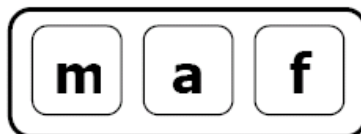


UNIVERSIDAD DE EL SALVADOR
FACULTAD DE CIENCIAS ECONÓMICAS
MAESTRÍA EN ADMINISTRACIÓN FINANCIERA



Gestión de Riesgo Operacional en El Salvador.

Trabajo de Graduación Presentado por:

HUGO ESTEBAN INTERIANO MELGAR

Para Optar al grado de:

MAESTRO EN ADMINISTRACIÓN FINANCIERA

UNIVERSIDAD DE EL SALVADOR



AUTORIDADES UNIVERSITARIAS

RECTOR INTERINO : LIC. JOSÉ LUIS ARGUETA ANTILLÓN
SECRETARIA GENERAL INTERINA: DRA. ANA LETICIA ZA VALETA DE AMAYA

AUTORIDADES DE LA FACULTAD DE CIENCIAS ECONÓMICAS

DECANO : LIC. NIXON ROGELIO HERNÁNDEZ VÁSQUEZ
VICEDECANO : LIC. MARIO WILFREDO CRESPIÓN ELÍAS, MSc
SECRETARIA : LICDA. VILMA MARISOL MEJÍA TRUJILLO
ADMINISTRADOR ACADÉMICO : LIC. EDGAR ANTONIO MEDRANO MELÉNDEZ
TRIBUNAL EXAMINADOR : LIC. JUAN VICENTE ALVARADO RODRÍGUEZ,
MAF
LIC. JONNY FRANCISCO MERCADO CARRILLO
LIC. VICTOR RENÉ OSORIO AMAYA

MARZO DE 2016

SAN SALVADOR

EL SALVADOR

CENTRO AMÉRICA

AGRADECIMIENTOS

Agradezco en mi primer lugar a Dios todo poderoso por permitirme estar con vida, gozar de salud y proporcionarme todos los medios necesarios para la finalización del presente trabajo de graduación.

Especial agradecimiento a mi Esposa María del Carmen, mi hija Katherine Esmeralda y mi hijo Lucas Gabriel, por todo su apoyo y comprensión durante este proceso.

A mis Padres por su disposición incondicional para brindarme todo su apoyo en cualquier momento que lo necesite para culminar la meta trazada.

A mis compañeros de la IX Promoción de la Maestría por su colaboración.

CONTENIDO

I. CAPÍTULO I. INTRODUCCIÓN A BASILEA II Y RIESGO OPERACIONAL.....	6
a) Marco Conceptual.....	6
b) Riesgo Operacional: Definición en El Salvador.....	7
c) Riesgo Operacional: Comité de Basilea.....	7
d) Riesgo Operativo:.....	7
e) Riesgo Legal:.....	8
f) Riesgo de crédito:.....	8
g) Riesgo de mercado:.....	8
h) Riesgo de liquidez:.....	9
i) Riesgo reputacional:.....	9
j) Riesgo técnico:.....	9
k) Riesgo discrecional:.....	9
l) Riesgo no discrecional:.....	10
II. CAPITULO II-REVISIÓN DE LOS PRINCIPIOS PARA LAS MEJORES PRÁCTICAS DE GESTIÓN DE RIESGO OPERACIONAL.....	10
2.1 Principios para las mejores prácticas para la Gestión del Riesgo Operacional.....	10
2.2 Review of the Principles for the Sound Management of Operational Risk-BIS.....	11
2.3 Recomendaciones resultantes de la encuesta.....	24
2.4 Basilea II y el Riesgo Operacional.....	25
a) Enfoque de indicador básico (BIA).....	27
b) Enfoque Estandarizado (TSA).....	28
c) Estándar Alternativo (ASA).....	29
d) Enfoques Avanzados de Medición (AMA).....	30
2.5 Riesgo Operacional hacia Enfoques más simples.....	32
a) BI Indicador del Negocio.....	33
b) Comparación del Indicador del Negocio (BI) con el indicador Gross Income (GI):.....	33
c) Implicaciones para la industria y Supervisores.....	33
d) Fórmula para el cálculo del capital económico por riesgo operacional.....	34
e) Propuesta de cuentas contables a utilizar para el cálculo del “Indicador del Negocio (BI)” en El Salvador.....	35

i) Componente de intereses.	35
ii) Componente de Servicios.	35
iii) Componente financiero.	36
III. CAPITULO III-CONCLUSIONES Y RECOMENDACIONES.	38
3.1 Conclusiones.	38
3.2 Recomendaciones	39
BIBLIOGRAFIA	40
ANEXO	41

I. CAPÍTULO I. INTRODUCCIÓN A BASILEA II Y RIESGO OPERACIONAL.

En el país el tema de la gestión de riesgos, es un tema que está incorporado desde la Ley de Bancos y Financieras, aprobada mediante Decreto Legislativo No. 697 del 02 de septiembre de 1999, publicado en el Diario Oficial No. 181, Tomo 344, del 30 de septiembre de 1999. Que incorpora en antepenúltimo inciso, previa opinión favorable del Banco Central de Reserva de El Salvador, el requerimiento de hasta dos puntos porcentuales adicionales de Fondo Patrimonial con relación al riesgo operacional, riesgo de mercado, riesgos derivados de operaciones crediticias en otros países.

Del mismo modo, la Ley de Supervisión y Regulación del Sistema Financiero, aprobado por medio de Decreto Legislativo No. 592 de fecha 14 de enero de 2011, en el inciso primero del artículo 7, determina que entidades están dentro del perímetro de actuación de la oficina que ejerce la vigilancia por parte del Estado, en materia de Instituciones y Entidades Bancarias, Bancos Cooperativos, Sociedades de Ahorro y Crédito, Compañías de Seguros, Mercados de Valores, Administradoras de Fondos de Pensiones, Etc.

Estableciendo la obligatoriedad, en el literal d) del artículo 35 de la Ley en comento; la adopción y actualización de políticas y mecanismos para la gestión de riesgos, debiendo entre otras, identificarlos, evaluarlos, mitigarlos y revelarlos acordes a las mejores prácticas internacionales. En ese contexto, se puede apreciar que el tema de la gestión prudente de riesgos en el Sistema Financiero de El Salvador, es un tema de interés nacional y el contar con mecanismos adecuados para la gestión coadyuvará al desarrollo económico del país; en virtud de lo anterior, se realizó el presente trabajo de investigación.

a) Marco Conceptual.

La definición de Riesgo, según el Banco de México, (2005) *Definiciones básicas de riesgos p.3.*; La palabra riesgo proviene del latín “risicare” que significa “atreverse”. En finanzas, el

concepto de riesgo está relacionado con la posibilidad de que ocurra un evento que se traduzca en pérdidas para los participantes en los mercados financieros, como pueden ser inversionistas, deudores o entidades financieras. El riesgo es producto de la incertidumbre que existe sobre el valor de los activos financieros, ante movimientos adversos de los factores que determinan su precio; a mayor incertidumbre mayor riesgo.

Por otra parte, de acuerdo con Cade (1999), “*Managing Banking Risk, Fitzroy Dearborn Publishers*”, el riesgo es un terreno donde, donde concurren lingüistas, filósofos, matemáticos, actuarios, y no hay definición única que sirva a todos ellos.

b) Riesgo Operacional: Definición en El Salvador.

Se entiende por riesgo operacional la posibilidad de incurrir en pérdidas debido a fallas en los procesos, de las personas, en los sistemas de información y a causa de acontecimientos externos; incluye el riesgo legal que consiste en la posibilidad de ocurrencia de pérdidas debido a fallas en la ejecución de contratos o acuerdos, al incumplimiento de normas, así como a factores externos tales como cambios regulatorios, procesos judiciales, entre otros. El Salvador, Superintendencia del Sistema Financiero (2011) *Normas para la Gestión del Riesgo Operacional NPB4-50, artículo 1, inciso segundo.*

c) Riesgo Operacional: Comité de Basilea.

Es el riesgo de pérdida causado por fallas o insuficiencia de los procesos, personas y sistemas internos, o por eventos externos. Esta definición incluye el riesgo legal, pero excluye los riesgos estratégico, de reputación y sistémico. Banco de Pagos Internacionales, Comité de Supervisión Bancaria de Basilea (2006), *Metodologías de los Principios Básicos.*

d) Riesgo Operativo:

El Riesgo Operativo o de las Operaciones es aquel que surge únicamente como consecuencia de la propia complejidad operativa del negocio, se restringe a fallos operativos o de los procesos y por tanto, es tan sólo una parte del riesgo operacional. El riesgo operacional, al

margen de la definición concreta que adopte, es un concepto mucho más amplio y en suma más complejo, Hoffman, 2002, p. 20 *Buenas Estrategias Prácticas para la Gestión del Riesgo Operacional*.

La definición de riesgo operacional es una clave, en vista de que para gestionar un riesgos primero hay que definirlo y dicha conceptualización debe ser de aceptación general, en el caso riesgo operacional, se han desarrollado diversas clasificaciones del riesgos, según el *Finantial Service Authority*, (1999) define catorce clasificaciones.

e) Riesgo Legal:

Es la posibilidad de ocurrencia de pérdidas debido a fallas en la ejecución de contratos o acuerdos, al incumplimiento de normas, así como a factores externos tales como cambios regulatorios, procesos judiciales, entre otros. Superintendencia del Sistema Financiero (2011) *Normas para la Gestión del Riesgo Operacional NPB4-50, artículo 1*.

f) Riesgo de crédito:

Es la posibilidad de pérdida, debido al incumplimiento de las obligaciones contractuales asumidas por una contraparte, entendida esta última como un prestatario o un emisor de deuda. Superintendencia del Sistema Financiero, (2011), *Normas para la Gestión Integral de Riesgos, NPB4-47*.

g) Riesgo de mercado:

Es la posibilidad de pérdida, producto de movimientos en los precios de mercado que generan un deterioro de valor en las posiciones dentro y fuera del balance o en los resultados financieros de la entidad. Superintendencia del Sistema Financiero, (2011), *Normas para la Gestión Integral de Riesgos, NPB4-47*.

h) Riesgo de liquidez:

Es la posibilidad de incurrir en pérdidas por no disponer de los recursos suficientes para cumplir con las obligaciones asumidas, incurrir en costos excesivos y no poder desarrollar el negocio en las condiciones previstas. Superintendencia del Sistema Financiero, (2011), *Normas para la Gestión Integral de Riesgos, NPB4-47*.

i) Riesgo reputacional:

Es la posibilidad de incurrir en pérdidas, producto del deterioro de imagen de la entidad, debido al incumplimiento de leyes, normas internas, códigos de gobierno corporativo, códigos de conducta, lavado de dinero, entre otros. Superintendencia del Sistema Financiero, (2011), *Normas para la Gestión Integral de Riesgos, NPB4-47*.

j) Riesgo técnico:

Es la posibilidad de pérdidas por inadecuadas bases técnicas o actuariales empleadas en el cálculo de las primas y de las reservas técnicas de los seguros, insuficiencia de la cobertura de reaseguros, así como el aumento inesperado de los gastos y de la distribución en el tiempo de los siniestros. Superintendencia del Sistema Financiero, (2011), *Normas para la Gestión Integral de Riesgos, NPB4-47*.

k) Riesgo discrecional:

Corresponde a la categoría de riesgos, que tienen instancias de aprobación, dentro de los cuales podemos citar los riesgos de crédito; de mercado y liquidez, para los cuales existen comités para el otorgamiento de créditos, o comités de inversiones para ejecutar en la práctica las políticas de inversiones, respecto de la calidad de los deudores o de los emisores,

emitiendo acuerdos, de aprobación de denegación, de las aprobaciones surgen las exposiciones de riesgo de crédito o de mercado.

1) Riesgo no discrecional:

Corresponde a la categoría de riesgos que no cuentan con instancias de aprobación en particular, correspondiendo a esta categoría los riesgos operacionales, lo anterior, por la transversalidad del riesgo que está presente en toda la entidad, por medio de los cuatro factores generadores de riesgo operacional, que son las personas, los procesos, los sistemas de información y los eventos externos.

II. CAPITULO II-REVISIÓN DE LOS PRINCIPIOS PARA LAS MEJORES PRÁCTICAS DE GESTIÓN DE RIESGO OPERACIONAL.

2.1 Principios para las mejores prácticas para la Gestión del Riesgo Operacional

En el mes de junio de 2011 el Comité de Supervisión Bancaria de Basilea publicó sus "Principios para las mejores prácticas para la Gestión del Riesgo Operacional", los cuales fueron diseñados para proporcionar una orientación a los bancos en la gestión del riesgo operacional. El detalle de los principios se presenta en Anexo. Los once principios incorporan las lecciones de la crisis financiera del 2008 y la evolución de una sólida práctica para la gestión del riesgo operacional. Los Principios cubren la gobernanza, el entorno de gestión del riesgo, el papel de la divulgación, y lo referente a las tres líneas de defensa (Primera línea la gestión de línea de negocio-Dueños de los Procesos; Segunda Línea de Defensa, la función de gestión del riesgo operacional independiente y la Tercera Línea de Defensa, la revisión independiente, la función de auditoría interna).

2.2 Review of the Principles for the Sound Management of Operational Risk-BIS

A la luz del gran número reciente de pérdidas relacionadas con los riesgos operacionales en los bancos, y en consonancia con una mayor concentración de la Comisión de seguimiento de la aplicación de sus normas, a principios del año 2014 el Comité de Basilea, realizó una revisión de la aplicación de sus principios. (Review of the Principles for the Sound Management of Operational Risk-BIS, 06 de octubre de 2014). El análisis implicó 60 bancos de importancia sistémica en 20 jurisdicciones y se cubrieron los 11 principios con un enfoque específico en la orientación relacionada con las tres líneas de defensa antes relacionadas.

Los resultados de la encuesta que se presenta a continuación, con la finalidad de que el lector, cuente con elementos actualizados, sobre la forma de como los países de las economías más desarrolladas del mundo están gestionando el riesgo operacional en la actualidad. En ese orden de ideas; el ejercicio fue diseñado por el Comité de Supervisión Bancaria de Basilea, en forma de cuestionario mediante el cual los bancos tenían que auto-evaluarse respecto de la aplicación de los 11 Principios. A pesar de que se llevó a cabo bajo la supervisión general del Comité de Basilea y las respectivas autoridades de supervisión, la revisión no implicaba una validación “in situ” de las respuestas.

Los objetivos del ejercicio fueron (i) establecer el grado en que los bancos han implementado los Principios, (ii) identificar brechas importantes en su ejecución; y (iii) detectar las prácticas recientes de gestión del riesgo operacional en los bancos que no se tratan actualmente por los principios.

En general, los bancos han avanzado lo suficiente en la aplicación de los principios introducidos originalmente en 2003 y revisadas en 2011.

Muchos bancos están todavía en el proceso de implementación de diversos principios. Los bancos de importancia sistémica (SIB) han puesto en práctica los principios y las herramientas de gestión de riesgos operacionales en diversos grados.

Históricamente, la aplicación de los principios fue fuertemente alineado con los enfoques del Marco de Basilea para el cálculo de los requisitos de capital de riesgo operacional, tales como

el método estándar (TSA) y el método de medición avanzada (AMA). Se espera que los bancos que aplican estos métodos más avanzados posean una administración más avanzada del riesgo operacional, que incluyan auto-evaluaciones de riesgos y de control (RCSAs), la recopilación de bases de datos internos de pérdidas por riesgo operacional, análisis de escenarios, la recopilación de datos externos, el análisis de indicadores clave de riesgo (KRI), así como el análisis de indicadores clave de rendimiento (KPI).

Algunos Bancos de Importancia Sistémica (SIB); sin embargo, todavía tienen que poner en práctica todos los principios y no se despliegan toda la gama de herramientas de gestión de riesgos operacionales. Esto puede deberse a que algunos de los bancos no están sujetos a los enfoques más avanzados de riesgo operacional y de las expectativas más altas para la gestión del riesgo. Por lo tanto, estos bancos pueden no tener una identificación adecuada de sus exposiciones de riesgo operacional.

Los métodos para gestión del riesgo operacional deben ser vistos como complementarios al cálculo de los requerimientos de capital por riesgo operacional, más que como consecuencia de esa actividad. La alineación de la aplicación de los principios de gestión de riesgos, con el perfil de riesgo y la importancia sistémica de los bancos, es más importante que los métodos seleccionados para el cálculo de los requerimientos de capital por riesgo operacional, también los mismos deben ser coherentes con el objetivo de una supervisión más intensa y eficaz en los bancos de importancia sistémica.

Esta revisión ha identificado varios retos y temas dentro de cada uno de los principios. Cuatro principios han sido identificados como uno de los menos implementados a fondo por los bancos, incluyendo (i) identificación del riesgo operacional y evaluación, (ii) la gestión del cambio, (iii) el apetito de riesgo operacional y la tolerancia, y (iv) divulgación. Además, las debilidades se han observado en la aplicación de los principios generales de las tres líneas de defensa.

La siguiente sección resume los desafíos y temas relacionados con estos principios. Principios fundamentales de la gestión del riesgo operacional, identificación del riesgo operacional y la evaluación.

En general, los bancos han puesto en práctica algunas de las herramientas de identificación de riesgos y evaluación operacionales, tales autoevaluaciones (RCSA) y análisis de escenarios y factores del ambiente de control, otros no están totalmente implementadas o no se están utilizando de manera efectiva a efectos de gestión del riesgo. Algunos bancos indicaron que las herramientas que habían sido implementadas fueron en gran medida utilizada a efectos de valoración de riesgo (es decir, la medición del capital y de asignación), mientras que otros indican que las herramientas no se han aplicado plenamente, ya que no se consideró necesario para los propósitos de medición de riesgos.

Además, se informó de una amplia gama de prácticas sobre la aplicación de muchas de estas herramientas. Por ejemplo, mientras que muchos bancos han implementado herramientas de gestión del riesgo operacional de varios niveles distintos (es decir RCSAs, análisis de escenarios, mapeo de procesos de negocio), otros bancos señalaron que han optado por implementar una herramienta que podría servir al propósito de dos o posiblemente tres herramientas juntos (es decir, un RCSA basado en escenarios, un RCSA basado en procesos, etc.). Por otra parte, en algunos bancos, se requerirá un considerable esfuerzo de gestión para garantizar la aplicación de todo el banco de ciertas herramientas. Estos incluyen los indicadores clave de riesgo e indicadores clave de rendimiento; recopilación de datos externos y su análisis; y el análisis comparativo, así como la creación y seguimiento de planes de acción generados a través de la utilización de las herramientas de gestión de riesgos operacionales.

La gestión del cambio (Principio 7), En general, hay muchos aspectos de la gestión de cambios que no se han aplicado plenamente por muchos de los bancos. El principio de la gestión del cambio tenía una de las calificaciones promedio más bajos asignados, lo que indica que los bancos continúan con problemas para implementar y mejorar sus programas de gestión

de cambios importantes, por ejemplo, nuevos productos o cambios en el ambiente informático.

Sólo alrededor del 66% de los 60 bancos encuestados, han aplicado plenamente las evaluaciones de riesgos y de control dentro del proceso de gestión del cambio para los nuevos productos e iniciativas. Si bien los principios definen cambios para incluir nuevos productos, actividades, procesos y sistemas, existe una amplia gama de prácticas y su relación con el marco de política para los procesos de gestión del cambio; por ejemplo, algunos bancos dijeron que su marco de gobierno no se aplicaba a todos los tipos de cambio como la subcontratación.

Muchos bancos también señalaron que la taxonomía del riesgo operacional no aplica, o no se aplica consistentemente, a diversos cambios que incluye nuevos productos, actividades, procesos y sistemas, la alineación con la taxonomía del banco permitiría la integración y agregación de resultados con el perfil de riesgo global.

Varios bancos respondieron que las funciones y responsabilidades relativas a la gestión del cambio se incluyeron dentro de cualquier marco de gestión del riesgo operacional de la entidad o de las políticas relacionadas con la gestión del cambio subyacente. Muchos bancos también señalaron la participación de varios grupos de control dentro de la segunda línea de defensa, en las evaluaciones de riesgos y de control, tales como el cumplimiento, legal, la continuidad del negocio, la tecnología, y otros grupos de gestión de riesgos. Sin embargo, una serie de bancos consideran que la segunda línea de defensa aún no aplica plenamente elementos para la gestión de cambios importantes o en el ambiente informático.

Además, un pequeño número de bancos señaló que estos otros grupos de control fueron los principales responsables de llevar a cabo las evaluaciones de riesgos y de control, lo que no está totalmente alineado con el concepto de las tres líneas de defensa. Algunos bancos también señalaron que la función de riesgo operacional de las empresas fue sólo participar en el proceso a través de la pertenencia al comité de aprobación y supervisión. La participación en un comité no puede proporcionar plenamente la oportunidad de ofrecer una contraparte efectiva a la primera línea de defensa en la evaluación del riesgo.

Relativo al apetito de riesgo operacional y la tolerancia comprendidos en el “Principio 4”. Muchos bancos en general, indicaron que el establecimiento de un apetito de riesgo operacional y la declaración de la tolerancia era más difícil para el riesgo operacional que para otras categorías de riesgo, como el riesgo de crédito y de mercado, y lo atribuyeron a la naturaleza y la omnipresencia de riesgo operacional. Para aquellos bancos que han establecido una declaración de apetito por el riesgo y la tolerancia operacional, una práctica comúnmente observada fue la inclusión de métricas, como pérdidas operacionales, porcentaje de los ingresos brutos. Sin embargo, estos indicadores tienden a ser retrospectivos en lugar de prospectivos. Como resultado, muchos bancos indicaron que se está trabajando para mejorar el estado del apetito y la tolerancia al riesgo operacional existente.

En el papel de la divulgación “Principio 11”, 39 de los 60 los bancos incluidos en el análisis, dijeron que su calidad general de divulgación del riesgo operacional es totalmente compatible, que apunta a la existencia de una sección específica para el riesgo operacional en el informe anual o plantillas de divulgación desarrolladas de forma individual en el Pilar 3 del Marco de Basilea. Sin embargo, no se divulga la información confidencial relativa a las brechas o problemas de control, lo que sugiere que estas revelaciones suelen ser principalmente las declaraciones de alto nivel.

La relativa falta de información sobre el perfil de riesgo operacional y cómo los bancos gestionan su riesgo operacional, puede ser atribuible a la aplicación inadecuada de una política de divulgación que está sujeta a la aprobación y supervisión por parte de la junta directiva.

El principio de las “Tres líneas de defensa”. La mayoría de los Bancos encuestados informaron de que cumplen plenamente con el principio de las "Tres líneas de defensa"; sin embargo, a juzgar por los comentarios presentados, es evidente que se está utilizando en la práctica, una amplia variedad de enfoques relacionados con la aplicación del principio de las tres líneas de defensa.

En algunos casos, los Bancos encuestados han clasificado inapropiadamente responsabilidades a través de cada una de las tres líneas de defensa (por ejemplo, se asignaron diversas responsabilidades de línea de negocio a la segunda línea de defensa).

Del mismo modo, 41 de los 60 Bancos encuestados también señalaron los desafíos más importantes en la consistencia de la aplicación y su capacidad para sustentar la revisión independiente de las herramientas operativas de gestión de riesgos utilizados por la primera línea de defensa. Señalaron la insuficiencia de recursos dentro del área de riesgos. Además, un gran número de Bancos encuestados, todavía tienen que desarrollar plenamente un programa de aseguramiento de la calidad que se aplica dentro de la segunda línea de defensa.

El 85% de los Bancos encuestados indicaron que se cumplieron las responsabilidades relativas a la tercera línea de defensa, señalaron que los que realizan la revisión del diseño, efectividad de los controles operativos de gestión de riesgos, procesos y sistemas del banco, no están involucrados en el desarrollo, implementación y funcionamiento del marco de gestión del riesgo operacional.

En igual proporción, los Bancos encuestados también dijeron que la cobertura de la auditoría interna es adecuada, agregaron que la revisión de la primera y segunda líneas de defensa es suficiente y acorde con otras funciones de gestión de riesgos en los que siguen un enfoque basado en el riesgo para determinar la frecuencia y el alcance de la auditoría; sin embargo, casi un tercio de los Bancos encuestados, señaló que se necesitan mejoras para garantizar el cumplimiento pleno y, tal como se describe en otras secciones de este informe, algunos bancos señalaron que la cobertura se limita a la revisión del modelo de riesgo operacional y sus insumos, en lugar de la aplicación del marco de gestión del riesgo operacional global.

Por otra parte, la mayoría de los Bancos encuestados indicó que la auditoría interna tiene los recursos suficientes para llevar a cabo sus responsabilidades como una tercera línea de defensa. Sin embargo, algunos bancos señalaron que la tercera línea de defensa necesita

mejoras en términos de definición, ejecución y seguimiento, y que la dotación de personal dentro de la auditoría interna era insuficiente.

El 28% de los bancos también señalaron que todavía están en el proceso de implementación de un enfoque más refinado para la asignación de responsabilidades específicas a las tres líneas de defensa.

Si no se aplican plenamente las prácticas de identificación y gestión de riesgos operacionales en forma adecuada, las entidades pueden incurrir en pérdidas financieras directas y materiales, y consecuentes pérdidas de reputación, y podría llevar a un impacto sistémico en otros bancos, clientes, contrapartes y el sistema financiero.

Los bancos señalaron que se encuentran en distintas fases de ejecución de cada uno de los Principios. La revisión también destacó varios principios que, en general, los bancos no habían implementado adecuadamente.

En particular, los bancos deben:

- a) Mejorar la aplicación de cada uno de los métodos de identificación de riesgos y evaluación del riesgo operacional, incluyendo autoevaluaciones, los indicadores de clave de riesgo, datos de pérdida externos, mapeo de procesos de negocio, análisis comparativo, y el seguimiento de los planes de acción generados por las diversas herramientas de gestión del riesgo operacional.
- b) Mejorar la aplicación de los programas y procesos de gestión del cambio y asegurar su seguimiento eficaz.
- c) Reforzar la aplicación de las tres líneas de defensa, sobre todo mediante el refinado de la asignación de funciones y responsabilidades.

- d) Mejorar la administración y supervisión de la gestión de alto nivel; articulación de las declaraciones del apetito de riesgo y tolerancia operacionales; y las revelaciones de riesgo.

Tal como se ha podido apreciar en el presente trabajo de investigación, la piedra angular de la gestión de riesgos, es la delimitación de la actuación de las distintas instancias dentro del marco del “Principio de las tres líneas de defensa”, por lo que a continuación se profundiza, sobre la aplicación práctica de dicho principio general en economías desarrolladas.

Los Bancos han establecido las funciones y responsabilidades de las tres líneas de defensa, incluyendo (i) la gestión de la línea de negocio, (ii) una función de gestión riesgo operacional corporativo independiente, y (iii) una revisión independiente.

La mayoría de los Bancos encuestados, dijeron que cumplen plenamente con el párrafo anterior. Sin embargo, sobre la base de las observaciones presentadas, se observa una serie de prácticas en relación con la aplicación de las tres líneas de defensa. En algunos casos, los bancos han clasificado de forma inapropiada las responsabilidades en cada una de las tres líneas de defensa (por ejemplo, diversas responsabilidades de línea de negocio se han asignado a la segunda línea de defensa).

Una práctica notable fue un conjunto de responsabilidades bien documentado y claramente articulada para cada una de las tres líneas de defensa de la siguiente manera:

La “Primera línea” de responsabilidades de defensa debe incluir el uso de herramientas de gestión de riesgo operacional para identificar y gestionar los riesgos, la evaluación y la mejora de los controles, seguimiento e información del perfil de riesgo operacional, asegurando que el perfil de riesgo operacional se adhiere al apetito de riesgo establecido y la tolerancia, el cumplimiento de las políticas, normas y directrices y la promoción de una fuerte cultura del riesgo.

Del mismo modo, la “Segunda línea” de responsabilidades de defensa debe incluir el diseño de herramientas operativas de gestión de riesgos utilizados por la empresa para identificar y gestionar los riesgos, la aplicación de "desafío independiente" con el uso y la producción de las herramientas de gestión de riesgos operacionales por la primera línea de defensa, desarrollo y mantenimiento de las políticas, normas y las directrices, la revisión y que contribuyen a la vigilancia e información del perfil de riesgo operacional, el diseño y la prestación de capacitación riesgo operacional y la conciencia, y la promoción de una fuerte cultura de riesgo.

Con respecto a la “Tercera línea” de responsabilidades de defensa incluye la verificación independiente de que el sistema de gestión del riesgo operacional, ha sido suficientemente bien diseñado e implementado por la primera y segunda líneas de defensa, revisando el "desafío independiente" aplicada por la segunda línea de defensa para la primera línea de uso y la producción de defensa de las herramientas de gestión de riesgos operacionales, la revisión de los procesos de seguimiento, presentación de informes y de gobierno, y la promoción de una fuerte cultura para la gestión del riesgo operacional.

En general tomando de referencia los resultados de la encuesta aludida, el comité anima a los bancos, a asegurar que un efectivo de tres líneas de modelo de defensa se implementa para identificar y gestionar el riesgo operativo de manera apropiada.

Para las estructuras bancarias complejas, el banco ha puesto en práctica un enfoque más refinado para la asignación de roles más específicos y responsabilidades de las tres líneas de defensa entre los departamentos involucrados. Muchos de los Bancos encuestados, están todavía en el proceso de implementación de un enfoque más refinado para la asignación de responsabilidades específicas para las tres líneas de defensa a los departamentos pertinentes.

Una práctica destacable fue la participación de los grupos de control corporativo con experiencia relevante (por ejemplo, el cumplimiento, legal, la continuidad del negocio, la gestión de riesgo tecnológico, etc.) en el apoyo a la segunda línea de defensa con varias herramientas para la gestión de riesgos operacionales.

Por lo anterior, el Comité exhorta a los bancos asignar funciones y responsabilidades de las tres líneas de defensa a los departamentos pertinentes, tales como las unidades de negocio, unidad de riesgos, otros expertos corporativos. Hay una fuerte cultura de riesgo y la buena comunicación entre las tres líneas de defensa para garantizar la buena gobernanza del riesgo operacional.

Sólo alrededor de dos tercios de los bancos dijeron que cumplen plenamente con este principio, explicando que aún están en el proceso de construcción de una fuerte cultura de gestión de riesgos. Esto es más probable debido a diversas herramientas de gestión de riesgos operativos se implementan aún sólo parcialmente. Los bancos también informaron de obstáculos en la comunicación y la formación que han obstaculizado el desarrollo de una sólida cultura de riesgos al interior de la entidad.

Por lo que las entidades deben reforzar su cultura de gestión del riesgo operacional a través de una estrategia de comunicación activa.

Continuando con la “Primera línea de defensa”, como se anotado anteriormente; esta corresponde a la gestión de la línea de negocio. Esto significa que la gobernanza del riesgo operacional reconoce que la gestión de la línea de negocio es responsable de identificar y gestionar los riesgos inherentes a los productos, actividades, procesos y sistemas de los que es responsable.

La mayoría de los bancos dijeron que sus unidades de negocios son responsables de identificar y gestionar los riesgos operativos inherentes a los productos, procesos, servicios y actividades para las que las unidades responsables y que las responsabilidades de la línea de negocio con respecto a la gestión de riesgos se describen en la política de gestión de riesgos del banco. Por otra parte, la mayoría de los bancos indicaron que la gestión de la línea de negocio tiene recursos expertos para evaluar y gestionar los riesgos operativos en los productos pertinentes. Sin embargo, algunos bancos señalaron que la asignación de responsabilidades necesita más refinamiento y mejora.

Mientras que muchos bancos consideran que los recursos y las herramientas pertinentes son adecuados, algunos indicaron la necesidad de mayores recursos. En la mayoría de los casos, la formación en la gestión de la línea de negocios, se proporciona regularmente a los elementos clave del sistema de gestión del riesgo operacional, y se proporcionan especificaciones para las actualizaciones de las herramientas y los cambios estructurales.

Por lo que los Bancos deben perfeccionar y mejorar las funciones y responsabilidades para la gestión de riesgos en la primera línea de defensa ante la gestión de riesgos; y asegurarse de que la actualización o capacitación de seguimiento se proporciona a la gestión de la línea de negocio.

Del mismo modo, la “Segunda línea de defensa”, que se le asigna a la Gerencia de riesgo operacional e incluyen interrelaciones con las unidades de negocio, desarrollo y diseño herramientas de gestión de riesgo operacional de la entidad, las actividades de medición del riesgo operacional y los sistemas de información de riesgo operacional.

El 25% de los Bancos encuestados, respondieron que están en el proceso de implementación de un enfoque más refinado para la asignación de responsabilidades específicas para las tres líneas de defensa a los departamentos pertinentes. Una práctica de destacar es la participación de otros grupos de control dentro de las sociedades (por ejemplo, el cumplimiento, legales, continuidad de negocio, gestión de riesgo tecnológico, etc.) como expertos para ayudar en la segunda línea de defensa de responsabilidad, en otras palabras en la Gerencia de Riesgos.

De la misma manera el 18% de los Bancos encuestados, también señalaron dificultades importantes en la aplicación consistente y que evidencia el desafío independiente para el uso de las herramientas de gestión de riesgos operacionales, por parte de la primera línea de defensa. En algunos Bancos encuestados, no hay suficientes recursos en el sistema de gestión de riesgos operacionales. Además, muchos de los Bancos encuestados no han desarrollado plenamente un programa de garantía de calidad que se aplica dentro de la segunda línea de defensa.

En virtud de lo anterior, el comité insta a los Bancos a asignar funciones y responsabilidades de las tres líneas de defensa a los departamentos correspondientes, tales como unidades de negocio, gerencias de riesgos, y para otros expertos corporativos; e implementar un programa de aseguramiento de la calidad dentro de la segunda línea de defensa para asegurar que un desafío independiente se aplica sistemáticamente.

Relativo a la Tercera línea de defensa, consiste en una revisión independiente del desarrollo e implementación de la gestión de riesgos operacionales al interior de la entidad. Los que realizan estas revisiones deben ser profesionales competentes y debidamente capacitados; y que no estén involucradas en el desarrollo, implementación y funcionamiento del marco. Esta revisión puede ser realizada por auditoría o por el personal independiente del proceso o sistema que se examina, así como también puede implicar partes externas debidamente cualificado.

La mayoría de los Bancos encuestados, respondieron que se cumplen con los criterios establecidos para la tercera línea de defensa y que especialistas que realizan la revisión; el diseño y la efectividad de los controles operativos de gestión de riesgos, procesos y sistemas del banco no están involucrados en el desarrollo, implementación y funcionamiento del marco de gestión del riesgo operacional. Por otra parte, la mayoría de los bancos indicaron que la auditoría interna u otras partes independientes cuentan con recursos suficientes para llevar a cabo sus responsabilidades como una tercera línea de defensa. Unos bancos señalaron que la tercera línea de defensa, necesita mejorar en términos de definición, ejecución y supervisión, y que la dotación de personal dentro de la auditoría interna es insuficiente.

La cobertura de auditoría interna, debe ser capaz de verificar de forma independiente que el marco ha sido implementado como se pretende y está funcionando con eficacia. Cuando se subcontratan actividades de auditoría, la alta dirección debería considerar la eficacia de los acuerdos subyacentes y la conveniencia de depender de una función de auditoría tercerizada como la tercera línea de defensa.

La mayoría de los Bancos encuestados, respondieron que la cobertura de la auditoría interna en la evaluación las herramientas y mecanismos de gestión del riesgo operacional, aplicadas por la primera línea, y creadas y diseñadas por la segunda línea son adecuados, y que la dichas

revisiones son suficientes y acordes con otras funciones de gestión de riesgos; en donde se sigue un enfoque basado en riesgo, para determinar la naturaleza, oportunidad y alcance de las auditorías. Sin embargo, casi un tercio de los bancos señalaron que se necesitan mejoras para garantizar el pleno cumplimiento, y como se indica en otras secciones de este estudio, algunos de los Bancos encuestados, señalaron que la cobertura se limita al modelo de riesgo operacional y sus insumos, en lugar del sistema de gestión de riesgo operacional de forma holística.

Aproximadamente la mitad de los bancos indicaron que la tercerización de la función de auditoría interna como un revisión independiente, no era aplicable; ya que estas actividades no se subcontratan, pero para los bancos que indicaban que habían tercerizado esta función, dentro de este grupo de Bancos encuestados la mayoría indicaron que tercerizar dicha función, era indicado.

Se considera que la cobertura de auditoría interna, debe incluir el juicio sobre la idoneidad y adecuación del marco del marco de gestión del riesgo operacional y los procesos operativos y de negocios de todo el banco. La auditoría interna no debe simplemente probar el cumplimiento de las políticas y procedimientos que la Junta Directiva aprobó, sino que también debe evaluar que el marco cumpla con las necesidades de organización y las expectativas de supervisión. Por ejemplo, mientras que la auditoría interna no debe establecer el apetito de riesgo específico o la tolerancia, si debe revisar la robustez del proceso de cómo se establecen estos límites y por qué y cómo se ajustan en respuesta a las circunstancias cambiantes.

El 73% de los Bancos encuestados, dijeron que la auditoría interna era totalmente compatibles, ya que el alcance de la auditoría interna incluye un pronunciarse sobre la idoneidad general del sistema de control interno y sobre la adecuación y correcta aplicación del marco de gestión del riesgo operacional y sobre la aplicación de los procesos operativos y de negocios a nivel de toda la entidad. Además, muchos Bancos encuestados señalaron que la auditoría interna no se limita a la prueba del cumplimiento de las políticas y procedimientos de la Junta Directiva

aprobó, sino que también evalúa si el sistema de gestión del riesgo operacional cumple con las necesidades de la organización y con las expectativas de supervisión.

Sin embargo, algunos Bancos encuestados indicaron que, a pesar de la auditoría interna emite una declaración de fiabilidad sobre la gobernanza, el control interno y gestión de riesgos para el banco, esto no proporciona evaluación integral para opinar sobre la aplicación integral del marco de gestión del riesgo operacional en forma holística.

En ese contexto, a criterio del comité los bancos deben asegurarse de que no es el enfoque y la cobertura suficiente de acuerdo con el plan de auditoría para el marco de gestión del riesgo operacional; y mejorar la ejecución y el seguimiento de la tercera línea de defensa.

2.3 Recomendaciones resultantes de la encuesta

Si no se aplican plenamente las mejores prácticas de identificación y gestión adecuada de los riesgos operacionales, esto puede resultar en pérdidas financieras directas y de gran materialidad, o las consecuentes pérdidas de reputación que aún y cuando salen de la esfera de gestión del riesgo operacional, en opinión del autor, estas deben ser tratadas como una consecuencia de la materialización de eventos de riesgo operacional; así como los efectos sistémicos en otros bancos, clientes, contrapartes y el sistema financiero en su conjunto. Como se muestra en este estudio, los Bancos encuestados; a pesar de pertenecer a economías desarrolladas aún están en diferentes de la implementación de los Principios. Lo que debe ser tomado en consideración para el desarrollo de la gestión del riesgo en el País. La revisión por pares, también destacó varios principios; para los que en general, los Bancos encuestados no los habían aplicado adecuadamente o se dirigió a la respuesta de la administración del riesgo más relevante según el criterio de sus directorios.

En tal escenario, el comité exhorta a los Bancos, en relación a la identificación y evaluación de riesgos, a aumentar el uso de datos externos a efectos de la gestión de riesgos; a participar en los consorcios de la industria, para mejorar la disponibilidad de datos de pérdida externos para

las distintas jurisdicciones; a seguir aplicando el uso de mapeo de procesos de negocio como una herramienta operativa de gestión del riesgo operacional; a implementar aún más el uso de indicadores de clave de riesgos e indicadores de rendimiento.

Aunado a lo anterior, se deben desarrollar y poner en práctica procesos de análisis comparativos que comparan los resultados de cada una de las herramientas, para evaluar la eficacia de otras herramientas dentro de las líneas de negocio, así como de las evaluaciones de las herramientas y productos a través de procesos y áreas geográficas similares; a utilizar el análisis de escenarios de riesgos operacionales, para fines de evaluación de la gestión de riesgos en toda la empresa, a garantizar que los planes de acción del riesgo operacional, así como las herramientas de identificación y evaluación son monitoreados en forma adecuada; y asegurarse de que hay un proceso formal para crear, controlar y corregir los planes de acción resultantes de la aplicación de las herramientas de gestión del riesgo operacional; y que consideran más procesos formales para la evaluación comparativa de las prácticas de gestión de riesgos operacionales externamente.

Los resultados de la encuesta desarrollada en el año 2014, por el Comité de Supervisión Bancaria de Basilea, reflejan que en los países desarrollados ha existido un avance limitado en la gestión de este riesgo en los últimos quince años, en vista de que según el “*Estudio de ISDA-BBA-RMA*, (1999), en esa fecha los bancos están en una fase inicial en la gestión del Riesgo Operacional.

2.4 Basilea II y el Riesgo Operacional

En inicio del presente estudio, se definió la conceptualización del Riesgo Operacional, explicándonos que es “El riesgo de pérdidas como resultado de procesos, personal y sistemas internos inadecuados o fallidos o de eventos externos”, incluye el Riesgo Legal, pero excluye el Riesgo Estratégico, de negocios y Reputacional, así como las pérdidas relacionadas con riesgos de crédito o de mercado más allá de los límites definidos, los costos de oportunidad.

Entre otros organismos de revisión, se creó el “*Industry Technical Working Group on Operational Risk (ITWGOR)*”,(1999) con el objetivo fundamental de responder al documento

consultivo del Comité de Basilea de junio de 1999, que revisaba el Acuerdo de Capitales de 1988 y que pretendía hacer el acuerdo más sensible al riesgo incorporando además otros riesgos no considerados anteriormente.

Las razones para Basilea II, se derivaron en que el acuerdo de Basilea I de 1988, tuvo consecuencias y debilidades involuntarias, como lo son oportunidades arbitraje de capitales, el cálculo de capital no incluyó al Riesgo Operacional, y la administración moderna del riesgo requiere el reconocimiento del Riesgo Operacional como una categoría de riesgo diferente, que conlleva la recolección de datos de eventos de pérdidas tanto internos como externos, que sean congruentes y la modelación de un capital económico por Riesgo Operacional.

Los principios en el Acuerdo de Basilea II, plantean como objetivos inmediatos, la medición de la idoneidad del capital más sensible al riesgo, mejor aceptación de las actividades complejas de los Bancos sistémicos e internacionalmente activos, una recomendación para integrar la administración del riesgo bancario y cuantificación del capital, el uso de las mejores prácticas y las herramientas disponibles.

Según Barquero, Mauricio, (2006), La nueva propuesta del Comité de Basilea relacionada con Estándares de Supervisión Bancaria, *ISBN: 84-690-0359-3*, Basilea II, establece 3 pilares, el Pilar I se denomina requisitos mínimos de capital (Datos de Gobierno y Marco Analítico); existiendo dos categorías en el ámbito de las pérdidas por riesgo operacional, de Alta frecuencia y bajo impacto, y de Baja frecuencia y alto impacto, que de acuerdo con Crouxty (1998) las pérdidas derivadas del riesgo operacional, también se pueden dividir en pérdidas esperadas y pérdidas inesperadas; el Pilar II Proceso de Revisión de Supervisión (Evaluación interna de capital) y el Pilar III Disciplina del Mercado (Revelación pública de información). El Pilar I, según Chofaras Dimitri (2001) “Economic Capital Allocation Whith Basel II (P4)” se refiere a los requerimientos de capital basados en tres métodos Indicador Básico, Método Estandarizado y Método de Medición Avanzada, según se presenta en la Tabla I:

Tabla 1.

Métodos de requerimientos de capital por riesgo operacional

Método del Indicador Básico (BIA)	Método Estandarizado (TSA)	Método de Medición Avanzada (AMA)
Parámetros especificados por el Supervisor	Parámetros especificados por el Supervisor	Parámetros especificados por el Banco Supervisor
Medición en todo el Banco	Medición en todo el Banco	Normas cualitativas y cuantitativas establecidas por el Supervisor.
Cargo de Capital = Indicador de la exposición (Ingreso Bruto * 15%)	Cargo de Capital = Indicador de la exposición (Ingresos Brutos de las líneas de negocios * Betas 12-18%)	Cargo de Capital= la medición de riesgo generada por el sistema de medición de riesgo operativo interno del Banco (flexibilidad significativa)

Nota: Fuente de elaboración Propia basada en estándares internacionales.

Tal como puede apreciarse en la tabla 1, existen tres métodos para calcular el capital económico por Riesgo Operacional, el enfoque de indicador básico (BIA), Enfoque Estandarizado (TSA); una derivación del Enfoque Estandarizado Alternativo; y Enfoques Avanzados de Medición (AMA), a continuación se presenta cada uno de ellos:

a) Enfoque de indicador básico (BIA)

Este método define un indicador de exposición, que son los ingresos netos de intereses más ingresos netos que no son de intereses, los cuales deben ser brutos de provisiones (e.g para intereses no pagados), gastos operativos, incluyendo las comisiones pagadas o recibidas por contratar proveedores externos de servicios.

Del mismo modo, deben incluir las utilidades/pérdidas obtenidas por ventas de valores registrados en los Libros de Banca de la Entidad (Banking Book), partidas extraordinarias o irregulares y los ingresos derivados de seguros, de acuerdo con la “*Convergencia internacional de medidas y normas de capital (2004)*”, del Comité de Supervisión Bancaria de Basilea, párrafo 650: “*Los ingresos brutos se definen como los ingresos netos en concepto de intereses más otros ingresos netos ajenos a intereses. Se pretende que esta medida (i) sea bruta de cualquier provisión dotada (por ejemplo, por impago de intereses); (ii) sea bruta de*

gastos de explotación, incluidas cuotas abonadas a proveedores de servicios de subcontratación; (iii) excluya los beneficios/pérdidas realizados de la venta de valores de la cartera de inversión; y (iv) excluya partidas extraordinarias o excepcionales, así como los ingresos derivados de las actividades de seguro”).

El cargo por capital se basa en el promedio de un porcentaje fijo del 15% de los ingresos brutos anuales positivos, en los últimos tres años, para mayor ilustración ver la siguiente Tabla 2:

Tabla 2.

Método del Indicador Básico.

Ejemplo de Cálculo de Método del Indicador Básico				Computo
BANCO X	AÑO 1	AÑO 2	AÑO 3	
Ingresos Brutos	1800	600	-100	
Alfa	15%	15%		
Requisitos de Capital Económico	\$270.00	\$90.00	\$0.00	\$180.00
Nota: creación propia adaptando metodologías de estándares internacionales				

El ejemplo de la tabla 2, corresponde al caso hipotético del BANCO X el cual durante el período de tiempo correspondiente a los años 1, 2 y 3; respectivamente, ha presentado ingresos brutos por US \$1,800.00; US \$600; y US \$-100.00, que al aplicarle el factor beta del 15% a cada año, excluyendo el año en que presentó ingresos negativos y luego el resultado se divide entre 2, nos da como resultado, un capital económico por US \$180.00.

b) Enfoque Estandarizado (TSA)

En este método, las actividades de los bancos se clasifican en un marco de 8 líneas de negocios, se calcula el cargo de capital por cada línea de negocios multiplicando los ingresos brutos anuales por cada línea de negocios por un factor asignado que van desde el 12% al

18%. En la Tabla III, se presenta el caso hipotético de un Banco, con el detalle de los ingresos correspondientes a tres años, los cuales están asociados a las siete líneas de negocios definidas por el Comité de Basilea, cada una multiplicada por el factor beta correspondiente a cada línea de negocios, por cada año, luego se suman los ingresos por línea por cada uno de los tres años y el resultado obtenido se divide entre tres, obteniendo como resultado un capital económico por riesgo operacional de US \$187.25, Ver Tabla 3.

Tabla 3

Ejemplo enfoque Estandarizado				
Líneas de Negocios	AÑO 1	AÑO 2	AÑO 3	Beta
Finanzas Corporativas	150	-20	-30	18%
Transacciones y Ventas	120	80	60	18%
Banca de Menudeo	600	500	550	12%
Banca Comercial	500	300	400	15%
Pagos y Liquidaciones	100	90	110	18%
Servicios de Agencias	75	50	60	15%
Administración de Activos	100	-20	-40	12%
Corretaje a Menudeo	110	90	70	12%
Ingresos Brutos Totales	\$1,755.00	\$1,070.00	\$1,180.00	
Aplicación de cálculos				
Líneas de Negocios	AÑO 1	AÑO 2	AÑO 3	Computo
Finanzas Corporativas	27	-3.6	-5.4	
Transacciones y Ventas	21.6	14.4	10.8	
Banca de Menudeo	72	60	66	
Banca Comercial	75	45	60	
Pagos y Liquidaciones	18	16.2	19.8	
Servicios de Agencias	11.25	7.5	9	
Administración de Activos	12	-2.4	-4.8	
Corretaje a Menudeo	13.2	10.8	8.4	
Ingresos Brutos Totales	\$250.05	\$147.90	\$163.80	\$187.25
Elaboración propia, a partir de estándares internacionales				

c) Estándar Alternativo (ASA)

Bajo el Enfoque Estándar Alternativo (ASA), la metodología es la misma que en el enfoque Estandarizado, con excepción para dos líneas de negocios (Banca de Menudeo y Banca

Comercial) para los cuales adicionalmente se debe multiplicar por 0.0035. Para mayor ilustración ver la Tabla 4 y aplicar la misma lógica del ejemplo detallado en el método Estándar. En el ejemplo propuesto para este método el ejercicio da como resultado un capital económico por riesgo operacional que asciende a la cantidad de US \$153.30

Tabla 4

Ejemplo Enfoque Estandarizado Alternativo					
Líneas de Negocios	AÑO 1	AÑO 2	AÑO 3	M	Beta
Finanzas Corporativas	150	-20	-30		18%
Transacciones y Ventas	120	80	60		18%
Banca de Menudeo (Prést. y Anticipos)	12000	9000	11000	0.035	12%
Banca Comercial (Prést. Y Anticipos)	10000	8000	9000	0.035	15%
Pagos y Liquidaciones	100	90	110		18%
Servicios de Agencias	75	50	60		15%
Administración de Activos	100	-20	-40		12%
Corretaje a Menudeo	110	90	70		12%
Ingresos Brutos Totales	\$22,655.00	\$17,270.00	\$20,230.00		
Aplicación de cálculos					
Líneas de Negocios	AÑO 1	AÑO 2	AÑO 3	Computo	
Finanzas Corporativas	27	-3.6	-5.4		
Transacciones y Ventas	21.6	14.4	10.8		
Banca de Menudeo	50.4	37.8	46.2		
Banca Comercial	52.5	42	47.25		
Pagos y Liquidaciones	18	16.2	19.8		
Servicios de Agencias	11.25	7.5	9		
Administración de Activos	12	-2.4	-4.8		
Corretaje a Menudeo	13.2	10.8	8.4		
Ingresos Brutos Totales	\$205.95	\$122.70	\$131.25	\$153.30	
Elaboración propia, a partir de estándares internacionales					

d) Enfoques Avanzados de Medición (AMA)

Bajo esta metodología, los bancos pueden usar sus sistemas internos de medición del riesgo operativo para calcular los cargos de capital con la aprobación de autoridad de supervisión, la autorización exigirá que se cumpla con los criterios cualitativos y cuantitativos que establece el Comité de Basilea más los criterios adicionales establecidos por las autoridades nacionales,

los modelos de medición avanzados deben estar sujetos a un periodo inicial de monitoreo antes de que pueden usarse para propósitos reglamentarios, en período de calibración.

Los criterios de calificación de los modelos de medición avanzados, parte del establecimiento de criterios cuantitativos clave, como lo son la utilización de Bases de Datos Externas, Bases de Datos de Riesgo Operacional Internas, análisis de escenarios y los factores del ambiente de negocio (BEICF) tanto internos como externos. Del mismo modo para el uso parcial como para su revisión esta metodología requiere de la aprobación del Supervisor, bajo los siguientes enunciados:

Para el Uso parcial: Según Nieto Giménez, Montesinos, María de los Angeles, Banco de España, 183 Estabilidad Financiera, NUM 8, “*El Tratamiento del Riesgo Operacional en Basilea II*”, la posibilidad del uso parcial de los modelos internos, está sujeto a la aprobación de su Supervisor, el banco que opte por la utilización parcial podrá determinar en qué parte de sus operaciones empleará el modelo de medición avanzada (AMA), basándose en criterios de estructura jurídica, ubicación geográfica u otros criterios determinados internamente. Para el resto de actividades se podrá utilizar tanto el método estándar como el básico. Para el uso parcial del modelo de medición avanzada, en combinación el método del indicador básico (BIA) o método estándar (TSA), se deben cumplir las siguientes condiciones:

- i. Se captura todo el Riesgo Operacional de la operación consolidada global del Banco.
- ii. Se cumple con todos los criterios específicos relevantes.
- iii. El modelo de Medición Avanzada captura una parte significativa del riesgo operacional del Banco.
- iv. El Banco tiene un plan para implantar el Modelo de Medición Avanzada en todas sus entidades legales y líneas de negocios importantes.

Para la revisión, no se permite que un Banco decida por sí mismo regresar a un enfoque más sencillo, como lo sería regresar a métodos estándar o básicos, cuando ha sido aprobado para un enfoque más avanzado.

Basilea II proporciona tres enfoques de medición para los bancos con diferentes niveles de complejidad en administración y perfiles de riesgo, conforme los Bancos pasan de enfoques más sencillos a los más avanzados, el cargo por capital de riesgo operacional se vuelve más congruente con su perfil de riesgo operacional, los ingresos brutos negativos o un mapeo inadecuado pueden distorsionar la cantidad de capital calculada para un Banco o línea de negocios asociada. Bajo este panorama, el juicio experto del supervisor sigue siendo de importancia crítica, la intervención del pilar II podría ser necesaria si no se alinean el riesgo y los niveles de capital.

2.5 Riesgo Operacional hacia Enfoques más simples.

En el mes de octubre de 2014, el Comité de Supervisión de Basilea, sometió a consulta de los Bancos, el documento “*Operational risk – Revisions to the simpler approaches*”, que se puede traducir como “Revisión del Riesgo Operacional-Enfoques más simples”. Que de acuerdo a la firma consultora Management Solutions (2014), Operational Risk-Revision to the approaches (consultive document), el documento en comento estuvo en consulta de octubre de 2014 al 06 de enero de 2015, el cual establece que la crisis financiera evidenció que los métodos de cálculo de requerimientos de capital por Riesgo Operacional, correspondiente al método del indicador básico (BIA), método estándar (TSA) y el método estándar alternativo (ASA), no estimaban correctamente este riesgo, infravaloraban el cálculo del capital económico por riesgo operacional; debido principalmente a la inadecuación del indicador de los Ingresos Brutos como indicador indirecto del riesgo operacional.

El documento considera; pero no hay un acuerdo definitivo; la eliminación de los métodos BIA, TSA y ASA e introduce el “Método Estándar (SA) Revisado”, que las entidades deberán empezar a utilizar. En el se ha sustituido el indicador indirecto de riesgo operacional de los Ingresos Brutos “Gross Income Indicator (GI)” por el Indicador del Negocio “Business Indicator (BI)” y se han calibrado los coeficientes regulatorios a aplicar, eliminando bajo esta metodología la utilización de líneas de negocio.

a) BI Indicador del Negocio.

Componente de intereses = Valor Absoluto { ingresos por intereses – gastos por intereses }

Componente Servicios = Valor absoluto { Ing. X Com. + Gastos X Comisiones + Otros Ing. de Expl. }

Componente Financiero

= Valor absoluto { Resultado neto cartera de negociación }

+ Valor Absoluto { Resultado neto cartera de inversión }

b) Comparación del Indicador del Negocio (BI) con el indicador Gross Income (GI):

El componente de interés en el GI era igual a los ingresos por intereses menos los gastos por intereses. En el BI, en cambio, el resultado es igual al valor absoluto de dicha diferencia. Por tanto, el componente de interés nunca es negativo, utilizando el BI.

El componente de servicios en el GI sumaba al resultado neto por comisiones el importe de otros ingresos de explotación. En contraste, con el BI se tiene en cuenta también el importe de otros gastos de explotación.

Respecto al componente financiero, el GI sólo tenía en cuenta el resultado neto de la cartera de negociación. El BI, en cambio, para calcular el componente financiero, suma los valores absolutos de los resultados de la cartera de negociación y de la cartera de inversión. El componente financiero en el BI tampoco puede ser negativo.

El GI consideraba otros componentes, como los ingresos por dividendos. El BI no incluye otros componentes distintos a los tres analizados (de interés, de servicios y financiero).

c) Implicaciones para la industria y Supervisores.

Las principales implicaciones que se derivarían de la aprobación de la nueva norma por parte del son las siguientes:

1. La utilización del método Estándar (SA) revisado, no requerirá la autorización del supervisor, ya que dicho método se convierte en la metodología básica a utilizar.
2. Las entidades deberán emplear el método Estándar (SA) revisado, por lo que deberán cambiar la metodología de cálculo de los requerimientos de capital por riesgo operacional. Así, los sistemas tecnológicos de la entidad se deberán adaptar a la nueva fórmula de cálculo, considerando las modificaciones sobre el indicador y sobre los coeficientes.
3. Las entidades deberán monitorizar el margen neto de intereses, dado que si es persistentemente alto o bajo se debe normalizar para el cálculo de los requerimientos de capital.
4. A pesar de la definición de la nueva métrica, Basilea considera que los requerimientos de capital no son un sustituto de los controles de los procesos de gestión del riesgo operacional. En este sentido, Basilea requiere a las entidades que, aun utilizando el método Estándar (SA) revisado, continúen aplicando los principios para una sólida gestión del riesgo operacional.
5. Las entidades internacionalmente activas con grandes exposiciones por riesgo operacional deberán evolucionar hacia métodos de medición avanzada (AMA) para el cálculo del riesgo operacional, pero mientras tanto deberán utilizar el método estándar (SA) revisado.

d) Fórmula para el cálculo del capital económico por riesgo operacional.

$$K.SA. = [\Sigma 1 - 3 \text{ años } \Sigma(BI_j \times \alpha_j)]/3$$

Donde K SA = La carga de capital bajo el revisada SA, BI = Valor anual del BI asignado al tramo "j" en un año determinado, y α coeficiente del tramo "j".

El valor del coeficiente “α” podría ser el mismo valor en los tres años, para los Bancos que sus “BI” siempre estarán ubicados en el mismo tramo del 10%, en vista de que los “BI” de los bancos en esa condición; no superaran, el rango del 0-100 Millones de Euros, lo anterior debido a que las utilidades de todos los Bancos del sistema al 31 de diciembre de 2014 ascendieron a US \$184,414,611.76, que al tipo de cambio Spot del día 21 de octubre de 2015 equivalen en Euros a € 162,494,150.82. (<http://www.finanzas.com/divisas/eur-usd/>”).

e) Propuesta de cuentas contables a utilizar para el cálculo del “Indicador del Negocio (BI)” en El Salvador.

En la Tabla V, se puede consultar los nombres de los códigos contables correspondiente a los códigos contables del componente de intereses. En la Tabla VI, se puede consultar los nombres de los códigos contables del componente de Servicios; y en la Tabla VII, se puede consultar los nombres de los códigos contables del Componente Financiero.

i) Componente de intereses.

Componente de intereses = Valor Absoluto { ingresos por intereses – gastos por intereses}

ABS {6110010100(+6110020100+ 6110040100+ 6110040200+6210010300- 7110010100-7110010200-7110010500-7110020100-7110030100-7110040100-8210010100-8210010200)}

ii) Componente de Servicios.

Componente Servicios = Valor absoluto { Ing. X Com. +Gastos X Comisiones + Otros Ing. de Expl. }

=6110010200+6110010300+6110010400+6110010500+6110010600+6210010200+6210030100+7110020200+7110030200+7110040200+7110070200+7110070300+7110070400+7210000100+8210020000+6210040200+6210040400+6210040500+6210040600+6310010100+6310010200+6310010300+6310010400+6310030100+6310030200

iii) Componente financiero.

Componente Financiero

$$\begin{aligned} &= \text{Valor absoluto } \{ \text{Resultado neto cartera de negociación} \} \\ &+ \text{Valor Absoluto} \{ \text{Resultado neto cartera de inversión} \} \end{aligned}$$

Saldo que refleje al final del año la cuenta 6110020100+6110010100.

Se entiende por libro de banca, (Banking Book) a las inversiones adquiridas hasta su vencimiento, sobre las cuales no existe intención de negociarlas. Por otra parte, se entiende por libro de negociación (Trading Book) a las inversiones adquiridas por los bancos, con la intención de ser negociadas y estas son más susceptibles a variaciones en los precios en el corto plazo.

Tabla 5.

Cuentas Componente de Intereses

Código contable	Nombre
6110010100	Intereses de préstamos a menos de un año plazo
6110020100	Intereses de la cartera de inversiones
6110040100	Intereses sobre depósitos en el Banco Central de Reserva.
6110040200	Intereses sobre depósitos en otras instituciones financieras.
6210010300	Intereses sobre operaciones en moneda extranjera.
7110010100	Intereses de ahorros.
7110010200	Intereses de depósitos a plazo.
7110010500	Intereses de depósitos en cuenta corriente.
7110020100	Intereses sobre préstamos para terceros.
7110030100	Intereses sobre préstamos para cubrir déficit de caja.
7110040100	Intereses sobre títulos de emisión propia.
8210010100	Intereses sobre préstamos por gastos de ejercicios anteriores.
8210010200	Intereses sobre títulos de emisión propia de ejercicios anteriores.

Fuente: Elaboración propia, a partir del catalogo de cuentas para bancos.

Tabla 6, Cuentas contables “Componente de Servicios”.

Componente Servicios.

Código contable	Nombre
6110010200	Comisiones por administración del crédito.
6110010300	Comisiones por desembolsos pendientes.
6110010400	Comisiones y recargos tarjeta de crédito.
6110010500	Comisiones por otorgamiento.
6110010600	Otras Comisiones y recargos.
6210010200	Comisiones por operaciones en moneda extranjera.
6210030100	Comisiones por avales y fianzas.
7110020200	Comisiones por préstamos para terceros.
7110030200	Comisiones por préstamos para cubrir déficit.
7110040200	Otras comisiones por títulos de emisión propia
7110070200	Comisiones y regalías sobre tarjetas de crédito.
7110070300	Comisiones pagadas por adquisición de títulos valores.
7110070400	Comisión por administración de reserva de liquidez.
7210000100	Comisiones por compra de moneda extranjera.
8210020000	Comisiones sobre títulos de emisión propia de ejer. Ant.
6210040200	Ingresos por cajeros a domicilio.
6210040400	Ingresos por alquiler de cajas de seguridad.
6210040500	Ingresos por custodia de valores.
6210040600	Otros ingresos.
6310010100	Recuperación de préstamos e intereses de Ejerc. Ant. a
6310010200	Recup. Inversiones financieras e intereses de Ejerc. Ant.
6310010300	Recuperaciones de gastos de ejercicios anteriores.
6310010400	Liberación de reservas de saneamiento.
6310030100	Ingresos por explotación de activos-Activo Fijo.
6310030200	Ingresos por explotación de activos-Bienes Rec. en pago.

Fuente: Elaboración propia, a partir del catalogo de cuentas para bancos.

Tabla 7, Cuentas contables “Componente Financiero”.

Cuentas contables componente financiero

Código contable	Nombre
6110020100	Intereses de la cartera de inversiones.
6110010100	Intereses sobre la cartera de préstamos.

Fuente: Elaboración propia, a partir del catalogo de cuentas para bancos.

III. CAPITULO III-CONCLUSIONES Y RECOMENDACIONES.

3.1 Conclusiones.

El riesgo operacional, corresponde a una categoría diferente al de los riesgos financieros, clasificándose dentro de los riesgos no discrecionales, en vista de que no es necesario otorgar un crédito, o adquirir títulos valores para presentar exposiciones a dicho riesgo.

Del mismo modo es considerado como riesgo transversal, debido a que coexiste con los riesgos financieros, y éste soporta los procesos, las personas, los sistemas y los eventos externos que incidirán en los riesgos financieros.

Para el caso de los riesgos discrecionales (los riesgos financieros) la premisa existente, es a mayor riesgo mayor rentabilidad; sin embargo, para el riesgo operacional, la premisa es a mayor gestión del riesgo menor capital económico por riesgo.

El objetivo ha sido presentar un acercamiento sobre las formas, en que en la actualidad, se está gestionando el riesgo operacional en las entidades domiciliadas en países desarrollados, y en nuestro país.

Lo anterior, encaminado a que con la finalidad de que los distintos grupos de interés que consulten este trabajo, conozcan elementos de análisis actualizados en materia de gestión del riesgo operacional; además de presentar, directrices para la cuantificación del capital económico por riesgo operacional bajo las metodologías de los enfoques del Indicador Básico (BIA), Método Estándar (TSA), y Estándar Alternativo (ASA).

Del mismo modo, se presentan las nuevas tendencias del riesgo operacional, sobre las cuales; un grupo importante de analistas, son de la idea de migrar hacia metodologías de cálculo de capital económico por riesgo operacional, bajo enfoques más simplificados.

Lo anterior; en vista de que, debido a los resultados de la crisis financiera del 2008, las herramientas y modelos complejos de cuantificación infravaloraron los cálculos de riesgo operacional.

En ese sentido, en este estudio se presenta una iniciativa que contiene propuestas de las cuentas contables a utilizar para calcular el nuevo “Indicador del Negocio”.

3.2 Recomendaciones

En vista de la importancia de la gestión prudente de riesgos para el desarrollo de la sociedad, se recomienda que en las materias impartidas en las distintas carreras de la Universidad, se continúe el estudio de los riesgos, priorizando los temas relacionados con el riesgo operacional, cuyo estudio detallado coadyuvará a la identificación de riesgo operacionales críticos a nivel país y con lo cual se podrán elaborar los correspondientes planes de mitigación en forma “Ex Ante”. Asimismo, se recomienda incluir en los planes de estudios, ejercicios prácticos de cuantificación del riesgo operacional bajo las metodologías incluidas en el presente estudio. Y dar seguimiento permanente a las nuevas tendencias en materia del riesgo operacional.

BIBLIOGRAFIA

- 1) Cade, Eddie (1999). *Managing Banking, Risks*, Fitzroy Dearborn Publishers.
- 2) Crouhy, Michel; Robert Mark, Dan Galial. (1998), *Risk Management*.
- 3) Banco de México, (2005) *Definiciones básicas de riesgos*
- 4) Banco de Pagos Internacionales, Comité de Supervisión Bancaria de Basilea (2006), *Metodologías de los Principios Básicos*.
- 5) Barquero, Mauricio, (2006), *La nueva propuesta del Comité de Basilea relacionada con Estándares de Supervisión Bancaria*, ISBN: 84-690-0359-3
- 6) Chofaras, Dimitris N., (2001) *Economic Capital Allocation Whith Basel II*.
- 7) *Convergencia internacional de medidas y normas de capital (2004)*, Comité de Supervisión Bancaria de Basilea
- 8) *Estudio de ISDA-BBA-RMA, 1999*.
- 9) *Financial Service Authority, 1999*.
- 10) Hoffman, 2002, *Buenas Estrategias Prácticas para la Gestión del Riesgo Operacional*.
- 11) *Industry Technical Working Group on Operational Risk (ITWGOR)*.
- 12) Nieto Giménez, Montesinos, María de los Angeles, Banco de España, 183 *Estabilidad Financiera*, NUM 8, “El Tratamiento del Riesgo Operacional en Basilea II”
- 13) *Normas para la Gestión del Riesgo Operacional NPB4-50*
- 14) *Normas para la Gestión Integral de Riesgos, NPB4-47*.
- 15) *Operational Risk-Revision to the approaches (consultative document) Management Solutions, 2014*.
- 16) *Principios para la gestión del riesgo operacional, Comité de Basilea*.
- 17) *Review of the Principles for the Sound Management of Operational Risk-BIS, 06 de octubre de 2014*.

ANEXO

PRINCIPIOS PARA LA GESTION DEL RIESGO OPERACIONAL

Los principios desarrollados por el Comité de Basilea sobre Supervisión Bancaria, publicados en junio de 2011 que es una actualización de los publicados en febrero de 2003,-disponible en “<http://www.bis.org>”; los que pretenden llevar a una sólida gestión del riesgo operacional que abarca las áreas de gobierno corporativo, gestión de riesgos y divulgación.

Los principios para la gestión del riesgo operacional son los siguientes:

1. La Junta Directiva debe tomar la iniciativa de establecer una cultura de gestión de riesgos sólida. La Junta Directiva y la alta gerencia deben establecer una cultura corporativa que se rija por una sólida gestión de riesgos y que apoye y promueva estándares e incentivos para un comportamiento profesional y responsable. En este sentido, es responsabilidad de la Junta Directiva asegurarse que exista una fuerte cultura de gestión del riesgo operacional a través de toda la organización.
2. Los Bancos deben desarrollar, implementar y mantener un marco de gestión que esté plenamente integrado en los procesos generales de gestión del riesgo del banco. El marco de gestión del riesgo operacional elegido por un banco dependerá de una serie de factores, incluyendo su naturaleza, tamaño, complejidad y perfil de riesgo.
3. La Junta Directiva debe establecer, aprobar y revisar periódicamente el marco. La Junta Directiva debe supervisar el trabajo de la alta gerencia para asegurarse que las políticas, procesos y sistemas han sido implementados efectivamente en todos los niveles de decisión.
4. La Junta Directiva debe aprobar y revisar una declaración respecto al apetito y la tolerancia al riesgo operacional, que describa la naturaleza, tipos y niveles de riesgo operacional que el banco está dispuesto a asumir.
5. La Alta Gerencia debe desarrollar una estructura de gobierno clara, eficaz y robusta, con líneas de responsabilidad bien definidas, transparentes y coherentes para ser aprobada por la Junta Directiva. La alta gerencia es responsable de una consistente aplicación y

mantenimiento de todas las políticas, procesos y sistemas para la gestión del riesgo operacional en todos los principales productos, actividades, procesos y sistemas de acuerdo al apetito y tolerancia al riesgo.

6. La Alta Gerencia debe asegurar la identificación y evaluación de los riesgos operativos inherentes a todos los principales productos, actividades, procesos y sistemas para asegurarse que dichos riesgos e incentivos sean entendidos.
7. La Alta Gerencia debe asegurarse que exista un proceso de aprobación para todos los nuevos productos, actividades, procesos y sistemas, de manera que se realice una evaluación a fondo del riesgo operacional.
8. La Alta Gerencia debe aplicar un proceso para monitorear regularmente los perfiles de riesgo operativo y las exposiciones más importantes a las pérdidas. Mecanismos adecuados de información deben ser implementados a nivel de la Junta Directiva, la alta gerencia y las líneas de negocio que apoyan la gestión proactiva del riesgo operacional.
9. Los Bancos deben tener un sólido ambiente de control que utilice políticas, procesos y sistemas, controles internos apropiados y estrategias apropiadas de mitigación y transferencia de riesgo.
10. Los Bancos deben ser resistentes y contar con planes de continuidad para asegurar una capacidad de operación en forma continua y limitar las pérdidas en caso de una interrupción de negocio severa.
11. La información pública de un banco debe permitir a los interesados evaluar el enfoque utilizado en la gestión del riesgo operacional.