisa de las necesidades básicas para una gerencia de riesgos operacionales, según Basilea y su documento “Buenas prácticas para la gestión y supervisión del riesgo operativo” (BCBS, 2003) y el documento “Convergencia internacional de medidas y normas de capital”.

Para la realización del organigrama, se utilizó la técnica de elaboración orientada hacia un tipo de estructura funcional, la presentación del mismo se realizó siguiendo metodologías de tipo verticales ramificadas de arriba hacia abajo, mostrando de este modo los distintos niveles jerárquicos de la estructura organizacional.

La estructura en sí, se expresó a través de rectángulos, respetando las técnicas actuales de confección de estructuras organizacionales, cada puesto o cargo fue unido por líneas que representan la comunicación de responsabilidad y autoridad a los puestos dependientes o subordinadas.

Así se creó una estructura estándar, entendiendo que esta misma debiese variar dependiendo de las necesidades de la institución y su nivel de complejidad en este ámbito.

Una vez analizados estos siete puntos fundamentales se procedió a establecer un organigrama que cumpliera con dichas necesidades y además se establecieron los roles, responsabilidades y desempeños esperados, basados en los siete puntos anteriormente mencionados.

3. Categorización y Codificación de los Eventos de Riesgo Operacional.

La tercera etapa de la elaboración del sistema de administración de riesgo operacional, comprendió la estimación de cuáles son los eventos que forman parte de este riesgo. Como se mencionó en el capítulo anterior, los eventos de riesgo operacional son categorizados según los criterios entregados por Basilea, estos criterios agrupan a los eventos que generan pérdidas atribuibles a la exposición de la entidad financiera a los riesgos operacionales.

El primer paso de esta fase por consecuencia comprendió la identificación de los eventos que son aceptados por la normativa internacional de Basilea como eventos de riesgo operacional, para aquello se analizó el documento presentado por el ente regulador “*Convergencias internacionales de medidas y normas de capital*” (BCBS, 2006) en donde en su Anexo 9 exhibe detalladamente los riesgos operativos de acuerdo a sus categorías y niveles.

Luego de esto y tomando en consideración posibles necesidades de adaptación en este ámbito por parte de la entidad reguladora chilena, se realizó un estudio de los tipos de eventos que la superintendencia de bancos e instituciones financieras admite como provenientes de riesgos operacionales, examinando el documento publicado por la entidad “*Riesgo operacional: conceptos y mediciones*” (pacheco, 2009) el cual expone los eventos de riesgo operativo, concluyendo que estos mismos no difieren de los presentados por la normativa internacional.

De este modo el proceso de identificación de los eventos de riesgo operacional se establecieron en base a la tabla de categorías y tipos de eventos de pérdidas asociados a riesgo operacional que la entidad reguladora expone en base a los requerimientos de Basilea II y III y los cuales no difieren de los considerados por la entidad reguladora nacional.

A continuación se exhibe el documento entregado por la SBIF categorizando los eventos en tres niveles.

Tabla 3: de categorías y tipos de eventos de pérdidas asociados a riesgo operacional

Categoría de Tipo de Eventos (nivel 1)	Definición	Categoría (nivel 2)	Ejemplos de actividades (Nivel 3)
Fraude interno	Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o soslayar regulaciones, leyes o políticas empresariales (excluidos los eventos de diversidad / discriminación) en las que se encuentra implicada, al menos, una parte interna a la empresa	Actividades no autorizadas	i) Operaciones no reveladas intencionalmente; ii) Operaciones no autorizadas con pérdidas monetarias; y iii) Valoración errónea intencional de posiciones
		Hurto y fraude	i) Fraude / fraude crediticio/ depósitos sin valor Hurto / extorsión / malversación / robo; ii) Apropiación indebida de activos; iii) Destrucción dolosa de activos; iv) Falsificación; v) Utilización de cheques sin fondos; vi) Contrabando; vii) Apropiación de cuentas, de identidad, etc.; viii) Incumplimiento / evasión intencional de impuestos; ix) Soborno / cohecho; y x) Abuso de información privilegiada
Fraude externo	Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o soslayar la legislación, por parte un tercero	Hurto y fraude	i) Hurto/ robo; ii) Falsificación; y iii) Utilización de cheques sin fondos
		Seguridad de los sistemas	i) Daños por ataques informáticos; y ii) Robo de información con pérdidas monetarias
Relaciones laborales y seguridad en el puesto de trabajo	Pérdidas derivadas de actuaciones incompatibles con la legislación o acuerdos laborales, sobre higiene o seguridad en el trabajo, sobre el pago de reclamaciones por daños personales, o sobre casos relacionados con la discriminación	Relaciones laborales	i) Cuestiones relativas a remuneración, prestaciones sociales, extinción de contratos; y ii) Organización laboral
		Higiene y seguridad en el trabajo	i) Imposibilidad en general (resbalones, caídas, etc.); ii) Casos relacionados con las normas de higiene y seguridad en el trabajo; y iii) Indemnización a los trabajadores
		Diversidad y discriminación	Todo tipo de discriminación
Incidencias en el negocio y fallos en los sistemas	Pérdidas derivadas de interrupción en los negocios o por fallas en los sistemas	Sistemas	i) Hardware; ii) Software; iii) Telecomunicaciones; y iv) Interrupción / incidencias en el suministro
Daños a activos materiales	Pérdidas derivadas por daños o perjuicios a activos materiales como consecuencia de desastres naturales u otros eventos	Desastres y otros acontecimientos	i) Pérdidas por desastres naturales; ii) Pérdidas humanas por causas externas (terrorismo, vandalismo)

Fuente: SBIF

Tabla N° 3: de categorías y tipos de eventos de pérdidas asociados a riesgo operacional continuación.

Categoría de Tipo de Eventos (nivel 1)	Definición	Categoría (nivel 2)	Actividades (Nivel 3)
Cientes, productos y prácticas empresariales	Pérdidas derivadas del incumplimiento involuntario o negligente de una obligación profesional frente a clientes concretos (incluidos requisitos fiduciarios y de adecuación), o de la naturaleza o diseño de un producto	Adecuación, divulgación de información y confianza	i) Abusos de confianza / incumplimiento de pautas; ii) Apropiamiento / divulgación de información; iii) Violación de la privacidad de clientes minoristas; iii) Quebrantamiento de privacidad; iv) Ventas agresivas; v) Pérdidas de cuentas; vi) Mal uso de información confidencial; y vii) Responsabilidad del prestamista
		Prácticas empresariales o de mercado impropias	i) Prácticas anti-competencia; ii) Prácticas impropias comerciales y de mercado; iii) Manipulación del mercado; iv) Comercialización de información privilegiada a favor de la empresa; v) Actividades no autorizadas; y vi) Lavado de dinero
		Productos defectuosos	i) Defectos del producto; y ii) Error de modelo
		Selección, patrocinio y riesgos	i) Fallida investigación a clientes según los protocolos; y ii) Superación de los límites de exposición frente a clientes
		Actividades de asesoramiento	Litigios sobre resultados de las actividades de asesoramiento
Ejecución, entrega y gestión de procesos	Pérdidas derivadas de errores en el procesamiento de operaciones o en la gestión de procesos, así como de relaciones con contrapartes comerciales y proveedores	Recepción, ejecución y mantenimiento de operaciones	i) Comunicación defectuosa; ii) Errores de introducción de datos, mantenimiento o descarga; iii) Incumplimiento de plazos o de responsabilidades; iv) Ejecución errónea de modelos / sistemas; v) Error contable / atribución a entidades erróneas; vi) Errores en otras tareas; vii) Fallo en la entrega; viii) Fallo en la gestión del colateral; y ix) Mantenimiento de datos de referencia
		Seguimiento y Monitoreo	i) Incumplimiento en la obligación reportar; y ii) Inexactitud de informes externos (incurriendo en pérdidas)
		Aceptación de clientes y documentación	i) Extravío de autorizaciones / rechazos de clientes; y ii) Documentos jurídicos inexistentes / incompletos
		Gestión de cuentas de clientes	i) Acceso no autorizado a cuentas; ii) Registros incorrectos de clientes (incurriendo en pérdidas); y iii) Pérdida o daño de activos de clientes por negligencia
		Contrapartes comerciales	i) Fallos con contrapartes no-clientes; y ii) Otros litigios con contrapartes distintas de clientes
		Distribuidores y proveedores	i) Subcontratación; y ii) Litigios con distribuidores

Fuente: SBIF

Las categorías resultantes para el registro de los eventos de riesgo se conformaron en tres niveles, siguiendo la metodología entregada por Basilea y la SBIF, el primer nivel muestra el origen a nivel macro del evento en cuestión y se separó bajo el siguiente orden:

Se utilizó una técnica de ordenamiento simple con el objetivo de codificar a cada evento de forma abreviada, actividad que facilitó posteriormente la implementación de la base de datos, sistemas de control y reportes.

Tabla 4: Codificación de eventos.

Categoría del Evento Según SBIF	Tipo de Carácter	Rango de Codificación
Categoría de Tipo de Eventos (nivel 1)	Letra Mayúscula	A -G
Categoría (nivel 2)	Numero	1-6
Actividades (Nivel 3)	Letra Minúscula	a-j

Fuente: Elaboración propia.

Como se aprecia en la tabla, el código que acompaña a cada categoría de nivel 1 corresponde a las letras mayúsculas del rango de la letra A hasta la letra G siguiendo el mismo orden que entrega la lista.

Por otro lado el segundo nivel corresponde a un subnivel del origen principal, el cual delimita de manera más específica el factor que involucró el surgimiento del evento, la codificación de este subnivel comprendió un rango desde el número 1 hasta el 6. Por último el nivel tres representa la actividad o proceso específico que se realizó y que produjo el evento de riesgo en cuestión, la codificación de este nivel comprendió letras minúsculas abarcando un rango desde la letra a hasta la letra j.

Figura N° 4: fuentes de los eventos de riesgo operacional.



Fuente: *Elaboración Propia.*

Así se definió y categorizó a los eventos que generan pérdidas por riesgo operativo, hecho que sirvió para posteriormente establecer de buena manera la base de datos de los eventos, esta base de datos es considerada un elemento fundamental para la administración del riesgo ya que de acuerdo a esta, es posible establecer modelos estadísticos que estimen y proyecten futuras pérdidas por riesgo operacional.

4. Diseño de la Base de Datos.

En esta etapa se entregó información acerca de las fuentes de información que se consideró como válida para formar parte de la base de datos interna del banco con el fin de desarrollar informes, estudios y proyecciones de las posibles pérdidas vinculadas al riesgo operacional. (Pacheco, 2009) señala que las fuentes de datos mínimas siguiendo metodologías avanzadas para registrar las pérdidas, y de acuerdo al marco regulatorio de Basilea corresponden a:

- ✓ Datos internos.
- ✓ Datos externos.
- ✓ Análisis de escenarios.
- ✓ Factores del entorno y de control interno.

Así se estableció que las principales fuentes de información para la producción de una base de datos fidedigna consideraron a las siguientes herramientas:

- ✓ Estadísticas.
- ✓ Informes.
- ✓ Auditorías internas.
- ✓ Auditorías Externas.
- ✓ Información entregada por el responsable del proceso.

Además, un segmento importante de esta etapa consistió en entregar los campos de información mínima que cada evento debiese tener para poder ser registrado de manera exitosa. Este registro de los eventos se consideró como la columna vertebral, en relación a la información relevante para posteriormente realizar estimaciones y proyecciones orientadas a las pérdidas, ya que dicha información específica fehacientemente cómo es afectada la institución en términos de impacto y frecuencia por los eventos de riesgo operacional.

Los campos mínimos necesarios para la adecuada recolección de información en torno a los eventos de riesgo ocurridos en una institución se establecieron de la siguiente forma:

- ✓ Referencia: este campo comprende el código que representa el origen del evento, de acuerdo a la nomenclatura entregada en la categorización de los eventos por riesgo operacional.
- ✓ Fecha de Inicio del Evento: este campo indicara el momento en el cual el evento se originó, independiente si este fue descubierto con un desfase importante de tiempo.
- ✓ Fecha de Descubrimiento: corresponde a la fecha en donde se descubre la existencia del evento independiente de si el mismo se generó con anterioridad.
- ✓ Cuantificación: se registra en este campo la cuantificación de la pérdida por el evento de riesgo operativo en el caso de que la misma sea cuantificable.
- ✓ Clasificación del evento: se clasifica al evento de acuerdo a la categorización por origen de tipo de riesgo operativo.
- ✓ Producto o servicio afectado: se identifica en este campo que producto o servicio entregado genero el evento de riesgo.
- ✓ Proceso: se identifica en este campo cual o cuales fueron los procesos que tuvieron algún grado de involucramiento a raíz del evento.
- ✓ Perdida no cuantificable: se registra en el caso de que el evento genere pérdidas que no sean fácilmente cuantificables, con el objetivo de generar información útil para que en el futuro el evento se puede cuantificar.
- ✓ Descripción del Evento: breve descripción básica del evento y su incidencia.

De esta manera se estableció un sistema de registros el cual es la piedra angular para la estimación de cargos de capital por medio de metodologías avanzadas y que por otro

lado facilita la implementación de indicadores de gestión para realizar controles y sistemas de monitoreo.

5. Diseño de la Matriz de Riesgo Operacional.

Esta fase consideró la elaboración de una matriz que permita identificar de manera adecuada los principales eventos de riesgo operacional en los que incurre la organización.

Por tanto la primordial función de esta herramienta consiste en el control y la gestión del riesgo identificando y cuantificando los procesos más importantes de la organización que puedan originar pérdidas económicas, enfocando el análisis de estos en términos de frecuencia (probabilidad) y severidad (impacto).

El instrumento para conocer este tipo de riesgo, es la construcción de una matriz, que permite identificar el riesgo operativo, con los niveles de riesgo (viabilidad e impacto) con la exposición asociada del riesgo operativo (Palma, 2011).

El diseño de esta matriz se puede resumir en las siguientes etapas:

1. CUANTIFICACIÓN DEL IMPACTO:

En esta etapa se categorizo a los eventos en relación a la magnitud del mismo. Para esto se estableció una tabla de medición del impacto, en la cual determinó los niveles o categorías de impacto posibles con el fin de categorizar a los eventos de acuerdo a esta variable. Así se estableció fraccionar los niveles de impacto en 5 grandes grupos enumerados a continuación.

Los criterios con los que se categorizó los niveles de severidad y probabilidad de un evento siguen la metodología propuesta por (Vizúete, 2009) la cual para el caso de la severidad expone medir el impacto en cinco grupos separados, considerando variables cuantitativas correspondientes a porcentajes de partidas financieras contables.

Tabla 5: Niveles de Severidad

Categoría	Rango de la Pérdida
<i>Insignificante</i>	0,1% Patrimonio Promedio
<i>Menor</i>	5% Patrimonio Promedio
<i>Moderado</i>	15% Ingreso Operacional Promedio
<i>Mayor</i>	50% Patrimonio Promedio
<i>Masivo</i>	100% Patrimonio Promedio

Fuente: Elaboración propia a partir de (Vizúete, 2009)

Por otro lado se establecieron además criterios de naturaleza cualitativa que complementan de buena manera la metodología anteriormente propuesta, es así como se proponen otras variables adicionales para medir la severidad de un evento exhibidas por (Palma, 2011) la siguiente tabla muestra las variables que adicionalmente fueron consideradas para la estimación del impacto o severidad de un evento en particular.

Tabla 6: Niveles de Severidad

Puntuación	Impacto económico	Reacción de los medios de comunicación	Acciones del Regulador
Insignificante	Bajo	No hay divulgación del evento	No interviene
Menor	Medio	Divulgación de carácter menor por internet y medios mínimos	Comentarios adversos pero no interviene
Moderado	Alto	Artículos en prensa, televisión, internet, alta divulgación por un día máximo	Acciones por parte del regulador que pueden incluir multas
Mayor	Grave	Reportaje en múltiples medios y noticiarios en TV nacional por más de un día	Multas Medianas
Masivo	Catastrófico	Repercusiones gubernamentales a nivel político y pérdida de confianza del público.	Multas significativas

Elaboración: propia a partir de (Palma, 2011)

2. CUANTIFICACIÓN DE LA PROBABILIDAD.

En esta etapa se entregó la metodología de cuantificación en relación a la probabilidad de ocurrencia de los eventos de riesgo operacional. De la misma manera que para estimar los niveles de impacto se debió elaborar una tabla la cual se encargó de agrupar los niveles de probabilidad de ocurrencia de los eventos. Así se estableció dividir los niveles de probabilidad en 5 secciones enumerados a continuación.

Tabla 7: Rango Cualitativo de Frecuencia

Categoría	Rango Cualitativo
Anormal	Cada 10 años
Remota	Cada 4 años
Frecuente	Anualmente
Viable	Semestralmente
Esperada	Diariamente

Elaboración: propia a partir de (Palma, 2011)

Para el cálculo matemático de la probabilidad de ocurrencia se propuso como horizonte de evaluación al periodo de tiempo correspondiente a un año.

Considerando que dicho periodo de tiempo equivale a 365 días, así el cálculo en términos porcentuales de la categoría anormal, así la probabilidad de un evento se calculó como el número de eventos registrados de acuerdo a los rangos establecidos, dividido número de eventos posibles dentro del rango.

Esto se ejemplifica para los límites de la categoría anormal obteniendo:

$$\frac{1}{3650} = 0,03\%$$

Bajo esta fórmula se establecerán los porcentajes de ocurrencia de cada categoría.

Tabla 8: límites porcentuales de frecuencia.

Categoría	Rango Cualitativo	Límite inferior	Límite superior
Anormal	Cada 10 años	0,00%	0,03%
Remota	Cada 4 años	0,03%	0,07%
Frecuente	Anualmente	0,07%	0,27%
Viable	Semestralmente	0,27%	0,55%
Esperada	Diariamente	0,55%	100,00%

Elaboración: propia a partir de (Vizuet, 2009)

3. ELABORACIÓN DE LA MATRIZ

En esta etapa se procedió a integrar las variables de probabilidad e impacto en un único instrumento, dicha combinación de elementos permitió generar una matriz que arrojó como resultado la caracterización de los eventos de riesgo operacional en términos del nivel de riesgo que representan.

Así se obtuvo una matriz que muestra gráficamente la posición en términos de riesgo que enfrenta una institución dada.

Figura N° 5: Matriz de Riesgos Operacionales.

Probabilidad			Impacto				
			1	2	3	4	5
			Insignificante	Menor	Moderado	Mayor	Masivo
			10	20	30	40	50
5	Esperada	25	250	500	750	1000	1250
4	Viable	20	200	400	600	800	1000
3	Frecuente	15	150	300	450	600	750
2	Remota	10	100	200	300	400	500
1	Anormal	5	50	100	150	200	250

Fuente: Elaboración Propia a partir de (González, 2007)

Para categorizar los niveles de riesgo se optó por la generación de cinco categorías a continuación enumeradas en escala de mayor a menor nivel de riesgo.

Tabla 9: Puntaje de riesgos y categorías.

Zona de Riesgo		Puntaje	
		Mínimo	Máximo
1	Riesgo Extremo	801	Mayor
2	Riesgo Alto	601	800
3	Riesgo Medio	401	600
4	Riesgo Bajo	201	400
5	Riesgo Inusual	50	200

Fuente: Elaboración Propia a partir de (González, 2007)

6. Diseño de Controles.

Posterior a la identificación de los riesgos se procedió a analizar los tipos de controles adecuados para cada riesgo, estimando en primera instancia las características esenciales requeridas para controles efectivos.

Luego de esto se desarrolló el conjunto de posibles acciones de control, concluyendo que las gestiones requeridas para el control y mitigación de los riesgos variarían según la naturaleza del riesgo en cuestión, presentando de manera general cuatro grandes tareas de control.

Figura N° 6: Acciones de control.



Fuente: Elaboración Propia.

7. Monitoreo.

En esta etapa se desarrolló la metodología a implementar para la elaboración de un sistema de monitoreo de riesgos operacionales efectivo. Además se estableció esta fase como el período culmine del sistema de administración de riesgo operacional, en donde se instauró como objetivo fundamental de esta etapa, el de determinar si los planes acción, herramientas, controles y estrategias establecidas están funcionando correctamente.

Entendiendo que el perfil de riesgo operacional derivado de datos de pérdidas históricas podría verse modificado por las acciones correctivas implementadas por la entidad financiera con posterioridad a la ocurrencia de los eventos reflejados en esos datos (Delfiner & Pailhé, 2009).

Un instrumento de alto beneficio que se utilizó para el cumplimiento del objetivo central de esta etapa, recayó en la confección de los denominados indicadores claves de riesgo o KRI por sus siglas en inglés.

De esta manera se diseñaron distintos indicadores de gestión de riesgo operacional con el objetivo de realizar de manera adecuada los seguimientos necesarios para asegurar el correcto funcionamiento del modelo de gestión.

Para lograr plasmar de manera adecuada el manejo de estos indicadores, se optó por simular valores en términos de probabilidad e impacto con el fin de exhibir detalladamente la correcta gestión e interpretación de la información en el sistema de administración.

Etapa cuantitativa.

La cuantificación de cargos de capital por riesgo operacional se basaron estrictamente en las pautas establecidas por el comité de Basilea, de este modo se realizó la estimación de capital requerido para cubrir los riesgos operativos de cada entidad bancaria que opera en el país, bajo la metodología BIA, y se presentó un modelo simulado de la utilización de técnicas avanzadas LDA.

Calculo de capital económico por método del indicador básico (BIA).

Para estimar el capital económico mediante el método del indicador básico (BIA). se siguió la metodología que presenta Basilea en su documento "Convergencia internacional de medidas y normas de capital" (BCBS, 2006) implementando la misma para las 24 entidades bancarias que operan en Chile.

El cálculo de capital económico correspondiente al método utilizado es el que se describe a continuación:

$$KBIA = [\sum (GL 1...n * \alpha)] / n$$

KBIA = La exigencia de capital en el método estándar.

GL = Ingresos brutos anuales medios, cuando sean positivos, de los tres últimos años.

n = Número de años (últimos tres años), en que los resultados fueron positivos.

$\alpha=15\%$, parámetro establecido por el Comité, que relaciona el capital exigido al conjunto del sector con el nivel del indicador en el conjunto del sector.

Por otro lado para realizar el mismo se extrajo de los estados financieros de las entidades las siguientes cuentas contables:

- ✓ Utilidad neta de operaciones financieras.
- ✓ Utilidad (pérdida) de cambio neta.
- ✓ Resultado por inversiones en sociedades.
- ✓ Ingreso neto por intereses y reajustes.
- ✓ Ingreso neto por comisiones.

Así se generó una planilla que registró cada cuenta mencionada, de las 24 entidades para los años 2010, 2011 y 2012 obteniendo un total de 360 datos que posteriormente formulados arrojaron los ingresos operacionales promedios y finalmente el cargo de capital requerido por entidad.

Estimación de cargos de capital por metodología LDA.

Para valoraciones por metodología avanzada se optó por simular valores en términos de frecuencia y probabilidad, para cuantificar las pérdidas económicas atribuibles a riesgos operacionales. Esta simulación se advirtió necesaria debido a la insuficiencia de información pública relativa a esta materia, lo cual imposibilitaba la tarea de exhibir ciertas características relevantes del modelo de gestión de riesgo operacional.

Se utilizó esta metodología debido principalmente a su universal aceptación tanto en la industria bancaria como en el ámbito académico.

Esta etapa se basó en gran medida en la investigación de Jiménez et al. (2008) “Enfoques de Medición de Riesgo Operacional” en donde se propone una metodología enfocadas en las pérdidas agregadas como una herramienta muy útil para aplicaciones en la cuantificación del riesgo operativo.

Esta metodología está compuesta por cuatro etapas:

1. Ajuste de la distribución de frecuencia.

De acuerdo al autor la función de probabilidad que posee una mejor capacidad de ajuste corresponde a la distribución de Poisson. Dicha función se encuentra caracterizada por un único parámetro, lambda (λ), el cual representa, por término medio, el número de eventos de pérdida ocurridos en un año.

2. Ajuste de la distribución de severidad

Esta etapa contempló el ajuste de la distribución de severidad, correspondiente al nivel de impacto de las pérdidas de los eventos, se propuso una distribución de tipo Weibul como una función con características aceptables a la hora de simular pérdidas económicas.

3. Obtención de la distribución de pérdidas agregadas.

La obtención de la distribución de pérdidas agregadas es consecuencia de la combinación de la distribución de frecuencia y severidad.

Este proceso correspondió al cómputo de un número aleatorio de eventos de pérdidas con valores, también aleatorios, bajo el supuesto de que las severidades son independientes entre sí y, al mismo tiempo, independientes de la frecuencia.

4. Estimar una pérdida máxima bajo un nivel de confianza del 99.9% (Op Var).

El último paso consistió en generar un denominado Op Var, que corresponde al valor esperado de la pérdida ubicada en el percentil 99,9% de la función de distribución de pérdidas agregadas, concluyendo empíricamente a un alto nivel de confianza que la pérdida ocasionada por el evento analizado no será mayor al valor que indica el percentil mencionado.

PROCESO DE SIMULACIÓN DE DATOS

El método seleccionado para realizar la simulación de valores de pérdidas fue el de la simulación de Monte Carlo, proceso que permite realizar la combinación de distribuciones de probabilidad de distinta naturaleza para otorgar una tercera función de pérdidas.

Tras repetir 5000 veces este experimento, se dispuso de una cantidad de datos u observaciones sobre el comportamiento de las pérdidas derivadas del riesgo operacional.

A continuación se presenta un esquema que resume la metodología LDA y una matriz estándar para registrar los tipos de pérdidas por línea de negocio.

Los procesos de simulación se realizaron por medio de Microsoft Excel, utilizando su funcionalidad de generar observaciones aleatorias basadas en distribuciones preestablecidas, además para la combinación de las distribuciones de severidad se desarrollaron técnicas de programación de conectores lógicos simples, para obtener la distribución de pérdidas agregada.

Los parámetros estadísticos utilizados se muestran en la siguiente tabla:

Tabla 10: Caracterización de frecuencias para simulación de Monte Carlo.

Línea de Negocio Evento	Banca Corporativa fraude Interno	
Frecuencia	Distribución	Poisson
	Parámetros	$\lambda = 10$
Severidad	Distribución	Weibull
	Parámetros	$\alpha=0,75 \quad \beta= 80$

Fuente: Elaboración propia a partir de Jiménez et al. (2008).

CAPITULO III. DISEÑO MODELO DE GESTION DE RIESGO OPERACIONAL

En este capítulo se presenta el diseño de un modelo de administración de riesgo operacional, este fue desarrollado de manera estandarizada y en base a los requerimientos que entrega el comité de Basilea, el modelo exhibe los elementos fundamentales que debe tener un sistema de este tipo, dejando lugar además para la eventual adaptación de las necesidades de distintas entidades financieras dependiendo de su tamaño, recursos y nivel de complejidad organizacional entre otros factores. El modelo en cuestión permitirá la identificación, medición, control y monitoreo de los riesgos operacionales de la entidad, que se sabe por su naturaleza cíclica, deberán permanecer en constante revisión y actualización.

Elementos del modelo:

- ✓ Políticas
- ✓ Estructura organizacional
- ✓ Sistema de registro de eventos
- ✓ Documentación, base de datos
- ✓ Organismos de control
- ✓ Sistema de monitoreo

Etapa 1: Establecimiento de políticas de riesgo operacional.

El principal objetivo de la creación de políticas de gestión de riesgo operacional consiste en enmarcar una estructura de administración que confiera en líneas generales las principales directrices de conducta y dirección en torno al riesgo operacional.

Para esto la primera actividad requerida es la instauración de una comisión o gerencia de administración del riesgo operacional, el cual tiene como primera tarea la creación de un documento que presente los principios de la gestión de este riesgo para la institución bancaria.

Para este modelo la elaboración de las políticas de riesgo operacional se basan en los principios de gestión de riesgo operacional, documento entregado BCBS denominado “*Buenas prácticas para la gestión y supervisión del riesgo operativo*” específicamente en la sección que enumera los principios generales de gestión de riesgo operacional, es necesario señalar que estas políticas conformaran un estándar mínimo, dejando espacio para la creación de un documento que se adapte a los requerimientos específicos de la institución que desee implementar el modelo entregado en esta investigación.

POLÍTICAS RIESGO OPERACIONAL

1. Será de vital responsabilidad para la gerencia de riesgo operacional el examinar los principales riesgos operativos que enfrenta la institución financiera, siendo su tarea fundamental dirigir la gestión de este riesgo definiendo la posición de la entidad en torno al riesgo operacional, y la generación de un sistema que evalúe, monitoree, controle y mitigue este tipo de riesgos.
2. El proceso de gestión de riesgo operativo debe por necesidad estar alineado con los procesos de auditoría interna que posee la entidad financiera, siendo este proceso una tarea efectuada por personal capacitado, competente e independiente de la gerencia de riesgo.
3. La gerencia de riesgo deberá identificar y evaluar el riesgo operacional inherente de la institución, de todas sus líneas de negocio, sus productos, actividades, procesos y sistemas relevantes.

4. Deberán existir niveles de responsabilidad para cada producto, actividad, procesos y sistema relevante que involucre a la organización este responsable será designado por la gerencia de riesgo operacional en conjunto con la aprobación de la alta gerencia de la institución bancaria.
5. La entidad tiene la responsabilidad de realizar seguimientos permanentes, para asegurar que se cumplen con los perfiles de riesgo operacional deseados por la alta gerencia y la unidad de riesgo operacional.
6. El banco deberá contar con políticas de control de procesos y procedimientos para controlar y cubrir los riesgos operativos más relevantes, estableciendo oportunamente si estos deberán ser asumidos, evitados, reducidos o transferidos.
7. La entidad deberá contar con planes de contingencia que velen por la continuidad del negocio y aseguren la correcta operación del banco para eventos de interrupción grave de la actividad.
8. Se debe entregar de manera oportuna y clara la información relevante en torno a la gestión del riesgo operacional a las entidades fiscalizadoras pertinentes con el objetivo de transparentar la gestión del riesgo operacional del banco.
9. Se realizaran evaluaciones periódicas tanto de la gestión del riesgo operacional como también de la calidad y transparencia de los informes entregados a las entidades fiscalizadoras.
10. Se deberá además proporcionar información de naturaleza pública en relación a la gestión del riesgo operacional en virtud de fomentar la transparencia del mercado.

DIRECTRICES DEL SISTEMA DE ADMINISTRACIÓN DE RIESGO OPERACIONAL S.A.R.O.

En conjunto con las políticas anteriores, las directrices que a continuación se presentan buscan alinear el funcionamiento que debe cumplir en específico el sistema de administración de riesgo operacional. Este instrumento por tanto se traduce como una herramienta que entrega las reglas de conducta y procedimiento en las que se orienta el sistema de administración, permitiendo de este modo el funcionamiento eficiente, efectivo y oportuno de la gestión de riesgo operacional.

1. El sistema además de gestionar debe ser capaz a su vez de promover y fortalecer una cultura de administración de riesgo operacional, con el objetivo de crear conciencia colectiva sobre la necesidad de considerar este riesgo en cada decisión que se tome dentro de la organización.
2. Toda persona que forme parte de la institución bancaria debe conocer y cumplir las normas internas y externas en relación a la gestión del riesgo operacional, además el sistema de administración debe ser capaz de proporcionar y divulgar adecuadamente la normativa vigente de riesgo operacional y velar por el cumplimiento de estas.
3. Los procesos y procedimientos deben necesariamente estar sometidos a permanentes análisis con el fin de generar propuestas de mejora continua de cada proceso, subproceso y tarea, siendo estos análisis calendarizados de manera pertinente.
4. Se debe establecer claramente cuáles son los perfiles de riesgos, entregando así un contexto de administración y de este modo adecuar los procesos a esta posición específica de la entidad en torno al riesgo operacional.
5. Es necesario una revisión permanente sobre los cambios en los perfiles de riesgo operativo para realizar los ajustes oportunos y pertinentes, comunicando los mismos según corresponda.
6. El sistema debe contar con sistemas de medición cuantitativos y cualitativos para evaluar los niveles de cumplimiento, la selección de estas herramientas quedara a criterio de la gerencia de riesgo operacional.
7. El sistema de administración debe ser capaz de generar una base de datos robusta que permita y asegure la captura oportuna de cualquier evento de riesgo operacional junto con proporcionar las herramientas informáticas que faciliten el acceso de la base de datos.
8. El sistema de administración debe ser capaz de generar informes y documentos relacionados a la gestión del riesgo operacional para que estos sean divulgados eficazmente a quienes corresponda.

Etapa 2: Estructura Organizacional de Riesgo Operacional.

La estructura organizacional de la gerencia de riesgo operacional tiene dentro de sus tareas identificar gráficamente las funciones del personal que la conforma junto con los distintos niveles jerárquicos y de responsabilidad existentes en términos organizacionales. Además señala claramente cuáles son los desempeños esperados de cada cargo dentro de la estructura. Para el caso de la gerencia de riesgo operacional esta deberá estar en línea con sus homónimas de riesgo de crédito y riesgo de mercado para de este modo favorecer a la integración total de los riesgos que debe enfrentar la organización.

La estructura organizacional que se presenta en esta investigación se confecciona basándose en los principios que entrega BCBS, para la correcta gestión del riesgo operacional y considera principalmente criterios referentes a necesidades mínimas, requeridas para cumplir con las exigencias cuantitativas y cualitativas que el comité de Basilea entiende como básicos.

Los principales criterios en este ámbito se centraron en los siguientes puntos:

1. Necesidad de un Gerente de Riesgo Operacional:

Se consideró adecuado exigir al modelo organizacional, un responsable a nivel de la alta gerencia, pues es indispensable un alto nivel de interdependencia y a su vez de integración con las demás gerencias de riesgo de crédito y de mercado, de manera de generar políticas de riesgo integrales y holísticas para la entidad.

Se expuso en el modelo que el eventual gerente será principal responsable de verificar el cumplimiento efectivo de todos los requisitos que conlleven a la adecuada administración de los riesgos operacionales.

Esto persiguiendo el cumplimiento del principio 3 del documento del regulador el cual señala que *“La alta gerencia deberá ser responsable del desarrollo de políticas, procesos y procedimientos destinados a la gestión de estos riesgos para todos los productos, actividades, procesos y sistemas relevantes para el banco”* (BCBS, 2003).

2. *Necesidad de Subgerencia por Área de Negocio.*

Basilea exige para sus estimaciones avanzadas, la separación de los eventos de pérdida por unidades o líneas de negocio, pues de esta manera se espera que dichas pérdidas puedan ser mejor identificadas, caracterizadas y controladas. Por esto se consideró adecuado incluir a un Subgerente de riesgo operacional por cuantas líneas de negocios tenga la entidad financiera, pudiendo llegar estas a 8 líneas de negocio como máximo según lo estipulado por (BCBS, 2006).

Así se estipuló la necesidad de una Subgerencia de acuerdo a las posibles líneas de negocio en las que opere la institución a continuación enumeradas.

1. *Finanzas corporativas*
2. *Negociación y ventas*
3. *Banca minorista*
4. *Banca comercial*
5. *Pagos y liquidación*
6. *Servicios de agencia*
7. *Administración de activos*
8. *Intermediación minorista*

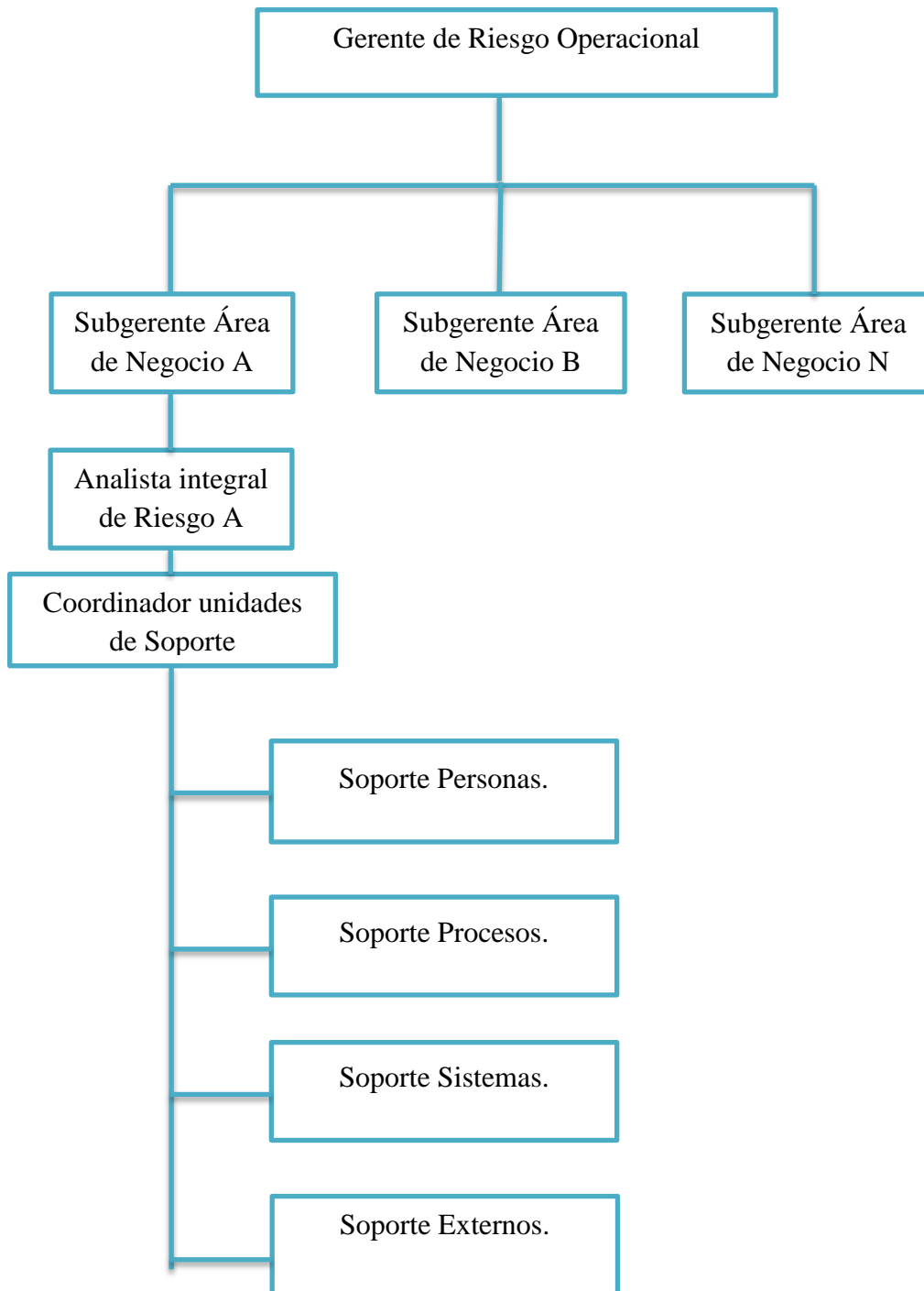
3. *Necesidad de Recurso Humano calificado.*

Los bancos deberán contar con un proceso rutinario que garantice el cumplimiento de un conjunto documentado de políticas, controles y procedimientos internos, algunos de estos procesos rutinarios a realizar tiene una naturaleza de revisión diaria, lo cual advierte la necesidad de apoyo a las gerencias en términos de recursos humanos capacitados para tareas de distinta complejidad y alcance.

De acuerdo a este punto se concluyó la necesidad de incorporar a cada área de negocios a los siguientes colaboradores, siguiendo un nivel de competencias, conocimientos y responsabilidades descendente.

1. *Analista integral de Riesgo de la línea de negocio.*
2. *Coordinador unidades de Soporte*
3. *Soporte Personas.*
4. *Soporte Procesos.*
5. *Soporte Sistemas.*
6. *Soporte Externos.*

Figura N° 7: Modelo Estandarizado Estructura gerencia de riesgo operacional



Fuente: Elaboración Propia.

DESCRIPCIÓN DE CARGOS

A continuación se presentan brevemente las principales funciones requeridas para cada cargo vinculado a la gerencia de riesgo operacional, destacando que únicamente se presenta un perfil general el cual contiene los desempeños básicos esperados para cada cargo.

De estas labores primordiales para el control adecuado de los riesgos operacionales, se deberá confeccionar un manual de funciones y perfiles de cargos, tarea que queda delegada a la gerencia de recursos humanos de la organización, la cual deberá establecer:

1. Descripción de funciones inherentes al mando.
2. Descripción de funciones específicas.
3. Niveles de experiencia.
4. Nivel de conocimientos académicos.
5. Competencias no académicas.
6. Responsabilidades.

Como se mencionó anteriormente la confección del manual de funciones y perfiles se deberá considerar las siguientes funciones principales por cargo:

Gerente de Riesgo Operacional.

Funciones Principales:

- ✓ Asegurar el correcto funcionamiento del sistema de administración de riesgo operacional.
- ✓ Realizar en conjunto con las demás gerencias de riesgo la gestión integral de los riesgos de la institución bancaria a nivel corporativo.
- ✓ Establecer mejoras a los sistemas de identificación, medición, control y monitoreo de los riesgos operacionales de la entidad bancaria.
- ✓ Establecer las necesidades de capital para cubrir los riesgos operacionales según normativa vigente.
- ✓ Generar documentos de carácter regulatorio y normativo en torno al riesgo operacional, así como establecer y actualizar las políticas y directrices de riesgo operacional de la organización conforme a posibles cambios del entorno regulatorio.

Subgerente Área de Negocio.

Funciones Principales:

- ✓ Asegurar el correcto funcionamiento del sistema de administración de riesgo operacional en su unidad de negocio.
- ✓ Establecer mejoras a los sistemas de identificación, medición, control y monitoreo de los riesgos operacionales en su línea de negocio.
- ✓ Velar por el cumplimiento de las normativas en torno al riesgo operacional
- ✓ Reportar al gerente de riesgos según periodos establecidos el comportamiento de la línea de negocio en relación al riesgo operacional.

Analista integral de Riesgo Operacional.

Funciones Principales:

- ✓ Controlar riesgos operacionales diariamente, e informar resultados de estos.
- ✓ Hacer seguimiento a las actividades, controles y análisis referidos a riesgos operacionales.
- ✓ Efectuar seguimientos de los indicadores claves de riesgo operacional y reportar estos.
- ✓ Generar nuevas iniciativas de seguridad de la información que fortalezcan los procesos del negocio.

Coordinador unidades de Soporte.

Funciones Principales:

- ✓ Apoyar al analista integral de riesgo en la ejecución de sus labores.
- ✓ Gestionar la ejecución y realización de actividades de los equipos de soporte.
- ✓ Asegurar la integridad de la información generada por el equipo de soporte.

Soporte Personas.

Funciones Principales:

- ✓ Realizar seguimiento estadístico de los eventos de riesgo operacional diariamente.
- ✓ Realizar análisis e informar de posibles desviaciones inesperadas en eventos vinculados a personas.
- ✓ Informar de posibles mejoras en procesos que vinculen eventos relacionados con personas a encargado de soporte de procesos.
- ✓ Entregar reportes de gestión de diferente índole para estudios de riesgos originados por personas.

Soporte Procesos.

Funciones Principales:

- ✓ Realizar seguimiento estadístico a cada proceso que origine eventos de riesgo operacional diariamente.
- ✓ Analizar e informar deficiencias en los procesos productivos.
- ✓ Rediseñar y mejorar continuamente los procesos productivos de la organización.
- ✓ Entregar reportes de gestión de diferente índole para estudios de riesgos originados por procesos.

Soporte Sistemas.

Funciones Principales:

- ✓ Realizar seguimiento estadístico de los eventos de riesgo operacional diariamente.
- ✓ Realizar seguimiento a los sistemas informáticos y no informáticos de la organización.
- ✓ Analizar e informar deficiencias en los sistemas de la organización.
- ✓ Proponer mejoras continuamente los sistemas de la organización.
- ✓ Entregar reportes de gestión de diferente índole para estudios de riesgos originados por falencias en los sistemas.

Soporte Externos

Funciones Principales:

- ✓ Realizar seguimiento estadístico de los eventos de riesgo operacional diariamente.
- ✓ Realizar análisis e informar de posibles desviaciones inesperadas en eventos de origen externo.
- ✓ Informar de posibles mejoras en procesos que vinculen eventos externos a encargado de soporte de procesos.
- ✓ Entregar reportes de gestión de diferente índole para estudios de riesgos originados por eventos externos.

Etapa 3: Categorización y Codificación de los Eventos de Riesgo Operacional.

El siguiente paso para el diseño del modelo comprende la definición y categorización de los eventos que generan pérdidas por riesgo operativo, para luego establecer la formulación de una base de datos la cual se considera un pilar fundamental para la administración del riesgo. En función a la información obtenida de los riesgos operacionales a los que incurre la organización es posible generar una matriz de riesgo que nos permita identificar los riesgos más relevantes en términos de impacto y frecuencia.

Se define evento como un incidente que se presenta en un proceso y cuya consecuencia es que el resultado final del mismo difiere de lo que se había planeado, este acontecimiento es debido a una falta de adecuación o de un fallo de los procesos, personal y los sistemas internos o bien por acontecimientos externos, la categorización de los eventos está formulada en base a los documentos entregados por el comité en su documento “*Convergencias internacionales de medidas y normas de capital*” y que además fueron validados por la SBIF como eventos de riesgo operacional.

CATEGORÍA DE TIPO DE EVENTO.

A. Fraude Interno:

1. Actividades no autorizadas:

- a. Operaciones no reveladas intencionalmente
- b. Operaciones no autorizadas con pérdidas monetarias
- c. Valoración errónea intencional de posiciones.

2. Hurto y fraude:

- a. fraude crediticio, depósitos sin valor hurto, extorsión, malversación
- b. Apropiación indebida de activos
- c. Destrucción dolosa de activos
- d. Falsificación
- e. Utilización de cheques sin fondo
- f. Contrabando
- g. Apropiación de cuentas e identidad
- h. Incumplimiento y evasión de impuestos
- i. Soborno, cohecho
- j. Abuso de información privilegiada.

B. Fraude Externo:

1. Hurto y fraude:
 - a. Hurto, Robo.
 - b. Falsificación.
 - c. Utilización de cheques sin fondos.
2. Seguridad de los sistemas:
 - a. Daños por ataques informáticos.
 - b. Robo de información con pérdida monetaria.

C. Relaciones Laborales y seguridad en el puesto de trabajo

1. Relaciones Laborales:
 - a. Cuestiones relativas a remuneración, prestaciones sociales, extinción de contratos.
 - b. Organización Laboral.
2. Higiene seguridad en el trabajo.
 - a. Imposibilidad general (resbalones, caídas, etc.)
 - b. Casos relacionados con las normas de higiene y seguridad en el trabajo
 - c. Indemnización de trabajadores.
3. Diversidad y discriminación:
 - a. Todo evento relacionado a algún tipo de discriminación.

D. Incidencias en el negocio y fallos en los sistemas

1. Sistemas:
 - a. Hardware.
 - b. Software.
 - c. Telecomunicaciones.
 - d. Interrupción incidencias en el suministro de algún servicio.
 - e.

E. Daños a activos materiales.

1. Desastres y otros acontecimientos:
 - a. Pérdidas por desastres naturales
 - b. Pérdidas humanas por causas externas (terrorismo, vandalismo)

F. Clientes, productos y prácticas empresariales.

1. Adecuación, divulgación de información y confianza:
 - a. Abusos de confianza
 - b. incumplimiento de pautas
 - c. Apropiamiento divulgación de información
 - d. Violación de la privacidad de clientes
 - e. Quebrantamiento de privacidad
 - f. Ventas agresivas
 - g. Pérdidas de cuentas

- h. Mal uso de información confidencial
- i. Responsabilidad del prestamista
- 2. Prácticas empresariales o de mercado impropias:
 - a. Prácticas anti-competencia
 - b. Prácticas impropias comerciales y de mercado
 - c. Manipulación del mercado
 - d. Comercialización de información privilegiada a favor de la empresa
 - e. Actividades no autorizadas
 - f. Lavado de dinero
- 3. Productos defectuosos:
 - a. Defectos del producto
 - b. Error de modelo
- 4. Selección, patrocinio y riesgos:
 - a. Fallida investigación a clientes según los protocolos.
 - b. Superación de los límites de exposición frente a clientes.
- 5. Actividades de asesoramiento:
 - a. Litigios sobre resultados de las actividades de asesoramiento.

G. Ejecución, entrega y gestión de procesos.

- 1. Recepción, ejecución y mantenimiento de operaciones:
 - a. Comunicación defectuosa.
 - b. Errores de introducción de datos, mantenimiento o descarga
 - c. Incumplimiento de plazos o de responsabilidades
 - d. Ejecución errónea de modelos, sistemas
 - e. Error contable, atribución a entidades erróneas
 - f. Errores en otras tareas.
 - g. Fallo en la entrega
 - h. Fallo en la gestión del colateral.
 - i. Mantenimiento de datos de referencia.
- 2. Seguimiento y monitoreo:
 - a. Incumplimiento en la obligación reportar.
 - b. Inexactitud de informes externos.
- 3. Aceptación de clientes y documentación:
 - a. Extravío de autorizaciones o rechazos de clientes.
 - b. Documentos jurídicos inexistentes o incompletos.

4. Gestión de cuentas de clientes:
 - a. Acceso no autorizado a cuentas.
 - b. Registros incorrectos de clientes.
 - c. Pérdida o daño de activos de clientes por negligencia.

5. Contrapartes comerciales:
 - a. Fallos con contrapartes no-clientes.
 - b. Otros litigios con contrapartes distintas de clientes.

6. Distribuidores y proveedores:
 - a. Subcontratación.
 - b. Litigios con distribuidores.

Una vez identificados los eventos, es posible efectuar una codificación de estos mismos, la función de esta tarea es la de facilitar la identificación del evento de acuerdo a la categoría de incidente del cual proviene, creando de esta manera una base de datos que presente información vital para la administración del riesgo operativo. La ventaja de generar este código asociado a un evento se presenta a la hora de generar filtros para el estudio individual de los eventos de riesgo operacional.

Tabla 11: Codificación de Evento de Riesgo Operacional

Categoría del Evento Según SBIF	Tipo de Carácter	Rango de Codificación
Categoría de Tipo de Eventos (nivel 1)	Letra Mayúscula	A -G
Categoría (nivel 2)	Número	1-6
Actividades (Nivel 3)	Letra Minúscula	a-j

Fuente: Elaboración propia.

Así un evento de riesgo operacional deberá ser registrado de la siguiente manera:

Categoría Nivel 1- Categoría Nivel 2-Categoría Nivel 3

Donde por ejemplo; A-2-j = corresponde al evento “Abuso de información privilegiada”.

Etapa 4: Diseño de la Base de Datos.

MATRIZ DE RIESGO

La matriz de riesgo puede ser considerada como un instrumento elemental para el diseño de un sistema de administración de riesgo operativo, su principal función considera el control y la gestión del riesgo identificando y cuantificando los procesos más importantes de la organización que puedan originar pérdidas económicas.

Una de las virtudes de esta herramienta se encuentra en su capacidad para obtener información acerca de la calidad y eficacia real de los controles y mitigadores actuales de los riesgos respecto de los resultados esperados que una organización tiene, así los beneficios más relevantes de implementar una matriz de riesgo consideran:

- ✓ Asignar un valor de riesgo a un proceso, de acuerdo al establecimiento de ciertos criterios basados en frecuencia e impacto.
- ✓ Proporciona información importante para la evaluación de la efectividad de la gestión y administración del riesgo en la organización.
- ✓ Entrega un diagnóstico inicial de la situación actual en torno al perfil de riesgo de la organización, de forma objetiva y cuantificable.
- ✓ Permite realizar comparaciones objetivas entre distintos procesos, actividades o eventos.
- ✓ Fundamental para el proceso de evaluación de controles y mitigadores del riesgo.
- ✓ Evalúa los procesos en relación a criterios de impacto y nivel de importancia, permitiendo un mayor control de las actividades más relevantes en términos de riesgo.
- ✓ Permite documentar los procesos y evaluar el riesgo de los mismos de manera integral.

Para efectos de la investigación la matriz de riesgo se considera un instrumento útil para efectuar el diseño y la planificación de un sistema que permita administrar el riesgo operativo de buena manera. Esta matriz permitirá un mejor uso de los recursos limitados de la organización, centrando la utilización de estos mismos en las actividades críticas de la gestión del riesgo operacional.

En consecuencia la matriz de riesgo operacional conforma un elemento base para el sistema de administración de riesgo operativo, pues su naturaleza gráfica consigue identificar claramente los riesgos que se debiesen priorizar en la organización, permitiendo de este modo la planificación de actividades que tengan como principal objetivo el efectivo control de los riesgos.

La confección de la matriz de riesgo operacional se compone de diferentes etapas a continuación presentadas y descritas.

1) IDENTIFICACIÓN:

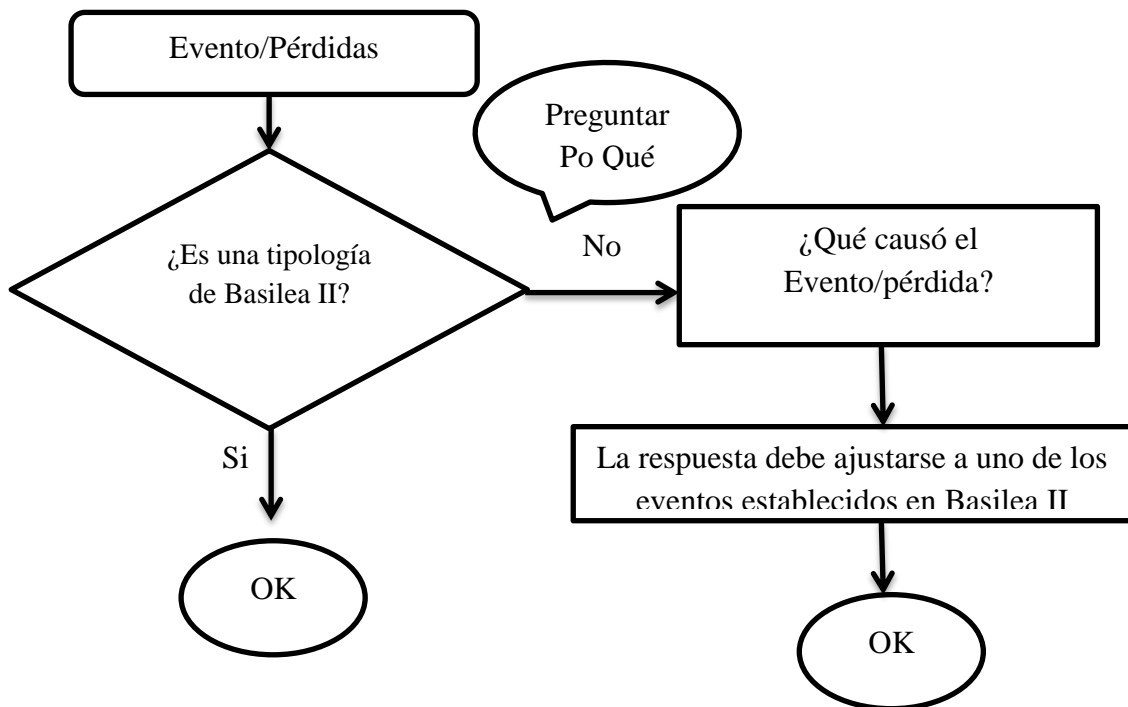
Este proceso es clave para la elaboración de la matriz ya que muestra la manera adecuada para reconocer los eventos que forman parte del riesgo operacional, esta etapa consiste en identificar y determinar los posibles eventos de riesgo que se derivan de cada proceso de la organización, para realizar esta tarea es necesario ejecutar las siguientes actividades:

a) IDENTIFICACIÓN DE LOS PROCESOS OPERACIONALES Y EVENTOS:

La primera tarea para la medición de los riesgos consiste en identificar cuáles son los procesos que realiza la organización. Es entonces importante para cualquier entidad bancaria contar con procesos adecuadamente identificados y definidos ya que los eventos de riesgo operacional nacen necesariamente de la existencia de un procesos y mientras mejor identificado, definido y gestionado este el proceso, menores serán las probabilidades de incurrir en eventos de pérdida por riesgo operacional.

Por otro lado es necesario identificar si los eventos corresponden a eventos de riesgo operacional, para aquello se presenta el siguiente diagrama propuesto por la superintendencia de bancos e instituciones financieras.

Figura N° 8: regla propuesta por ORX para clasificar los eventos/pérdidas por riesgo operacional.



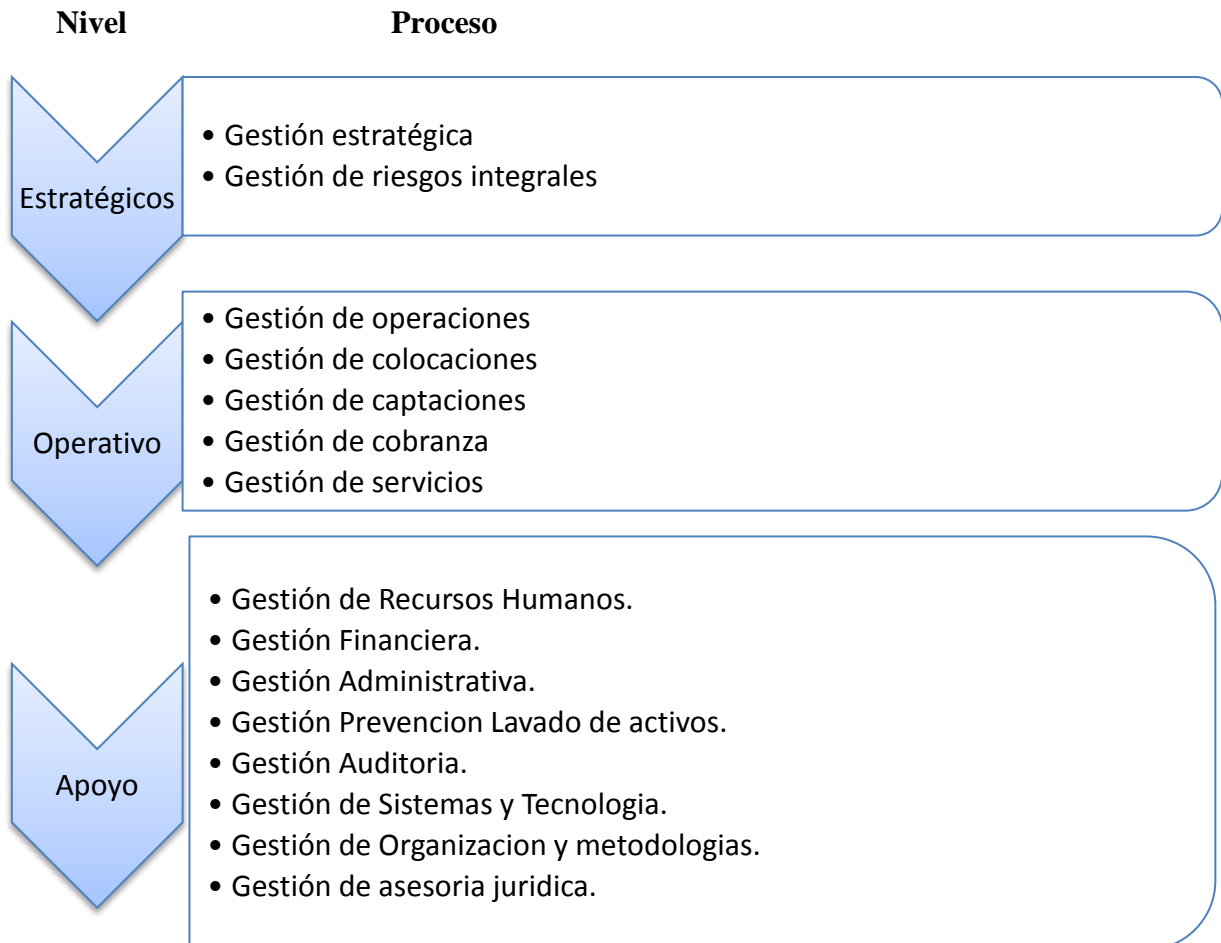
Fuente: Elaboración propia a partir de SBIF

Mapa de Procesos

La adecuada identificación de los procesos permite la agrupación de estos en distintos niveles que difieren tanto en importancia como en complejidad, como consecuencia cada uno de estos niveles posee distintos tipos de procesos y se concentran en tres grandes niveles, procesos gobernantes o estratégicos, procesos productivos u operativos y los procesos habilitantes de soporte o apoyo.

Mapa de Procesos entidad financiera.

Figura N° 9: Procesos por niveles.



Fuente: Elaboración: propia a partir de (Vizuet, 2009)

Proceso Estratégico o Gobernante:

Son aquellos que permiten definir y desarrollar estrategias estableciendo objetivos a largo plazo para la organización. Estos procesos pueden ser muy diversos y variaran de dependiendo de la institución, la implementación de estos procesos proporciona elementos claves para la organización como por ejemplo la visión misión políticas y valores de la empresa, por lo tanto los procesos de este tipo que están vinculados a la gestión del negocio y toma de decisiones de la alta gerencia.

Es importante reconocer los procesos gobernantes a cabalidad pues los eventos por riesgo que se deriven de procesos de este nivel poseen un alto grado de impacto, considerando esto es necesario que los procesos estratégicos sean exhaustivamente analizados y que los eventos que provengan de este tipo de procesos tengan una alta prioridad para ser controlados.

Como ejemplos de eventos de riesgo operacional derivados de este tipo de procesos tenemos:

- ✓ Utilización de metodologías inadecuadas de gestión de riesgo.
- ✓ Falta de herramientas tecnológicas que soporten la gestión operacional.
- ✓ Errores en cálculo de provisiones.
- ✓ Falta de adecuación al entorno de la organización
- ✓ Falta de capacitación a personal
- ✓ Falta de políticas de divulgación de información y manuales de conducta.
- ✓ Falta de políticas de comportamiento ético y moral.

Proceso Productivo:

Se definen como los procesos que agregan valor al cliente e inciden de manera directa en la satisfacción o insatisfacción del cliente. Forman parte integral de la cadena de valor de la organización y generalmente son procesos que consumen gran cantidad de recursos en la empresa.

Estos procesos también son parte importante de la organización y así como en los procesos gobernantes, los procesos productivos poseen un alto impacto en términos de pérdidas en el caso de incurrir en eventos de riesgo a este nivel, por lo cual es necesario examinarlos con gran atención.

Como ejemplos de eventos de riesgo operacional derivados de este tipo de procesos tenemos:

- ✓ Pago de documentos con errores de forma y firma.
- ✓ Autorización de pagos por personal no facultado.
- ✓ Perdida física de documentos por mala gestión o descuido.
- ✓ Entrega de documentación falsa.
- ✓ Incumplimiento de envío de información a autoridades fiscalizadoras.
- ✓ Errores en conciliaciones bancarias.
- ✓ Gastos financieros sin acreditación o no justificados.

Procesos de Apoyo:

En esta categoría se encuentran los procesos necesarios para el control y las mejoras de los sistemas de gestión que no caen en ninguna de las categorías anteriormente definidas, este tipo de procesos apoyan a los procesos principales del negocio y su objetivo principal es optimizar los recursos de la organización para asegurar el desarrollo sostenido de la institución

Igualmente importantes en términos generales los eventos que se derivan de estos procesos generalmente poseen un menor impacto en comparación a los eventos de los otros niveles.

Como ejemplos de eventos de riesgo operacional derivados de este tipo de procesos tenemos:

- ✓ No cumplir adecuadamente con las fechas de firma de contratos de trabajo
- ✓ Falta de descripción de cargos
- ✓ Falta de actualización de nóminas de pago.
- ✓ Cálculos errados en el pago de la nómina.
- ✓ Demandas por despidos injustificados
- ✓ Demandas por accidentes laborales
- ✓ Declaraciones inoportunas de impuestos.
- ✓ Incumplimiento por cálculos errados en requisitos de liquides.
- ✓ Perdidas por fallas en sistemas tecnológicos.
- ✓ Interpretaciones jurídicas no adecuadas.

B). IDENTIFICAR LOS EVENTOS DE RIESGO.

Una vez identificado los procesos que realiza la entidad para funcionar adecuadamente, será necesario realizar un exhaustivo análisis de cada uno de estos, con el objetivo de identificar los eventos de riesgo operativo que pudiesen afectar a la entidad, algunos de estos eventos fueron mencionados en la etapa anterior, cabe señalar que la existencia de eventos así como frecuencia de estos variara de institución en institución dependiendo de que tan bien estén identificados, diseñados y gestionados estén los procesos que realiza el banco.

Para esta etapa es imprescindible la generación de una base de datos robusta, nutridas de fuentes de información histórica de eventos hayan surgido en la entidad, para aquello es posible valerse de distintas fuentes como por ejemplo:

- ✓ Estadísticas.
- ✓ Informes.
- ✓ Auditorías internas.
- ✓ Auditorías Externas.
- ✓ Información entregada por el responsable del proceso.
- ✓ Datos externos.

Además se debe agregar a esta base de datos el registro de cada evento de riesgo operativo que afecte la entidad en un momento dado, permitiendo, una vez obtenido un volumen de información importante, anticipar y proyectar los posibles eventos futuros de pérdidas por riesgo operativo. Para la confección de esta base de datos se presenta una tabla tipo, con los campos mínimos a completar una vez se registre un evento de riesgo operacional.

A continuación se entregan los campos de la base de datos y una breve descripción del contenido que cada una.

- ✓ Referencia: este campo comprende el código que representa el origen del evento, de acuerdo a la nomenclatura entregada en la categorización de los eventos por riesgo operacional.
- ✓ Fecha de Inicio del Evento: este campo indicara el momento en el cual el evento se originó, independiente si este fue descubierto con un desfase importante de tiempo.
- ✓ Fecha de Descubrimiento: corresponde a la fecha en donde se descubre la existencia del evento independiente de si el mismo se generó con anterioridad.
- ✓ Cuantificación: se registra en este campo la cuantificación de la pérdida por el evento de riesgo operativo en el caso de que la misma sea cuantificable.

- ✓ Clasificación del evento: se clasifica al evento de acuerdo a la categorización por origen de tipo de riesgo operativo.
- ✓ Producto o servicio afectado: se identifica en este campo que producto o servicio entregado genero el evento de riesgo.
- ✓ Proceso: se identifica en este campo cual o cuales fueron los procesos que tuvieron algún grado de involucramiento a raíz del evento.
- ✓ Perdida no cuantificable: se registra en el caso de que el evento genere pérdidas que no sean fácilmente cuantificables, con el objetivo de generar información útil para que en el futuro el evento se puede cuantificar.
- ✓ Descripción del Evento: breve descripción básica del evento y su incidencia.

Tabla 12: Ejemplo planilla de registro de evento.

Fecha de Inicio del Evento	Fecha de Descubrimiento	Cuantificación (\$ Pesos)	Clasificación del evento	Producto o servicio afectado	Proceso	Perdida no cuantificable	Descripción del Evento
12/11/2013	28/11/2013	490.000	Incidencias en el negocio y fallos en los sistemas	Cuenta corriente banca en línea	Proceso de seguridad en línea		Pérdida resultante de falla en sistema de telecomunicaciones

Fuente: Elaboración Propia.

Etapa 5: Diseño de la Matriz de Riesgo Operacional.

CARACTERIZACIÓN DE CAUSAS, EFECTOS Y CONTROLES:

El proceso de identificación de eventos de riesgo operativo genera información útil para lograr establecer cómo estos eventos afectan a cada proceso, lo que a su vez permite una adecuada identificación de las causas que ocasionaron el evento en cuestión, esta identificación se torna especialmente ventajosa cuando se requiere implementar acciones correctivas para evitar que se produzca el evento en un futuro.

La matriz de riesgo operativo clasificara cuantitativamente los eventos de acuerdo a su nivel de riesgo y exposición asociada, en donde el riesgo se encuentra en función de dos variables fundamentales la probabilidad de ocurrencia y el impacto o severidad. La probabilidad alude a la posibilidad matemática de que el evento ocurra, mientras que el impacto se presenta como el resultado potencial del acontecimiento, en otras palabras que sucedería o cómo afectaría a la entidad en términos monetarios si el evento se produjese.

Para determinar el nivel de probabilidad de un evento será necesario analizar el grado de repetición que dicho evento tiene, es decir cuántas veces ocurre el evento específico en un intervalo de tiempo determinado. Para aquello es vital recurrir al análisis de la base de datos anteriormente diseñada o a las fuentes de información consideradas validas presentadas en esta investigación.

Por otro la cuantificación del impacto se reflejara por medio del nivel de pérdida económica que trae como consecuencia que el evento se materialice.

De este modo definiremos el riesgo en función de la probabilidad y el impacto con la siguiente formula.

$$\text{Riesgo} = \text{Probabilidad} * \text{Impacto}$$

ELEMENTOS DE LA MATRIZ DE RIESGOS.

Esta etapa consiste en establecer los niveles de impacto y probabilidad de las pérdidas producidas por cada evento de riesgo operacional.

1. CUANTIFICACIÓN DEL IMPACTO:

Como se ha mencionado anteriormente en este ítem se considera la magnitud del evento una vez ocurrido este, para esta etapa se confeccionará una tabla de medición del impacto, la cual determina los niveles o categorías de impacto de acuerdo a lo que define la organización, por lo tanto se entiende que la tabla puede variar dependiendo de las necesidades de la entidad, para este modelo se estableció fraccionar los niveles de impacto en 5 grandes grupos enumerados a continuación.

Tabla 13: Niveles de impacto y características.

Puntuación	Impacto económico	Reacción de los medios de comunicación	Acciones del Regulador
Insignificante	Bajo, Perjuicios tolerables	No hay divulgación del evento	No interviene
Menor	Medio, pérdida financiera media	Divulgación de carácter menor por internet y medios mínimos	Comentarios adversos pero no interviene
Moderado	Alta pérdida financiera	Artículos en prensa, televisión, internet, alta divulgación por un día máximo	Acciones por parte del regulador que pueden incluir multas
Mayor	Pérdida financiera grave	Reportaje en múltiples medios y noticiarios en TV nacional por más de un día	Multas Medianas
Masivo	Pérdida que pone en riesgo la continuidad del negocio.	Repercusiones gubernamentales a nivel político y pérdida de confianza del público.	Multas significativas

Fuente: Elaboración propia a partir de Palma, (2011).

CARACTERIZACIÓN DE LOS NIVELES DE IMPACTO

Insignificante:

En este caso el evento se caracteriza por afectar de manera leve a la institución, este suceso no altera la continuidad del negocio, se puede señalar que este tipo eventos conforman la gran parte de la matriz de riesgos. Dentro de sus características principales tenemos que presentan pérdidas en términos económicos tolerables, su impacto mediático es casi nulo y no existe involucramiento de entidades regulatorias por estos acontecimientos.

Menor:

En este nivel es posible encontrar un ligero grado de deterioro en el proceso que involucra al evento, la pérdida económica es perceptible para quienes intervienen en el proceso y al igual que para la categoría anterior, existe un alto número de eventos asociados a este nivel de impacto, la pérdida económica es de carácter medio, el impacto mediático leve y el nivel de intervención de agentes reguladores es a través de comentarios negativos sin llegar a multas o sanciones.

Moderado:

En esta categoría el evento pone en riesgo el funcionamiento del proceso en donde se origina el suceso, la pérdida económica es de carácter considerable y a diferencia de los grupos anteriores este tipo de eventos se presentan con una menor frecuencia. En resumen este tipo de eventos es considerado inusual, su nivel de pérdida es considerable, existe una divulgación mediática importante por un periodo leve de tiempo y además la entidad o entidades reguladoras pueden realizar acciones que involucren multas económicas.

Mayor:

Los eventos que pertenecen a este grupo ponen en riesgo la continuidad del negocio en un mediano plazo, la pérdida económica es cuantiosa o grave, el proceso se puede ver altamente afectado, el impacto mediático es fuerte y se prolonga en el tiempo existiendo además multas medianas por parte de las entidades reguladoras.

Masivo:

En este tipo de eventos la pérdida económica es tan intensa que incluso puede llegar a una pérdida total de la institución, no existen muchos eventos en este grupo, pero sin lugar a dudas se deben considerar y vigilar. La pérdida económica pone en riesgo la continuidad del negocio de manera inmediata, en términos mediáticos se presentan repercusiones gubernamentales a nivel político y pérdida de confianza del público y las entidades reguladoras reaccionan con multas significativas.

ESTIMACIÓN DE BANDAS DE SEVERIDAD

Con la intención de estimar los niveles de impacto de forma general y objetiva para eventos de riesgo operacional es necesario confeccionar una banda de severidad utilizando como referencia herramientas como el estado de resultados y el balance general de la institución financiera. Para esto se utilizará información contable específicamente el patrimonio y el ingreso operacional de la entidad de los últimos tres años, siendo el promedio de estos el dato con el cual se estimaran las bandas de severidad para el cálculo de los niveles de impacto.

Tabla 14: Niveles de Patrimonio e Ingreso.

Institución	Año N-2	Año N-1	Año Actual (N)	Promedio
Patrimonio	30000000	35000000	36000000	33666666,7
Ingresos Operacionales	40000000	47000000	48700000	45233333,3
0,1% Patrimonio	40000	47000	48700	45233,3333
5% Patrimonio	2000000	2350000	2435000	2261666,67
50% Patrimonio	20000000	23500000	24350000	22616666,7

Fuente: Elaboración propia a partir de (Vizuet, 2009)

Tabla 15: Niveles de Severidad

Categoría	Rango de la Pérdida
Insignificante	0,1% Patrimonio Promedio
Menor	5% Patrimonio Promedio
Moderado	15% Ingreso Operacional Promedio
Mayor	50% Patrimonio Promedio
Masivo	100% Patrimonio Promedio

Fuente: Elaboración propia a partir de (Vizuet, 2009)

Tabla 16: Ejemplo rangos establecidos.

categoría de Impacto	Rangos Establecidos	Límite Inferior	Limite Superior
Insignificante	0.1%	\$ 0	\$ 33.667
Menor	5%	\$ 33.667	\$ 1.683.333
Moderado	15% (RO)	\$ 1.683.333	\$ 6.785.000
Mayor	50%	\$ 6.785.000	\$ 16.833.333
Masivo	>50%	\$ 16.833.333	Mayor

Fuente: Elaboración propia a partir de (Vizuet, 2009)

2. CUANTIFICACIÓN DE LA PROBABILIDAD.

Este elemento considera la frecuencia con la que el evento por riesgo operacional se hace efectiva, en otras palabras cuantas veces ocurre el evento en un determinado intervalo de tiempo. De la misma manera que el impacto se debe elaborar una tabla que se encargue de agrupar los niveles de probabilidad de ocurrencia de los eventos de riesgo operacional.

El intervalo de tiempo estándar para la cuantificación de eventos por riesgo operacional corresponde a un año. La ventaja de este periodo de evaluación radica en que bajo este mismo intervalo de tiempo se confeccionan importantes documentos de evaluación como lo son el balance general y el estado de resultados. Además se establece como periodo mínimo de tiempo de análisis el valor de un día de operaciones.

La función de probabilidad se denota de la siguiente manera:

$$\text{Probabilidad de ocurrencia} = \frac{\text{Número de Eventos registrados anualmente}}{\text{Número Posible de Eventos}}$$

A cada nivel se le otorgara además una cuantificación en términos de tiempo el cual se presenta en la siguiente tabla.

Tabla 17: categorías de probabilidad.

Categoría	Probabilidad de ocurrencia	Frecuencia cuantitativa
1. Anormal.	Insignificante sucede sólo en escenarios excepcionales	Una vez cada 10 años o menos.
2. Remota.	Podría ocurrir alguna vez	Una vez cada 4 años
3. Frecuente.	Debería ocurrir alguna vez	Una cada año
4. Viable.	Probablemente ocurra una vez	Semestralmente
5. Esperada	Ocurrirá en muchas circunstancias	Puede presentarse de manera diaria

Elaboración: propia a partir de (Palma, 2011)

Para el cálculo matemático de la probabilidad de ocurrencia convendremos que un año equivale a 365 días, así por ejemplo para el cálculo en términos porcentuales de la categoría anormal, tenemos un evento dividido por la cantidad de días equivalentes a diez años obteniéndose:

Numero de evento registrado de acuerdo a los rangos establecidos, dividido número de eventos posibles dentro del rango.

$$\frac{1}{3650} = 0,03\%$$

Bajo esta fórmula se establecerán los porcentajes de ocurrencia de cada categoría.

Tabla 18: limites porcentuales.

Categoría	Rango Cualitativo	Límite inferior	Límite superior
Anormal	Cada 10 años	0,00%	0,03%
Remota	Cada 4 años	0,03%	0,07%
Frecuente	Anualmente	0,07%	0,27%
Viable	Semestralmente	0,27%	0,55%
Esperada	Diariamente	0,55%	100,00%

Elaboración: propia a partir de (Vizuete, 2009)

3. ELABORACIÓN DE LA MATRIZ.

Una vez determinados y categorizados los niveles de impacto y probabilidad es posible combinar dichos elementos y así dar forma a la matriz de Impacto-Frecuencia o también conocida como mapa de riesgos, esta matriz revelará el nivel de riesgo al cual está expuesto la institución lo que presenta una ventaja pues gracias a la confección de este instrumento es posible priorizar criteriosamente cuales son los riesgos que requieren una mayor atención y recursos para su mitigación.

Figura N° 11: Matriz de Riesgos Operacionales.

Probabilidad			Impacto				
			1	2	3	4	5
			Insignificante	Menor	Moderado	Mayor	Masivo
			10	20	30	40	50
5	Esperada	25	250	500	750	1000	1250
4	Viable	20	200	400	600	800	1000
3	Frecuente	15	150	300	450	600	750
2	Remota	10	100	200	300	400	500
1	Anormal	5	50	100	150	200	250

Fuente: Elaboración Propia a partir de (González, 2007)

Tabla 19: Categoría por puntaje.

Zona de Riesgo		Puntaje		Acción
		Mínimo	Máximo	
E	Riesgo Extremo	801	Mayor	Requiere acción inmediata
A	Riesgo Alto	601	800	Requiere atención de la alta gerencia
M	Riesgo Medio	401	600	Requiere especificación de responsabilidad gerencial
B	Riesgo Bajo	201	400	Administrar mediante procedimientos de rutina
I	Riesgo Inusual	50	200	Administrar mediante registro

Fuente: Elaboración Propia a partir de (González, 2007)

Una vez obtenida la información resultante de la matriz, se procede a clasificar el riesgo operativo posicionándolo en uno de los cinco niveles entregados en la tabla anterior considerando además que:

CLASIFICACIÓN DE TIPO DE RIESGO

Riesgo Extremo:

Corresponde a un riesgos operativos extremos, expresados con la letra E y el color rojo, los eventos de este tipo se caracterizan por poseer un alto impacto y además la probabilidad de que ocurra es a lo menos frecuente.

Riesgo Alto:

Corresponde al nivel de riesgo operativos altos, expresados con la letra A y el color naranja, poseen de igual manera alta probabilidad y alto impacto sin embargo en una escala menor que los riesgos extremos.

Riesgo Medio:

Corresponden a riesgos operativos medios, representados con la letra M y el color amarillo, para este tipo de riesgos existe un alto impacto y baja probabilidad de ocurrencia o una alta probabilidad de ocurrencia pero un bajo impacto en términos económicos.

Riesgo Bajo:

Corresponden a los riesgos operativos bajos, representados por la letra B y el color verde su característica es que poseen una baja probabilidad y a su vez un bajo impacto.

Riesgo Inusual:

Corresponden a los riesgos operativos inusuales, representados por la letra I y el color azul, se caracterizan por poseer los mínimos impactos y probabilidades posibles.

RIESGO INHERENTE

La integración de los elementos probabilidad de ocurrencia e impacto bajo el supuesto de la inexistencia de todo tipo de controles proporciona en consecuencia una matriz de riesgo inherente, es decir en la organización no se realiza ningún tipo de tarea con el objetivo de disminuir el riesgo al cual está expuesta por el solo hecho de operar. Este riesgo inherente en consecuencia, puede ser visto como un punto de partida, que se presenta en términos de riesgo en el negocio bancario y es útil para conocer la calidad y eficacia de los controles una vez implementados.

El riesgo inherente se encuentra inserto en toda actividad, pues surge de la exposición y la incertidumbre de posibles eventos o cambios impredecibles de los escenarios actuales del negocio y su entorno, este riesgo no se puede eliminar del todo sin embargo la identificación de este permitirá una mejor gestión para mitigarlos.

Por otro lado la exposición al riesgo se puede definir como el grado de riesgo que se asume en cierta posición una vez realizadas acciones de control para mitigar el riesgo. Por tanto se entiende que al no existir control el nivel de exposición será equivalente al nivel de riesgo como se expresa en la siguiente ecuación.

Exposición = Riesgo - Control

Además es posible señalar que el grado de exposición es inverso a la efectividad de los controles y mitigantes que se mantienen ante un determinado riesgo, es decir entre más controles tenga sobre un riesgo, más disminuye la exposición a sufrir una pérdida.

EXPOSICIÓN: el grado de exposición es una función inversa de los controles y mitigantes que se defina para cada riesgo, como se detallan en la tabla.

Tabla 20: grado de exposición.

Puntuación	Exposición
1	Menor
2	Limitada
3	Media
4	Significativa
5	Mayor

Fuente: Elaboración: propia a partir de (Palma, 2011)

Tabla 21: caracterización de los niveles de exposición.

Puntuación	Existencia de procedimientos	Controles	Planes de mitigación de riesgos
Menor	Procedimientos de carácter exhaustivo correctamente actualizados diariamente	Roles detallados Controles automáticos	De ocurrir el riesgo es posible continuar con el negocio al existir transferencia de riesgos a terceros.
Limitada	Procedimientos que priorizan la cobertura de las áreas principales y actualizados mensualmente	Roles claros Mayoría de responsabilidades definidas Gran parte son automáticos y preventivos	Existencia de planes de contingencia, casi todo el riesgo se ha transmitido a un tercero.
Media	Procedimientos únicamente para áreas vitales, actualizaciones periódicas	La mayoría de roles definidos Algunos controles automáticos otros manuales Pocos controles preventivos	El riesgo ha sido parcialmente transferido a un tercero
Significativa	Escasez de procedimientos sin actualizaciones	Lo que existen son acciones correctivas de largo plazo. La mayoría de controles son manuales	No es posible continuar con las operaciones, pues tan solo una pequeña parte de los riesgos han sido transferidos
Mayor	Procedimientos mínimos o nulos, ausencia de actualizaciones	No existe definición de roles, controles ni de responsabilidades	No existe transferencia de riesgo alguno, No existe plan de contingencia,

Fuente: Elaboración: propia a partir de (Palma, 2011)

Etapa 6: Diseño de Controles.

CONTROL ACCIONES Y EFECTIVIDAD:

Luego de identificar los riesgos se deben analizar los tipos de controles adecuados para cada riesgo y posteriormente estimar que tan efectivos son estos al ser aplicados. Las características elementales que debe poseer un control para cumplir de buena forma su cometido son:

- ✓ *Debe permitir medir el nivel de logro de los objetivos planteados.*
- ✓ *Debe apoyar a la medición y cuantificación de los resultados.*
- ✓ *Debe identificar diferencias si existiesen entre el objetivo esperado y el resultado real.*
- ✓ *Debe apoyar la generación de medidas correctivas ya sea previniendo o componiendo fallas.*
- ✓ *Por naturaleza debe ser un proceso cíclico.*

El diseño eficaz de un sistema de control radica en primera instancia en el principio del autocontrol el cual establece métodos participativos al interior de la organización, buscando implementar un entorno de integridad y eficiencia de acuerdo a la propia ejecución y desarrollo del sistema de control, esto conlleva a ser conscientes de sus propios procesos y actuar conforme a ellos, lo que permite detectar las eventuales desviaciones y hacer los correctivos correspondientes. Esta característica se alinea eficazmente con la necesidad del sistema de establecer responsables por cada proceso haciendo más viable la implementación de los controles. En el marco de la autogestión cada responsable deberá hacerse cargo de diferentes tareas para asegurar el correcto funcionamiento de los procesos así dentro de las principales tareas por responsable se pueden mencionar:

- ✓ *Generar un ambiente de control eficiente para gestionar la frecuencia e impacto del riesgo que compete a sus funciones y responsabilidades.*
- ✓ *Suministrar y comunicar información relativa a la efectividad de los controles al responsable del riesgo y a otros interesados.*
- ✓ *Recoger y analizar información relacionada a la efectividad de los controles, y su conversión en información indicativa.*
- ✓ *Generar e implementar las acciones correctivas necesarias en virtud de la información recolectada.*
- ✓ *Reportar a las instancias establecidas las debilidades o interrupciones de los controles en los plazos adecuados.*

Por otro lado es necesaria, además, la utilización de indicadores de gestión que permitan establecer parámetros cuantificables en relación al funcionamiento adecuado de los controles y estimar si estos están alineados correctamente con los objetivos propuestos por la organización.

Una herramienta efectiva para este objetivo corresponde al indicador KRI indicadores claves de riesgo por sus siglas en inglés, estos indicadores pueden ser de carácter tanto cualitativo como cuantitativo, para la gestión de riesgo operacional se presentan indicadores de ambas naturalezas. Algunas de las ventajas de la utilización de esta herramienta son:

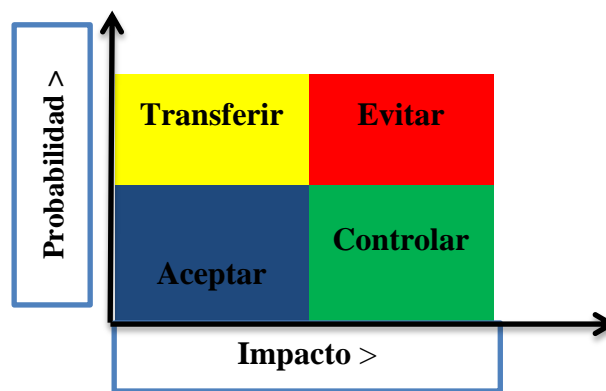
- ✓ *Establecer niveles de riesgo actuales, a través de medidas precisas del estado de un riesgo identificado y la efectividad para su control.*
- ✓ *Útiles para el control del RO, permitiendo acciones preventivas o que minimicen pérdidas materiales al posibilitar una acción temprana.*
- ✓ *Posibilitan detectar tendencias y cambios en el nivel de riesgo*
- ✓ *Ofrecen señales de alerta temprana al hacer resaltar los cambios en el entorno, eficiencia de los controles y exposición a riesgos potenciales antes que se materialicen.*

Los KRI son una métrica que proporciona información sobre el nivel de exposición a un riesgo operacional específico en el que se encuentra en la institución dado un intervalo de tiempo. Al analizar estos evolutivamente se logra conocer de manera temprana el comportamiento de los riesgos, los KRI contribuyen a la gestión de control de riesgos implantando rangos de tolerancia a los riesgos, estos umbrales deben ser establecidos por la alta gerencia de riesgos, para efectos de este modelo de gestión de riesgo operativo, tanto los responsables, como los indicadores se dividirán por área de negocio. Algunos de los indicadores que son posibles de elaborar para el seguimiento del comportamiento del riesgo operacional en la entidad se presentaran en la etapa que corresponde a la fase de monitoreo del sistema de administración de riesgo operacional.

ACCIONES DE CONTROL

En esencia las acciones de control van a depender de las características de evento variando desde el nivel de evento extremo determinado anteriormente hasta el nivel de riesgo insignificante. Es importante recalcar que la principal función de un elemento de control de riesgo es la mitigación o eliminación de este, en otras palabras un elemento de control es considerado efectivo, cuando disminuye los niveles de exposición al riesgo que se está intentando controlar. Así las principales cuatro acciones a realizar se muestran en la siguiente figura:

Figura N 12: acciones de control.



Fuente: Elaboración propia.

La figura presenta la orientación a seguir de acciones de control en base a los niveles de impacto y probabilidad que el evento de riesgo posee.

En esta etapa se debe decidir en torno a las acciones para minimizar los riesgos operacionales, obteniendo el valor del riesgo neto cifra que corresponde al riesgo residual, este valor es la resultante de la diferencia entre el riesgo inherente del evento y el control realizado.

Las posibles acciones en esta etapa corresponden a las siguientes:

- ✓ *Evitar.*
- ✓ *Controlar, Reducir Probabilidad.*
- ✓ *Controlar, Reducir Impacto.*
- ✓ *Transferir.*
- ✓ *Asumir.*

DESCRIPCIÓN DE ACCIONES

Evitar riesgo:

Para este caso se considera que el evento de riesgo no es aceptado por la entidad, por lo tanto este necesariamente se debe eliminar, para esto se analiza el proceso que originó el evento de riesgo y se elimina, una vez anulado el proceso por consecuencia se elimina el riesgo, esta acción no debe de ser abusada ya que si bien es simple de implementar puede traducirse en falta de competitividad.

Controlar, Reducir Probabilidad:

En este caso se reconoce la existencia de un riesgo y se opta por disminuir los niveles de frecuencia del evento de riesgo, para esto se hace uso de los controles los cuales se generan por medio de un plan de acción.

El plan de acción debe ser formalizado por medio de un documento elaborado por el responsable del proceso que origina el evento de riesgo, debiendo obligatoriamente ser aprobado por la gerencia de riesgo de la entidad. En este documento se presentan las tareas específicas a llevar a cabo para minimizar el riesgo, por medio de la disminución de la frecuencia del evento, además se determina de quienes depende implementar las tareas y se estiman los plazos para realizar el plan de acción y por último se señala quien será el encargado de hacer el seguimiento correspondiente, tarea que generalmente deberá llevar a cabo el departamento o gerencia de riesgo operacional.

Controlar, Reducir Impacto:

En este caso el evento de riesgo posee altos niveles de exposición, dichos niveles superan los límites que la entidad está dispuesta a asumir por tanto la tarea de los responsables radica en generar procedimientos que limiten el grado de impacto del evento, a un nivel el cual la compañía esté dispuesto a asumir, para esto es necesario desarrollo de metodologías y planes de acción de equivalentes características en términos de requisitos que los planes para reducir probabilidad, con la diferencia que los nuevos planes se concentraran en disminuir el impacto del evento a un nivel en el cual la entidad se sienta cómoda.

Transferir Riesgo:

Esta acción comprende transferir las repercusiones negativas del evento por riesgo operacional de manera completa o parcial a una institución aseguradora que esté dispuesta a asumir el riesgo.

Asumir:

Se puede considerar como la acción más simple y común para enfrentar los riesgos, esta actividad es válida cuando las pérdidas no son muy significativas, el umbral de decisión para asumir el riesgo o por el contrario realizar otra actividad mitigadora, tiene directa relación con la situación financiera y patrimonial de la entidad bancaria.

Eficiencia del control:

Esta medida establece si el control cumple o no el objetivo para el cual fue diseñado, su rango de eficiencia posee dos variables a seleccionar.

- a. **Satisfactorio:** El control efectivamente cumple su objetivo disminuyendo los niveles de riesgo.
- b. **Insatisfactorio:** El control no cumple con su objetivo, los niveles de riesgo continúan siendo los mismos o la disminución del riesgo es insignificante.

Categoría del Control:

En este ítem se establece la naturaleza del control, esta puede ser de tres tipos, los cuales a su vez se pueden realizar tanto de manera manual como de forma automatizada, a continuación se presenta la definición de cada una de las categorías:

Tabla 22: Categorías de Control

Categoría	Definición	Ejemplos
Preventivo	Anticipan eventos de riesgo antes de suceder.	Manual de Organización y Funciones. Indicadores y normas de desempeño. Cuadro de responsables. Políticas y procedimientos.
Detectivos	Identifican eventos en el momento de presentarse	Auditoría. Conciliación.
Correctivos	Aseguran tomar acciones para revertir un evento no desea	Atribuciones de corrección y aplicación de ajustes en procesos de riesgo operacional.

Elaboración: propia a partir de (Vizquete, 2009)

Periodicidad del Control:

Determina el grado de frecuencia con que se efectúa el control puede ser diario, semanal, mensual, trimestral o anual dependiendo de las características del evento que se esté midiendo.

De acuerdo a las características relativas al nivel de riesgo inherente que del evento presenta, será posible estimar los niveles de periodicidad de los controles según la siguiente tabla:

Tabla 23: Periodicidad en controles.

Nivel de riesgo inherente	Prioridad	Descripción
Alto	1	Revisión de carácter mensual
Medio	2	Revisión de carácter semestral
Bajo	3	Revisión de carácter Anual

Elaboración: propia a partir de (Vizuete, 2009)

Riesgo residual:

Para cuantificar la eficacia de los controles es necesario entender el concepto de riesgo residual, este riesgo corresponde al resultante del nivel de riesgo una vez aplicados los controles, puede entenderse también como el nivel de exposición de la entidad en relación al riesgo que no es posible de eliminar del todo, en cuanto más efectivos sean los controles obtendremos un nivel de riesgo residual menor.

$\text{Riesgo Residual} = \text{Riesgo Inherente} - \text{Controles Efectivos}$

Etapa 7: Sistema de Monitoreo.

El monitoreo es una etapa fundamental para la adecuada administración del riesgo y por consecuencia lo es también para la administración del riesgo operacional, en esta fase del modelo de gestión se realizan los seguimientos a los planes de acción, planes de contingencia, así como el nivel de cumplimiento de los controles aplicados y el resultado de los indicadores estadísticos.

En palabras simples el objetivo fundamental de esta etapa es determinar si los planes acción, herramientas, controles y estrategias establecidas están funcionando correctamente.

Siendo esta etapa la última del ciclo de administración del riesgo, se considera adecuado recordar que debido a la naturaleza cíclica del modelo de gestión, dichas etapas deben necesariamente repartirse continuamente, pues es esta iteración constante la que permite asegurar la vigencia del modelo y además exhibe en el caso que existiesen las insuficiencias del sistema, lo cual lógicamente obliga a la mejora del mismo por medio de la adaptación y perfeccionamiento del modelo de gestión de riesgo operacional.

Es necesario establecer que dicho seguimiento se debe realizar con prioridad al igual como se presentaron la prioridad del establecimiento de controles, para el caso del seguimiento y monitoreo se persigue la misma lógica. Así los eventos que posean características de alta frecuencia e impacto, puesto que son estos eventos los que tienen un mayor potencial de convertirse en pérdidas importantes para la institución bancaria.

Tabla 24: Nivel de priorización.

Nivel de riesgo inherente	Prioridad	Descripción
Alto	1	Alto nivel de seguimiento
Medio	2	Nivel de seguimiento medio
Bajo	3	Bajo nivel de seguimiento

Elaboración: propia a partir de (Vizuete, 2009)

DISEÑO DE INDICADORES CLAVES DE RIESGO, KRI.

Como se precisó anteriormente los KRI corresponden a indicadores claves de gestión de riesgo, para efectos de esta investigación dichos indicadores se confeccionarán bajo la necesidad de monitorear la gestión del riesgo operacional y de establecer medidas que comparen la efectividad de los controles realizados en distintos periodos de tiempo, además se presenta la posibilidad de establecer rangos de tolerancia a los riesgos operacionales lo que se traducirá en menores tiempos de respuesta para los casos en que se requiera acciones inmediatas.

El diseño de los KRI's básicos para la realización de monitoreo de los riesgos, comprende indicadores con características de análisis de tipo vertical y horizontal, estos estudios permitirán evaluar y distinguir diferencias entre dos periodos de tiempo.

Algunos de los principales indicadores se muestran a continuación:

- ✓ *Indicadores de desviaciones por periodo:*

$$\frac{(Total\ eventos\ Año\ N - Total\ eventos\ Año\ N-1)}{Total\ eventos\ Año\ N-1} * 100$$

$$\frac{(Total\ pérdidas\ Año\ N - Total\ pérdidas\ Año\ N-1)}{Total\ pérdidas\ Año\ N-1} * 100$$

Estos indicadores además se extenderán a variaciones agrupadas por origen del evento, mostrando las diferencias porcentuales de estos en diferentes periodos de tiempo, por tanto se extiende el análisis horizontal para variaciones de frecuencia e impacto (pérdidas económicas) para las siguientes variables:

- ✓ *Fraude Interno*
- ✓ *Fraude Externo*
- ✓ *Relaciones Laborales y seguridad en el puesto de trabajo*
- ✓ *Incidencias en el negocio y fallos en los sistemas*
- ✓ *Daños a activos materiales.*
- ✓ *Clientes, productos y prácticas empresariales.*
- ✓ *Ejecución, entrega y gestión de procesos.*
- ✓ *Código de evento individualizado.*

Además del análisis horizontal se entregan indicadores de análisis de tipo vertical, con el objetivo de identificar los pesos relativos de los eventos y frecuencias de los factores de eventos y los eventos individuales.

$$\frac{Pérdida\ atribuida\ a\ evento\ individual}{Total\ de\ pérdidas} * 100$$

$$\frac{\text{Numero de eventos individual}}{\text{Total de eventos}} * 100$$

Para establecer los pesos por factor de riesgo se confeccionará una tabla con la siguiente información:

Tabla 25: pesos relativos de impacto.

Factor	Pérdida económica	Peso porcentual (%)
Fraude Interno		
Fraude Externo		
Relaciones Laborales y seguridad en el puesto de trabajo		
Incidencias en el negocio y fallos en los sistemas		
Daños a activos materiales.		
Clientes, productos y prácticas empresariales.		
Ejecución, entrega y gestión de procesos.		
Fraude Interno		
Total		

Fuente: Elaboración propia a partir de CRS Consulting Ltda.

Se puede observar que las pérdidas están separadas según la categoría principal de la clasificación de eventos de riesgo operacional, en donde además el peso porcentual corresponde a la pérdida económica del factor dividido el total de pérdidas económicas del periodo multiplicado por cien.

Continuamos con los pesos relativos por factor y evento.

Tabla 26: pesos relativos de frecuencia.

Factor	Numero de eventos	Peso porcentual (%)
<i>Fraude Interno</i>		
<i>Fraude Externo</i>		
<i>Relaciones Laborales y seguridad en el puesto de trabajo</i>		
<i>Incidencias en el negocio y fallos en los sistemas</i>		
<i>Daños a activos materiales.</i>		
<i>Clientes, productos y prácticas empresariales.</i>		
<i>Ejecución, entrega y gestión de procesos.</i>		
<i>Fraude Interno</i>		
Total		

Fuente: Elaboración propia a partir de CRS Consulting Ltda.

Se puede observar que la tabla sigue un comportamiento similar a la tabla de impactos, a diferencia que la variable a analizar en esta etapa corresponde a la frecuencia de los eventos.

Las frecuencias están separadas igualmente según la categoría principal de la clasificación de eventos de riesgo operacional, en donde además el peso porcentual corresponde a la frecuencia (número de eventos ocurridos en el periodo de análisis) del factor dividido el total de frecuencias del periodo multiplicado por cien.

Tabla 27: Pesos relativos por tipo de riesgo.

Tipo de riesgo	Numero de eventos	Peso porcentual (%)
Riesgo Extremo		
Riesgo Alto		
Riesgo Medio		
Riesgo Bajo		
Riesgo Inusual		
Total		

Fuente: Elaboración propia a partir de CRS Consulting Ltda.

Para la elaboración de estos indicadores de riesgo se persigue la misma lógica que las dos tablas anteriores, esta vez analizando los tipos de riesgos que enfrenta la entidad de acuerdo a la categorización entregada en este capítulo, de igual manera es importante identificar los pesos relativos de los riesgos bajo la misma metodología usada en las tablas anteriores.

Finalizando se entregan indicadores complementarios, entendiendo que estos ayudaran a la gestión de riesgos operacionales debido a nivel de relación existente entre estos ratios y la generación de pérdidas económicas atribuibles a eventos operacionales.

- ✓ *Diferencia porcentual del número de quejas de clientes entre dos periodos.*
- ✓ *Diferencia porcentual del número de multas de entidades reguladoras.*
- ✓ *Diferencia porcentual del número de instancias de caídas de sistemas.*
- ✓ *Ratio de personal temporal versus personal permanente.*

Tabla 28: Seguimiento de riesgos por evento individual

Código del Evento	Probabilidad	Ponderación Probabilidad	Impacto	Ponderación Impacto	Producto o servicio afectado	Calificación del Riesgo

Fuente: Elaboración propia a partir de CRS Consulting Ltda.

Para terminar esta etapa se presenta el formato para el seguimiento de los riesgos según su línea de negocio y categoría de evento, en esta matriz se deberá integrar las estimaciones de porcentaje y frecuencia porcentual y además la categoría del tipo de riesgo y su color asociado de acuerdo a la tabla N° 19.

Tabla 29; Integración de riesgos por línea de negocios y tipo de evento.

Tipo De Evento (I)	Línea De Negocios (J)								Total
	Finanzas corporativas	Negociación y ventas	Banca minorista	Banca comercial	Pagos y liquidación	Servicios de agencia	Administración de activos	Intermediación minorista	
Fraude Interno	Frecuencia Impacto Riesgo Color	Frecuencia Impacto Riesgo Color	Frecuencia Impacto Riesgo Color	Frecuencia Impacto Riesgo Color	Frecuencia Impacto Riesgo Color	Frecuencia Impacto Riesgo Color	Frecuencia Impacto Riesgo Color	Frecuencia Impacto Riesgo Color	
Fraude Externo	Frecuencia Impacto Riesgo Color	Frecuencia Impacto Riesgo Color	Frecuencia Impacto Riesgo Color	Frecuencia Impacto Riesgo Color	Frecuencia Impacto Riesgo Color	Frecuencia Impacto Riesgo Color	Frecuencia Impacto Riesgo Color	Frecuencia Impacto Riesgo Color	
Incidencias en el negocio y fallos en los sistemas	Frecuencia Impacto Riesgo Color	Frecuencia Impacto Riesgo Color	Frecuencia Impacto Riesgo Color	Frecuencia Impacto Riesgo Color	Frecuencia Impacto Riesgo Color	Frecuencia Impacto Riesgo Color	Frecuencia Impacto Riesgo Color	Frecuencia Impacto Riesgo Color	
Clientes, productos y prácticas empresariales.	Frecuencia Impacto Riesgo Color	Frecuencia Impacto Riesgo Color	Frecuencia Impacto Riesgo Color	Frecuencia Impacto Riesgo Color	Frecuencia Impacto Riesgo Color	Frecuencia Impacto Riesgo Color	Frecuencia Impacto Riesgo Color	Frecuencia Impacto Riesgo Color	
Fraude Interno	Frecuencia Impacto Riesgo Color	Frecuencia Impacto Riesgo Color	Frecuencia Impacto Riesgo Color	Frecuencia Impacto Riesgo Color	Frecuencia Impacto Riesgo Color	Frecuencia Impacto Riesgo Color	Frecuencia Impacto Riesgo Color	Frecuencia Impacto Riesgo Color	
Total									

Fuente: Elaboración Propia a partir de BCBS

CAPÍTULO IV: RESULTADOS APLICACIÓN DE METODOLOGÍAS.

El presente capítulo exhibe los resultados de la aplicación de las metodologías de estimación de capital económico para cubrir las pérdidas atribuidas a riesgos operacionales. Como se mencionó en el segundo capítulo de esta investigación se escogieron dos metodologías a implementar, en donde el principal factor de selección recae, en el nivel de información necesaria para realizar las estimaciones, puesto que para la mayoría de las metodologías es necesario información que no es posible obtener de manera pública.

De este modo se presentan los resultados de la estimación de capital económico mediante el método de indicador básico BIA y se entregan los resultados de las simulaciones para la estimación de capital económico por metodología avanzada, específicamente mediante el enfoque de distribución de perdidas agregadas LDA.

Método Indicador Básico

Recordando que este tipo de método se encuentra dentro del grupo de las metodologías menos avanzadas, estas están principalmente orientadas a estimaciones y cálculos en base a los ingresos que percibe la entidad financiera, las metodologías menos avanzadas poseen el común denominador de establecer valoraciones simples en donde se calcula por medio de un factor constante la cantidad requerida de capital económico para cubrir los riesgos operacionales dependiendo únicamente de sus niveles de ingresos como variable estimativa principal.

Específicamente BIA es considerada por el comité de Basilea como una aproximación adecuada para que las entidades, gradualmente integren de forma progresiva metodologías más avanzadas en su gestión del riesgo operacional.

Como se mencionó en capítulos anteriores, bajo esta metodología los bancos deben cubrir el riesgo operativo con un capital equivalente a la media de los tres últimos años de un porcentaje fijo (α) correspondiente el 15% de sus ingresos brutos anuales positivos.

Así el cargo de capital queda expresado mediante la siguiente ecuación.

$$KBIA = [\sum (GL\ 1\dots n * \alpha)] / n$$

Dónde:

KBIA = La exigencia de capital en el método estándar.

GL = Ingresos brutos anuales medios, cuando sean positivos, de los tres últimos años.

n = Número de años (últimos tres años), en que los resultados fueron positivos.

α =15%, parámetro establecido por el Comité, que relaciona el capital exigido al conjunto del sector con el nivel del indicador en el conjunto del sector.

El estudio de estimación de capital económico atribuible riesgos operacionales para la banca chilena, comprendió el análisis de los estados financieros de cada entidad para los años 2010, 2011 y 2012, los ingresos brutos determinados fueron estimados bajo la denominación de ingreso bruto entregada por la superintendencia que regula el sector bancario nacional.

Una vez que se estima el requerimiento de capital por riesgo operacional, mediante el método BIA, este debe ser convertidos a un “equivalente de activos ponderados por riesgo” multiplicándolos por 12,5 (recíproco del coeficiente de capital mínimo de 8% fijado por el Comité) esto según Basilea II, para el caso de Basilea III el activo ponderado por riesgo se multiplica por su recíproco 9,52381 en donde el requisito de índice mínimo se eleva al 10,5%, luego de estos se deben integrar los requisitos de este tipo de riesgos a las ecuaciones de capital regulatorio, dependiendo de la normativa establecida, para efectos de esta investigación dicho paso no se realizó debido a que la misma se centra únicamente en el requisito de riesgo operacional obviando los demás riesgos que pertenecen al índice.

✓ *Ecuación de Índice de Basilea II.*

$$\frac{\text{Capital Total}}{APR c + 12,5 * Kor + 12,5 * RM} \geq 8\%$$

✓ *Ecuación de Índice de Basilea III.*

$$\frac{\text{Capital Total}}{APR c + 9,52381 * Kor + 9,52381 * RM} \geq 10,5\%$$

A continuación se presentan los resultados obtenidos bajo la metodología BIA.

Tabla 30: Estimación de capital económico por riesgo operacional metodología BIA en Millones de Pesos.

Entidad	Utilidad neta de operaciones financieras	Utilidad (pérdida) de cambio neta	Resultado por inversiones en sociedades	Ingreso neto por intereses y reajustes	Ingreso neto por comisiones	Ingreso operacional bruto	Ingreso operacional promedio	Ingreso operacional con factor 15% BIA
Banco de Chile 2010	19452	63762	1926	769722	292262	1147124	1223073	183461
Banco de Chile 2011	26927	-7973	3300	871320	308773	1202347		
Banco de Chile 2012	24747	35136	-229	952838	307257	1319749		
Banco del Estado de Chile 2010	-41821	102540	768	524113	146518	732118	832218	124833
Banco del Estado de Chile 2011	106475	-31350	1449	610080	165234	851888		
Banco del Estado de Chile 2012	77230	15769	168	634594	184888	912649		
Banco Internacional 2010	2369	6765	15	19026	3985	32160	32588	4888
Banco Internacional 2011	15048	-3771	5	18943	4441	34666		
Banco Internacional 2012	8126	1944	7	17633	3229	30939		
Scotiabank Chile 2010	10726	26533	408	178214	39544	255425	253584	38038
Scotiabank Chile 2011	26801	-10726	548	186637	41633	244893		
Scotiabank Chile 2012	1094	29177	458	186848	42858	260435		
Banco de Crédito e Inversiones 2010	-36628	101845	7051	515724	148564	736556	808962	121344
Banco de Crédito e Inversiones 2011	131523	-66762	8482	555350	169271	797864		
Banco de Crédito e Inversiones 2012	37762	63268	6559	595183	189694	892466		
Corpbanca 2010	-9410	44611	296	224410	58221	318128	357093	53564
Corpbanca 2011	97745	-26783	250	193000	60362	324574		
Corpbanca 2012	54994	30696	367	256876	85644	428577		
Banco Bice 2010	14979	6223	97	53606	30414	105319	115180	17277
Banco Bice 2011	26681	-1948	111	56896	31054	112794		
Banco Bice 2012	34912	1919	108	59829	30658	127426		

Fuente: Elaboración propia a partir de los estados financieros entregados por la SBIF.

Entidad	Utilidad neta de operaciones financieras	Utilidad (pérdida) de cambio neta	Resultado por inversiones en sociedades	Ingreso neto por intereses y reajustes	Ingreso neto por comisiones	Ingreso operacional bruto	Ingreso operacional promedio	Ingreso operacional con factor 15% BIA
HSBC Bank (Chile) 2010	12615	4411	9	4182	2975	24192	21835	3275
HSBC Bank (Chile) 2011	10366	7914	6	3371	1306	22963		
HSBC Bank (Chile) 2012	-930	7482	10	10958	829	18349		
Banco Santander-Chile 2010	38755	57233	1171	939719	263582	1300460	1347602	202140
Banco Santander-Chile 2011	170857	-76660	2140	972300	277836	1346473		
Banco Santander-Chile 2012	-64079	146378	267	1042734	270572	1395872		
Banco Security 2010	28410	4241	154	56360	24723	113888	118977	17847
Banco Security 2011	29786	-5976	178	60350	27524	111862		
Banco Security 2012	29143	5497	118	67838	28584	131180		
Banco Falabella 2010	3080	2060	7	72389	9650	87186	107322	16098
Banco Falabella 2011	11031	-2893	10	89060	9862	107070		
Banco Falabella 2012	7666	1205	6	106706	12128	127711		
Deutsche Bank (Chile) 2010	30955	6684	7	-5143	-709	31794	19891	2984
Deutsche Bank (Chile) 2011	51742	-14425	5	-14162	-745	22415		
Deutsche Bank (Chile) 2012	18876	-1147	8	-11630	-644	5463		
Banco Ripley 2010	298	15	1	30922	7767	39003	39762	5964
Banco Ripley 2011	1006	10	0	29793	7793	38602		
Banco Ripley 2012	2160	-6	1	31438	8087	41680		
Rabobank Chile 2010	-9790	10917	0	13782	850	15759	18792	2819
Rabobank Chile 2011	2831	-10794	1	23599	1709	17346		
Rabobank Chile 2012	-4200	-1567	1	27990	1046	23270		

Fuente: Elaboración propia a partir de los estados financieros entregados por la SBIF.

Entidad	Utilidad neta de operaciones financieras	Utilidad (pérdida) de cambio neta	Resultado por inversiones en sociedades	Ingreso neto por intereses y reajustes	Ingreso neto por comisiones	Ingreso operacional bruto	Ingreso operacional promedio	Ingreso operacional con factor 15% BIA
Banco Consorcio 2010	-3435	7312	0	15530	415	19822	25717	3858
Banco Consorcio 2011	17389	-10470	0	19112	739	26770		
Banco Consorcio 2012	11655	4250	127	12518	2008	30558		
Banco Penta 2010	4932	2108	72	-1845	9611	14878	17916	2687
Banco Penta 2011	17385	-2397	83	-6624	8985	17432		
Banco Penta 2012	15926	3910	81	-7715	9237	21439		
Banco Paris 2010	66	-5	1	31071	5846	36979	30692	4604
Banco Paris 2011	270	8	0	25144	5030	30452		
Banco Paris 2012	121	-9	1	22371	2161	24645		
BBVA 2010	38904	21703	219	146789	67409	275024	277906	41686
BBVA 2011	84021	-25874	313	161832	57154	277446		
BBVA 2012	16791	60807	320	152777	50554	281249		
Banco Itaú Chile 2010	4747	23122	29	118062	32700	178660	190308	28546
Banco Itaú Chile 2011	-1913	5015	13	140832	34429	178376		
Banco Itaú Chile 2012	18347	15289	57	141677	38517	213887		

Fuente: Elaboración propia a partir de los estados financieros entregados por la SBIF.

Entidad	Utilidad neta de operaciones financieras	Utilidad (pérdida) de cambio neta	Resultado por inversiones en sociedades	Ingreso neto por intereses y reajustes	Ingreso neto por comisiones	Ingreso operacional bruto	Ingreso operacional promedio	Ingreso operacional con factor 15% BIA
Banco do Brasil S.A. 2010	1550	-1667	0	1060	239	1182	2059	309
Banco do Brasil S.A. 2011	-1662	2690	0	917	191	2136		
Banco do Brasil S.A. 2012	3279	-1637	0	1069	147	2858		
JP Morgan Chase Bank, N. A. 2010	24907	10476	9	868	-396	35864	29282	4392
JP Morgan Chase Bank, N. A. 2011	30671	1478	6	463	41	32659		
JP Morgan Chase Bank, N. A. 2012	12503	2654	8	3425	733	19323		
Banco de la Nación Argentina 2010	0	17	0	461	78	556	920	138
Banco de la Nación Argentina 2011	0	43	0	973	83	1099		
Banco de la Nación Argentina 2012	0	-15	0	1057	62	1104		
The Bank of Tokyo-Mitsubishi UFJ, LTD 2010	-355	1182		718	332	1877	2861	429
The Bank of Tokyo-Mitsubishi UFJ, LTD 2011	38	1273		1453	335	3099		
The Bank of Tokyo-Mitsubishi UFJ, LTD 2012	-475	1559		1935	588	3607		
DnBNor Bank Asa 2010	0	-10027	0	965	662	-8400	1311	197
DnBNor Bank Asa 2011	0	14013	0	3431	711	18155		
DnBNor Bank Asa 2012	0	-11405	0	4533	1049	-5823		

Fuente: Elaboración propia a partir de los estados financieros entregados por la SBIF.

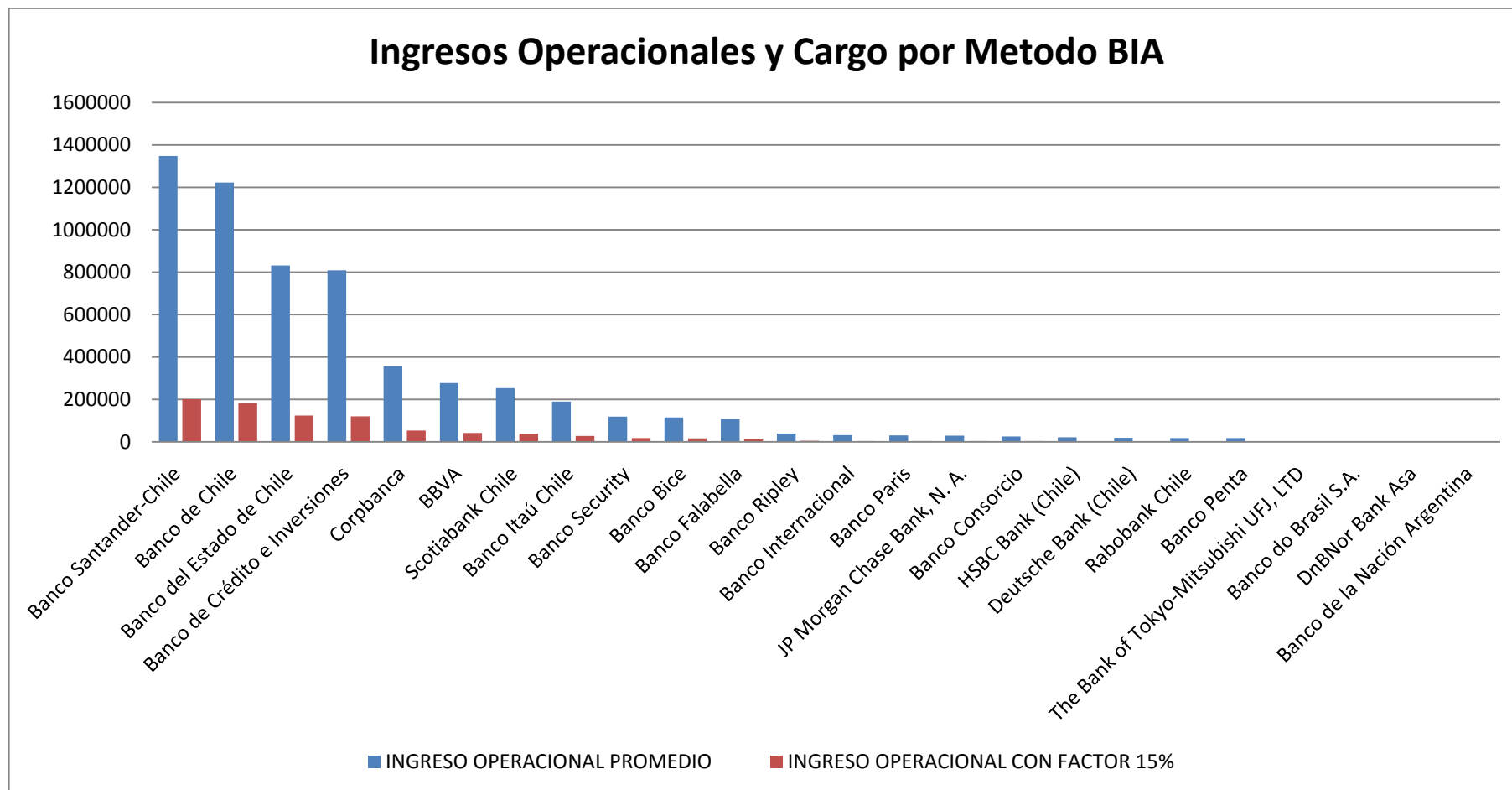
Gracias a tabla es posible observar que para la estimación del capital regulatorio mediante la metodología BIA, requiere como base el cálculo de los ingresos operacionales anuales netos de la entidad, estos se obtienen de cinco cuentas contables, siendo la más significativa la cuenta de ingresos neto por interés y reajustes, ya que es esta cuenta la que en la mayoría de las entidades, lidera en términos de cantidad de los ingresos obtenidos.

El valor final que posteriormente se multiplica por el factor del 15% es el resultante del promedio de los ingresos operacionales obtenidos para los tres años, y es este valor el cual posteriormente se debe agregar a la ecuación de índice de Basilea, junto con sus homónimos de riesgo de crédito y mercado.

Los resultados obtenidos por este método son estrictamente dependientes de la cantidad de ingresos que la entidad percibe, por lo tanto esta técnica de estimación se considera un tanto rígida producto de este hecho, además la utilización de esta metodología para estimar cargos de provisiones por riesgo operacional no promueven la adecuada gestión de este riesgo, pues independiente de que se realicen acciones que se orienten a la mitigación de los riesgos operacionales, estas no alteraran positivamente en una eventual disminución de las provisiones requeridas.

El gráfico a continuación presentado, exhibe en resumen los resultados obtenidos de la tabla anterior, mostrando los ingresos operacionales de cada entidad y resultado de la ponderación de estos por el factor del 15%. Como es posible observar las entidades que poseen un mayor grado de participación de mercado y en consecuencia mayores ingresos operacionales, son las entidades que deben responder con un mayor cargo de capital bajo este método, es así como vemos a las entidades que lideran el sector, como banco de Chile, banco Santander y banco del Estado de Chile, con una carga elevada de capital regulatorio versus entidades bancarias que menores niveles de ingresos como banco Do Brasil, DnBNor Bank Asa y banco de la Nación Argentina que en consecuencia a sus bajos ingresos poseen los menores cargos de capital bajo esta metodología

Grafico N° 1 : Ingresos operacionales de la banca chilena y cálculo de capital bajo metodología BIA.



Fuente: Elaboración propia a partir de estados financieros presentados por la SBIF.

En el gráfico se observan los valores de los ingresos operacionales promedios de los periodos antes señalados, luego se puede además observar el requisito de capital que corresponde bajo esta metodología a la ponderación del ingreso promedio por un factor del 15%.

La relación directa en cuanto a los ingresos obtenidos y el cargo de capital por riesgo operacional bajo esta técnica de cuantificación resulta un costo significativo para la entidad, que por lo demás no genera ningún tipo de incentivo al control de los riesgos operacionales puesto que la variable que determina el requerimiento económico tan solo hace énfasis en el volumen de ingresos y no en la eficiencia y calidad de los controles y administración del riesgo, aun así esta metodología puede presentar una primera mirada de autoevaluación en torno a los riesgos operacionales y sirve como punto de partida para acercarse a metodologías más flexibles y que se orienten en mayor medida a la administración efectiva del riesgo operativo.

Metodologías de Medición Avanzada

Siguiendo con un enfoque de los modelos AMA (Advanced Measurement Approach) y con el objetivo de establecer un sistema que realice los cálculos de los cargos de capital económico por riesgo operacional a través de técnicas avanzadas, se presenta una metodología que estima en relación a la situación particular de la entidad cuales debiesen ser sus requisitos de capital regulatorio para cubrir el riesgo operacional.

De los enfoques avanzados el que actualmente ha adquirido un mayor posicionamiento en la práctica corresponde al modelo loss distribution approach (LDA) representando un estándar en términos de estimaciones estadísticas de riesgo. Esta técnica ostenta las características necesarias para cumplir de manera adecuada el objetivo de generar estimaciones efectivas de cálculo de capital económico para cubrir las eventuales pérdidas derivadas de la operación de una entidad financiera.

El ejercicio de aplicación comprendió simular variables de frecuencia e impacto mediante el método de simulación de Montecarlo con cinco mil escenarios posibles, así se seleccionaron dos eventos con diferentes perfiles de riesgo y se calcularon sus respectivos valores en riesgo operativo, cifra que corresponde al percentil 99,9 de la distribución de pérdida de dicho riesgo.

Los parámetros de las distribuciones de probabilidad corresponden a los siguientes:

Tabla 31: Parámetros de simulación.

Línea de Negocio Evento		Banca Corporativa fraude Interno	Banca Minorista Ejecución y entrega de Procesos
Frecuencia	Distribución	Poisson	Poisson
	Parámetros	$\lambda = 10$	$\lambda = 100$
Severidad	Distribución	Weibull	Weibull
	Parámetros	$\alpha=0,75 \quad \beta= 80$	$\alpha=0,5 \quad \beta= 10$

Fuente: Elaboración propia a partir Jiménez et al (2008).

Los eventos de pérdida simulados sirven como un ejercicio práctico a la hora de entender cómo se debe gestionar el riesgo según metodologías avanzadas. Cabe destacar que la utilización de este tipo de técnicas debe ser aprobada por el ente supervisor en este caso la superintendencia de bancos e instituciones financieras.

Para efectos de este ejercicio se optó por simular datos aleatorios siguiendo distribuciones de probabilidad con los parámetros presentados en la tabla número 31, así para el ejercicio de la línea de negocios banca minorista, relacionados a eventos de tipo ejecución y entrega de procesos se trabajó con 6.750.000 datos en su totalidad y para el evento de fraude interno, dentro de la línea de negocio de la banca corporativa, se trabajó con 125.000 datos simulados, esta diferencia se atribuye al contraste de frecuencias representadas por el valor lambda, en donde la frecuencia del evento proveniente de la banca minorista excede diez veces al evento de la banca corporativa .

El ejercicio comprendió las estimaciones de las pérdidas máximas esperadas en el percentil 99,9% de la función de distribución obtenida. Los eventos seleccionados como ya se mencionó, fueron para línea de negocio banca corporativa, de la categoría de evento que corresponde al fraude interno y para la línea de negocio de la banca minorista el evento que comprende la categoría de ejecución, entrega y gestión de procesos.

Los resultados obtenidos de la simulación fueron los siguientes:

Tabla 32: Estadística descriptiva pérdidas.

Banca Corporativa Fraude Interno	
Error típico	7
Desviación estándar	494,77
Varianza de la muestra	244795,92
Curtosis	1,24
Coficiente de asimetría	0,99
Mínimo	0
Máximo	3691
Cuenta	5000
Pérdida Esperada	\$860.547
Var Op 95%	\$1.805.434
Var Op 99%	\$2.357.581
Var Op 99,9%	\$2.905.292

Fuente: Elaboración propia a partir de datos de la investigación.

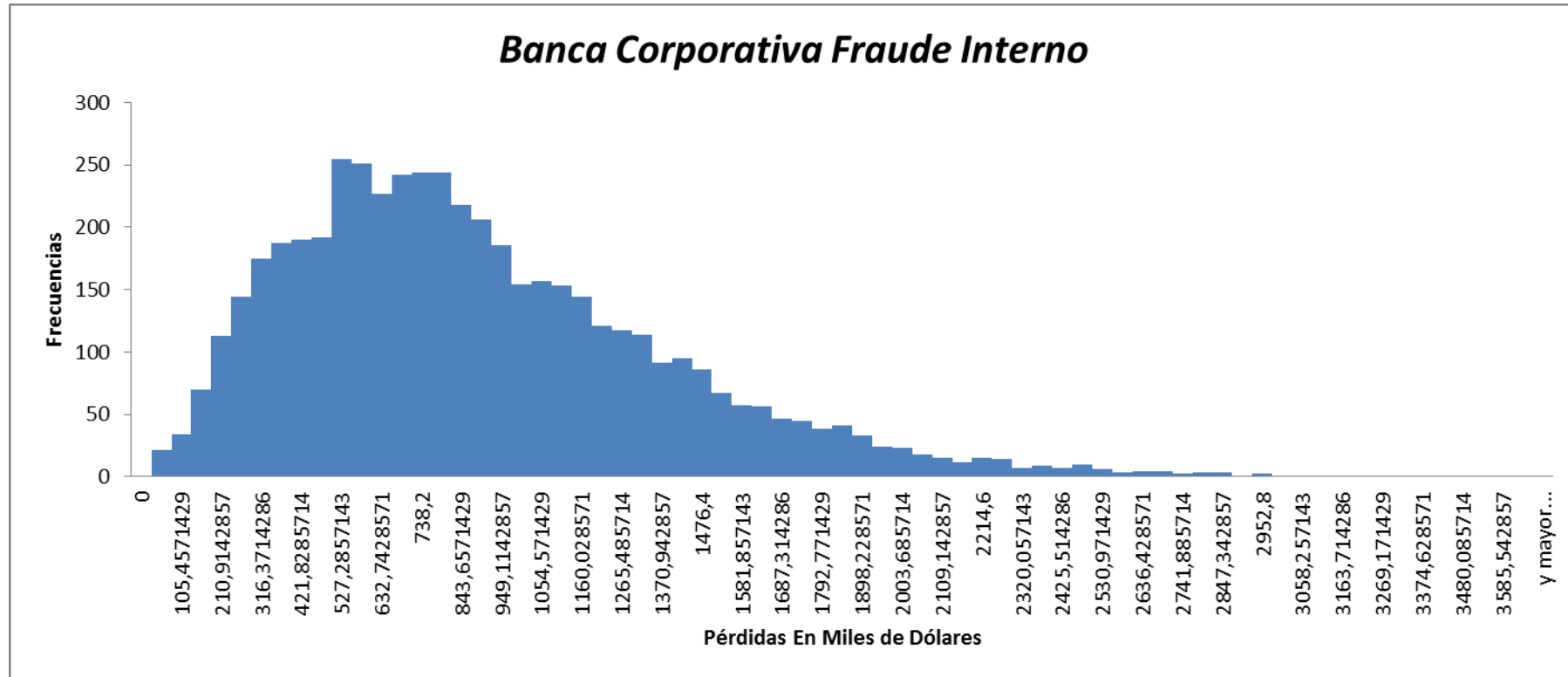
Para el caso del segmento de banca corporativa se observa una pérdida esperada que alcanza los \$860.547 valores en dólares ya que las distribuciones seleccionadas como base estaban fijadas en esta divisa.

Si bien el valor esperado representa la pérdida que posiblemente ocurra, para la estimación mediante LDA el valor más relevante corresponde al del percentil 99,9% que el comité establece como el valor en riesgo a registrar como provisión. El valor en riesgo operativo con un nivel de confianza del 99,9% no debería sobrepasar el monto de los \$2.905.292 y es este monto el que se debe provisionar para este ejercicio en particular.

El gráfico que se presenta a continuación corresponde al histograma de pérdidas económicas atribuidas a eventos relacionados con fraudes internos para la línea de negocio de la banca corporativa.

HISTOGRAMA DE PÉRDIDAS BANCA CORPORATIVA FRAUDE INTERNO

Gráfico N° 2 : Histograma segmento banca corporativa, Fraude interno.



Fuente: Elaboración propia a partir de datos de la investigación.

Del histograma anterior es posible de observar una distribución asimétrica positiva en donde la minoría de las pérdidas está en la parte derecha de la media aritmética, además este tipo de distribución presenta un alargamiento o sesgo hacia la derecha característica propia de este tipo de asimetrías positivas, es decir, la distribución de las pérdidas tiene a la derecha una cola más larga que a la izquierda, hecho que es posible apreciar claramente.

Por otro lado se observa también que la distribución posee un alto grado de concentración, lo que es una característica de las distribuciones de tipo leptocúrticas las cuales poseen puntas de mayor altura en relación a una distribución de tipo normal.

Siguiendo con el ejercicio de estimación de pérdidas para el percentil 99,9% derivados del evento ejecución y entrega de procesos, para la línea de negocios de la banca minorista se obtuvieron los siguientes resultados:

Tabla 33: Banca Minorista Ejecución y entrega de Procesos

Banca Minorista Ejecución y entrega de Procesos	
Error típico	6,83
Desviación estándar	483,23
Varianza de la muestra	233508,55
Curtosis	0,77
Coefficiente de asimetría	0,62
Mínimo	624,76
Máximo	4428,67
Cuenta	5000,00
Pérdida Esperada	1.997.491
Var 95%	2.847.530
Var 99%	3.329.036
Var 99,9%	4.071.886

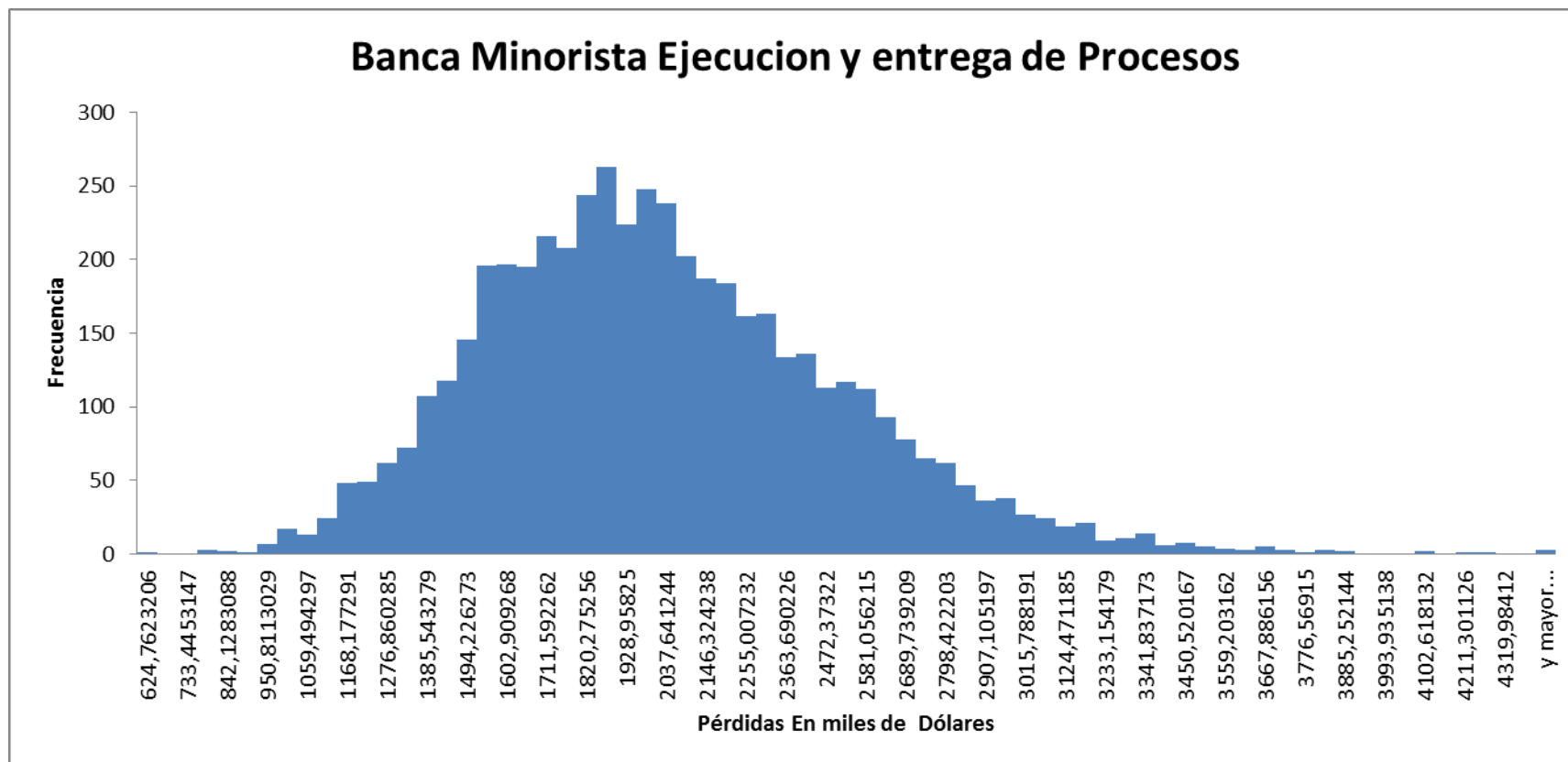
Para el caso del segmento de banca minorista se observa una pérdida esperada que alcanza el monto de \$1.997.491 valor mayor al del evento anterior producto de la mayor frecuencia de ocurrencia de este evento derivado del mayor volumen de transacciones y expresado estadísticamente con un lambda diez veces superior al de la banca corporativa.

Nuevamente el valor esperado representa la pérdida que posiblemente ocurra, sin embargo, para la estimación mediante LDA el valor principal recae en el del percentil 99,9% que el comité establece como el valor en riesgo a registrar como provisión.

El valor en riesgo operativo con un nivel de confianza del 99,9% no debería sobrepasar el monto de los \$4.071.886 de dólares y es este monto el que se debe provisionar para este ejercicio en particular.

A continuación se presenta el gráfico correspondiente al histograma de pérdidas económicas atribuidas a eventos relacionados con la ejecución y entrega de procesos para la línea de negocio de la banca minorista.

Grafico N° 3 : Histograma segmento banca minorista, Ejecucion y entrega de Procesos.



Fuente: Elaboración propia a partir de datos de la investigación.

Del histograma anterior es posible de observar una distribución con asimétrica positiva, que si bien se presenta en una menor medida en relación a la distribución anterior, es igualmente un elemento fácil de distinguir debido al alargamiento de la cola izquierda.

También se observa que la distribución está concentrada por lo tanto también posee una naturaleza de tipo leptocúrtica, aunque ligeramente menor que en el ejemplo anterior.

En conclusión ambas distribuciones poseen características de distribuciones leptocúrtica, lo que conlleva una alta concentración de pérdidas provocando puntas más altas que una distribución normal y ambas distribuciones muestran elementos de asimetría positiva, lo que se traduce en colas más estiradas hacia la derecha y una mayor distribución de datos hacia la izquierda.

Es importante señalar que si bien ambas distribuciones comparten características similares, estas son más marcadas en la distribución de pérdidas que representa el evento de fraude interno para la banca corporativa.

Como consecuencia de esto se puede además señalar que para la banca corporativa existen valores de pérdida extrema al 99,9% de confianza que triplican su pérdida esperada, versus el evento extremo para la banca minorista que tan solo duplica su nivel de pérdida si se contrasta la pérdida esperada con la pérdida extrema del percentil 99,9%.

De este modo bajo la metodología avanzada ambos montos de pérdida extrema esperada con un nivel de confianza del 99,9% deben ser categorizados según lo presentado en el capítulo III, ya sean estos riesgos extremos, altos, medios, bajos o inusual dependiendo de los niveles que la entidad estime convenientes o siguiendo el modelo de bandas de frecuencia y severidad propuesto.

Es importante mencionar que estas estimaciones simuladas representan el posible comportamiento de un evento de pérdida en relación a su impacto y nivel de frecuencia, sin embargo los cálculos estimativos reales se deben necesariamente realizar a través de una base de datos interna y de calidad propia de la entidad, previa aprobación de la SBIF, esta base de datos debe contener al menos cinco años de registros y es en base a esta información con la que se estimaran los cargos de capital una vez caracterizadas las distribuciones de pérdidas y frecuencia obteniendo la función de distribución de pérdidas agregadas (LDA) específica y única para esa entidad financiera.

Por último la estimación de capital regulatorio en su totalidad para esta metodología comprenderá la sumatoria de la totalidad de los VarOp al 99,9% de los eventos registrados para cada categoría de evento y segmento de negocio en el que el banco opere.

CONCLUSIONES

Es necesario en una primera instancia señalar que el riesgo operacional ha estado siempre presente en las organizaciones, sin embargo este adquiere una mayor relevancia una vez presentado el documento del comité de supervisión bancaria de Basilea denominado “Buenas prácticas para la gestión y supervisión del riesgo operativo” el año 2003 posterior a esto se ratifica su importancia integrando el riesgo operacional al conjunto de recomendaciones sobre la gestión de los riesgos conocida como Basilea II y Basilea III, dichos documentos conceptualizan al riesgo operacional y entregan las directrices claves para su adecuada administración y cuantificación, ocurrido aquello y de manera progresiva las entidades ya sean estas financieras o de otro sector industrial han entendido el valor que adquiere la adecuada gestión de este riesgo para la correcta administración de sus organizaciones.

Tras el análisis de distintos documentos entregados por el comité se puede concluir que para su adecuada administración es necesario contar con estrategias que definan claramente los principios de identificación, medición, monitoreo, control y mitigación del riesgo operacional. Además se destaca que la apropiada integración de este riesgo con sus homónimos de mercado y crédito resulta un elemento evidentemente clave a la hora de gestionar adecuadamente los riesgos desde una perspectiva holística.

Existe un alto grado de flexibilidad a la hora de desarrollar metodologías de gestión de riesgo operacional, lo cual favorece la utilización de enfoques personalizados que permiten un mayor grado de adaptación para las entidades según diferentes factores como el tamaño, volumen de operaciones, nivel de complejidad entre otros.

Sin embargo, el apropiado diseño de un sistema de administración de riesgo operacional debe necesariamente contener ciertos elementos mínimos que en su conjunto favorezcan la gestión de este riesgo, en cuanto a estas exigencias mínimas, en esta investigación se destaca, la confección de políticas, documentación, estructura organizacional, registro de eventos, procedimientos de control y monitoreo como los elementos estándar de un sistema de estas características.

Estas etapas de administración del riesgo operacional si bien operan de manera independiente deben a su vez retroalimentarse las unas de las otras con el propósito de generar en su conjunto el cumplimiento de sus objetivos. Este objetivo en términos generales se puede resumir en la adecuada identificación, medición, control y monitoreo. Cada una de estas etapas requiere de distintas herramientas de gestión como por ejemplo documentos formales que establezcan políticas de gestión de riesgo, sistemas de registros adecuados en cuanto a su capacidad de reconocer y almacenar información relevante en torno a los riesgos operacionales, instrumentos de calificación de riesgos como las matrices de riesgos operacionales y sistemas de control y mitigación bien elaborados, así como también la confección de indicadores KRI's que logren exhibir la información de forma precisa y en los momentos precisos para favorecer la toma de decisiones de las entidades.

El campo de la gestión del riesgo operacional corresponde a uno sumamente nuevo, en donde todavía existe un largo camino por recorrer, sobre todo en el ámbito de la implementación del mismo.

Prueba de esta constante adecuación hacia la mejora continua del tratamiento de este riesgo, es el exhaustivo trabajo que ha estado realizando el comité de Basilea en relación a la elaboración de distintos documentos que buscan consolidar dentro de un marco normativo internacional la administración del riesgo operacional. Un punto interesante en torno a lo mencionado consta de la exclusión de la evaluación del riesgo estratégico y reputaciones como riesgos operacionales debido a la dificultad que estos presentan a la hora de ser cuantificados, no obstante es posible que en eventuales documentos estos riesgo sean agregados de una manera u otra.

Tras la investigación se estima que, dentro de las metodologías existentes de cuantificación de cargos de capital para cubrir este riesgo, los que mejor se ajustan para la adecuada gestión de los mismos, corresponden a los métodos de estimación avanzada. Esto esencialmente porque su orientación hacia las pérdidas se adapta de mejor manera que los métodos estándar que se basan en estimaciones enfocadas en los ingresos operacionales de las entidades bancarias.

Se logró observar que una diferencia importante en torno a los métodos avanzados de cuantificación de riesgo operacional y las metodologías más básicas, además de la evidente diferencia en complejidad, se encuentran en el enfoque generalista que poseen las metodologías básicas, versus la perspectiva más flexible e individualizada de los enfoques avanzados.

Por parte de las metodologías básicas existe una indudable carencia de incentivos reales a la gestión de los riesgos, pues el hecho de ser técnicas de cuantificación orientadas a los ingresos como única variable estimadora, las convierte en un sistema caro de prevención de riesgos y sin estímulos a la mitigación de los mismos ya que los aspectos de gestión y control eventualmente implementados no impactarán en el cargo de provisiones por riesgo operacional, pues son únicamente los niveles de ingresos operacionales los que determinan el total de capital económico a provisionar.

En contraste a lo anteriormente mencionado las técnicas de cuantificación de capital económico mediante metodologías avanzadas, muestran un alto nivel de estímulo a la mitigación de los riesgos operacionales, ya que su enfoque de medición se centra en las pérdidas económicas de la entidad, dejando la variable de los ingresos operacionales en un segundo plano, como consecuencia el hecho de generar controles que disminuyan las pérdidas económicas impactaran positivamente en los niveles de provisión de capital económico requerido para cubrir los riesgos operacionales, lo que se entiende como una virtud a la hora de promover una buena gestión de riesgos operacionales.

Dicho esto es igualmente importante mencionar que existe una diferencia significativa en términos de complejidad de cálculo de capital económico entre las metodologías básicas y las avanzadas. En donde los métodos avanzados hacen un fuerte énfasis en la implementación de técnicas de estadística avanzadas, como por ejemplo la utilización de la metodología de valor en riesgo la cual estima los niveles máximos esperados de eventuales pérdidas derivadas de riesgos operacionales para un periodo determinado de tiempo y bajo un nivel de confianza que alcanza el 99,9%.

Dentro de las simulaciones realizadas se logró además observar que este estricto nivel de confianza del 99,9% conlleva provisiones muy por encima de la media esperada, tema que puede generar debate dentro de la industria.

La técnica de valor en riesgo debe necesariamente estimar modelos estadísticos distintos para cada categoría de evento y su línea de negocio asociada, este requerimiento es comprensible luego de que un tipo de categoría de evento puede ciertamente variar significativamente de comportamiento dependiendo del segmento de negocio en el cual se encuentre, además previo a todo lo mencionado es imperativa la aprobación por parte del ente regulador, en este caso la Superintendencia de Bancos e Instituciones Financieras para la utilización de metodologías de medición avanzada.

Si bien Basilea permite la estimación de funciones de distribución de pérdidas agregadas separadas por categoría de evento y línea de negocio, se recomienda también realizar estimaciones de modelos estadísticos aún más profundos.

Una aproximación ideal comprendería la estimación de las distribuciones de pérdidas individualizadas por evento y no por categoría de evento como propone el comité. Así por ejemplo para un evento de categoría de fraude interno, debiese permitir un análisis de inclusive un mayor valor predictivo a los presentados por el comité de Basilea, de manera que los bancos realicen estudios estadísticos de tantas subcategorías de eventos existan o bien exhiba la entidad.

El comité señala que para una categoría cualquiera como por ejemplo fraude interno, se debe realizar tan solo una distribución de pérdidas que agrupe a todos los eventos que se consideren fraudes internos. Sin embargo se recomienda no realizar esta agrupación y determinar funciones de distribución como tantos eventos existan, lo que permitiría un mayor nivel predictivo.

Esta acción puede generar la disminución de los niveles de confianza establecidos como parámetros por Basilea, al ser estos compensados con una mayor capacidad predictiva de los futuros eventos desglosados de manera más meticulosa, traduciéndose aquello en una oportunidad de disminuir los niveles de capital requerido para cubrir los riesgos operacionales.

Para finalizar se considera pertinente mencionar que las entidades financieras deben idear e implementar adecuados sistemas de administración de los riesgos operacionales en toda la organización, aplicar sus políticas, manuales y herramientas de gestión, esto con el objetivo de minimizar los posibles impactos negativos que se deriven de la operación de la entidad financiera y asegurar su correcto funcionamiento.

BIBLIOGRAFÍA

- Arbeláez et al. (2006). Riesgo operacional: reto actual de las entidades financieras. *Revista Ingenierías Universidad de Medellín*, 98-110.
- Bernal, J., & Roncancio, N. (2009). Guía Práctica del Sistema de Administración de Riesgo Financiero.
- Burneo, K., Berggrun, L., & Edmundo, L. (2013). El riesgo operacional, sae 16 y as5: herramientas de control y mejora. *Strategy & Management Business*, 43-64.
- Castillo, M., & Mendoza, Á. (2004). Diseño de una metodología para la identificación y la medición del riesgo operativo en instituciones financieras. *Revista de Ingeniería Universidad de los Andes*, 45-52.
- Comité de Supervisión Bancaria de Basilea. (Febrero de 2003). Buenas prácticas para la gestión y supervisión del riesgo operativo.
- Comité de Supervisión Bancaria de Basilea. (Junio de 2006). Convergencia internacional de medidas y normas de capital.
- CRS Consulting Ltda. (2007). Estructuración de la metodología y del manual para la implementación del sistema de administración del riesgo operativo- saró, en crs consulting ltda.
- Delfiner, M., & Pailhé, C. (Enero de 2009). Técnicas cualitativas para la gestión del Riesgo Operacional. *Munich Personal RePEc Archive*, 1-38.
- Elizalde, A., & Repullo, R. (2004). Capital regulatorio y capital económico: un análisis de sus determinantes.
- Faulín, J., & Ángel, J. (s.f.). *Universitat Oberta de Catalunya*. Recuperado el 03 de Septiembre de 2013, de http://www.uoc.edu/in3/emath/docs/Simulacion_MC.pdf
- Fernández-Laviada, A. (2010). *La gestión del riesgo operacional: de la teoría a su aplicación*. Noriega Editores.
- Franco & Murillo, (2008). Loss distribution approach (lda): metodología actuarial aplicada al riesgo operacional. *Revista Ingenierías Universidad de Medellín*, 143-156.
- Havas Digital. (31 de Agosto de 2011). <http://www.ebanking.cl/>. Recuperado el 08 de Septiembre de 2013, de <http://www.ebanking.cl/tag/havas-digital>

- Idrobo Luzuriaga, M. E. (2012). Matriz de riesgo operativo, una herramienta efectiva en la planificación de actividades de auditoría interna para entidades del sistema financiero.
- Jiménez, E., Fera, J., & Martín, J. (2008). Enfoques de Medición de Riesgo Operacional en la Banca. *Panorama Socioeconómico*, 18-33.
- Lopetegui, G. (1996). Regulación y supervisión de liquidez.
- López, D. (Agosto de 2009). <http://www.sbif.cl/>. Recuperado el 01 de Septiembre de 2013, de http://www.sbif.cl/sbifweb/internet/archivos/publicacion_8511.pdf
- Mora, A. (2010). Una recomendación para cuantificar el riesgo operativo en entidades financieras en Colombia . *Scielo*, 185-211.
- Morales, M. (2007). La administración del riesgo de crédito en la cartera de consumo de una institución bancaria.
- Norman, G. (Agosto de 2009). *Universidad Nacional de Colombia, Medellín*. Recuperado el 09 de Septiembre de 2013, de http://www.unalmed.edu.co/~ndgiral/Archivos%20Lectura/Archivos%20curso%20Riesgo%20Operativo/gestion_riesgo_introduccion_2009.pdf
- Nucamendi, A., & Rosales, R. (2012). El abc de la regulación bancaria de Basilea. *Análisis Económico*, 105-139.
- Palma, C. (2011). ¿Cómo construir una matriz de riesgo operativo? *Ciencias Económicas*, 629-635.
- Romero, L. R. (Septiembre de 2009). Riesgo Operacional: Implementación del Método Estándar y Estándar Alternativo en Basilea II.
- Tamames, R., & Gallego, S. (1996). diccionario de Economía y Finanzas. España: Alianza Editorial.
- VIZUETE, W. (s.f.). Desarrollo de un mapa de riesgos operacionales caso aplicado en una institución financiera (banca de consumo).