



UNIVERSIDAD CATÓLICA ANDRÉS BELLO
ESTUDIOS DE POSTGRADO
POSTGRADO EN INSTITUCIONES FINANCIERAS

**DISEÑO DEL MARCO PARA LA GESTIÓN DEL RIESGO
OPERACIONAL EN LA BANCA UNIVERSAL
VENEZOLANA**

AUTOR: MARÍA EUGENIA SOUTO HERRERO

C.I N° V.-14.892.786

PROFESOR: SONIA TAVARES

***TRABAJO ESPECIAL DE GRADO COMO REQUISITO PARA
OPTAR AL TÍTULO DE ESPECIALISTA EN INSTITUCIONES
FINANCIERAS***

***MENCIÓN ANÁLISIS Y GESTIÓN DE INSTITUCIONES
FINANCIERAS***

NOVIEMBRE 2009



ÍNDICE DE CONTENIDO

Introducción	1
Capítulo I: Marco Metodológico de la Investigación	3
Planteamiento del problema	3
Variables	4
Objetivos de la investigación	5
Objetivo general	5
Objetivos específicos	5
Tipo de investigación	5
Justificación de la investigación	6
Delimitación de la investigación	7
Diseño de la investigación	7
Instrumentos y técnicas para recolectar y analizar la información	8
Cronograma de las actividades realizadas	9
Factibilidad de la investigación	10
Capítulo II: Marco Teórico de la Investigación	11
Marco regulatorio	11
Comité de Supervisión de Basilea	11
Superintendencia de Bancos y de Otras Instituciones Financieras	12



Marco conceptual	13
Definición de Riesgo	13
Gestión Integral de Riesgos	13
Perfil de Riesgo	13
Definición de Riesgo Operacional	14
Origen de los Riesgos Operacionales	15
Tipos de Riesgos Operacionales	15
Evento de Riesgo Operacional	19
Pérdida por Riesgo Operacional	19
Capítulo III: Marco de Gestión para determinar el Perfil de Riesgo Operacional	21
Enfoque Macro	23
Enfoque Micro	24
Capítulo IV: Unidades participantes en la gestión del Riesgo Operacional	34
Capítulo V: Importancia de la determinación del Perfil de Riesgo Operacional	42
Conclusiones y Recomendaciones	47
Referencias Bibliográficas	51
Anexos	53



ÍNDICE DE FIGURAS

N° 1: Factores y tipología de Riesgo Operacional	18
N°2: Relación entre los eventos de Riesgo Operacional, las causas y sus consecuencias	19
N° 3: Esquema de gestión del Riesgo Operacional	23
N°4: Mapa de riesgos operacionales	28
N°5: Modelo organizativo de gestión de Riesgo Operacional	36
N°6: Tipos de pérdida y perfil de Riesgo Operacional	44
N°7: Perfil de Riesgo Operacional y tipos de mitigación	44



INTRODUCCIÓN

La administración de riesgos se ha convertido en una pieza fundamental dentro de la gestión de las instituciones financieras en todo el mundo, entre otras cosas por la globalización de los servicios financieros que han hecho más complejo el negocio, por el aumento de la competencia que implica el lanzamiento continuo de nuevos productos al mercado, y por la ocurrencia de crisis y escándalos internacionales que cada día demandan de éstas una mejor gestión de riesgos, a fin de que perduren en el tiempo y contribuyan con el sostenimiento de la economía y el desarrollo de la sociedad.

En este sentido, la presente investigación profundiza en la gestión del riesgo operacional que deben realizar las instituciones bancarias en Venezuela. La misma se desarrolla en cinco capítulos que comprenden desde la parte metodológica, fundamental para el logro de toda investigación, hasta el planteamiento de la importancia que representa para una institución bancaria ser capaz de determinar su perfil de riesgo operacional.

El Capítulo I está diseñado para mostrar la parte metodológica, la cual tiene como finalidad determinar el problema a investigar, identificar cuáles objetivos se pretenden lograr con la investigación, qué tipo de investigación se realizará en función del problema planteado, qué argumentos la justifican y qué instrumentos y técnicas serán utilizados para recolectar y analizar la información considerada de interés para el investigador.

En los siguientes capítulos se comienza a dar respuesta a los objetivos que se plantearon en la parte metodológica.

El Capítulo II comprende el marco teórico de la investigación, en él se incluyen todas aquellas definiciones y contenidos teóricos, que son necesarios para entender el origen y el entorno que rodea al tema objeto de



la investigación. En este caso particular se presenta tanto el marco regulatorio como el marco conceptual vinculado con la gestión del riesgo operacional.

El Capítulo III desarrolla el marco de gestión para determinar el perfil de riesgo operacional en una institución bancaria, planteándose dos enfoques uno macro y uno micro, basados tanto en lo establecido por la Superintendencia de Bancos y Otras Instituciones Financieras (SUDEBAN) como en las regulaciones aplicadas en otros países, siendo este el caso de la documentación emitida por el Comité de Basilea.

El Capítulo IV identifica y justifica cuáles son las unidades dentro de una institución bancaria que, de acuerdo a las funciones que realizan, deben participar en la gestión del riesgo operacional.

Finalmente, el Capítulo V relaciona la determinación del perfil de riesgo operacional con la gestión de este riesgo, resaltando la importancia que ello representa en la gestión integral de riesgos que realiza la institución bancaria y en la consecuente reducción de pérdidas.

La gestión del riesgo operacional es un tema sensible y de relevancia creciente en las instituciones financieras venezolanas, ya que el elevado uso de la tecnología, el incremento en la tercerización de los procesos, el importante papel que juega el recurso humano dentro de ellas y los posibles desastres naturales, son aspectos que ponen a prueba su fortaleza operacional y financiera. Sin embargo, con base en la información publicada por algunas de estas instituciones, podría decirse que su gestión del riesgo operacional es incipiente y no vislumbra los beneficios que les representa, razón por la cual esta investigación pretende diseñar un marco de gestión que permita prevenir pérdidas y asegurar una adecuada asignación de capital por este tipo de riesgo.



CAPÍTULO I:

MARCO METODOLÓGICO DE LA INVESTIGACIÓN

Planteamiento del problema

Entre los riesgos que deben gestionar las instituciones financieras venezolanas para evitar pérdidas se encuentra el riesgo operacional.

El Comité de Basilea¹ en el año 2001 emite un nuevo acuerdo, luego del emitido en el año 1988, que incluye al riesgo operacional dentro del cálculo de los requisitos mínimos de capital, con la finalidad de crear una base sólida para la regulación del capital y de perfeccionar la gestión de riesgos, incentivando a los bancos a desarrollar métodos adecuados para calcular las pérdidas esperadas e inesperadas por riesgo operacional y a mantener capital suficiente para cubrirlas.

En Venezuela, la Superintendencia de Bancos y Otras Instituciones Financieras (SUDEBAN)², regula la gestión de riesgos a través de la resolución 136.03 referente a las Normas para una adecuada administración integral de riesgos, publicada en mayo del 2003, en la cual se incluye al riesgo operacional dentro de la gestión integral de riesgos.

¹ El Comité de Supervisión Bancaria de Basilea es uno de los órganos del Banco Internacional de Pagos, está encargado de formular normas de supervisión y prácticas bancarias, no vinculantes, para ser aplicadas luego por cada país, mediante acuerdos e inclusión en sus normas legales, con especial énfasis en el área de Riesgos.

² Ente regulador de las instituciones financieras en Venezuela.



Diseñar un marco para gestionar el riesgo operacional es de interés para las instituciones bancarias venezolanas, no sólo porque es un riesgo inherente a todos los procesos que ejecutan y su gestión depende tanto de aspectos cualitativos como cuantitativos, sino porque además es una exigencia del ente regulador y es un tema que, por ser de data reciente, casi no ha sido desarrollado en el país.

Adicionalmente, considerar la gestión del riesgo operacional como necesaria dentro de la administración integral de riesgos, se traduce en reducción de pérdidas financieras y prevención de pérdidas de imagen o de reputación para la institución bancaria, pudiendo ser éstas tan importantes como para determinar su existencia en el futuro.

En este sentido es fundamental que la institución bancaria logre un entendimiento homogéneo de los conceptos asociados al riesgo operacional, identificando aquellas unidades o áreas dentro de ella que deban participar activa y directamente en su gestión. Todo ello con la finalidad de determinar su perfil de riesgo operacional, es decir, conocer el tipo y la cantidad de los riesgos operacionales asumidos por la institución bancaria, para de esta manera enfocar su gestión y relacionarlos con un nivel de capital apropiado que permita cubrir las posibles pérdidas.

Variables

- Variable independiente: Riesgo operacional.
- Variable dependiente: Gestión del riesgo operacional.
- Variable vinculante: Instituciones bancarias venezolanas.



Objetivos de la investigación

Objetivo General

Diseñar un marco que integre el enfoque cuantitativo y cualitativo de la gestión del riesgo operacional en las instituciones bancarias venezolanas, que permita determinar el perfil de riesgo operacional y asegure la asignación adecuada de capital por este tipo de riesgo.

Objetivos Específicos

- a) Definir los conceptos asociados a la gestión del riesgo operacional.
- b) Diseñar un marco para la gestión del riesgo operacional, que permita determinar el perfil de riesgo operacional en una institución bancaria.
- c) Identificar aquellas áreas que, de acuerdo a sus funciones dentro de la institución bancaria, deben participar en la gestión del riesgo operacional.
- d) Determinar la importancia del perfil de riesgo operacional, para la gestión integral de riesgos en una institución bancaria.

Tipo de investigación

El estudio de los aspectos relacionados con la gestión del riesgo operacional no ha sido profundizado en las instituciones financieras venezolanas, a diferencia de otros riesgos que por tradición las afectan, como el riesgo de crédito o el riesgo de mercado, los cuales han sido investigados ampliamente en el transcurso del tiempo.

En este sentido, tomando en cuenta que se está realizando una investigación sobre un riesgo poco estudiado y que los resultados de ésta servirán de base



para plantear futuras investigaciones más específicas, se considera que la misma es de tipo exploratoria.

Justificación de la investigación

A nivel mundial la administración de riesgos en las instituciones financieras se ha convertido en una pieza fundamental dentro de su gestión, debido a la complejidad de su negocio producto de la globalización de los servicios financieros, al lanzamiento de nuevos productos al mercado y aumento de la competencia, a la ocurrencia de crisis y escándalos internacionales, y a la importancia que este sector reviste para el sostenimiento de la Economía y el desarrollo de la sociedad en los países.

La gestión de riesgos en las instituciones financieras venezolanas está regulada por la Superintendencia de Bancos y Otras Instituciones Financieras (SUDEBAN). Sin embargo, con la finalidad de profundizar ciertos aspectos en lo que respecta a la gestión de riesgos, además de cumplir con la normativa local, éstas acuden a mejores prácticas provenientes de regulaciones aplicadas en otros países, entre las cuales se encuentra la documentación emitida por el Comité de Basilea.

En Venezuela, el riesgo operacional es un tema reciente, la SUDEBAN lo incorpora en la gestión de riesgos en el año 2003 y después de seis años aún existen algunas instituciones bancarias que no están en cumplimiento con la resolución que lo definió o que la cumplen de forma superficial, razón por la cual la investigación que se pretende realizar está orientada a diseñar un marco de gestión para el riesgo operacional, que permita determinar un perfil de riesgo y una adecuada asignación de capital.

Por lo antes expuesto dicha investigación reviste importancia para el sector bancario venezolano y permitirá al investigador especializarse en un tema novedoso y desconocido para algunos profesionales de la banca venezolana.



A pesar de ser un tema nuevo la investigación a realizar es factible, ya que existen instituciones financieras con presencia internacional que muestran en sus informes anuales los avances de su gestión de riesgos, siendo esto un punto de referencia que permite establecer comparaciones en cuanto a las prácticas utilizadas.

Delimitación de la investigación

A continuación se establecen los alcances y límites en cuanto a lo que se pretende abarcar en la investigación:

- Delimitación del espacio: En la investigación que se pretende realizar se determinará un marco de gestión para el riesgo operacional, aplicable a instituciones de la banca universal venezolana.
- Delimitación de la población: La investigación que se pretende realizar es de tipo exploratoria y el diseño es bibliográfico, en este sentido no se definirá una población a observar, encuestar o medir. Sin embargo, es de resaltar que dentro de la información a analizar se incluirán los informes anuales de tres bancos universales venezolanos como son Mercantil Banco, Provincial y Banesco, y los de dos bancos con presencia global como son Santander y BBVA, en lo que se refiere a gestión de riesgos.
- Delimitación del tiempo: En la investigación que se pretende realizar no se determinará un período de tiempo específico ya que la gestión de riesgos es un proceso continuo que se retroalimenta en el tiempo.

Diseño de la investigación

La estrategia que se adoptará para responder al problema planteado, es decir el diseño de la investigación a realizar, es bibliográfico. El propósito del



diseño bibliográfico es aportar nuevos conocimientos, a partir de la búsqueda, análisis, crítica e interpretación de información obtenida y registrada por otros investigadores en fuentes documentales, tanto impresas como electrónicas.

Los análisis e interpretaciones se realizarán sobre la normativa vigente que establece los lineamientos para la gestión de riesgos en las instituciones financieras venezolanas, y sobre papeles de trabajo que incluyen las mejores prácticas aplicadas en otros países. Asimismo, se considerarán las prácticas de importantes bancos a nivel mundial y de bancos universales venezolanos, dadas a conocer a través de sus informes anuales, y las sugeridas por empresas consultoras, referentes a la gestión del riesgo operacional y a la determinación del perfil de riesgo operacional.

La información que se recolectará para realizar el análisis tiene su origen en entes reguladores, instituciones financieras y empresas consultoras, por lo que la misma se considera confiable y consistente con el tema investigado, no estando comprometida ni su credibilidad ni su confiabilidad. De igual forma toda la información será recabada utilizando el mismo método y durante el mismo período de tiempo, a fin de hacerla consistente.

Instrumentos y técnicas para recolectar y analizar la información

La técnica es el procedimiento a través del cual se obtiene la información y los instrumentos son los medios materiales para recogerla y almacenarla. Los objetivos de esta investigación serán alcanzados empleando:

- Instrumentos y técnicas de recolección de datos: La información necesaria será obtenida a través de la revisión del contenido y el análisis documental de las fuentes, tanto impresas como electrónicas,



que se consideren pertinentes para el desarrollo de la investigación; y será almacenada en una computadora personal y una unidad de almacenamiento (pendrive).

- Instrumentos y técnicas de procesamiento y análisis de datos: Una vez revisados los contenidos de las fuentes impresas y electrónicas, se seleccionará la información y luego será analizada aplicando técnicas lógicas como la síntesis, la inducción y la deducción.

Cronograma de las actividades realizadas

La presente investigación se llevó a cabo en seis etapas, las cuales se presentan a continuación:

- Etapa I: Identificación de las fuentes impresas y electrónicas a utilizar y recopilación de información. Fecha estimada: Abril 2009. Cumplida.
- Etapa II: Lectura inicial de los documentos disponibles y elaboración de un esquema preliminar. Esta etapa también comprende la evaluación de la pertinencia, confiabilidad y la utilidad de la información para el desarrollo de la investigación. Fecha estimada: Abril 2009. Cumplida.
- Etapa III: Análisis e interpretación de la información seleccionada a fin de dar respuesta a los objetivos planteados. Fecha estimada: Mayo 2009. Cumplida.
- Etapa IV: Formulación del esquema definitivo y desarrollo de los capítulos. Fecha estimada: Junio - Agosto 2009. Cumplida.
- Etapa V: Presentación de los resultados obtenidos a través de la formulación de conclusiones y recomendaciones que sirvan de punto de partida para la gestión del Riesgo Operacional en las instituciones bancarias venezolanas. Fecha estimada: Octubre 2009. En curso.



- Etapa VI: Entrega y revisión del informe final. Fecha estimada: Noviembre 2009. En curso.

Factibilidad de la investigación

En cuanto a los recursos necesarios para llevar a cabo esta investigación, se identifican:

- Recursos humanos: Están representados por el investigador que la realizará, con el objetivo de obtener el título de Especialista en Instituciones Financieras.
- Recursos materiales: Entre estos recursos se encuentran el uso de un computador personal, un programa procesador de palabras, acceso a internet y las direcciones de páginas web de entes reguladores de las instituciones financieras en Venezuela, de organismos promotores de mejores prácticas en la gestión de riesgos, de empresas consultoras y de instituciones financieras venezolanas y del alcance mundial.
- Recursos financieros: Los costos de realizar esta investigación no son significativos y serán asumidos por el investigador.
- Acceso a las fuentes de información: Se realizará la investigación en base a la información de uso público mostrada por entes reguladores de las instituciones financieras en Venezuela, de organismos promotores de mejores prácticas en la gestión de riesgos, de empresas consultoras y de instituciones financieras venezolanas y a nivel mundial.



CAPÍTULO II:

MARCO TEÓRICO DE LA INVESTIGACIÓN

Marco Regulatorio

Comité de Supervisión de Basilea

El ente promotor de Basilea es el Banco Internacional de Pagos (Bank for International Settlements - BIS), organización que promueve la estabilización y cooperación monetaria y financiera a nivel internacional, y que actúa como banco central de los bancos centrales europeos.

Uno de los órganos del Banco Internacional de Pagos, es el Comité de Supervisión Bancaria de Basilea, el cual está encargado de formular normas de supervisión y prácticas bancarias, no vinculantes, para ser aplicadas luego por cada país, mediante acuerdos e inclusión en sus normas legales, con especial énfasis en el área de riesgos.

En el primer acuerdo, emitido en el año 1988, se hace referencia a la gestión del riesgo de crédito y riesgo de mercado y en el segundo acuerdo, emitido en el año 2001, se incluye al riesgo operacional dentro del cálculo de los requisitos de capital mínimo.

El segundo acuerdo, mejor conocido como Basilea II, tiene como finalidad construir una base sólida para la regulación prudente del capital, alineando la adecuación del capital a los riesgos reales a los cuales están expuestas las instituciones financieras, de igual forma persigue perfeccionar la gestión de riesgos generando incentivos para mejorarla y establece tres pilares para contribuir en el logro de un sistema financiero, sólido, seguro y eficiente. Dichos pilares son:



- Pilar I: Cálculo de requerimientos mínimos de capital, señalando a los bancos como principales responsables de medir la exposición a los riesgos más significativos y de mantener un nivel de capitalización adecuado.
- Pilar II: Supervisión rigurosa basada en el riesgo y en una intervención oportuna, como complemento del cálculo de los requerimientos mínimos de capital.
- Pilar III: Disciplina del mercado, referente a la transparencia informativa considerando aspectos cuantitativos y cualitativos en la revelación de información.

Aunque lo establecido en este acuerdo no es mandatorio para las instituciones financieras venezolanas, el ente regulador en Venezuela (SUDEBAN) y los entes reguladores de la región, han adoptado estas normas a objeto de mejorar la administración de riesgos y su ámbito de control en las instituciones financieras.

Superintendencia de Bancos y de Otras Instituciones Financieras

En Venezuela las autoridades en materia financiera no han formalizado una posición en cuanto a la implantación de Basilea II. Sin embargo, en el año 2003, la SUDEBAN emitió la resolución 136.03 Normas para una adecuada administración integral de riesgos, señalando los lineamientos básicos que deberán observar las instituciones financieras en el establecimiento de un proceso de administración integral de riesgos.



Marco conceptual

Definición de riesgo

El riesgo es la incertidumbre acerca de un evento futuro, que puede estar asociado a un resultado favorable o adverso.

En el ámbito financiero se define el riesgo como “la posibilidad de que se produzca un acontecimiento, que conlleve a pérdidas materiales en el resultado de las operaciones y actividades que desarrollen las instituciones financieras”.³

Gestión integral de riesgos

La SUDEBAN define la administración integral de riesgos como un conjunto de objetivos, políticas, procedimientos y acciones que se implementan para identificar, medir, monitorear, limitar, controlar, informar y revelar los distintos tipos de riesgos a que se encuentran expuestas las instituciones financieras.

Basilea II menciona explícitamente al riesgo de crédito, riesgo de mercado, riesgo de tasa de interés y riesgo operacional dentro del grupo de riesgos a los cuales están expuestas las instituciones financieras, mientras que la SUDEBAN incluye además de los ya mencionados, el riesgo de liquidez, riesgo legal y riesgo de reputación.

Perfil de riesgo

El perfil de riesgo puede definirse como el inventario de riesgos al cual está expuesta una institución financiera, determinando los impactos y las probabilidades de que estos riesgos se materialicen.

³ SUDEBAN. Resolución 136.03 “Normas para una adecuada administración integral de riesgos”.



El Comité de Basilea en su documento Buenas prácticas para la gestión y supervisión del riesgo operativo, define el perfil de riesgo como el nivel de riesgo de las actividades y/o categorías de riesgo de una empresa.

La gestión de riesgos en una institución financiera debe estar acorde con su perfil de riesgo.

Definición de riesgo operacional

El Comité de Basilea en su documento titulado Buenas prácticas para la gestión y supervisión del riesgo operativo, define el riesgo operacional como “el riesgo de sufrir pérdidas debido a la inadecuación o a fallos de los procesos, personas o sistemas internos o bien a causa de acontecimientos externos”. Esta definición incluye el riesgo legal, entendido como la posibilidad de ser sancionado, multado u obligado a pagar daños punitivos como resultado de acciones supervisoras o de acuerdos privados.

En este mismo documento se señala que el riesgo operacional debe ser considerado con la misma importancia que se consideran otros riesgos, pero hace la salvedad de que no es un riesgo aceptado directamente a cambio de un beneficio esperado, sino que es algo que se puede producir en el acontecer diario de las operaciones.

Por su parte la SUDEBAN define al riesgo operacional como “la potencialidad de sufrir pérdidas inesperadas por sistemas inadecuados, fallas administrativas, eventos externos, deficiencias en controles internos y sistemas de información originadas, entre otros, por errores humanos, fraudes, incapacidad para responder de manera oportuna o hacer que los



intereses de la institución financieras se vean comprometidos de alguna u otra manera”⁴.

Origen de los riesgos operacionales

Los riesgos operacionales en una institución bancaria se originan por factores externos o internos, los cuales cambian constantemente siendo influenciados por la situación del entorno y por las condiciones internas particulares de cada institución, respectivamente.

Entre los factores externos se encuentran el surgimiento de nuevas regulaciones o las modificaciones a las ya existentes, la ocurrencia de fusiones o adquisiciones, las nuevas exigencias de los mercados, la globalización de las operaciones, las modalidades de fraudes, las catástrofes y los desastres naturales.

Con respecto a los factores internos, estos involucran situaciones relacionadas con el recurso humano, la banca electrónica, los sistemas y la tecnología, la subcontratación de servicios, todo lo concerniente a la ejecución de los procesos y la dirección de la organización.

Tipos de riesgos operacionales

Tanto la definición de riesgo operacional que provee Basilea II, como la que asume SUDEBAN, distinguen cuatro factores generadores de este riesgo, los cuales son:

- Proceso: Está relacionado con la existencia de recursos inadecuados, deficiencias en los procedimientos y en políticas internas; así como

⁴ SUDEBAN. Resolución 136.03 “Normas para una adecuada administración integral de riesgos”.



también, con el incumplimiento de leyes y normativas, tanto internas como las exigidas por entes reguladores.

- Empleados: Se refiere a aquellas situaciones que afectan al recurso humano. También incluye actos intencionados o no por parte de los empleados, que estén asociados a violaciones de leyes, normas o políticas internas.
- Tecnológico: Está relacionado con situaciones que impliquen problemas en los sistemas, en las telecomunicaciones, datos y en los elementos informáticos.
- Externo: Agrupa aquellas situaciones que se generan como consecuencia de cambios regulatorios, de incumplimientos en contratos con terceros o de hechos de política, fraude, robo y atraco. De igual forma abarca interrupciones del negocio producto de fuerzas naturales, vandalismo, terrorismo, daños en la infraestructura.

El Comité de Basilea en su documento Buenas Prácticas para la gestión y supervisión del riesgo operativo, establece que la definición de riesgo operacional adoptada por cada banco debe abarcar la tipología de riesgos operacionales a los cuales está expuesto y recoger las causas principales de las pérdidas que se produzcan como consecuencia de ellos. En este sentido clasifica los tipos de riesgo operacional en siete categorías⁵, identificándolos como posibles fuentes de pérdidas importantes. Dichas categorías son las siguientes:

⁵ El Comité de Basilea establece esta clasificación en su documento Convergencia Internacional de Medidas y Normas de Capital. En el Anexo “Clasificación de Eventos de Riesgo Operacional según el Comité de Basilea”, puede observarse el detalle de dicha clasificación.



- Fraude interno: Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o evadir regulaciones, leyes o políticas empresariales en las que se encuentra implicada, al menos, una parte interna de la institución. Ejemplo: Utilización de información confidencial en beneficio de la cuenta de un empleado.
- Fraude externo: Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o evitar la legislación, por parte de un tercero a la empresa. Ejemplo: Atraco, usurpación de identidad, fraude en tarjetas de débito y crédito.
- 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 diversidad/discriminación. Ejemplo: Incumplimiento de las normas de higiene y salud laboral.
- Clientes, 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. Ejemplo: Venta de productos y ofrecimiento de servicios no autorizados.
- Daños a activos materiales: Pérdidas derivadas de daños o perjuicios a activos materiales como consecuencia de desastres naturales u otros acontecimientos. Ejemplo: Terremotos, vandalismo.
- Incidencias en el negocio y fallos en los sistemas: Pérdidas derivadas de incidencias en el negocio y de fallos en los sistemas. Ejemplo:



Interrupción en el servicio de electricidad, fallas en las telecomunicaciones.

- 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. Ejemplo: Litigios con los proveedores, documentación jurídica incompleta.

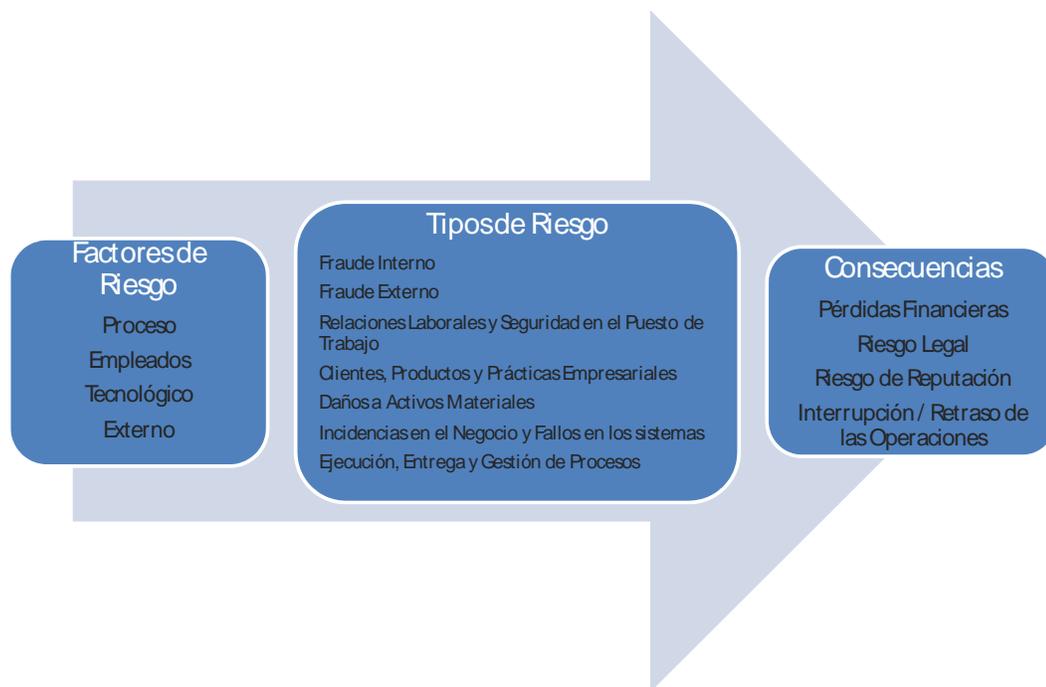


Figura N° 1: Factores y tipología de Riesgo Operacional (Diseño e investigación propia).

Irregularidades relacionadas con los factores de riesgo mencionados pueden generar distintos tipos de riesgos operacionales, dependiendo del área que impacten y la consecuencia que se produzca a partir de ellas.



Evento de riesgo operacional

Se considera evento de riesgo operacional a cualquier incidente ocasionado por fallos o errores en los procesos, por el personal, por fallas en los sistemas internos o por factores externos, cuya ocurrencia pueda exponer a la organización a pérdidas financieras directas o pérdidas indirectas como afectación de la reputación, riesgos legales o costos de oportunidad.

En otras palabras un evento de riesgo operacional es la materialización del riesgo operacional.

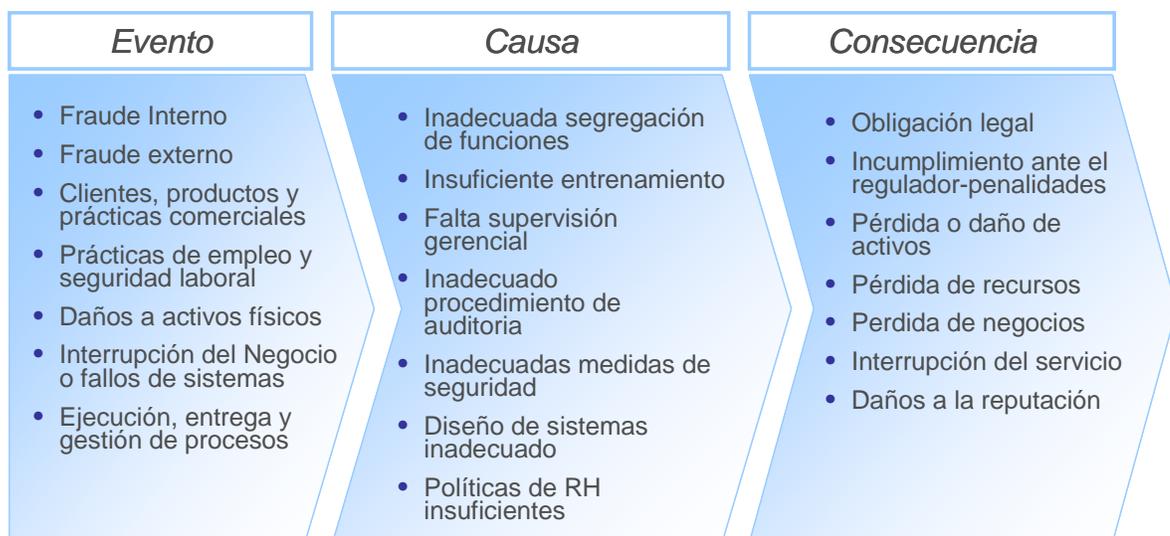


Figura N°2: Relación entre los eventos de Riesgo Operacional, las causas y sus consecuencias (Diseño e investigación propia).

Pérdida por riesgo operacional

Una pérdida por riesgo operacional, se define como el impacto negativo en resultados o en el patrimonio de la institución, como consecuencia de



cualquier evento de riesgo operacional; es decir, es la consecuencia en términos monetarios de la ocurrencia de un evento de riesgo operacional.

El riesgo operacional causa dos tipos de pérdidas, estas son contables o directas y no contables o indirectas.

Las pérdidas contables evidencian los niveles de riesgo de la institución y son aquellas mostradas específicamente en los registros contables.

Las pérdidas no contables son aquellas que permiten establecer estimaciones hacia posibles pérdidas que afecten a la institución, estas pueden ser:

- Exposición o Potenciales: Se refieren al impacto de los eventos ocurridos antes de ser analizados y registrados contablemente.
- Lucro cesante: Referidas a la pérdida de ingresos o de negocios futuros.
- De reputación: Se refieren a los eventos que causan afectación de la imagen de la institución al verse involucrada involuntariamente en transacciones ilícitas con clientes, por fallas operacionales, fallas en el cumplimiento de leyes y regulaciones, o por cualquier otro evento externo.



CAPÍTULO III:

MARCO DE GESTIÓN PARA DETERMINAR EL PERFIL DE RIESGO OPERACIONAL

El artículo 3 de la resolución 136.03 emitida por la SUDEBAN, señala que las instituciones financieras venezolanas deben aplicar técnicas básicas para la administración integral de riesgos, y considera como tales la identificación, medición y control de los riesgos.

En lo que respecta al riesgo operacional, en el numeral 4 del artículo 7 señala que deben implementarse

“procedimientos de evaluación acerca de la correcta interacción de los procesos, actividades, sistemas y prácticas utilizadas en las áreas operativas y administrativas a los fines de controlar y monitorear situaciones o condiciones que puedan derivar en pérdidas o inadecuadas asignaciones de recursos”.

Asimismo, señala la importancia de “implementar mediciones de pérdidas que se originen por actividades, áreas o procesos internos, a los fines de contar con registros históricos que permitan determinar áreas o procesos con mayor susceptibilidad a la generación de pérdidas”. Todo ello con la finalidad de minimizar los factores generadores de riesgo operacional.

Por su parte el Comité de Basilea, en su documento Buenas prácticas para la gestión y supervisión del riesgo operativo, es más concreto y entiende por la gestión del riesgo operacional a la “identificación, evaluación, seguimiento y control o cobertura” del riesgo y reconoce que el método que elija cada banco para gestionarlo dependerá de una serie de factores, como son su tamaño, su sofisticación y la naturaleza y complejidad de sus actividades.



En lo que se refiere a la participación de la junta directiva, ambos entes consideran que las instituciones financieras deben involucrar a sus miembros y a la alta gerencia en la gestión integral de todos los riesgos de la organización, enfatizando su participación en el proceso de toma de riesgos.

Considerando lo establecido por la SUDEBAN y por el Comité de Basilea, la gestión de riesgos se enfocará partiendo de dos enfoques complementarios, uno a nivel macro y el otro a nivel micro.

Tal como se muestra en la Figura N°2 ambos enfoques están enmarcados en la cultura de riesgo y control⁶ de la organización, ya que en la medida que una organización posea una sólida cultura de riesgo y control, en esa misma medida los riesgos serán entendidos y gestionados adecuadamente, y los controles serán comprendidos y ejecutados como los medios para proteger el negocio y minimizar las consecuencias que los riesgos pudieran causar en él.

La cultura de riesgo y control debe ser reforzada en forma periódica a lo largo de toda la organización, incluyendo aquellos conceptos relacionados con la gestión de riesgos que sus integrantes deben conocer, ejemplificando hechos de la actividad diaria que los ilustren acerca de cómo actuar frente a determinadas situaciones y destacando lo importante de su participación y la forma en la cual pueden ser parte de la gestión de riesgos en la organización.

La implantación exitosa de un marco para la gestión del riesgo operacional requiere de la participación activa y del compromiso de todos los miembros

⁶ La cultura de riesgo es definida por PricewaterhouseCoopers como el “conjunto de valores, actitudes y prácticas compartidas que caracterizan la forma cómo una organización considera y enfrenta los riesgos de sus actividades del día a día”; también define la cultura de control como el entendimiento de los controles por parte de la organización.



de la organización. En este sentido, es necesario sensibilizar a todo el personal en este tema incluyendo a la alta dirección de la organización, ya que de ella se requiere un apoyo e incentivo absoluto, con el fin de impulsar el cumplimiento de las directrices que emanen de la unidad responsable de su gestión y de las regulaciones nacionales y las mejores prácticas internacionales.

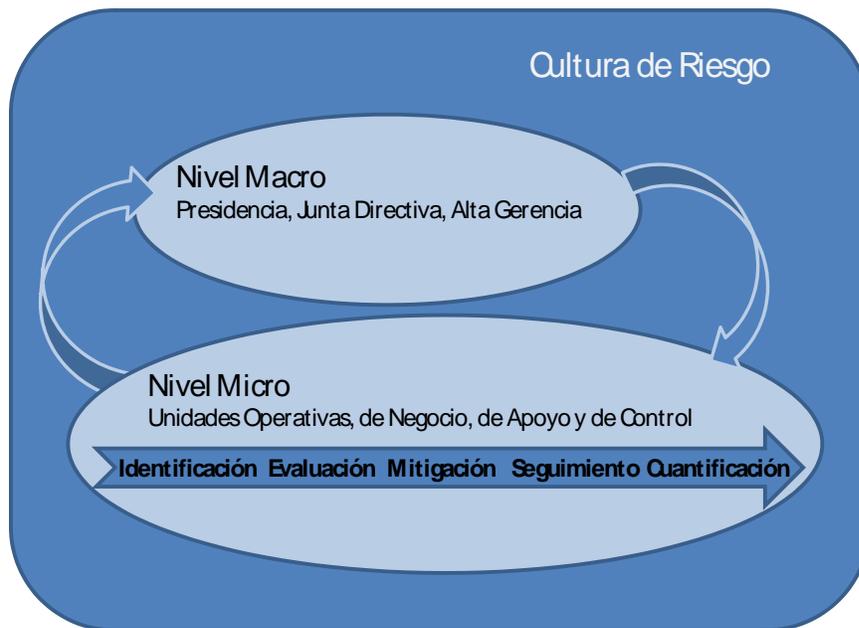


Figura N° 3: Esquema de Gestión del Riesgo Operacional (Diseño e investigación propia).

1.- Enfoque Macro

Este enfoque se basa en lo establecido por el Comité de Basilea y por la SUDEBAN, en relación a que la junta directiva debe involucrarse en el conocimiento y evaluación de los principales riesgos operacionales que afectan a la institución, a fin de orientar las decisiones hacia el perfil de riesgo deseado.



En ese sentido, este enfoque parte de la planificación estratégica de la institución y consiste en obtener un inventario de los riesgos operacionales que afectarían su cumplimiento, para ello es necesario tener amplio conocimiento del negocio y analizar cada uno de los objetivos estratégicos planteados, considerando como afecta la situación del entorno a los objetivos del negocio y analizando los eventos de pérdida por riesgo operacional que hayan ocurrido.

En este análisis están involucrados los integrantes de la junta directiva, el presidente de la institución y la alta gerencia. Una vez identificados estos riesgos, deben ser valorados estimando el impacto en términos de la pérdida que pudiera representar para la institución financiera el incumplimiento de ese objetivo y la frecuencia estimada de que ello ocurra. Para ello la institución debe establecer escalas en base a las pérdidas que hayan ocurrido en el pasado, que permitan definir cuales riesgos está dispuesta a aceptar y cuales exceden su capacidad de aceptación.

En el caso de estos últimos, la institución debe responder ante los riesgos ya sea reduciéndolos, compartiéndolos o evitándolos y los participantes de alto nivel mencionados, deben promover el diseño de las respuestas adecuadas por parte de las unidades responsables de gestionarlos y efectuar el seguimiento de las acciones que se planteen realizar.

2.- Enfoque Micro

El Comité de Basilea en su documento Buenas prácticas para la gestión y supervisión del riesgo operativo, señala que la alta gerencia debe responsabilizarse de la puesta en práctica, a lo largo de toda la organización, del marco para la gestión del riesgo operacional que apruebe la junta directiva. Asimismo señala que las instituciones financieras deben desarrollar políticas, procesos y procedimientos para su gestión y que los bancos



deberán identificar y evaluar los riesgos operacionales inherentes a todos sus productos, actividades, procesos y sistemas relevantes.

El enfoque micro que aquí se presenta está fundamentado en lo establecido por Basilea, y está dirigido a toda la organización considerando las unidades operativas, de negocio, de control y de apoyo.

La gestión del riesgo operacional debe coexistir con el día a día de todos los individuos que integran la organización, sin embargo debe lograrse la creación de un área encargada de coordinarla y de dictar los lineamientos para que la misma se ejecute adecuadamente, observando el marco legal que rige la materia y las mejores prácticas.

Esta área debe mantenerse relacionada con aquellas encargadas de gestionar los demás riesgos que afectan a la institución financiera y reportar sus avances a una unidad de riesgo integral que reporte directamente a la junta directiva, a fin de que la gestión de riesgos sea global y de que el ente mencionado se mantenga informado de los logros en la gestión del riesgo operacional.

Según lo establecido por Basilea II y por la SUDEBAN en relación a las fases que deben integrar el marco de gestión del riesgo operacional, y luego de revisar los informes anuales de importantes instituciones financieras a nivel internacional como son el Grupo BBVA y Santander, se consideran las siguientes fases:

1. Identificación

La identificación de riesgos operacionales en las instituciones financieras se logra a través de dos vías, una de ellas es el análisis de los eventos que suceden por causas operacionales en el acontecer diario de la organización y la otra se corresponde con las evaluaciones realizadas a sus procesos y a los productos que ofrece.



Los eventos de riesgo operacional constituyen una guía para identificar focos de riesgo que luego deben ser analizados con más detalle en la evaluación de un proceso. El análisis de un evento debe contemplar fundamentalmente la identificación de sus causas y sus consecuencias, tanto operativas como económicas.

Para realizar la identificación de riesgos operacionales en los procesos, se debe revisar cierta información y contar con la participación del personal encargado de ejecutarlos. En cuanto a la información necesaria, se considera importante entender el objetivo del proceso, conocer el marco regulatorio que le aplica, identificar las áreas de la organización involucradas, conocer los resultados de auditorías anteriores realizadas y la ocurrencia o no de eventos de riesgo operacional asociados al proceso.

Las herramientas usadas en la identificación de riesgos pueden ser entrevistas, análisis de los flujos del proceso y cuestionarios preparados previamente.

Como se mencionó anteriormente los eventos de riesgo operacional son un punto de partida para identificar y evaluar riesgos, por ello es necesario que exista una base de datos de eventos de pérdida que los agrupe y permita a la organización contar con una estructura de datos significativa, organizada, y transparente.

Dicha base de datos debe contener información cuantitativa y cualitativa. La información cualitativa incluirá lo referente a las causas, consecuencias, unidades involucradas y descripción del evento; por su parte dentro de la información cuantitativa debe incluirse la exposición monetaria del evento, la pérdida que se produjo (en caso de que se haya producido) y el número de veces que ocurrió.



La identificación de riesgos es la base para su evaluación y cuantificación. En el momento de identificar los riesgos es necesario tener una posición neutra frente a los controles, a fin de tener una visión clara de cuáles son los riesgos inherentes⁷ a los cuales está expuesto el proceso independientemente de los controles que existan.

2. Evaluación

Una vez identificados los riesgos, su evaluación consiste en determinar la severidad y la frecuencia de cada uno de ellos. La severidad se refiere al impacto en términos monetarios que produciría la materialización del riesgo y la frecuencia es la medida expresada por el número de veces que pudiera ocurrir en un periodo determinado. Asimismo, deben considerarse impactos cualitativos que pudieran materializar riesgos de reputación para la institución.

Para evaluar un riesgo se debe considerar la naturaleza del proceso, los controles existentes, los controles que serían necesarios, las implicaciones legales y en la reputación, y los niveles de calidad esperados.

La evaluación permite determinar el impacto de los riesgos identificados y en función de ello dirigir los recursos disponibles, dependiendo de la prioridad que representen para la institución, lo que a su vez sirve de base para analizarlos, cuantificarlos y realizar la asignación de capital requerido por riesgo operacional.

⁷ El riesgo inherente se define como la posibilidad de que ocurran errores o irregularidades significativas, sin considerar el efecto del control interno, es decir, el riesgo inherente es aquel riesgo que es propio del trabajo a realizar. Por su parte el riesgo residual es el riesgo resultante de la aplicación de acciones de mitigación y, por tanto, constituye el riesgo a asumir.



A partir de la evaluación que se realiza de los riesgos se generan los llamados mapas de riesgos. Los mapas de riesgos constituyen una representación gráfica de los riesgos identificados, según su severidad y frecuencia. La figura siguiente es un mapa de riesgos.



Figura N°4: Mapa de riesgos operacionales (PriceWaterhouseCoopers. Workshop de Riesgo Operacional).

Como puede observarse, si el riesgo es considerado bajo o aceptable, debe ser monitoreado para asegurar que se mantenga en niveles aceptados por la institución. Por el contrario, si el riesgo no se considera bajo o aceptable, se deben diseñar e implantar planes de acción que permitan mitigarlo, o que al menos aseguren un tratamiento adecuado del riesgo.

Al igual como se mencionó en el Enfoque Macro, para la elaboración de los mapas de riesgo, la organización debe definir escalas de medición en base a las pérdidas que hayan ocurrido en el pasado, que permitan definir cuales



riesgos está dispuesta a aceptar la institución y cuales exceden su capacidad de aceptación.

3. Mitigación

Una vez realizada la evaluación de riesgos, se determina que acciones deben diseñarse para responder (evitar, compartir, aceptar, reducir) ante los riesgos identificados.

Las acciones de mitigación nacen a partir de los riesgos identificados y dependen de la relación costo-beneficio, es decir el costo del mitigante no debe ser mayor a la pérdida que se persigue evitar mitigando el riesgo. Asimismo, al decidir acerca de la implantación de un mitigante se debe considerar el tiempo y la factibilidad de su implantación.

La responsabilidad de implantar el mitigante recae sobre el área o unidad de la institución que se vería afectada por la pérdida ocasionada como consecuencia de la materialización del riesgo identificado, es decir, la responsabilidad no recae necesariamente en la unidad encargada de ejecutar el proceso en el cual se identificó el riesgo operacional.

Dentro de la gestión de riesgos operacionales en las instituciones financieras existen dos grandes mitigantes, el uso de pólizas de seguro y la implantación de un programa de continuidad de negocio (PCN)⁸, ambos orientados a la mitigación de riesgos de alta severidad como podrían ser desastres naturales

⁸ El Programa de Continuidad de Negocio es un proceso que identifica los impactos potenciales que amenazan a la Organización y provee un marco para su recuperación, gracias a la capacidad de responder eficazmente al resguardo de los empleados, los intereses de los accionistas, la reputación, la imagen y las actividades de creación de valor.



y fallas que interrumpen la continuidad de las operaciones durante un período de tiempo significativo.

4. Seguimiento

Un efectivo proceso de seguimiento es esencial para gestionar adecuadamente el riesgo operacional.

Las actividades de seguimiento continuas ofrecen la ventaja de detectar y corregir deficiencias en políticas, procesos y procedimientos existentes, y a su vez, la pronta detección y el manejo de estas deficiencias, reduce sustancialmente la severidad potencial de un evento de pérdida.

El monitoreo, incluido el reporte regular a la junta directiva y la alta gerencia, debe ser parte de las actividades en el proceso de gestión de los riesgos operacionales. Una comunicación efectiva es importante para asegurar que los responsables de implementar la mitigación de los riesgos entiendan la necesidad de tomar las acciones requeridas, lo cual provee transparencia a la gestión de riesgo operacional.

El seguimiento permite mostrar la situación, evolución y comportamiento de los eventos ocurridos y de los riesgos identificados, así como también de la efectividad de las acciones de mitigación. El seguimiento se realiza a través de:

- Reportes de eventos, realizados periódicamente con determinada frecuencia y que divulguen información acerca de la gestión y estatus de los riesgos operacionales, es decir reportes donde se muestre la ocurrencia de eventos de riesgo operacional en el tiempo, clasificándolos según las categorías establecidas por Basilea, haciendo mención de sus causas y de las consecuencias originadas. La elaboración regular de estos reportes y su distribución a los niveles



apropiados, sirve como medio de comunicación a los altos niveles de la organización.

- Monitoreo a los resultados de las evaluaciones de Riesgo Operacional realizadas.
- Monitoreo de los Indicadores Claves de Riesgo (KRI's).
- Seguimiento a los planes de acción implantados como consecuencia de las evaluaciones de riesgo de procesos y de productos.

A este respecto el Comité de Basilea establece que la alta dirección deberá recibir periódicamente informes de la unidad encargada de la gestión del riesgo operacional, que recojan información interna sobre aspectos financieros, operativos y de cumplimiento, así como información externa sobre acontecimientos y condiciones que sean pertinentes para la toma de decisiones. Además, establece que la junta directiva deberá recibir información de alto nivel que sea suficiente para poder formarse una opinión acerca del perfil de riesgo operacional general del banco y estudiar las implicaciones estratégicas y sustanciales para su actividad.

5. Cuantificación:

El paso previo y necesario para cuantificar el riesgo operacional, es identificar los riesgos y evaluar su impacto y frecuencia de ocurrencia.

En la cuantificación del riesgo operacional la información y sus fuentes son aspectos fundamentales, se requiere de datos que aseguren la integridad y confianza en los análisis y conclusiones que se extraigan, ya que en base a estos análisis se tomarán decisiones de importancia para el negocio y la continuidad de las operaciones de la institución financiera.

A este respecto el Comité de Basilea en su documento Buenas prácticas para la gestión y supervisión del riesgo operativo indica que



“algunas empresas han comenzado a cuantificar su exposición al riesgo operativo utilizando diversos métodos. Uno de ellos es utilizar el historial de pérdidas de un banco, que puede revelar datos muy útiles para evaluar la exposición de un banco al riesgo operativo y desarrollar una política para cubrir o controlar el riesgo. Una manera muy eficaz de utilizar correctamente esta información es establecer un marco para registrar y consignar sistemáticamente la frecuencia, gravedad y otros aspectos importantes de cada caso de pérdida. Algunos bancos también combinan los datos sobre pérdidas internas con datos sobre pérdidas externas, análisis de escenarios y factores de evaluación del riesgo”.

Asimismo dicho comité recomienda que:

- Las instituciones financieras deberán incluir todas las pérdidas por riesgo operacional relevantes, de acuerdo a la definición de este tipo de riesgo y a los tipos de eventos de pérdidas
- Los datos internos de pérdida sean integrales e incluyan la totalidad de las actividades y posiciones relevantes en todos los subsistemas y en todas las ubicaciones geográficas pertinentes.
- La institución financiera recopile información sobre la fecha del evento, cualquier recuperación con respecto a las cantidades brutas de las pérdidas, así como información de carácter descriptivo sobre las causas del evento de pérdida. El grado de detalle de la información descriptiva deberá estar en proporción al importe bruto de la pérdida.

Como se indicó en el aparte de la Identificación, la mayor fuente de información de riesgos operacionales, está representada en la ocurrencia de eventos internos o externos que puedan exponer a la organización a



pérdidas reales o potenciales y afectar el patrimonio y/o la reputación de la misma. En este sentido la institución financiera debe diseñar metodologías y herramientas, incluyendo la creación de repositorios de información que permitan agrupar los eventos de riesgo ocurridos en el tiempo y realizar los análisis para establecer tendencias, investigar las causas y tomar medidas que mitiguen las pérdidas ocasionadas y prevengan la ocurrencia de futuros eventos.

La importancia de almacenar en forma estandarizada esta información, radica en su utilización como insumo principal para la determinación del perfil de riesgo operacional de la institución financiera, que permitirá definir los niveles de riesgos que ésta aceptará, mitigará, transferirá o evitará, para posteriormente determinar cuál será el nivel de capital necesario para cubrir las pérdidas operativas inesperadas.



CAPÍTULO IV:

UNIDADES PARTICIPANTES EN LA GESTIÓN DEL RIESGO OPERACIONAL

El Comité de Basilea no indica expresamente que unidades deben involucrarse en la gestión del riesgo operacional, sin embargo señala la importancia de que toda la organización participe en ello y resalta la función de la unidad de auditoría interna y de la junta directiva como actores principales en la supervisión de dicha gestión.

En su documento titulado Buenas prácticas para la gestión y supervisión del riesgo operativo, el Comité de Basilea establece que

“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”.

“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”.



Por su parte la SUDEBAN, en su mencionada resolución N°136.03, exige el establecimiento de una estructura de administración integral de riesgos que sea formal, eficiente y eficaz, que permita la identificación, medición y control de los riesgos, y que incluya la participación de los más altos ejecutivos de la organización y de la junta directiva.

La SUDEBAN hace referencia directa a la participación de la junta directiva, el consejo de administración, la presidencia y la alta dirección, en la evaluación de todos los riesgos y en la toma de decisiones orientadas a la modificación de los límites que garanticen el perfil de riesgo deseado. Igualmente, señala que la junta directiva o el consejo de administración deberán constituir un Comité de Riesgos, cuyo objetivo sea la administración, identificación, medición y mitigación de los riesgos a que se encuentra expuesta la institución financiera, de manera que el perfil de riesgos sea el deseado por ésta. Dicho comité tendrá bajo su supervisión la unidad de administración integral del riesgos, la cual será responsable de proponer las políticas de riesgos para la institución financiera de acuerdo con los lineamientos fijados por la junta directiva, velar por el cumplimiento de los límites de exposición al riesgo y establecer las líneas de comunicación con las unidades adscritas a las áreas de prevención y control de legitimación de capitales, legal, auditoría interna y/o contraloría.

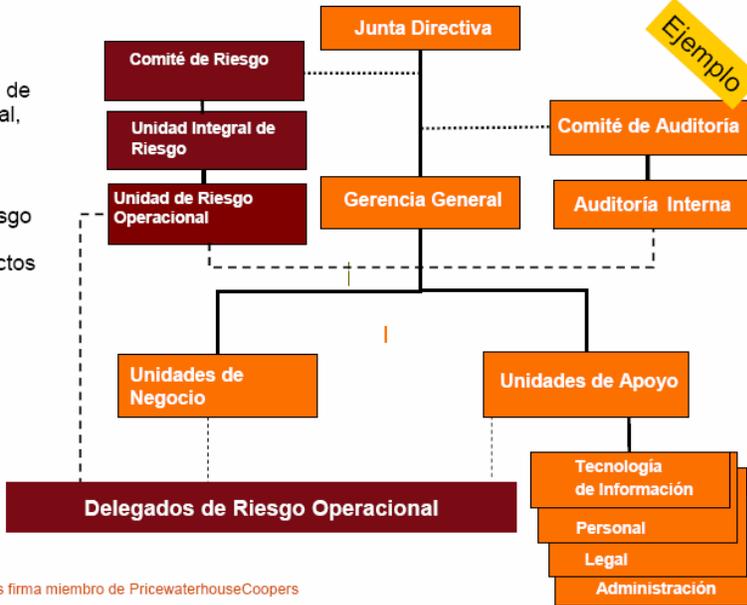
Según la empresa consultora PricewaterhouseCoopers, los siguientes son ejemplos de estructura organizativa para la gestión integral de riesgos:



Modelo organizativo de Gestión de Riesgo Operacional

Centralizado:

- Existe una Unidad de Riesgo Operacional, independiente de Auditoría Interna
- Estructura de Delegados de Riesgo Operacional - responsables directos en unidades de negocio y apoyo

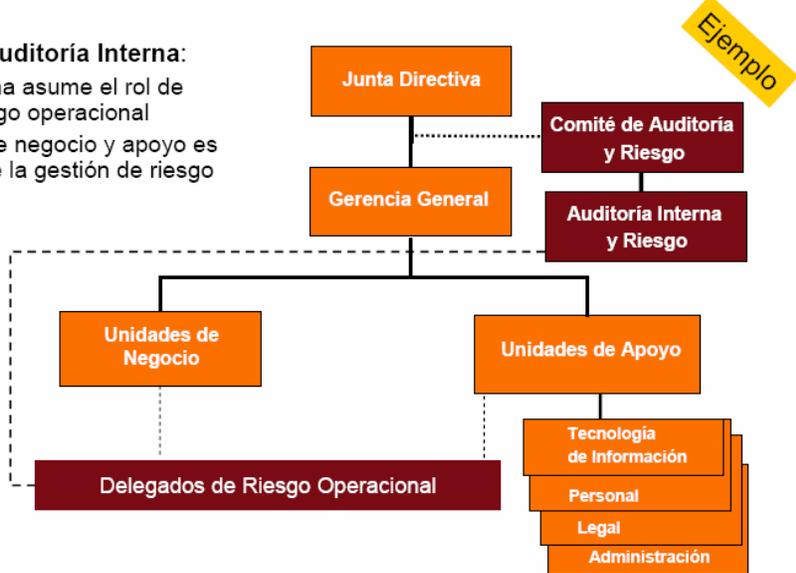


Espiñeira, Sheldon y Asociados firma miembro de PricewaterhouseCoopers

Modelo organizativo de Gestión de Riesgo Operacional

Liderado por Auditoría Interna:

- Auditoría Interna asume el rol de gestión de riesgo operacional
- Cada unidad de negocio y apoyo es responsable de la gestión de riesgo



Espiñeira, Sheldon y Asociados firma miembro de PricewaterhouseCoopers

Figura N°5: Modelo organizativo de gestión de Riesgo Operacional. (PriceWaterhouseCoopers. Workshop de Riesgo Operacional).



Cómo se observa, ni la normativa local ni las mejores prácticas, indican expresamente que unidades deben involucrarse en la gestión del riesgo operacional.

Luego de revisar los informes anuales de instituciones financieras con alcance internacional y de bancos universales venezolanos, puede inferirse que la gestión del riesgo operacional es una actividad que depende de todas las unidades de la organización, es decir, que cada una de ellas debe tomar conciencia de aquellos riesgos operacionales presentes en la ejecución de sus procesos, y que a su vez deben ser capaces de identificarlos y de comunicarlos a la unidad responsable de su gestión.

Dichos informes revelan la existencia de una estructura formal, creada para la gestión de riesgos, que incluye una unidad de riesgo integral a la cual reportan unidades encargadas de gestionar cada uno de los riesgos que afectan a las instituciones financieras (mercado, crédito, operacional, etc). Esta unidad de riesgo integral reporta a un comité de alto nivel, que a su vez reporta a la junta directiva de la institución financiera.

En lo que se refiere a la unidad encargada de gestionar el riesgo operacional, ésta posee unidades satélites en las líneas de negocio y en las geografías en las cuales la institución financiera tiene presencia. A su vez estas unidades, siguiendo las directrices y de acuerdo a las metodologías, procedimientos y herramientas creadas, deben consolidar los eventos de riesgo que ocurran en sus unidades de negocio, asegurar el registro correcto y oportuno de estos en la base de datos diseñada, realizar evaluaciones de riesgo a procesos, aplicaciones y a nuevos productos, generar informes de resultados, hacer seguimiento a los KRI's implantados, al avance los planes de acción que se implanten y al cumplimiento de políticas, procesos y procedimientos aprobados para el manejo del riesgo operacional.



La labor de las unidades de riesgo operacional en las líneas de negocio no termina con la evaluación de riesgos, éstas también deben monitorear situaciones internas-externas que sean consideradas riesgosas para la institución y, en este sentido, deben conocer de los resultados de las revisiones de auditoría realizadas.

A continuación se mencionan algunas unidades que, de acuerdo a las funciones que realizan, se consideran claves dentro de la gestión del riesgo operacional, tomando como punto de partida la interrelación que debe existir entre la unidad encargada de gestionar dicho riesgo y las demás unidades de la institución bancaria.

- Auditoría interna

Esta unidad informa de incumplimientos detectados y de su impacto operacional, ya que a través de las revisiones que realiza al resto de las unidades que integran la institución financiera, identifica riesgos existentes en los procesos, conoce de la ocurrencia de eventos de riesgo operacional y verifica el cumplimiento de las políticas y procedimientos de riesgo operacional en esas unidades.

Asimismo, la unidad de auditoría interna debe ser informada de los riesgos que identifiquen las unidades de Riesgo Operacional en los procesos y de las pérdidas reales y potenciales asociadas, a fin de que sirvan como insumo para sus planes de revisión.

- Legal

La unidad de Legal debe asesorar en el entendimiento del marco regulatorio vigente y en el conocimiento de las obligaciones legales que de él se deriven, a fin de asegurar su cumplimiento durante los procesos de evaluación de riesgos operacionales y de que sean considerados en el desarrollo de los



planes de mitigación que ameriten recomendaciones en materia legal. También debe informar acerca de eventos de riesgo legal vinculados con riesgos operacionales y de las pérdidas relacionadas con acciones legales o demandas (probabilidad de éxito e impacto financiero).

De igual forma, la unidad de Riesgo Operacional debe informar al área Legal de los riesgos que se hayan identificado en los procesos de la organización y de las pérdidas reales y potenciales asociadas.

- Prevención y control de legitimación de capitales

Esta unidad debe identificar y comunicar aquellos eventos de legitimación de capitales relacionados con riesgos operacionales, debe informar sobre las áreas y procesos susceptibles de legitimación de capitales a fin de que sean evaluados y apoyar en el desarrollo de normas, procedimientos de control y planes de mitigación, en los aspectos relacionados con temas de legitimación de capitales.

La unidad de prevención y control de legitimación de capitales también debe ser informada de los riesgos identificados por la unidad de riesgo operacional en las áreas y procesos de la organización, y de las pérdidas reales y potenciales asociadas.

- Operaciones

Las unidades de operaciones deben identificar y notificar la ocurrencia de eventos de riesgo tecnológico y riesgo operacional, así como los relacionados con los activos de información. Asimismo deben apoyar en el desarrollo de los planes de mitigación, a través de diagnósticos y recomendaciones en materia de tecnología y procesos.



Las unidades de operaciones deben ser informadas de los riesgos identificados por la unidad de riesgo operacional en las áreas y procesos de la organización, y de las pérdidas reales y potenciales asociadas.

- Contraloría y análisis financieros

La unidad de contraloría debe identificar riesgos operacionales que se deriven de la inadecuada aplicación de políticas contables y/o divulgación de información financiera. Así mismo, debe informar de la ocurrencia de eventos de naturaleza contable relacionados con riesgos operacionales, de la creación de provisiones y, en caso de ser necesario, debe apoyar en el desarrollo de las evaluaciones de riesgos y de los planes de mitigación en lo referente al tema contable.

La unidad de contraloría debe ser informada periódicamente de los riesgos operacionales presentes en la organización así como de las pérdidas reales y potenciales asociadas.

- Recursos humanos

La unidad de recursos humanos debe aplicar mecanismos de monitoreo y control a la conducta de los empleados, a fin de detectar riesgos relacionados con el factor gente y reportarlos a la unidad de riesgo operacional. Asimismo, esta unidad debe estar informada de los riesgos operacionales presentes en la organización y debe apoyar en la mitigación de aquellos riesgos relacionados con el recurso humano.

- Mercadeo y comunicaciones internas

La unidad de mercadeo debe diseñar y ejecutar campañas dirigidas a clientes y empleados, orientadas a reforzar todos aquellos aspectos que



permitan prevenir conductas internas y externas, que puedan traducirse en fuente de riesgos operacionales para la institución financiera.

De igual forma, la unidad de comunicaciones debe definir las estrategias y acciones a seguir, en relación al suministro de información a los medios de comunicación en momentos de crisis.

- Seguridad

La unidad de seguridad debe actuar como soporte en la investigación de actividades fraudulentas, tanto internas como externas, así mismo debe informar y apoyar en la mitigación de aquellos riesgos operacionales vinculados a la infraestructura de la institución bancaria y que pudieran afectarla físicamente.

Esta unidad es informada periódicamente de los riesgos operacionales presentes en la organización así como de las pérdidas reales y potenciales asociadas.



CAPÍTULO V:

IMPORTANCIA DE LA DETERMINACIÓN DEL PERFIL DE RIESGO OPERACIONAL

El Comité de Basilea define perfil de riesgo como “el nivel de riesgo de las actividades y/o categorías de riesgo de una empresa”.

Existen dos conceptos asociados al perfil de riesgo que son la tolerancia al riesgo y el apetito de riesgo, la tolerancia es la cantidad y la naturaleza de los riesgos que la institución financiera es capaz de aceptar, mientras que el apetito de riesgo es la cantidad y la naturaleza de los riesgos que ésta desea aceptar en razón de su rentabilidad y objetivos estratégicos.

El nivel de apetito y de tolerancia dentro de una institución financiera pudieran ser iguales, sin embargo dependiendo de las metas y la planificación que ésta se haya fijado, el apetito de riesgo puede ser superior o inferior a la tolerancia de la institución.

El Comité de Basilea, en su segundo acuerdo, incluyó el tratamiento explícito del riesgo operacional con incidencia directa en el requerimiento de capital de la institución financiera y establece que si este riesgo no se controla adecuadamente puede verse afectado el perfil de riesgo de la institución, quedando expuesta a pérdidas.

Asimismo, en su documento Buenas prácticas para la gestión y supervisión del riesgo operativo, establece que la formalidad y sofisticación del marco para su gestión debe estar acorde con el perfil de riesgo de la institución financiera y que debe abarcar tanto su apetito de riesgo como su tolerancia al mismo, “en virtud de sus políticas para gestionar estos riesgos y de sus criterios para establecer prioridades entre las actividades desarrolladas a tal



efecto, especificando hasta qué punto y de qué manera se transfiere el riesgo operativo fuera el banco”.

En función de esto, la gestión del riesgo operacional depende del perfil de riesgo de la institución, tomando en cuenta que cuanto mayor sea el apetito de riesgo de ésta, más adecuada debe ser la gestión de riesgos operacionales a fin de que los objetivos sean logrados reduciendo las pérdidas ocasionadas por este tipo de riesgo. Considerando la posibilidad de que ocurran pérdidas esperadas y pérdidas inesperadas que deben corresponderse con un nivel adecuado de capital a fin de asegurar su cobertura.

El perfil de riesgo operacional puede entenderse como el inventario de riesgos operacionales a los cuales está expuesta una institución financiera, clasificados según las categorías establecidas por Basilea y evaluados según su severidad y frecuencia. Estableciendo para ello ciertos niveles, que permitan distinguir las pérdidas por riesgos operacionales que estaría dispuesta a aceptar la institución según su fortaleza financiera.

El Comité de Basilea establece que las instituciones financieras deberán vigilar periódicamente su perfil de riesgo operacional y las exposiciones sustanciales a pérdida, reexaminando sus estrategias de control y reducción de riesgos.

Los siguientes gráficos muestran una distribución de pérdidas por riesgo operacional, en el cual se evidencia que las más frecuentes son pérdidas de montos poco significativos que se asumen como parte del negocio, mientras que las menos frecuentes son pérdidas inesperadas cuyo efecto puede ser importante o no dependiendo del impacto que tengan en la operatividad del negocio de la institución bancaria.

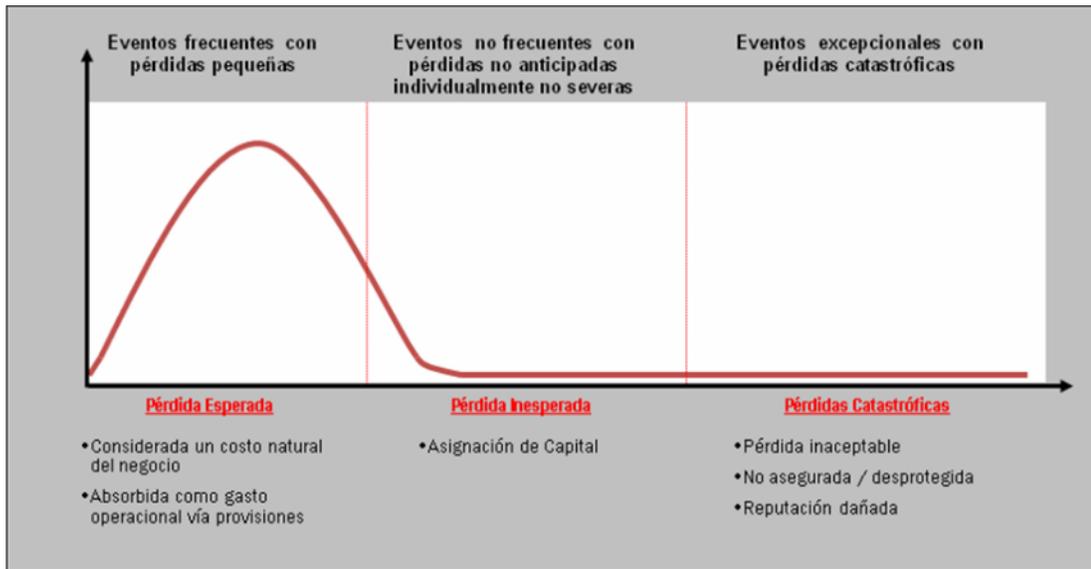
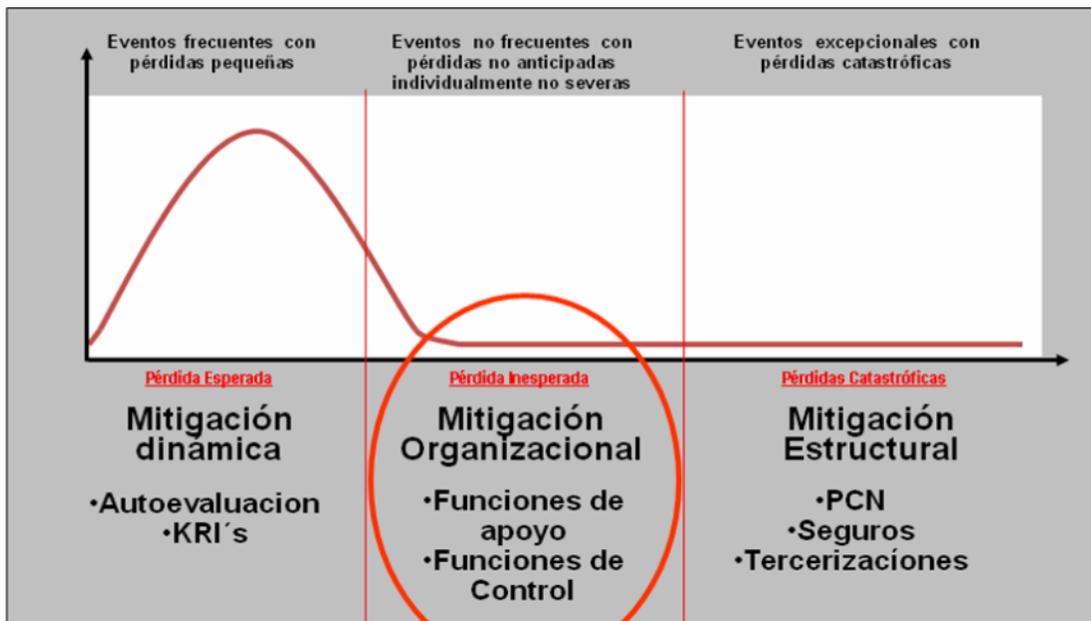


Figura N°6: Tipos de pérdida y perfil de riesgo operacional. (Grupo Santander --Enfoque de RO basado en la gestión de Procesos).



A mayor gestión, menor capital

Figura N°7: Perfil de riesgo operacional y tipos de mitigación. (Grupo Santander --Enfoque de RO basado en la gestión de Procesos).



Los gráficos hacen referencia a la mitigación de riesgos operacionales en relación con los tipos de pérdidas. Tomando como base lo expuesto en el tercer capítulo de esta investigación, la mitigación dinámica se refiere a la implantación y seguimiento de los mitigantes que surgen como resultado de las evaluaciones de riesgo operacional y del análisis de los eventos ocurridos, y que están orientados a aceptar, reducir y controlar dichos riesgos; la mitigación organizacional hace referencia a cubrir aquellas pérdidas que son inesperadas con el capital destinado por la institución financiera para tal fin; y la mitigación estructural se refiere a los grandes mitigantes que emplean las instituciones financieras en caso de eventos catastróficos y que están orientados a evitar y compartir dichos riesgos, como son el programa de continuidad de negocio y el programa de pólizas de seguro.

Por lo expuesto anteriormente, determinar el perfil de riesgo operacional es un aspecto importante dentro de la gestión integral de riesgos en las instituciones financieras, ya que:

- Crea una visión objetiva de la exposición al riesgo operacional, que facilita tomar acciones que minimicen el impacto de este riesgo en la institución financiera.
- Mejora la capacidad de decidir acerca de situaciones que la expongan a niveles de riesgo operacional superiores a aquellos que desee aceptar, por lo cual aumenta la transparencia en la gestión de riesgos.
- Alinea la gestión del riesgo operacional con la planificación estratégica de la organización.
- Existe mayor consistencia entre la gestión del riesgo operacional y los principales riesgos asumidos por la organización.



- Disminuye la vulnerabilidad de la institución financiera ante cambios significativos del entorno, lo cual se traduce en reducción de pérdidas financieras y del riesgo de reputación.
- Contribuye a lograr una adecuada asignación de capital por riesgo operacional.



CONCLUSIONES Y RECOMENDACIONES

El negocio financiero requiere administrar los riesgos que se derivan de su actividad, ya que una adecuada gestión de éstos tiene efectos positivos sobre la estabilidad de una industria cada vez más compleja y diversificada en cuanto a los servicios financieros que provee a sus clientes.

El riesgo operacional está presente en el día a día de las actividades que realiza una institución bancaria, razón por la cual éste riesgo difiere de otros tipos de riesgos, y se potencia cuando éstas realizan actividades nuevas o lanzan nuevos productos, participan en mercados que desconocen o realizan negocios en lugares lejanos.

El Comité de Basilea reconoce que la gestión del riesgo operacional siempre ha sido una parte importante del esfuerzo de las instituciones bancarias por evitar el fraude, mantener la integridad de los controles internos, reducir los errores en las operaciones, etc. Sin embargo, resulta novedoso considerar la gestión del riesgo operacional desde un punto de vista profesional y metodológico, es decir, en forma integral y comparable con lo riguroso de la gestión del riesgo de crédito o del riesgo de mercado.

Mundialmente los recientes casos conocidos de pérdidas en instituciones financieras, ocasionadas por causas de índole operacional han impulsado tanto a las instituciones como a los entes supervisores a tomar con seriedad la gestión de los riesgos operacionales.

Aunque en Venezuela dicha gestión todavía se está iniciando, inspirada y tomando como punto de partida la gestión del riesgo operacional que se realiza en instituciones financieras de alcance internacional, según los resultados de la encuesta anual realizada por Espiñeira Sheldon y Asociados en el año 2008, la mayoría de las empresas venezolanas reconocía que la



gestión integral de riesgos es un conjunto de conceptos integrados que agrega valor, ayuda a gestionar eficazmente los riesgos y representa una ventaja competitiva para las organizaciones.

El Comité de Basilea reconoce que el método que cada institución bancaria elija para la gestión del riesgo operacional dependerá de factores como su tamaño y la especialización de sus actividades, pero destaca la existencia de elementos que son fundamentales y deben ser comunes para lograr una adecuada gestión de éste riesgo. Entre estos elementos se encuentra la existencia de estrategias claramente definidas y seguimiento de las mismas por parte de la junta directiva y de la alta gerencia, la existencia de una sólida cultura de gestión del riesgo operacional y de control interno, y la aplicación de metodologías y procedimientos para la identificación, evaluación, cuantificación y mitigación de riesgos, considerando la existencia de una estructura de reporte para la transmisión interna de información y planes de contingencia en caso de eventos graves que interrumpen la continuidad de las operaciones.

La determinación del perfil de riesgo operacional de una institución bancaria, es una actividad estructurada y conjunta de todas las áreas que forman parte de ella, para lo cual es necesario un cambio en la cultura organizacional, donde la cooperación, la participación activa de la alta dirección, el apoyo de áreas de control como auditoría, legal y prevención de legitimación de capitales y la coordinación de funciones es fundamental, a fin de que éstas no se solapen unas con otras.

A través de la investigación partiendo de informes anuales de instituciones financieras venezolanas, se pudo evidenciar que la información histórica del riesgo operacional, tanto cualitativa como cuantitativa que permita realizar estudios comparativos dentro del sector, actualmente es escasa. A nivel internacional se observa más transparencia en cuanto a la información



disponible, sin embargo la comparación no es tarea fácil porque no todas las instituciones financieras publican el mismo tipo de información.

Esta situación constituye un gran reto para el sector financiero nacional, ya que la disponibilidad y transparencia de la información entre las instituciones financieras facilita la evaluación, análisis, medición, control, monitoreo y mitigación de los riesgos operacionales en ellas, al mismo tiempo que las encamina hacia la puesta en ejecución de las mejores prácticas enunciadas por el Comité de Basilea.

La cuantificación del riesgo operacional es una fase de suma importancia dentro de su gestión, ya que ella es el resultado de la identificación y evaluación de riesgos y a su vez permite determinar el perfil de riesgo operacional de la institución, pero dicha actividad no es tarea fácil.

Dada esta situación es necesario que la organización se familiarice con el lenguaje de riesgo operacional y que existan procedimientos claros que permitan la identificación y clasificación de los riesgos operacionales y de los eventos que ocurran. Asimismo, deben existir sistemas contables y de manejo de información que estén diseñados acorde con los procedimientos de detección y recolección de eventos de riesgo operacional.

El sector financiero venezolano debería promover la recolección de información de pérdidas entre las instituciones y permitir que aquellas que participen, compartan información. Esto lograría bases de datos más completas y con información más detallada, para medir la frecuencia, severidad y tendencia de las pérdidas, y obtener a su vez aproximaciones a pérdidas esperadas e inesperadas, a fin de orientar a las instituciones financieras en el desarrollo de modelos estadísticos de medición del riesgo operacional, que sean fiables y que provean enfoques de asignación de capital apropiados, siguiendo los métodos exigidos por el Comité de Basilea.



Un sólido proceso de gestión de riesgos es la base de una evaluación acertada de las posiciones de capital de una institución financiera. La junta directiva y la alta gerencia debe entender el tipo y nivel del riesgo asumido por el banco y la forma en que los riesgos asumidos se relacionan con niveles de capital adecuados, así como también asegurar la pertinencia de los procesos de gestión de riesgos, considerando el perfil de riesgo y la planificación estratégica.

Un marco adecuado para la suficiencia del capital debe asegurar la seguridad y solidez del sistema financiero y alentar continuas mejoras en la evaluación del riesgo.

La reciente crisis financiera pone de manifiesto que la herramienta más eficaz para enfrentarla es la prevención, a través de la gestión integral de los riesgos, la asignación adecuada de capital y la existencia de provisiones para los riesgos significativos en función del perfil de riesgos de cada institución.

Es indiscutible que la gestión del riesgo operacional es un elemento que facilita el logro de los objetivos del negocio, permitiéndole a la institución financiera prepararse ante cambios adversos del entorno, reduciendo de esta forma las pérdidas operacionales y fortaleciendo la cultura de riesgo y su reputación ante los grupos de interés con los cuales se relaciona como son clientes, reguladores, proveedores y la competencia.



REFERENCIAS BIBLIOGRÁFICAS

- Arias, F. (2006). *El proyecto de investigación* (5ta ed.). Caracas, Venezuela: Epísteme.
- Banescó. (2008). *Informe Anual*. Venezuela.
- Comité de Supervisión Bancaria de Basilea. (2001). *El nuevo acuerdo de capital*. (Documento PDF). URL <http://www.bis.org>
- Comité de Supervisión Bancaria de Basilea. (2003). *Buenas prácticas para la gestión y supervisión del riesgo operativo*. (Documento PDF). URL <http://www.bis.org>
- Comité de Supervisión Bancaria de Basilea. (2004). *Convergencia internacional de medidas y normas de capital*. (Documento PDF). URL <http://www.bis.org>
- Grupo BBVA. (2008). *Informe Anual*. España.
- Grupo Santander. (2008). *Informe Anual*. España.
- Hernández, E. (2008). Workshop *Top Down + Bottom Up: Una respuesta exitosa ante el reto del riesgo operacional*. Ponencia presentada en curso dictado por Espiñeira, Sheldon & Asociados, firma miembro de PWC. Caracas.
- Mercantil Banco Universal. (2008). *Memorias Anuales*. Venezuela.
- Marroquin, Y. (2003). *El Riesgo Operativo*. Ponencia presentada en conferencia sobre la gestión del Riesgo Operacional. Brasil.
- Santalla, Z. (2008). *Guía para la elaboración formal de reportes de investigación*. Caracas, Venezuela: UCAB.



SUDEBAN. (2003). *Resolución 136.03 Normas para una adecuada administración integral de riesgos*. Caracas: Autor.



ANEXO

CLASIFICACIÓN DE EVENTOS DE RIESGO OPERACIONAL SEGÚN EL COMITÉ DE BASILEA



Categorías de tipos de eventos (Nivel 1)	Definición	Categorías (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	Operaciones no reveladas intencionalmente. Operaciones no autorizadas (con pérdidas pecuniarias). Valoración errónea de posiciones (intencional).
		Hurto y fraude	Fraude / fraude crediticio/ depósitos sin valor. Hurto / extorsión / malversación / robo. Apropiación indebida de activos. Destrucción dolosa de activos. Falsificación. Utilización de cheques sin fondos. Contrabando. Apropiación de cuentas, de identidad, etc. Incumplimiento / evasión de impuestos (intencional). Soborno / cohecho. Abuso de información privilegiada (no a favor de la empresa).
Fraude externo	Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o soslayar la legislación, por parte de un tercero.	Hurto y fraude	Hurto/ robo. Falsificación. Utilización de cheques sin fondos.
		Seguridad de los sistemas	Daños por ataques informáticos. Robo de información (con pérdidas pecuniarias).
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 diversidad /discriminación.	Relaciones laborales	Cuestiones relativas a remuneración, prestaciones sociales, extinción de contratos. Organización laboral.
		Higiene y seguridad en el trabajo	Responsabilidad en general (resbalones, etc.) Casos relacionados con las normas de higiene y seguridad en el trabajo. Indemnización a los trabajadores.
		Diversidad y discriminación	Todo tipo de discriminación.
Clientes, 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	Abusos de confianza / incumplimiento de pautas. Aspectos de adecuación / divulgación de información (know your customer KYC, etc.). Quebrantamiento de la privacidad de información sobre clientes minoristas. Quebrantamiento de privacidad. Ventas agresivas. Confusión de cuentas. Abuso de información confidencial. Responsabilidad del prestamista.



		Prácticas empresariales o de mercado improcedentes	Prácticas restrictivas de la competencia. Prácticas comerciales / de mercado Improcedentes. Manipulación del mercado. Abuso de información privilegiada (a favor de la empresa). Actividades no autorizadas. Blanqueo de dinero
		Productos defectuosos	Defectos del producto (no autorizado, etc.) Error de los modelos.
		Selección, patrocinio y riesgos	Ausencia de investigación a clientes conforme a las directrices. Superación de los límites de riesgo frente a clientes.
		Actividades de asesoramiento	Litigios sobre resultados de las actividades de asesoramiento.
Daños a activos materiales	Pérdidas derivadas de daños o perjuicios a activos materiales como consecuencia de desastres naturales u otros acontecimientos.	Desastres y otros acontecimientos	Pérdidas por desastres naturales. Pérdidas humanas por causas externas (terrorismo, vandalismo).
Incidencias en el negocio y fallos en los sistemas	Pérdidas derivadas de incidencias en el negocio y de fallos en los sistemas.	Sistemas	Hardware. Software. Telecomunicaciones. Interrupción / incidencias en el suministro.
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.	Comunicación defectuosa. Errores de introducción de datos, mantenimiento o descarga. Incumplimiento de plazos o de Responsabilidades. Ejecución errónea de modelos / sistemas. Error contable / atribución a entidades erróneas. Errores en otras tareas. Fallo en la entrega. Fallo en la gestión del colateral. Mantenimiento de datos de referencia.
		Seguimiento y presentación de Informes.	Incumplimiento de la obligación de informar. Inexactitud de informes externos (con generación de pérdidas).
		Aceptación de clientes y documentación.	Inexistencia de autorizaciones / rechazos de clientes. Documentos jurídicos inexistentes / incompletos.
		Gestión de cuentas de clientes.	Acceso no autorizado a cuentas. Registros incorrectos de clientes (con generación de pérdidas). Pérdida o daño de activos de clientes por Negligencia.
		Contrapartes comerciales.	Fallos de contrapartes distintas de clientes Otros litigios con contrapartes distintas de Clientes.
		Distribuidores y proveedores.	Subcontratación. Litigios con distribuidores.

Fuente: Convergencia Internacional de Medidas y Normas de Capital. Comité de Basilea.