UNIVERSIDAD NACIONAL DE INGENIERÍA
FACULTAD DE INGENIERÍA INDUSTRIAL Y DE SISTEMAS

"MODELO PARA LA GESTIÓN DEL RIESGO OPERACIONAL EN LAS EMPRESAS DEL SECTOR FINANCIERO"

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE

INGENIERO INDUSTRIAL

POR LA MODALIDAD DE ACTUALIZACIÓN DE CONOCIMIENTOS

PRESENTADO POR:

CARLOS ALEJANDRO BOBADILLA GUERRERO

LIMA, PERÚ

MAYO DEL 2004

INDICE

DESCRIPTORES TEMÁTICOS

- Modelo de gestión
- Riesgo operacional
- Acuerdo de Capital de Basilea
- Eventos de riesgo
- Frecuencia y severidad
- Mapas de riesgo operacional
- Requerimientos de capital
- Medidas de mitigación
- Variables de influencia
- Indicadores clave de riesgo

RESUMEN

En el sector financiero se define el riesgo operacional como “el riesgo de que se produzcan perdidas como resultado de procesos, personal o sistemas internos inadecuados o defectuosos, o bien a consecuencia de acontecimientos externos”. Estos riesgos, si no son adecuadamente gestionados, pueden comprometer la viabilidad de las entidades y afectar a sus clientes y a los grupos de interés relacionados. El Comité de Supervisión Bancaria de Basilea (CSBB), conformado por representantes de las entidades supervisoras de los países con mayor desarrollo económico, ha formulado pautas para la gestión de los riesgos operacionales, referentes al papel y a las responsabilidades que competen a la dirección de las empresas, a la necesidad de crear un ambiente propicio para la gestión de los riesgos, y al establecimiento de estrategias, políticas y normas para su identificación, mitigación y control.

La propuesta del CSBB considera tres enfoques para la determinación del capital mínimo que las entidades deben mantener para cubrir sus riesgos operacionales: el método del indicador básico, el método estándar y los métodos de medición avanzada. Estos tres enfoques suponen, en ese mismo orden, sistemas más sofisticados y confiables de medición y control y, por consiguiente, menores requerimientos de capital. Los dos primeros enfoques determinan el capital mínimo en función del volumen de las operaciones, mientras que los métodos de medición avanzada, implican el uso de modelos matemáticos, bases de datos históricas, la integración de los procesos de medición dentro de los procesos del negocio, la identificación de los factores de riesgo, y el análisis de escenarios.

En el caso del Perú, en el año 2003 la Superintendencia de Banca y Seguros publicó una primera resolución sobre la gestión de los riesgos de operación. En esta norma se recogen las principales recomendaciones del CSBB, básicamente sobre el papel de la dirección, las políticas y procedimientos, y los aspectos administrativos de la gestión. También se ha dispuesto que las empresas auditoras y las clasificadoras de riesgo, incluyan en las evaluaciones que realicen, sus apreciaciones sobre los sistemas de gestión de estos riesgos. Se espera que, en breve plazo, se den disposiciones referentes a los requerimientos de capital económico por riesgo operacional.

Independientemente de la necesidad de cumplir con las regulaciones, la gestión del riesgo operacional constituye una necesidad de carácter estratégico para las empresas financieras, por ser una fuente de ventajas competitivas y además un medio para la creación de valor, para la empresa y los grupos de interés relacionados. Por ello es necesario asegurar que la gestión produzca el mejor resultado posible, y ello se puede lograr sólo si hay una definición clara de la estrategia, se diseñan los procesos adecuados, y se cuenta con los medios necesarios y un ambiente favorable. El conjunto de estos cuatro factores constituye el modelo de gestión.

La estrategia comprende la definición de los objetivos, la estructura organizacional y las políticas de gestión. Los procesos son las acciones concretas que constituyen el "día a día" de la gestión de los riesgos: identificación, mitigación, medición, seguimiento y generación de informes. Los medios comprenden la tecnología, las metodologías y procedimientos, y los recursos humanos. Por último está el ambiente adecuado, conformado por la cultura organizacional, el estilo de la dirección y la comunicación.

Los procesos constituyen el núcleo del modelo de gestión, y la clave para que estos se realicen de manera exitosa radica en que sean las unidades de negocio las que lleven el papel protagónico en su realización, contando con la orientación y el soporte técnico de una unidad central especializada, la cual debe estar además encargada de los aspectos corporativos de la gestión y del

desarrollo e implantación de las herramientas necesarias. Existen cinco procesos principales: identificación, mitigación, medición, seguimiento y generación de informes.

La identificación consiste en determinar qué riesgos existen y cuál puede ser su impacto, qué factores determinan los riesgos, en qué procesos ocurren, qué controles hay y como se puede mejorarlos, qué acciones se deben realizar y quién debe ejecutarlas.

Mediante la mitigación se trata de reducir la frecuencia y/o el impacto de los eventos de riesgo. Para ello existen diversas alternativas que, por lo general, implican costos adicionales. Por ello es que se deben considerar cuidadosamente los beneficios de las medidas de mitigación en relación al costo de implementarlas. Cuando los costos no lo justifiquen, las pérdidas derivadas de estos riesgos deben considerarse como parte del costo de estar en el negocio, incluirse en el precio de los productos y cubrirse con provisiones.

La medición proporciona información cuantitativa para la toma de decisiones, a través de los indicadores clave de riesgo, la explotación de bases de datos de eventos y pérdidas, el uso de modelos causales y de capital, y el control del desempeño de los grupos e individuos. La aplicación de métodos de medición avanzada requiere el uso de herramientas analíticas, como son la inferencia estadística, la regresión lineal múltiple, los modelos econométricos, el análisis multivariado, y otras técnicas relacionadas.

El seguimiento es el proceso de vigilar la evolución del riesgo a través de los indicadores clave y de las variables de influencia o *drivers*, para identificar señales de alerta que permitan tomar medidas correctivas oportunas. El seguimiento debe enfocarse fundamentalmente como una labor preventiva que debe dar valor añadido a los procesos, y no simplemente limitarse a identificar las razones de los eventos cuando ya es tarde para remediar sus consecuencias.

La generación de informes es el proceso que, a partir de los datos generados en los procesos anteriores presenta información consolidada y resumida, útil para las diferentes unidades de negocio así como para la alta dirección. Esta información incluye los mapas de riesgo, los informes de auto evaluación, el avance de proyectos, los eventos de pérdida, y los análisis de escenarios.

Los procesos descritos deben tener su soporte en los medios adecuados y suficientes: tecnología, metodologías y procedimientos, y recursos humanos; y debe además disponerse de un ambiente favorable para la gestión, que comprenda una cultura organizacional sólida, en el que sea evidente la identificación y el compromiso de la dirección y en el que existan canales de comunicación apropiados, para la transmisión y realimentación de la información.

INTRODUCCIÓN

Hasta hace poco tiempo el término riesgo tenía un significado casi exclusivamente negativo, y se le asociaba con el peligro de pérdidas o daños resultantes de accidentes, siniestros o catástrofes de todo tipo, sin embargo, el riesgo siempre ha sido un componente intrínseco en cualquier proceso de toma de decisiones, especialmente en el ambiente de los negocios, en donde está plenamente aceptado que el asumir determinados riesgos está directamente relacionado con la posibilidad de obtener beneficios. Es por esta razón que el conocimiento y la gestión adecuada de los riesgos, no sólo es un tema de seguridad y prevención sino que además se ha convertido en uno de los ingredientes principales para el éxito de cualquier empresa.

En el caso puntual de las empresas del sector financiero, el riesgo no sólo es inevitable, sino que es consustancial al negocio mismo y además es una de las fuentes fundamentales de beneficios. Como bien afirma el Dr. Chris Marrison[1], "Los bancos hacen dinero de dos maneras: proporcionando servicios y tomando riesgos", consecuentemente, si las ganancias están en relación directa con los riesgos asumidos, entonces un buen esquema de gestión de los riesgos se convierte en fuente de ventajas competitivas y, por lo tanto, debe considerarse dentro del plan estratégico de las empresas.

Existen tres tipos principales de riesgos que deben ser manejados por las entidades financieras: riesgos de mercado, riesgos de crédito y riesgos

[1] Marrison, Chris, *The Fundamentals of Risk Measurement*, editorial Mac Graw-Hill, Nueva York, 2002, página 1.

operacionales. El Comité de Supervisión Bancaria de Basilea ha definido como riesgo operacional: "el riesgo de que se produzcan pérdidas como resultado de procesos, personal o sistemas internos inadecuados o defectuosos, o bien a consecuencia de acontecimientos externos" [2].

Los notable innovación en los productos financieros y los desarrollos tecnológicos de los últimos años, entre ellos la automatización de los procesos que realizan los bancos, el número cada vez mayor de servicios que se brindan a través de la Internet, las fusiones entre entidades con la consiguiente necesidad de integrar sistemas, y la tendencia a la "tercerización" de aquellos procesos que no están el la "línea" del negocio, han aumentado considerablemente la variedad de los posibles eventos de riesgo operacional, eventos que pueden ser cada vez más frecuentes y con un mayor impacto económico.

El propósito de este trabajo es mostrar un modelo básico para la gestión del riesgo operacional en las empresas del sector financiero, a partir de la normativa establecida para tal efecto por la Superintendencia de Banca y Seguros - SBS, y de acuerdo a las recomendaciones del Comité de Supervisión Bancaria de Basilea, cuyos objetivos son la determinación del patrimonio que estas entidades deben asignar a la cobertura del riesgo operacional. Los conceptos que han servido de base para la preparación de este trabajo, provienen de la revisión de la literatura especializada, de información obtenida de fuentes públicas, principalmente a través de la Internet, y de la experiencia profesional del autor.

El modelo de gestión que aquí se plantea comprende cuatro componentes principales: la estrategia, los procesos, los medios y el ambiente. Este modelo debe estar integrado dentro de los procesos de negocio de la empresa y alineado con el plan estratégico orientado al logro de sus objetivos a largo plazo. En este trabajo se dan los lineamientos generales para que el modelo se

---

[2] Comité de Supervisión Bancaria de Basilea, *Presentación del Nuevo Acuerdo de Capital de Basilea, Documento de Consulta*, Banco de Pagos Internacionales, abril del 2003, página 11. Documento disponible en el sitio web www.bis.org

materialice en una estructura organizativa apropiada, correspondiendo a cada empresa establecer los enfoques particulares que deberán aplicarse al momento de definir al detalle cada uno de sus componentes.

El trabajo consta de 9 capítulos. El capítulo 1 se ocupa de los conceptos generales sobre los riesgos financieros y operacionales, incluyendo las recomendaciones del Nuevo Acuerdo de Capital de Basilea y las disposiciones dadas por la SBS sobre esta materia. En el capítulo 2 se señala que la gestión del riesgo operacional, no solo es consecuencia de la evolución y tendencias del sector financiero, sino que además constituye una necesidad de carácter estratégico y una forma de generar ventajas competitivas sostenibles; el modelo de gestión surge así como un medio para orientar los esfuerzos de toda la organización hacia el logro de los mejores resultados.

Los capítulos del 3 al 6 abordan cada uno de los cuatro componentes del modelo. El capítulo 7 se ocupa de las consideraciones de carácter económico, e incluye un ejemplo para enfocar la evaluación de la inversión inicial y los gastos relacionados con la gestión. El capítulo 8 se ocupa del nuevo papel que le corresponde a la función de auditoria interna y el capítulo 9 contiene las conclusiones y recomendaciones. Finalmente se señalan los principales libros y fuentes consultadas y se incluyen 5 anexos con información que se considera importante para la cabal comprensión del tema.

CAPITULO 1: MARCO CONCEPTUAL

1. MARCO CONCEPTUAL

1.1. EL RIESGO EN EL SECTOR FINANCIERO

Las empresas del sector financiero están expuestas a diferentes tipos de riesgos, los cuales se pueden clasificar en las siguientes seis categorías principales:

- Riesgo de mercado: Es el riesgo de pérdidas derivado de un movimiento adverso en el nivel o en la volatilidad del precio de mercado de los instrumentos financieros, asociados a una cartera, posición o entidad. Incluye los riesgos de tipos de interés, tipos de cambio, precio de las acciones y precio de los derivados y *commodities.*
- Riesgo de crédito: Es el riesgo de pérdidas que se deriva de la posibilidad de incumplimiento de la contraparte en una operación que incluya un compromiso de pago. Se incluyen en esta categoría lo riesgos de insolvencia (contraparte y emisor), el riesgo país, y el riesgo de liquidación.
- Riesgo de liquidez: Es el riesgo de no poder deshacer una posición en el mercado sin afectar el precio del producto correspondiente, haciendo difícil u onerosa su cobertura. Incluye también el riesgo de no poder financiarse en el mercado interbancario en la cuantía necesaria.
- Riesgo legal: Es el riesgo de pérdida debido a la posibilidad de que un contrato no pueda ser ejecutado porque las operaciones

no se encuentren dentro del marco legal establecido por la autoridad competente o bien por condicionamientos de tipo fiscal no contemplados inicialmente.

- Riesgo operacional: Su definición se verá más adelante.
- Riesgo de reputación: Es el relativo a las pérdidas que podrían resultar como consecuencia de la no concreción de oportunidades de negocio atribuibles a un desprestigio de la institución, por falta de capacitación del personal clave, fraude o errores en la ejecución de alguna operación.
- Riesgo Estratégico: Es el riesgo inherente a las decisiones propias del negocio y que puede afectar la rentabilidad de la empresa, como por ejemplo la inversión en el desarrollo de un nuevo producto, la expansión de las operaciones a otras zonas geográficas, o la fusión con otra empresa.
- Riesgo Sistémico: Es el riesgo de que los problemas que pudieran presentarse en alguna entidad financiera, en algún mercado o en determinado país, puedan trasladarse al conjunto de las entidades financieras, a otros mercados o a otros países.

1.2. DEFINICIÓN DE RIESGO OPERACIONAL

Hasta hace pocos años el riesgo operacional no había sido visto como un tipo especifico de riesgo, sin embargo, siguiendo el ejemplo de otras industrias, como es el caso de las del sector energético, el sector financiero empezó a reconocerlos como un riesgo de características particulares y a destinar recursos cada vez más importantes para detectarlo, clasificarlo, medirlo y gestionarlo. Posiblemente es debido a ello que el Comité de Supervisión Bancaria de Basilea, al que en adelante nos referiremos como el Comité o con las siglas CSBB, decidió incluir un requerimiento explícito de capital para este tipo de riesgo, en la revisión del "Acuerdo de Basilea de 1988", denominado "Nuevo Acuerdo de

Capital de Basilea" (NACB), conocido también como "Basilea II" o "BIS II", cuya entrada en vigencia está prevista para el año 2006.

Inicialmente se entendía por riesgo operacional todo aquel tipo de riesgo que no podía calificarse como riesgo de mercado o de crédito. Actualmente el Comité define el riesgo operacional como "El riesgo de que se produzcan perdidas como resultado de procesos, personal o sistemas internos inadecuados o defectuosos, o bien a consecuencia de acontecimientos externos". Esta definición incluye el riesgo legal pero no incluye el riesgo estratégico ni el de reputación

1.3. CLASIFICACIÓN DE LOS EVENTOS DE PÉRDIDA

El tercer documento consultivo (CP3) del NACB define siete tipos diferentes de eventos de perdida por riesgo operacional [3]:

I. Fraude Interno: Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o a 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.

II. Fraude externo: Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o a soslayar la legislación, por parte un tercero.

III. Relaciones laborales y seguridad en el puesto de trabajo: Pérdidas derivadas de actuaciones incompatibles con la legislación o acuerdos laborales, de higiene o seguridad en el

[3] Comité de Supervisión Bancaria de Basilea: *El Nuevo Acuerdo de Capital de Basilea, Documento de Consulta*, Banco de pagos Internacionales, abril del 2003, página 207. Documento disponible en el sitio web: www.bis.org

empleo, del pago de reclamaciones por daños a las personas, o de eventos de diversidad / discriminación.

IV. Prácticas con clientes, productos y negocios: 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.

V. 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.

VI. Incidencias en el negocio y fallos en los sistemas: Pérdidas derivadas de incidencias en el negocio y de fallos en los sistemas.

VII. 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.

La clasificación detallada de estos riesgos, contenida en el CP3, se consigna en el anexo C.

1.4. FRECUENCIA Y SEVERIDAD

Los eventos de pérdida por riesgo operacional, pueden ser a su vez clasificarse según las siguientes características básicas:

- Frecuencia: El número de veces que el evento tiene lugar durante un periodo de tiempo determinado, generalmente un año.

- Severidad: El impacto que el evento tiene en términos de la pérdida económica ocasionada.

Según los resultados de un estudio realizado por el CBSB, publicado en enero del 2002, en base a los datos proporcionados por 30 bancos que desarrollan operaciones a nivel internacional, con respecto a los eventos de pérdida registrados durante un periodo de 3 años, las entidades que realizan operaciones de banca de inversión, comercial y minorista, presentan, en promedio, las relaciones entre tipos de riesgo operacional, frecuencia y severidad, que se muestran en el Cuadro 1.

CUADRO 1: Frecuencia y severidad de los eventos de riesgo operacional[4]

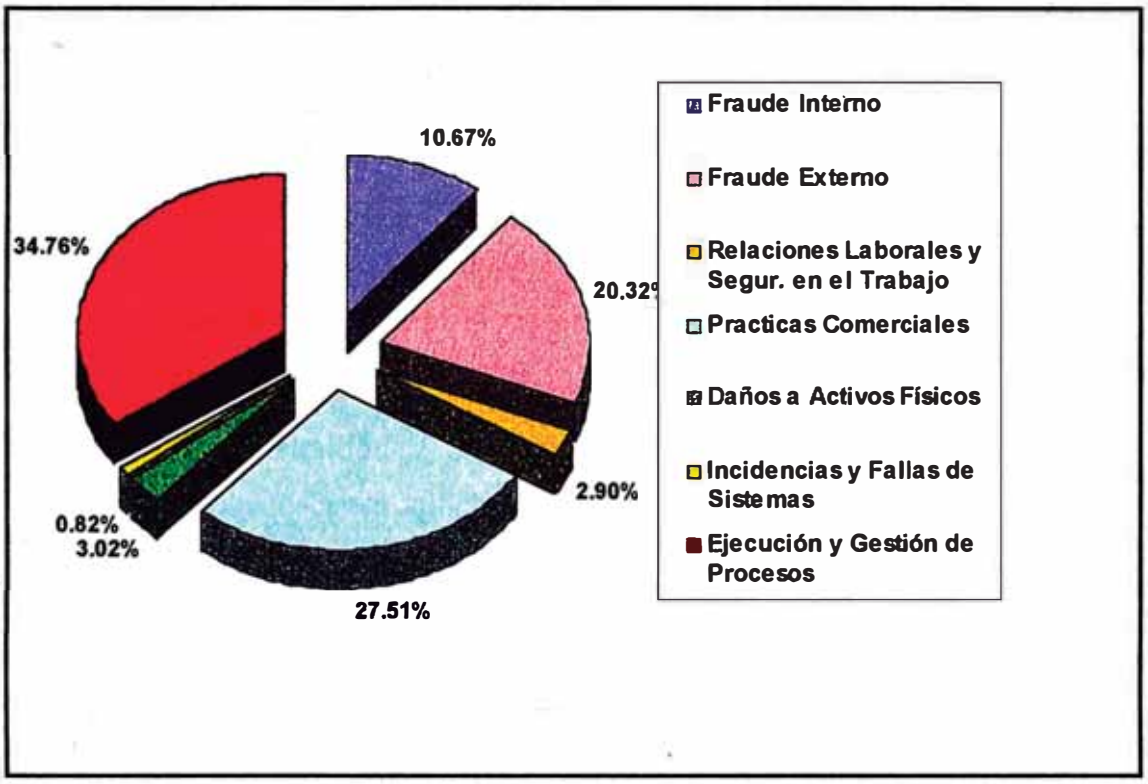
Tipo de evento	Frecuencia	Severidad
Fraude interno	Baja	Alta
Fraude externo	Alta / media	Baja / media
Relaciones laborales y seguridad en el puesto de trabajo	Baja	Baja
Prácticas con clientes, productos y negocios	Baja / media	Alta / media
Daños a activos materiales	Baja	Baja
Incidencias en el negocio y fallas en los sistemas	Baja	Baja
Ejecución, entrega y gestión de procesos	Alta	Baja

El estudio referido también proporcionó información sobre la distribución de los importes totales de los eventos de pérdida informados, por tipo de evento. En número total de eventos informados fue de 27,371 por un importe total de 2,613 millones de

[4] Fuente: Alexander, Carol (editora), *Operational Risk, Regulation, Analysis and Management*, editorial Pearson Education Ltd., Prentice-Hall, Financial Times, Gran Bretaña, 2003, página 132

euros. En el Grafico 1 se muestra la distribución porcentual del referido importe.

GRÁFICO 1: Distribución de los eventos de pérdida informados por 30 bancos internacionales según el estudio del CBSB[5]



1.5 MAPAS DE RIESGO OPERACIONAL

Las diferentes combinaciones de frecuencia y severidad permiten una primera aproximación para el análisis de los riesgos operacionales, que consiste en la construcción de los denominados mapas de riesgo, que resultan de clasificar los posibles eventos, según sus combinaciones características de frecuencia y severidad.

[5] Fuente de los datos: Comité de Supervisión Bancaria de Basilea, *The Quantitative Impact Study for Operational Risk: Overview of Individual Loss data and Lessons Learned,* página 8, Banco de Pagos Internacionales, enero del 2002. Documento disponible en el sitio web www.bis.org. Gráfico: Elaboración propia

Para cada una de estas combinaciones habrá un enfoque de gestión apropiado.

I. Baja severidad / baja frecuencia: Son eventos que requieren mínima o nula atención, pues as posibles pérdidas pueden ser tan pequeñas e improbables que el costo de prevenirlos puede que no compense los posibles ahorros. La gran variedad de estos eventos hace difícil su identificación.

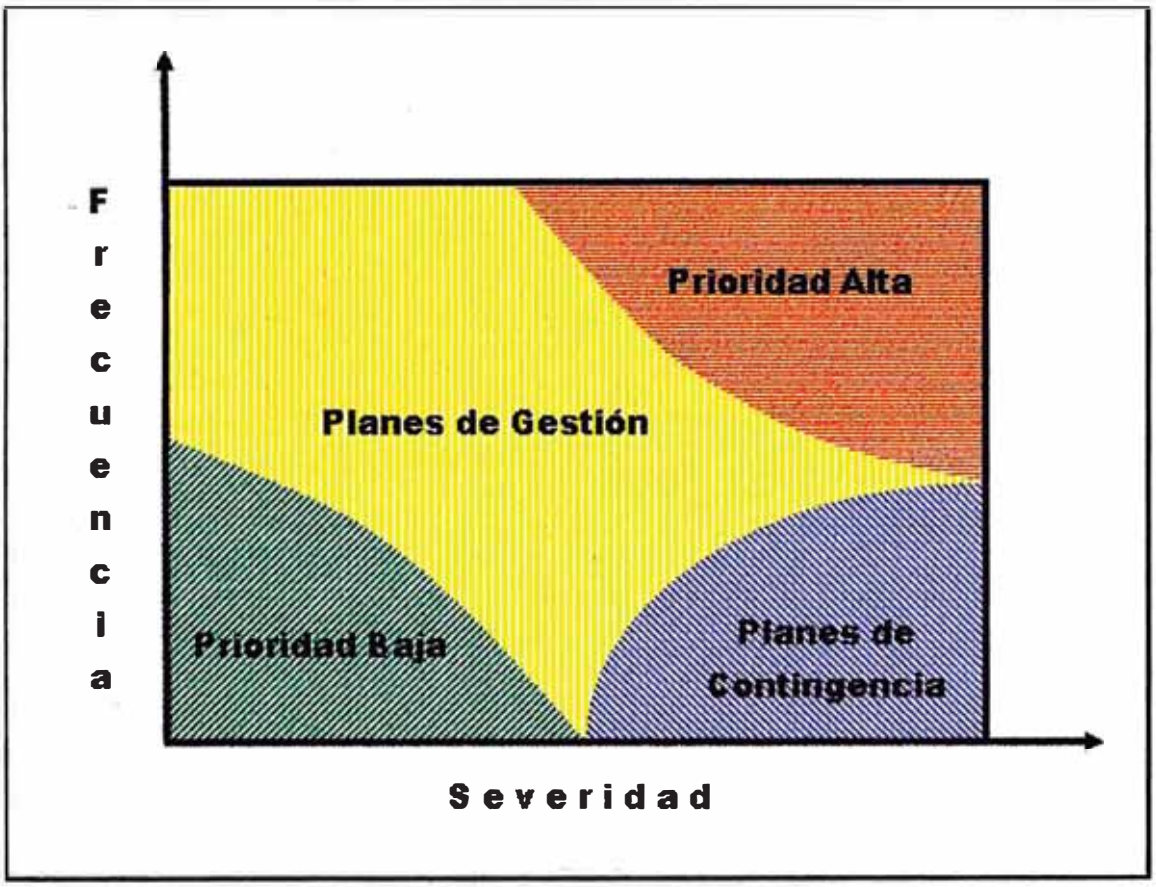
II. Baja severidad / alta frecuencia: Son que no implican pérdidas individuales significativas, peri si una elevada la pérdida acumulada anual, por tanto es necesario gestionarlos de forma permanente. Se trata casi siempre de eventos conocidos y e identificables.

III. Alta severidad / baja frecuencia: Son eventos fáciles de identificar pero difíciles de predecir, pero que de producirse tendrán un gran impacto. Esta es la zona típica para desarrollar planes de contingencia y para establecer estrategias se transferencia del riesgo.

IV. Alta severidad / alta frecuencia: Son eventos fáciles de predecir e identificar y que una vez detectados requieren acciones inmediatas para suprimir los efectos negativos de su elevada severidad. Son eventos que ante la falta de reacción se tornaran recurrentes y darán lugar a pérdidas elevadas.

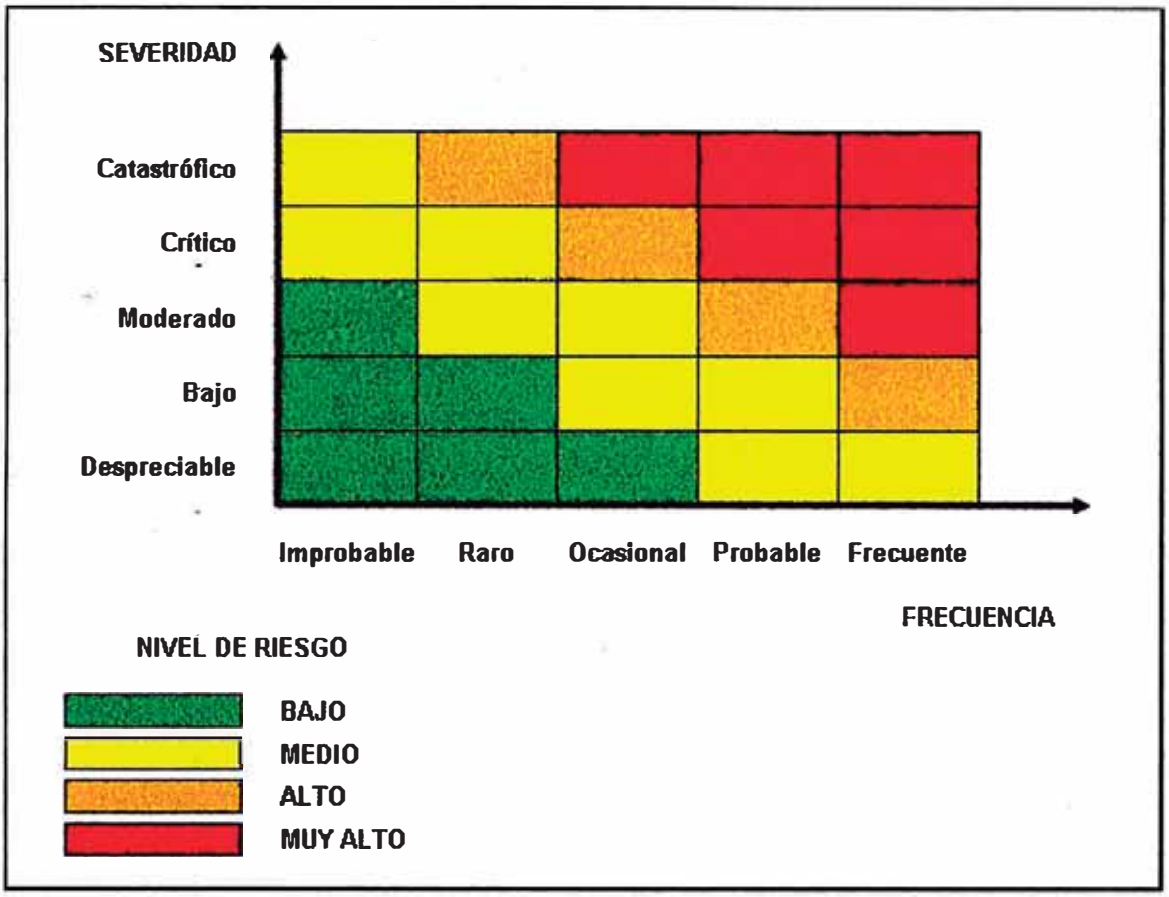
En el Gráfico 2 se ilustra un ejemplo de mapa de riesgo, en el que los eventos se distribuyen, en un diagrama cartesiano, según sus atributos característicos, indicando las cuatro zonas correspondientes a las diferentes combinaciones de severidad y frecuencia, así como las estrategias de gestión que se aplican a los eventos que corresponden a cada zona.

GRÁFICO 2: Estrategias de gestión para cada zona de eventos en un mapa típico de riesgo operacional



Otra forma de presentar un mapa de riesgo se ilustra en el Gráfico 3, en el cual se han definido cinco rangos, tanto para la frecuencia como para la severidad. En este caso de lo que se trata es de establecer una escala de "nivel de riesgo", que resulte de las diferentes combinaciones de los rangos de ambas variables. De esta manera, a cada tipo de evento se le asigna un determinado nivel de riesgo, de manera que todos los eventos con igual nivel sean objeto de una estrategia de acción similar.

Grafico 3: Mapa de riesgo con identificación de niveles



1.6. EL COMITÉ DE SUPERVISIÓN BANCARIA DE BASILEA Y EL NUEVO ACUERDO DE CAPITAL

El CSBB fue creado en 1975, por los gobernadores de los bancos centrales de los países del Grupo de los Diez (G-10), bajo los auspicios del Banco de Pagos Internacionales – BIS [6], con sede en la ciudad de Basilea, en Suiza. Su objetivo es elaborar normas generales sobre aspectos de regulación y supervisión de la actividad financiera, que sirvan de guía a las entidades supervisoras de los países integrantes. Actualmente el comité está conformado por

[6] Siglas de *Bank for International Settlements*

representantes de los bancos centrales y autoridades supervisoras de Alemania, Bélgica, Canadá, España, Estados Unidos, Francia, Italia, Japón, Luxemburgo, Países Bajos, Suecia, Suiza y Reino Unido.

Los acuerdos del CSBB no tienen el carácter de normas internacionales ni obligan a los países miembros, sin embargo si constituyen una doctrina que tiene una influencia considerable. En 1988, el Comité publicó el denominado Acuerdo de Basilea, que por primera vez definió estándares para la supervisión y para la medida de solvencia de las entidades financieras a nivel mundial, respecto a sus riesgos de crédito. Para 1993 estos estándares ya habían sido adoptados e implementados por la mayoría de países.

En 1999, el Comité publicó el primer documento consultivo sobre el denominado Nuevo Acuerdo de Capital de de Basilea (NACB), conocido también como BIS II, que incorpora modificaciones sustanciales a los criterios de medición del riesgo de crédito y de la suficiencia de capital de las entidades. Además actualiza y amplia estándares sobre los riesgos de mercado, que unos años antes habían sido incorporados al acuerdo de 1988, e incluye apartados específicos para los riesgos operacionales.

La tercera versión del documento consultivo del NACB fue publicada en abril del año 2003, estando prevista su implementación y entrada en vigencia a partir del año 2007. Aunque el acuerdo será aplicado, en primera instancia, en los grandes bancos de las economías más desarrolladas, que realizan operaciones internacionales, este ha sido diseñado para que pueda ser adoptado por entidades de cualquier tamaño en cualquier país.

El NACB se ha estructurado en tres "pilares":

- Pilar 1, Suficiencia de Capital: Las entidades financieras deben contar con un capital mínimo suficiente para hacer frente a sus riesgos, de manera que se pueda asegurar su continuidad y su viabilidad, sin comprometer los recursos ni los intereses del público. Para ello se establecen diferentes enfoques de medición de los riesgos, de crédito, de mercado y operacionales, asignando requerimientos mínimos de capital por cada uno de ellos. Las alternativas de medición van desde las sencillas y fáciles de aplicar, hasta las más sofisticadas. Se entiende que los bancos que apliquen las formas más avanzadas de medición serán los que tengan una visión más clara y exacta de los riesgos que enfrentan y, por lo tanto, tendrán requerimientos de capital menores.

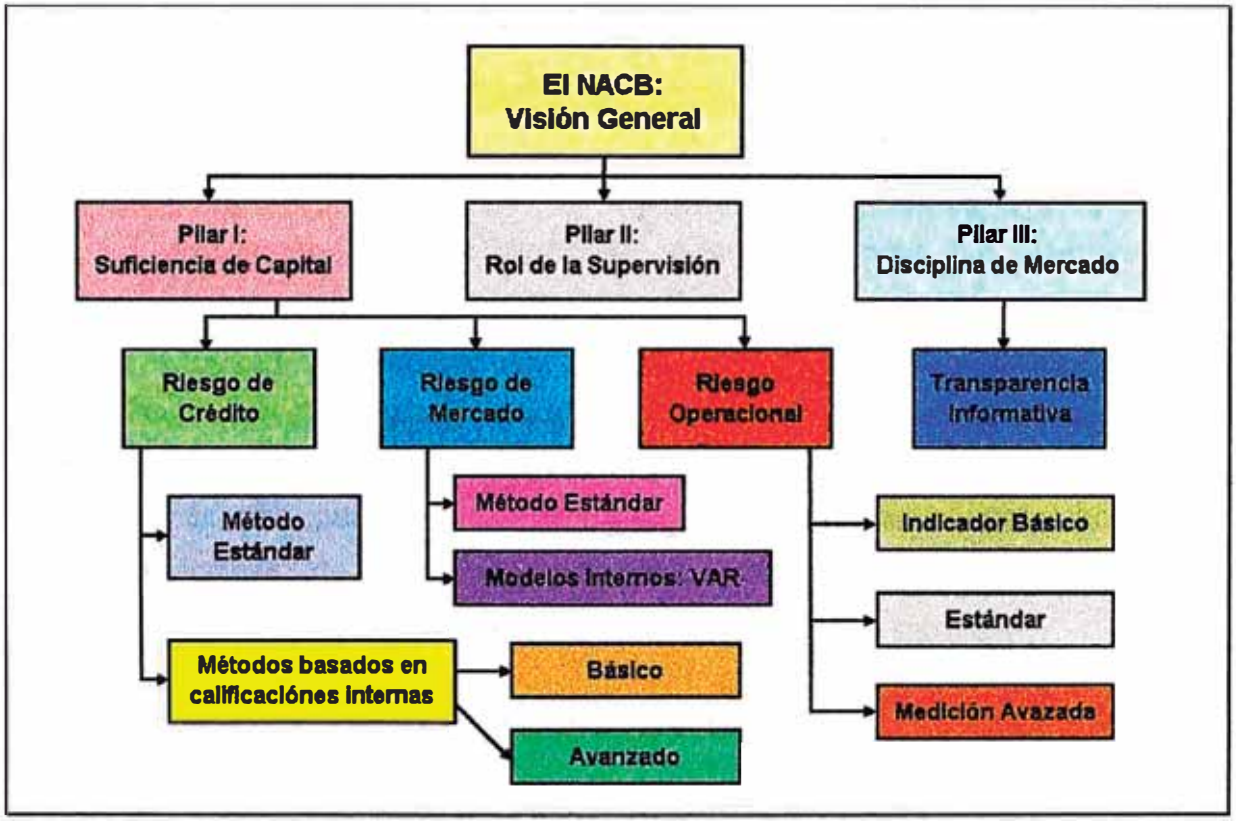
- Pilar 2, Rol de la Supervisión. Las entidades reguladoras y supervisoras de la actividad financiera, evaluarán constantemente a las empresas, para verificar que las mediciones de los riesgos sean razonables, que el capital de respaldo sea suficiente y que los sistemas de gestión sean los adecuados. En los casos de aplicación de métodos avanzados, los supervisores controlarán que los sistemas de información y las bases de datos reúnan los estándares de calidad exigidos por el acuerdo. También se establece que los supervisores podrán realizar exigencias adicionales de capital, no consideradas en el Pilar 1, para cubrir cualquier otro tipo de riesgo o cuando las características o la situación de la empresa o del mercado así lo requieran.

- Pilar 3, Disciplina y Transparencia de Mercado: Las entidades financieras deberán proporcionar información sobre sus políticas y prácticas de gestión de los riesgos, ya sea que empleen los enfoques avanzados o los más simples. La idea es proporcionar a los inversionistas, clientes, proveedores y corresponsales, información clara sobre cómo es que la

empresa administra sus riesgos. Esto significará, en los casos en que se perciba una menor calidad de gestión, una caída en el valor de la acción y en el nivel de calificación de riesgo de la empresa.

En el gráfico No. 4 se ilustra una visión general del NACB.

GRÁFICO 4: Visión del Nuevo Acuerdo de Capital de Basilea



1.7. REQUERIMIENTOS DE CAPITAL POR RIESGO OPERACIONAL

Desde la publicación del primer documento consultivo sobre el nuevo acuerdo, el CSBB ha incluido apartados específicos para que las entidades supervisoras exijan a las empresas requerimientos mínimos de capital, con el propósito de cubrir el riesgo de pérdidas

"inesperadas" por eventos de riesgo operacional. Se considera que las pérdidas "esperadas" deben haber sido plenamente identificadas y cubiertas con provisiones[7].

En el primer pilar del nuevo acuerdo se plantea, en base a las investigaciones sobre datos proporcionados por los principales bancos con operaciones internacionales, que el riesgo operacional consume en promedio un 15% del denominado "capital económico", y establece tres enfoques posibles para su medición y control: el método del indicador básico, el método estándar y los métodos de medición avanzada.

Adicionalmente a estos enfoques cuantitativos, el Comité ha elaborado un conjunto de recomendaciones contenidas en el documento titulado "Prácticas Adecuadas para la Gestión y Supervisión de los Riesgos de Operación", cuya última versión fue publicada en febrero del 2003. Un resumen de su contenido se incluye en el acápite 1.8 y el documento completo en el anexo E.

Por otra parte, el Comité recomienda que los bancos adopten técnicas de mitigación del riesgo operacional, entre ellas la subcontratación de actividades y la cobertura con seguros.

1.7.1. EL MÉTODO DEL INDICADOR BÁSICO

El requerimiento de capital se calcula promediando los ingresos brutos anuales de los tres años anteriores y multiplicando el promedio por el factor 0.15, también denominado α. La definición de ingresos brutos comprende:

a) El margen de intermediación financiero, es decir los ingresos por intereses menos los gastos por intereses.

[7] Para una definición de pérdida esperada y pérdida inesperada, véase el acápite siguiente.

b) Los ingresos netos por servicios, es decir las comisiones cobradas menos las comisiones pagadas

Estos ingresos deben ser brutos en tanto que se calculen antes de provisiones, no incluyan beneficios/pérdidas por compra venta de valores de la cartera de inversión, y tampoco consideren los rubros de ingresos y gastos extraordinarios.

El NACB no establece requisitos específicos a las entidades que apliquen este método. Sin embargo en el acuerdo se sugiere que se cumplan las recomendaciones del Comité, incluidas en el documento sobre "Prácticas Adecuadas", referido anteriormente.

1.7.2. EL MÉTODO ESTÁNDAR

En el método estándar, se vuelve a utilizar los ingresos brutos como base de cálculo para el grado de riesgo de las operaciones del banco. Sin embargo, en lugar de calcular el nivel de capital para toda la empresa, como ocurre con el método del indicador básico, los bancos deberán calcular un requerimiento de capital por cada una de las líneas de negocio definidas por el Comité[8]. Esto se determina multiplicando los ingresos brutos de cada una de las ocho líneas de negocio definidas en el NACB, por unos factores predeterminados, también denominados Beta (β), según se indica en el Cuadro 2.

La exigencia total de capital por riesgo operacional será la suma de los requerimientos de capital para todas y cada una de sus líneas de negocio. Para poder utilizar los métodos estándar y de medición avanzada, los bancos deberán

[8] Comité de Supervisión Bancaria de Basilea, *El Nuevo Acuerdo de Capital de Basilea, Documento de Consulta*, Banco de Pagos Internacionales, abril del 2003, páginas 126 y 127. Documento disponible en el sitio web: www.bis.org

demostrar que cuentan con sistemas para el control del riesgo operacional, que cumplan los criterios mínimos establecidos por el NACB.

CUADRO 2: Factores de riesgo para el Método Estándar

Líneas de Negocio	Factor β
Finanzas Corporativas	18%
Negociación y Ventas	18%
Banca Minorista	12%
Banca Comercial	15%
Liquidación y Pagos	18%
Servicios de Agencia	15%
Administración de Activos	12%
Intermediación Minorista	12%

Para poder aplicar este método, y los métodos de medición avanzados, los bancos deben cumplir ciertos requisitos:

a) El directorio y la gerencia deberán estar activamente implicados en la supervisión del marco de gestión del riesgo operacional

b) Deben tener implantado un sistema de gestión del riesgo operacional, conceptualmente sólido y aplicado en su integridad

c) Contar con recursos suficientes y adecuados, para aplicar la metodología de gestión del riesgo operacional, en las diferentes líneas de negocio y en las áreas de control y auditoria.

Tanto los bancos que utilicen el método del indicador básico como aquellos que utilicen el método estándar para el riesgo operacional no podrán reconocer el efecto de las coberturas de seguros para reducir sus exposiciones al riesgo operacional.

1.7.3. PÉRDIDAS ESPERADAS E INESPERADAS [9]

Los conceptos de pérdida esperada e inesperada son la base para los enfoques cuantitativos para la medición de diferentes tipos de riesgos. Estos conceptos son el resultado del desarrollo de las técnicas de medición de riesgos en los últimos años, en particular del riesgo de mercado, y, más recientemente, del riesgo de crédito. En términos generales, el propósito de los modelos de medición de riesgos es estimar la distribución de probabilidad de las pérdidas futuras. Para ello, es necesario definir tanto el concepto de pérdida que el modelo intenta capturar como el período sobre el cual se va a medir esta pérdida (horizonte temporal). Una vez estimada dicha distribución, las pérdidas que se pueden derivar de una cartera se pueden clasificar en tres categorías:

- Pérdida esperada, que es la media de la distribución de pérdidas y representa las pérdidas previstas, es decir, las que por término medio se espera que se produzcan.
- Pérdida inesperada, que es una medida de la variabilidad de las pérdidas de la cartera y representa las pérdidas potenciales imprevistas. Es igual a la pérdida asociada a un nivel de confianza

[9] El texto de este apartado ha sido adaptado de: González Mosquera, Luis, "Capital Regulatorio y Capital Económico: Prociclicidad del nuevo Acuerdo de Capital y Análisis de Escenarios de Crisis", en *Estabilidad Financiera* No. 2, marzo del 2002, Banco de España. Documento disponible en el sitio web: ww.bde.org

suficientemente elevado de la distribución de pérdidas, menos la pérdida esperada.

- Pérdida en situaciones extremas, que es toda aquella pérdida por encima del nivel de confianza elegido para calcular las pérdidas inesperadas. Pueden ser consecuencia de sucesos extremos contemplados en la distribución de pérdidas, pero no en el nivel de confianza de la pérdida inesperada. También pueden ser el resultado de crisis no contempladas en la estimación de la distribución de pérdidas.

El Gráfico 5 ilustra los tres tipos de pérdidas asociadas a la función de distribución de las pérdidas y frecuencias de los eventos. En este contexto, el capital económico se define habitualmente como el capital necesario para cubrir las pérdidas inesperadas. Desde un punto de vista conceptual, la pérdida esperada, dado su carácter predecible, debe considerarse como parte del costo y debe estar incorporada en el precio y cubierta con provisiones. Por su parte, la pérdida en situaciones extremas deberá ser cuantificada mediante análisis de escenarios y tener reflejo tanto en la elaboración de planes de contingencia como en la asignación de capital y fijación de límites a la asunción de riesgos. Según esta definición, el capital económico, no coincide con el que mantendrían las entidades en ausencia de regulación, y que es el que usualmente se denomina "capital disponible".

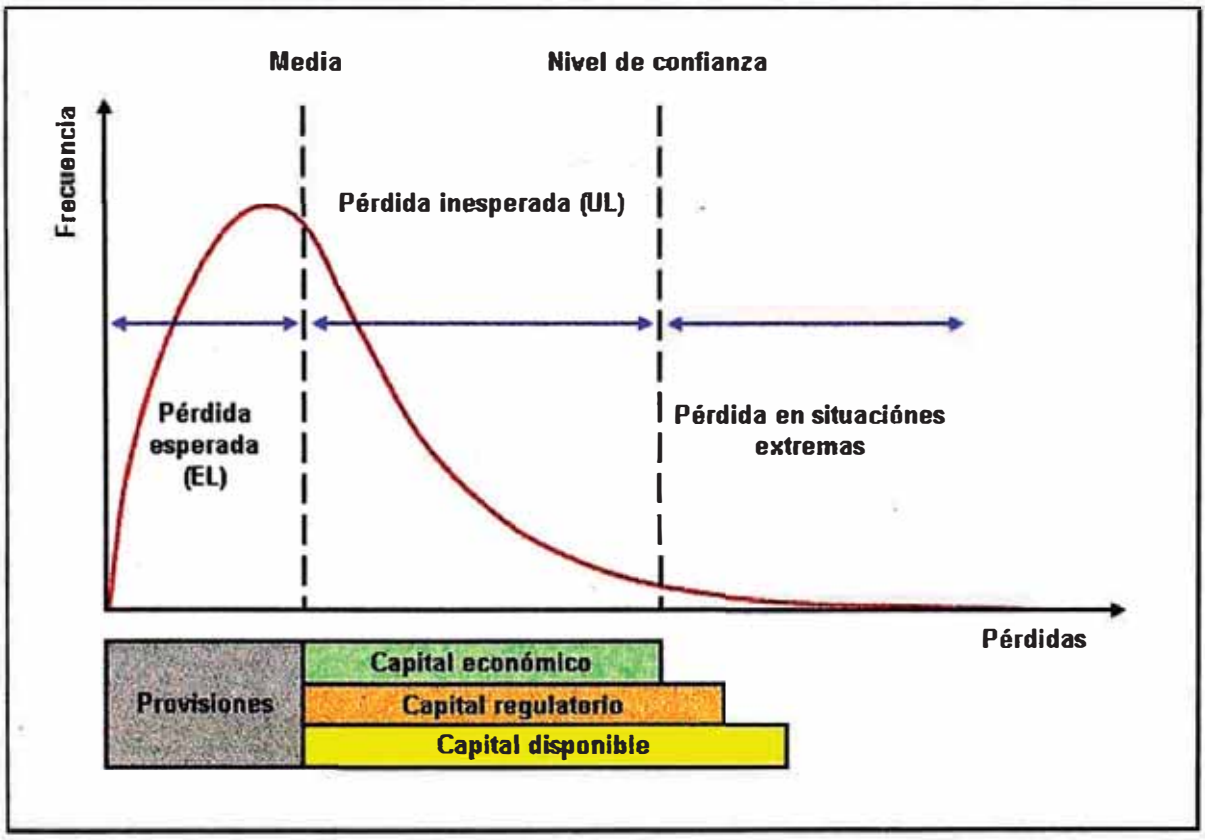
El capital económico es el capital necesario para alcanzar un determinado nivel de solvencia, al cubrir las pérdidas inesperadas de aquellos riesgos para los que se pueda calcular su distribución, mientras que el capital disponible deberá considerar adicionalmente, de alguna forma, el capital necesario para hacer frente tanto a riesgos para los que no se

pueden calcular sus pérdidas inesperadas como a las pérdidas en situaciones extremas.

En resumen, en el marco conceptual descrito, que ilustra el gráfico 1, se distinguen tres medidas del capital:

a. Capital económico. Es el capital necesario para cubrir las pérdidas inesperadas.
b. Capital regulatorio. Es el mínimo necesario para cumplir los requerimientos del regulador.
c. Capital disponible. Es el capital que las entidades realmente mantienen.

Gráfico 5: Requerimientos de capital y tipos de pérdida



A partir de las definiciones anteriores se presentan tres cuestiones que deben ser resueltas. La primera de ellas es determinar la relación entre las tres medidas del capital. Idealmente, todas ellas, de una u otra forma, deben estar relacionadas con el nivel de riesgo de la entidad. En general, para aquellos riesgos cuantificables mediante modelos de medición avanzados, el capital regulatorio debería situarse por encima del capital económico, para un nivel de confianza o solvencia dado, en la medida en que no solo hará referencia a la pérdida inesperada, en un horizonte temporal determinado y en condiciones normales, sino que deberá incorporar sucesos poco frecuentes que puedan afectar a la solvencia de la entidad. Esta relación es coherente con el objetivo de acercar el capital económico y regulatorio, para evitar tanto arbitrajes como posibles desventajas competitivas, ya que exigirá más capital a las entidades que tomen mayores riesgos.

Una segunda cuestión a resolver es si la variabilidad del capital económico y la del capital regulatorio deben ser iguales. En este sentido, se puede apuntar que, en la medida en que el capital regulatorio se sitúe por encima del económico y tenga en cuenta de forma permanente sucesos poco frecuentes, su variabilidad a lo largo del tiempo debería ser inferior a la del capital económico, que solo incorporará dichos sucesos cuando se produzcan dentro del período de observación considerado para su cálculo.

Por último, el capital disponible, que por definición debe ser superior al capital regulatorio, deberá incorporar todos aquellos riesgos no contemplados de forma explícita en el capital regulatorio. Esta relación se recoge formalmente en el nuevo Acuerdo de Capital, donde se establece que los

supervisores esperan que las entidades operen con niveles de capital superiores al mínimo que resulte del método de medición empleado, y podrán exigir a las entidades que así sea. Para determinar el capital necesario, el nuevo acuerdo considera que los reguladores deben tomar en cuenta el perfil de riesgos de las entidades, que pone en relación su nivel de riesgo total, incluyendo los riesgos o factores externos no considerados en el método de medición, con sus sistemas de gestión y control de riesgos.

El nuevo acuerdo también establece que, en ningún caso, el capital puede ser considerado como sustitutivo de un control de riesgos adecuado ni por parte de la entidad ni de los supervisores. Los supervisores deben contar con herramientas adicionales al nivel de capital para garantizar la solvencia de las entidades. Estas herramientas son el proceso de revisión supervisora, para asegurar que las entidades cuentan con procedimientos internos suficientes para valorar la adecuación de su capital en relación con los riesgos asumidos y los controles establecidos, y la disciplina del mercado, que exige una mayor transparencia, para que los participantes en el mercado puedan evaluar el grado de solvencia de las entidades y actuar en consecuencia.

El gráfico 5 resume e ilustra las relaciones comentadas en este apartado sobre las diferentes medidas del capital y la importancia del establecimiento de mecanismos de control adicionales para controlar los distintos tipos de pérdidas que se pueden derivar del desarrollo de la actividad de las entidades. Los sistemas de control serán básicos para reducir las pérdidas tanto de los riesgos cuantificables, mediante, por ejemplo, el establecimiento de límites, como de los no

cuantificables, con el desarrollo, por ejemplo, de procedimientos adecuados que los mitiguen.

1.7.4. MÉTODOS DE MEDICIÓN AVANZADA

Los métodos de medición avanzada son procedimientos analíticos para calcular las pérdidas esperadas e inesperadas, por medio de modelos de distribución de probabilidades construidos en base a los datos históricos con los que cuente cada entidad.

Según lo establecido por el NACB, los bancos que opten por este método pueden emplear metodologías propias para medir su exposición al riesgo operacional, metodologías que deberán ser aprobadas por las entidades supervisoras

El procedimiento para determinar las distribuciones de probabilidad, ya sea que se trate de distribuciones empíricas o paramétricas, requiere contar con datos históricos, suficientes y confiables, sobre los eventos de riesgo y sobre las pérdidas efectivamente producidas.

Los lineamientos generales que deberán seguir los bancos que adopten estos métodos son:

- El desarrollo de cualquier método de medición avanzado debe seguir el enfoque *"bottom-up"*, es decir que debe estar basado en la experiencia real sobre eventos de pérdidas
- Las entidades supervisoras exigirán que el requerimiento de capital por riesgo operacional sea igual a la suma de la pérdida esperada (EL) y de la pérdida inesperada (UL), a menos que el banco pueda

demostrar que la primera ya ha sido medida y tomada en cuenta como parte de sus prácticas internas

- El cálculo de la pérdida inesperada, es decir la pérdida máxima estimada con un nivel de confianza de 99.9%, deberá estar respaldado por datos suficientes y por técnicas analíticas adecuadas.
- El total del capital regulatorio por riesgo operacional será calculado como la suma de los cargos por los riesgos individuales. Se admitirán otras formas de cálculo siempre que el banco pueda demostrar que cuenta con estimados sólidos y confiables, a satisfacción del supervisor, sobre las correlaciones entre los distintos tipos de riesgos
- Cada banco debe de registrar su propio historial de datos de pérdidas y utilizar los datos relevantes de otros bancos, individuales o agregados, de acuerdo con las ocho líneas de negocio y los 7 tipos de pérdida definidos por el NACB. Además debe efectuar regularmente pruebas para validar sus modelos con datos de pérdidas reales
- Los bancos que apliquen estos métodos deberán contar con procesos confiables, sólidos, transparentes, adecuadamente documentados y que sean verificables

El acuerdo establece además que las empresas que adopten métodos avanzados podrán utilizar los seguros como elemento para reducir su riesgo, en las medidas para el cálculo de los requerimientos de capital, hasta por un importe no mayor al 20% del requerimiento total por riesgo operativo, y siempre que se cumplan las condiciones previstas en el

acuerdo, relativas al asegurador y a las características de las pólizas.

1.8. PRÁCTICAS ADECUADAS PARA LA GESTIÓN Y SUPERVISIÓN DE LOS RIESGOS DE OPERACIÓN [10]

En forma complementaria a los tres métodos de medición del riesgo operacional, el BIS II ha planteado 10 principios cualitativos, que deben ser implementados por las empresas que aspiren a ser calificadas en orden a poder utilizar los métodos de medición más avanzados, y así poder ser elegibles para un menor requerimiento de capital por riesgo operacional. Estas entidades deben estar en capacidad de demostrar que cumplen con los diez principios y que además cuentan con un modelo sólido para la estimación cuantitativa de estos riesgos.

Loe diez principios señalados mencionados se resumen a continuación:

I. El directorio debe estar al tanto de los principales aspectos de los riesgos operacionales del banco, y debe aprobar y revisar periódicamente el esquema de gestión para estos riesgos.

II. El directorio debe asegurarse que el esquema de gestión del riesgo operacional esté sujeto a una auditoria interna efectiva.

III. La alta gerencia tiene la responsabilidad de implementar el esquema de gestión aprobado por el directorio y todos los niveles de dirección deben estar al tanto de sus responsabilidades.

IV. Los bancos deben identificar y evaluar los riesgos operacionales de todos los productos, actividades, procesos y

[6] Comité de Supervisión Bancaria de Basilea, *Sound Practices for the Management and Supervisión of Operational Risk*, Banco de Pagos Internacionales, febrero del 2003. El texto completo del documento se incluye como Anexo E del presente trabajo.

sistemas, tanto los existentes como aquellos en proyecto o en fase de desarrollo.

V. Los bancos deben establecer el procedimiento para monitorear regularmente los perfiles de riesgo operacional y su exposición a pérdidas materiales.

VI. Los bancos deben contar con políticas, procesos y procedimientos para controlar los riesgos operacionales. Deben evaluar la factibilidad de estrategias alternativas de mitigación y ajustar sus exposiciones apropiadamente.

VII. Los bancos deben contar con planes de contingencia y de continuidad de servicio, que aseguren su capacidad de operar en forma continua en caso de una interrupción del negocio.

VIII. Los supervisores deben exigir a los bancos que tengan una estrategia efectiva de gestión del riesgo operacional, como parte de un enfoque integral para la gestión de los riesgos.

IX. Los supervisores deben llevar a cabo evaluaciones periódicas e independientes de las estrategias de gestión del riesgo operacional de los bancos.

X. Los bancos deben hacer una divulgación pública suficiente de manera que los participantes del mercado evaluar su enfoque para la gestión de los riesgos operativos.

1.9. NORMATIVA DE LA SUPERINTENDENCIA DE BANCA Y SEGUROS

En el mes de enero del 2002, la Superintendencia de Banca y Seguros del Perú, en su calidad de entidad a cargo de la supervisión y regulación de la actividad de intermediación financiera y de seguros, publicó la resolución No. 006-2002, en la que aprueba el Reglamento para la Administración de los Riesgos de Operación de las empresas supervisadas.

Las principales disposiciones de este reglamento son:

- Se define el riesgo de operación, adoptando la definición establecida por el CBSB
- Se establecen las responsabilidades del directorio y de la gerencia
- Se establecen las funciones de la unidad a cargo de la administración de los riesgos de operación
- Se dispone que las entidades supervisadas deben disponer de una estructura organizacional para una adecuada administración de los riesgos de operación
- Se dispone que las empresas deben de contar con un manual de riesgos de operación, incorporado en su manual de organización y funciones, que contemple como mínimo lo siguiente:

    a. Funciones y responsabilidades de las unidades de negocio y de apoyo en la administración de los riesgos de operación.

    b. Descripción de la metodología aplicada para la medición y evaluación de los riesgos de operación.

    c. Procedimiento para informar al Directorio y a la Gerencia, sobre la exposición a los riesgos de operación de la empresa y de cada unidad de negocio.

    d. Procedimiento para la aprobación de propuestas de nuevas operaciones, productos y servicios que considere, entre otros, su descripción general, los riesgos identificados y las acciones a tomar para su control.

- Establece lineamientos para la administración de los factores que originan los riesgos de operación: procesos internos, tecnología, personas y eventos externos
- Dispone la obligación de presentar anualmente a la Superintendencia, un informe sobre la evaluación de los riesgos de operación, desagregado por proceso o por unidad de negocio

Esta resolución no contempla ninguna directiva que se refiera a requerimientos de capital específicos por riesgo operacional, sin embargo el consenso general es que este tema debe estar aún en estudio, por parte del supervisor, y que será regulado más adelante.

En el Anexo A se incluye el texto completo de la resolución SBS No. 006-2002.

CAPÍTULO 2: MODELO PARA LA GESTIÓN DEL RIESGO OPERACIONAL

2. MODELO PARA LA GESTIÓN DEL RIESGO OPERACIONAL

2.1. EVOLUCIÓN RECIENTE Y TENDENCIAS EN LA ACTIVIDAD FINANCIERA

Tal como se ha mencionado en los acápites anteriores, durante los últimos años las empresas del sector financiero se han enfrentado a una serie de cambios sustanciales, tanto en su entorno como en la definición de su propia actividad. Según González y López[11], los principales factores que han dado lugar a estos cambios han sido los siguientes:

- La desregulación: Es decir la desaparición gradual de las barreras de protección a las empresas del sector financiero y la flexibilización de los límites a sus actividades.
- La desintermediación: Entendida como la pérdida de presencia en los mercados de los intermediarios financieros tradicionales, debido a la aparición de otro tipo de agentes y/o instituciones que intervienen como competidores.
- La titulización: Este término, que es una traducción del vocablo inglés *securitization*, se refiere a la sustitución de las formas tradicionales de crédito bancario, por derechos sobre determinados activos convertidos en valores negociables.

[11] Sebastián González, Altina y López Pascual, Joaquín, *GESTIÓN BANCARIA, LOS NUEVOS RETOS EN UN ENTORNO GLOBAL*, 2da. Edición, Mcgraw-Hill / Interamericana de España, Madrid, 2001.

- La innovación financiera: Es el proceso de transformación de las entidades, procesos, mercados e instrumentos financieros, como anticipación y respuesta a nuevas exigencias de los inversores y clientes de servicios financieros.
- La transnacionalidad de los mercados: Se refiere a la posibilidad de comprar y vender productos financieros, en cualquier parte del mundo, e inclusive en tiempo real, sin que para ello sean obstáculos las barreras geográficas y las fronteras nacionales.
- El desarrollo tecnológico: Los avances en la tecnología de las comunicaciones y en los sistemas informáticos, han ampliado el acceso a la información, dando lugar a cambios en los hábitos de gestión y de negociación de los productos financieros, y en los mismos mercados.

  La globalización: Es el proceso e integración de los mercados en un sólo mercado mundial, eliminando las barreras geográficas y funcionales entre los agentes de los mercados. La globalización ha supuesto un aumento en el tamaño de los mercados y una mayor competencia, favoreciendo a los consumidores finales que pueden disponer de bienes y servicios más baratos y de mejor calidad; pero también ha incrementado la exposición al riesgo de las empresas, ha ocasionado el recorte de sus márgenes, el aumento en su nivel de endeudamiento y, como consecuencia, su grado de vulnerabilidad ante las crisis.

Los factores señalados han obligado a las empresas financieras a diversificar sus actividades, a desarrollar nuevos productos, a incursionar en nuevos mercados, a desarrollar canales alternativos de distribución y a adaptarse a las nuevas tecnologías. Todo lo anterior ha implicado un incremento significativo de los niveles de riesgo propios de la actividad tradicional y el surgimiento de nuevos tipos de riesgo. En el caso del riesgo operacional, los factores señalados, especialmente el desarrollo tecnológico y la innovación

financiera, han aumentado la variedad de los posibles eventos de pérdida y el impacto económico que estos pueden ocasionar sobre las entidades.

En un aspecto más amplio, la transformación de las organizaciones, que han ido cambiando de un esquema con muchos niveles de jefatura, y muchos controles, hacia esquemas con menos niveles y menos jefes pero con más empleados especialistas, siguiendo el modelo de "orquesta sinfónica" que Druker[12] señala como prototipo de la organización moderna, han conducido a modelos organizativos con estructuras más "planas", en donde los especialistas trabajan con mayor autonomía y casi sin supervisión, y en donde los resultados se consiguen a través del desempeño conjunto de los miembros de los equipos.

El surgimiento de este nuevo tipo de organización, consecuencia de la necesidad de utilizar conocimientos cada vez mayores, en un ambiente de creciente competencia, en muchos casos no ha ido aparejado de la evolución en los sistemas de control, lo cual ha devenido en situaciones en las que hay muchos especialistas, que trabajan prácticamente solos, y toman decisiones con poco o ningún control. Esto ha hecho que el riesgo operacional se extienda por todo lo ancho de las organizaciones, a diferencia de años atrás en que el mismo se concentraba mayormente en los niveles de jefatura.

Por otra parte, los estados, a través de los organismos de supervisión, se han visto en la necesidad de desarrollar nuevos sistemas de supervisión que, sin afectar la libertad de las empresas, permitan garantizar la estabilidad y solvencia del sistema financiero. De esta necesidad es que han surgido iniciativas, como es el caso del NACB, cuyo propósito es el de fomentar, entre las entidades financieras, una visión más dinámica de los riesgos, procurando que

[12] Druker. Peter F., *LA SOCIEDAD POST CAPITALISTA*, Editorial Norma, Bogotá, 1994.

se calculen de antemano las posibles pérdidas y que se tomen las medidas necesarias para preservar no sólo la rentabilidad sino también la solvencia de las empresas.

2.2. ENFOQUE ESTRATÉGICO PARA LA GESTIÓN DEL RIESGO OPERACIONAL

Independientemente de la necesidad de que las instituciones financieras cumplan con las normas dictadas por los organismos supervisores, las tendencias recientes en el sector enfocan la gestión del riesgo operacional como una necesidad de carácter estratégico, en tanto considera a la misma como un proceso de mejora continua, como fuente de generación de ventajas competitivas sostenibles y como medio para la creación de valor, para la empresa y los grupos de interés relacionados.

Lo anterior no constituye un enfoque arbitrario, sino que deriva del hecho de que la gestión adecuada del riesgo operacional representa una oportunidad para mejorar el desempeño de la empresa, frente a las otras del sector, mediante la aplicación de las estrategias de diferenciación y de liderazgo en costos[13], ya sea de una sola de ellas o bien de una combinación de ambas, en la medida que le proporciona los siguientes beneficios:

- Reduce las pérdidas causadas por los eventos de riesgo, como resultado de la adopción de medidas de mitigación
- Reduce el impacto financiero imprevisto, en caso de que ocurran los eventos de riesgo, debido a las provisiones constituidas como resultado de la medición
- Desarrolla una cultura de riesgo dentro de la empresa, que favorece y facilita la gestión

[13] Para una explicación detallada de estas estrategias véase: Porter, Michael E., *ESTRATEGIA COMPETITIVA, TECNICAS PARA EL ANÁLIS DE LOS SECTORES INDUSTRIALES Y DE LA COMPETENCIA*, Compañía Editorial Continental-CECSA, México, 1987.

- Hace posible el cumplimiento de la regulación sobre la materia
- Aumenta la competitividad, debido a la mayor fortaleza financiera
- Reduce los costos, como resultado de menores pérdidas y menores requerimientos de capital

Existen además los siguientes beneficios para los accionistas:

- Aumento en el valor de la acción, debido a mejores cifras en los estados financieros y a la percepción de que se trata de una inversión segura con buen potencial de crecimiento
- Mejora en los rentabilidad, debido a controles más precisos y al enfoque en la prevención
- Mayor transparencia en la información, que permite una mejor visión de los riesgos y de las oportunidades

Los beneficios también alcanzan a los empleados:

- Mayor seguridad en el empleo, debido a una reducción en la vulnerabilidad de la empresa
- Incremento en sus niveles de conocimiento y destreza, y por consiguiente de su "empleabilidad", entendida como la capacidad de ser considerados como elementos competentes dentro del mercado laboral

Los clientes también obtienen beneficios:

- Trabajar con una empresa que les brinda atención segura y oportuna
- Precios competitivos, debido a un mejor control de los costos

Los proveedores se benefician de:

- El aumento en su nivel de competitividad, como consecuencia de que la mayor exigencia por parte de sus clientes influirá en la mejora de sus propios procesos

- Tener un cliente viable que les asegurará un mercado e ingresos en el largo plazo.

Por lo tanto, la gestión adecuada del riesgo operacional constituye una oportunidad para la creación de valor, para la empresa y para los grupos de interés relacionados, proporciona ventajas competitivas, y contribuye a las estrategias de diferenciación y de liderazgo en costos; sin embargo, para lograr todo esto no es suficiente cumplir con las disposiciones dadas por los organismos a cargo de la regulación, e implantar sistemas apropiados de control, sino que además es necesario que este esfuerzo produzca el mejor resultado posible.

2.3. DEFINICIÓN DEL MODELO DE GESTIÓN

Para lograr los mejores resultados, la gestión del riesgo operacional requiere de la definición de una estrategia y del diseño de procesos adecuados, y debe de apoyarse en los medios necesarios y en un ambiente favorable. El conjunto de estos cuatro factores constituye el modelo de gestión, que una vez comunicado y comprendido, debe potenciar las capacidades y orientar los esfuerzos, de toda la organización, hacia el logro de los mejores resultados.

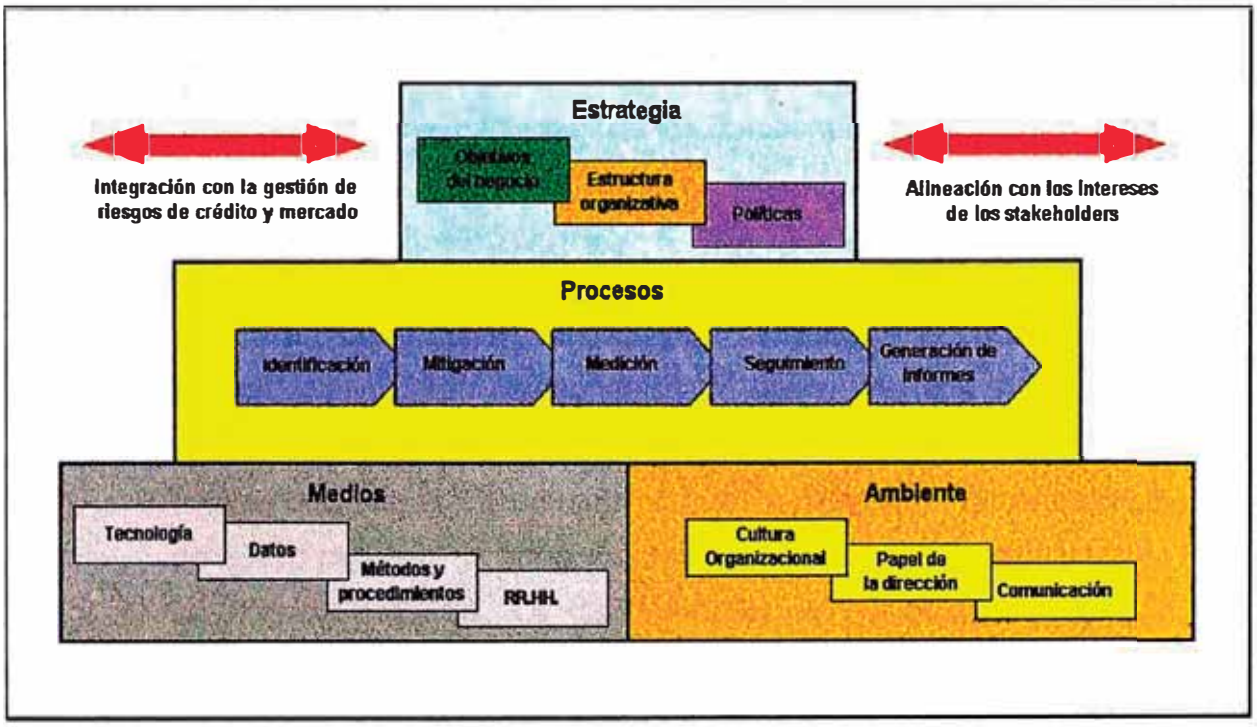
Llegamos así a la siguiente definición de lo que es un modelo de gestión: el conjunto de la estrategia, los procesos, los medios y el ambiente apropiado, definidos e integrados con el propósito de potenciar las capacidades y orientar el esfuerzo de todos los integrantes de una organización, hacia el logro de los mejores resultados.

Para lograr el propósito de conseguir el mejor resultado posible, un modelo de gestión debe:

- Definir con claridad la estrategia, especificando los objetivos, la estructura organizacional, y las políticas.
- Definir los procesos y las tareas, y asignar las responsabilidades.
- Asignar los recursos necesarios para que los procesos se lleven a cabo de manera eficiente.
- Procurar un ambiente que favorezca la iniciativa, la creatividad y la competitividad, alineados con los objetivos de la organización.

El Gráfico 6 ilustra el modelo de gestión propuesto, el mismo que constituye una variante de lo que Haubenstock[14] denomina *Operational Risk Management Framework*, concepto que ha sido adaptado para este trabajo, de acuerdo a la experiencia profesional del autor.

Grafico 6: Modelo para la gestión del riesgo operacional



[14] Alexander, Carol (Editora), op. cit. capítulo 12 (escrito por Michael Haubenstock).

CAPÍTULO 3: LA ESTRATEGIA

3. LA ESTRATEGIA

El primer paso en el establecimiento del modelo debe ser la definición de la estrategia de gestión, esto es el marco general y el enfoque para la administración de los riesgos. Tal como señala el Comité en el documento sobre las *Sound Practices*, esta tarea involucra al directorio, que debe definir las políticas de gestión del riesgo operacional, y a la gerencia, que tiene la responsabilidad de aplicar estas políticas en forma de planes concretos.

La definición de la estrategia de riesgo operacional debe integrarse con la gestión de los demás riesgos inherentes a los negocios de la organización, principalmente los riesgos de crédito y de mercado, y debe estar alineada con las expectativas de los grupos de interés relacionados.

3.1. OBJETIVOS DEL NEGOCIO

Los diversos componentes del plan estratégico de una empresa financiera involucran componentes de riesgo que son inherentes a las diferentes actividades del negocio, por ejemplo la instalación de nuevas oficinas, el lanzamiento de nuevos productos, la contratación de nuevo personal, la adopción de nuevas tecnologías y la incursión en nuevos negocios. La disponibilidad de información sobre los clientes, e inclusive sobre los competidores, pueden ayudar en la toma de decisiones, pero aun la mejor elección no esta libre de riesgos.

En el caso del riesgo operacional, las empresas enfrentan la posibilidad de ser afectadas por fraudes de diversos tipos, fallas en los sistemas de proceso de datos, ataques de *hackers*, e inclusive por la destrucción de instalaciones clave a causa de accidentes. Es cierto que estos eventos no son recurrentes sino ocasionales, sin embargo sus consecuencias pueden ser catastróficas.

Los conceptos y herramientas para la administración de los riesgos, principalmente de crédito y de mercado, son bastante conocidos en el sector financiero. No obstante, la gestión del riesgo operacional es relativamente nueva como una disciplina independiente y los avances en este campo hasta ahora se han concentrado en la identificación, medición y mitigación de este tipo de riesgos y en el análisis de procesos, todo ello con la finalidad de optimizar el capital regulatorio.

El nuevo enfoque de gestión, mencionado en el capítulo 2, considera que, dado que todas las decisiones de negocio tiene implicancias de riesgo operacional, la gestión de estos riesgos no solo debe enfocarse desde el punto de vista del capital regulatorio sino que debe de contribuir a optimizar el valor de la empresa, para los accionista y proveedores de capital, y en general a la creación de valor para todos los grupos de interés o *stakeholders*, como son los clientes, los proveedores, y la comunidad, reduciendo los costos de las pérdidas y mejorando la eficiencia de los procesos.

Para conseguir este propósito, el punto de partida es vincular los objetivos del negocio con las estrategias de gestión del riesgo operacional y establecer técnicas que permitan reducir las posibles pérdidas, procurando la eficiencia de los procesos, asegurando la eficacia de los controles, difundiendo las buenas prácticas y ordenando las prioridades de los esfuerzos.

3.2. LA ESTRUCTURA ORGANIZATIVA

Una vez que se ha definido la estrategia, el siguiente paso es establecer la forma de organización apropiada para implementarla. La estructura organizativa para la gestión del riesgo operacional, así como la consecuente definición de roles y responsabilidades, debe de reflejar los objetivos estratégicos de la empresa en este campo: el cumplimiento de la regulación, el desarrollo de ventajas competitivas y la creación de valor para los accionistas y grupos de interés. De acuerdo a este enfoque, la responsabilidad fundamental de estos riesgos debe corresponder a las unidades de negocio que los originan, en tanto que son ellas las que tiene el manejo diario de los procesos, tratan con los clientes, utilizan tecnología, introducen nuevos productos, supervisan a su personal y están en contacto con fuentes externas de riesgo.

Del mismo modo, las unidades de apoyo, tales como recursos humanos, sistemas de información, finanzas, asuntos legales y seguridad, además de tener la responsabilidad de controlar sus propios riesgos, tienen la responsabilidad de desarrollar e implantar políticas y procedimientos, asignar recursos, controlar procesos, y dar asesoría a toda la organización, en aquellos aspectos de la gestión de riesgos que están en el campo de su especialidad.

Independientemente de las responsabilidades "de línea" en materia de riesgo operacional, que se derivan de las funciones propias de las unidades de negocio y de apoyo, un modelo de gestión eficiente requiere que se definan ciertas responsabilidades "corporativas" y funciones especializadas en una unidad independiente, cuyo papel sea el de establecer políticas, desarrollar herramientas como son los mapas de riesgo, los programas de auto evaluación y las bases de datos de eventos y pérdidas y apoyar su implementación, coordinar

actividades de capacitación, y desarrollar modelos de medición del riesgo y de determinación de los requerimientos de capital.

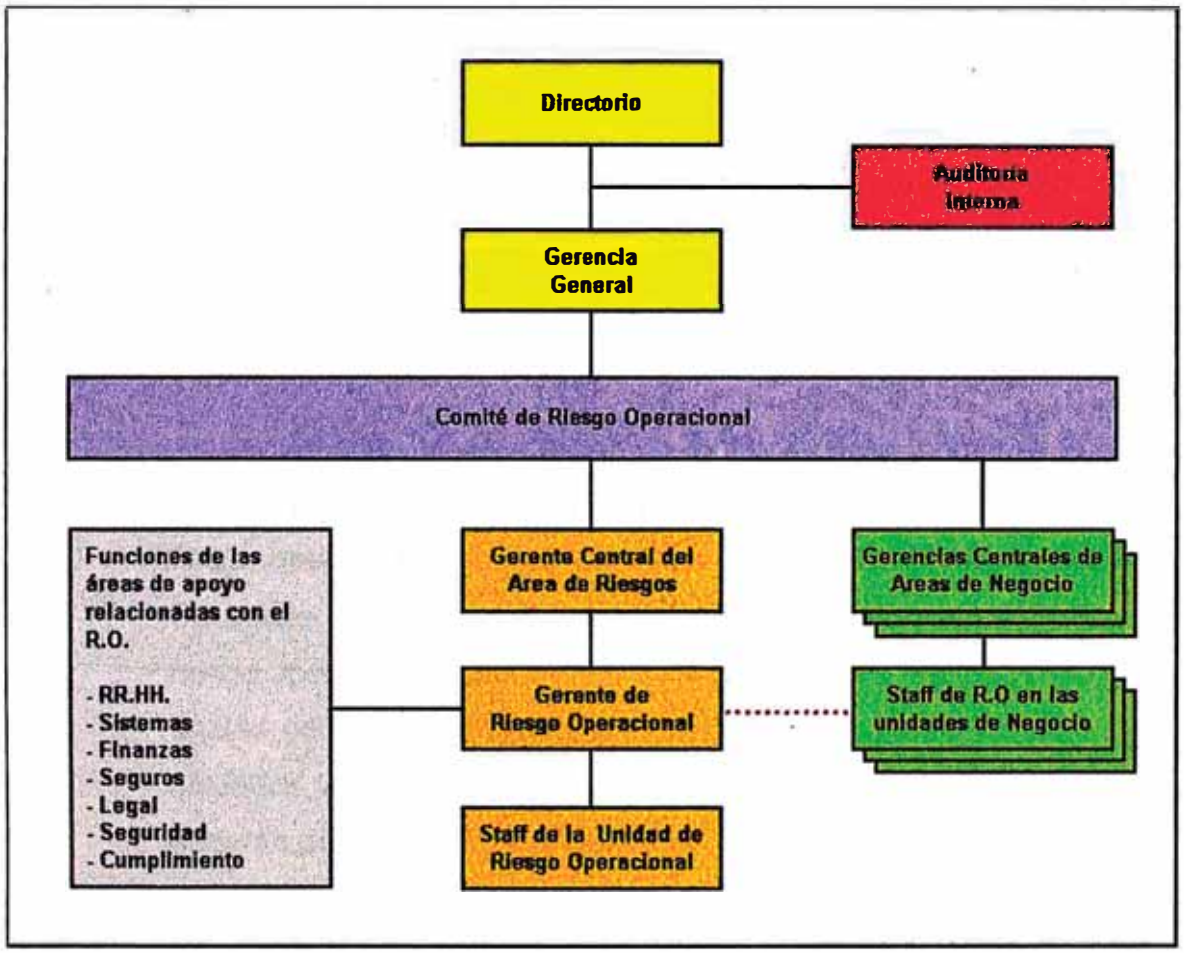
Es importante además que se diferencien claramente las responsabilidades de línea de las corporativas, ya que los riesgos ocurren realmente en la línea y los procedimientos de análisis y de control pueden ser muy diferentes entre diferentes líneas de negocio. La función corporativa de riesgo operacional debería enfocarse en aquellas actividades que crucen a través de las diferentes líneas de la organización, dejando en manos de estas la gestión de aquellos riesgos propios de sus actividades. El valor agregado que la función corporativa aporte, debe corresponder a actividades como son el análisis de riesgos entre líneas de actividad, el intercambio de experiencias y de buenas prácticas, el análisis comparativo o *benchmarking*, la explotación de bases de datos externas, el cálculo de requerimientos de capital y la consolidación de reportes para la alta dirección.

Otro aspecto importante de la estructura organizativa es el que se refiere a los "Comités de Riesgo Operacional". Cada unidad de negocio y de apoyo debe constituir un comité, que se encargue de dirigir, coordinar, aprobar y controlar el desarrollo de los planes y acciones necesarios para la gestión de los riesgos operacionales, en el marco definido por los órganos de decisión de la empresa. También debe existir un comité a nivel corporativo, cuya función debe ser la de aprobar el perfil de riesgo de la empresa, es decir la distribución de los riesgos, por línea de negocio y por tipo de riesgo, asegurar la correcta asignación de los recursos, la difusión de los eventos de riesgo y aprobar las políticas de riesgo y la asignación del capital económico.

La definición de la estructura organizativa debe incluir además la descripción de funciones, los niveles de autoridad y la forma en que se asignarán y distribuirán los costos. Es recomendable además que

la ubicación de la unidad de riesgo operacional, dentro de la estructura corporativa, sea dentro de la unidad central o área de riesgos del banco, y su que responsable reporte directamente al ejecutivo de mayor jerarquía en el área de riesgos.

Gráfico 7: Ejemplo de estructura organizativa para el riesgo operacional



3.3. LAS POLÍTICAS

Las empresas financieras deben tener una declaración de política que establezca los principios generales de gestión del riesgo operacional. Esta declaración de política, hasta donde sea posible, debe ser específica para cada línea de negocio, de manera que

cada miembro de la organización pueda captar la relevancia del tema en los términos más familiares posibles.

Las declaraciones de política usualmente se inician con el enunciado de los objetivos de la gestión del riesgo operacional. Algunos ejemplos de objetivos pueden ser: optimización del capital invertido, la reducción de las pérdidas operativas, prevención de errores, mejora de la calidad de servicio, reforzamiento de la imagen del banco, etcétera. Este enunciado de objetivos puede ser complementado por una descripción del proceso mediante el cual la empresa gestionará el riesgo operacional a partir de una definición clara del mismo. También puede mencionarse la forma en que la planificación estratégica del negocio y las medidas de desempeño, incluirán el componente de riesgo operacional.

Adicionalmente, la declaración de política puede contener también referencias al modelo de estructura organizativa para la gestión del riesgo operacional, y a las funciones y responsabilidades asignadas. Se puede mencionar a los comités que tendrán que ver temas de riesgo operacional, como parte de sus funciones, las funciones de la unidad central de riesgo operacional, las responsabilidades de las unidades de negocio y la forma en que las unidades de apoyo deberán de participar en la gestión.

Los principios para la gestión del riesgo operacional también pueden ayudar a definir los aspectos culturales de este proceso, ya que establecen el patrón de comportamiento que se espera por parte de los equipos que forman la organización. Por ejemplo, un principio puede establecer que las experiencias con eventos de riesgo operacional deben ser registradas y compartidas en forma abierta y transparente. Otro principio puede estar referido a que las necesidades de capital por riesgo operacional serán utilizadas como un indicador clave para medir la contribución de cada unidad a

cumplimiento de los objetivos de la empresa. También es importante reforzar la visión de que son las unidades de línea las responsables de sus propios controles y que, por lo tanto, sus indicadores de desempeño se verán afectados por los beneficios de sus aciertos o las consecuencias negativas de sus errores. Durante el proceso del diseño del modelo, es posible que surjan otros principios que puedan ser incorporados en la política de gestión, y de esta forma servir de base para una adecuada toma de decisiones.

Finalmente, la declaración de política también puede contener referencias a lo que se espera del uso de las herramientas informáticas y de los reportes que estas generen. Por ejemplo, tratándose de los sistemas de auto evaluación o de bases de datos, la política puede establecer que cada unidad debe ser la responsable de mantener su información actualizada. La política también puede establecer que tipo de información deberá proporcionar cada unidad de negocio, con fines de consolidación.

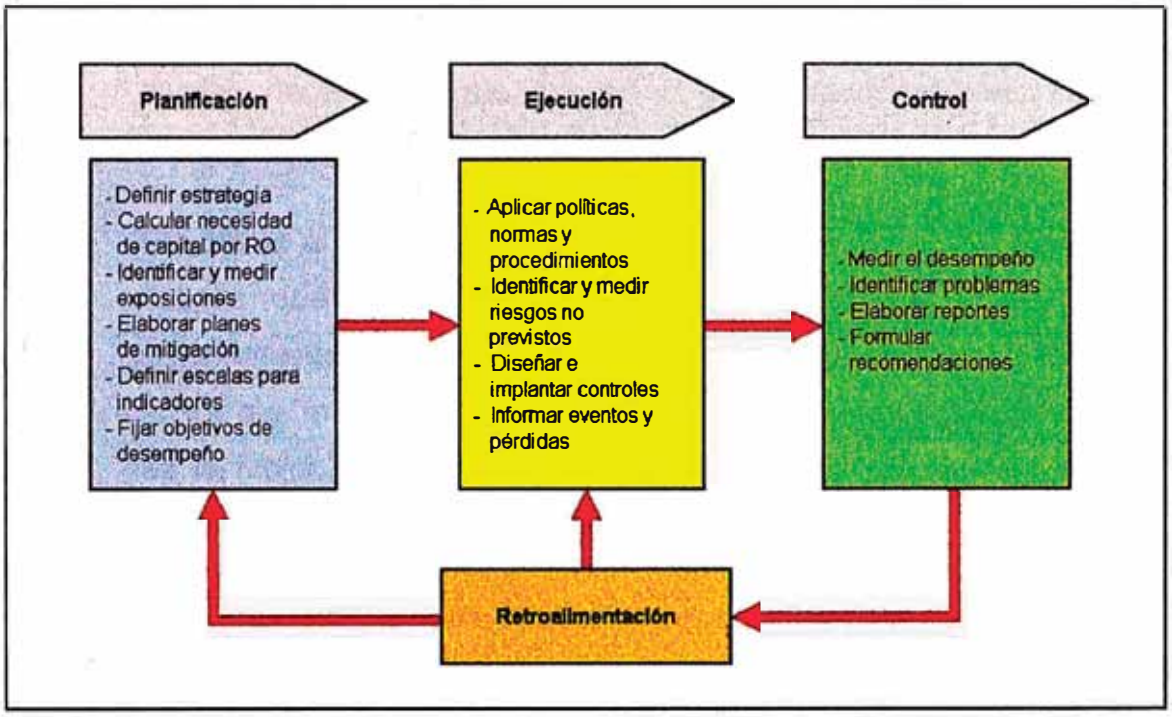
3.4. EL RIESGO OPERACIONAL EN LOS PLANES DE NEGOCIO

De la misma manera como se enfoca actualmente los riesgos de crédito y de mercado, el riesgo operacional debe estar incorporado dentro de los planes de negocio, incluyendo el desarrollo de nuevos productos, y de los procesos operativos, y debe ser considerado, gestionado y evaluado de manera proactiva, abarcando las tres etapas principales de los planes de negocio: planeamiento (incluyendo la formulación de la estrategia), ejecución y control.

En la etapa de planeamiento se debe formular la estrategia general, establecer los objetivos, asignar los recursos, y elaborar los planes detallados considerando, por supuesto, el análisis de los posibles riesgos. Siguiendo el enfoque "*bottom up*", cada unidad de negocio debe determinar su capital por riesgo operacional, identificar y medir

su exposición a los riesgos, formular sus planes de mitigación, elaborar las escalas para sus indicadores de riesgo, y fijar sus objetivos de desempeño.

Grafico No. 8: El riesgo operacional en los planes de negocio



En la etapa de ejecución, que comprende la puesta en marcha y desarrollo de los planes de negocio, la gestión del riesgo operacional cubre las actividades y controles relacionados con todos los riesgos previstos en la etapa de planificación, desde el momento en que se producen las ventas hasta la atención de los reclamos de los clientes. En esta etapa, las operaciones deben realizarse según los procedimientos establecidos, deben llevarse a cabo auto evaluaciones para detectar riesgos no previstos, analizar e implementan controles, medir las exposiciones, informar aquellos riesgos y eventos cuyos indicadores exceden los límites establecidos y aplicar las medidas de mitigación.

La etapa de control comprende el seguimiento y evaluación del desempeño, con relación a los objetivos establecidos en la primera etapa. La gestión comprende la generación de informes que abarquen todos los aspectos del riesgo operacional de la organización, identificando los procesos en los que se ha presentado las desviaciones con lo previsto y determinando las causas. Finalmente se formulan las recomendaciones y se realizan los ajustes necesarios, que pueden ir desde modificaciones en los procesos hasta la reformulación de los planes.

En cuanto al desarrollo de nuevos productos, estos llevan implícitos riesgos que pueden no haber sido identificados y evaluados anteriormente, por ello la constitución de comités riesgo operacional, en los que intervengan todas las áreas involucradas en el desarrollo, es la mejor forma de prevenir el riesgo antes de que un nuevo producto sea lanzado al mercado.

Como ya se ha señalado anteriormente, la responsabilidad de incorporar las consideraciones de riesgo operacional en la formulación de los planes de negocio debe ser responsabilidad de las unidades de línea en cuyo ámbito se desarrollen las operaciones. La guía de acción será la respectiva declaración de políticas Las unidades de apoyo y la unidad central de riesgo operacional aportarán las herramientas y brindarán el soporte técnico necesario.

En el gráfico No. 6 se ilustran las tareas de gestión del riesgo operacional que corresponden a las tres etapas del plan de negocios.

3.5. LA UNIDAD DE GESTIÓN DEL RIESGO OPERACIONAL

Tal como se ha visto en el acápite 3.2, la gestión del riesgo operacional requiere que se definan responsabilidades, y equipos de gestión, tanto a nivel de línea (vertical) como a nivel corporativo

(horizontal). Si bien las unidades de línea tienen la responsabilidad sobre los aspectos del "día a día" de la gestión, debe existir una unidad especializada que centralice los aspectos corporativos de la gestión, como son la formulación de políticas generales, desarrollo e implementación de metodologías, herramientas, procedimientos, y de la asesoría a las unidades de negocio.

La existencia de una unidad "central" no implica que exista una gestión "centralizada", como es la tendencia actual en los casos de otros riesgos como los de mercado y de crédito. En temas de riesgo operacional no puede haber centralización porque, a diferencia por ejemplo del riesgo de crédito, no existen procedimientos para autorizar la toma de tales riesgos. Evidentemente tampoco es posible "denegar" la ocurrencia de una estafa, una falla de sistemas, o un accidente, todos ellos acontecimientos que pueden ocurrir en cualquier área del banco.

Por otra parte, contar con una unidad a cargo de determinadas funciones corporativas relacionadas con el riesgo operacional, es una tendencia comprobada en el sector financiero. En efecto, entre las conclusiones de una investigación llevada a cabo en 1999, sobre la base de 55 entidades con operaciones a nivel internacional, dentro de las cuales se encontraban 37 de los 100 mayores bancos globales[15], se estableció que el modelo organizativo más aceptado es el de una unidad central de riesgo operacional, cuyo responsable reporta directamente al ejecutivo de mayor nivel dentro del área de riesgos del banco. Esta unidad tiene una estructura bastante ligera, con no más de 5 personas en promedio, y su labor es complementada por un *staff*, encargado de las funciones de soporte y control en las unidades de negocio individuales, como parte de

[15] Robert Morris Associates (RMA), *Operacional Risk: The New Frontier*, publicado en 1999 por la British Bankers Association, la International Swaps and Derivatives Association y la firma RMA conjuntamente con Price Waterhouse Coopers. Información obtenida del sitio web www.rmahq.org.

cada una de ellas o integrando la función corporativa, pero en todos los casos operando de manera coordinada.

Entre las funciones encargadas a la unidad de riesgo operacional, algunas de las cuales ya han sido señaladas, el referido estudio ha identificado las siguientes:

- Establecer definiciones y políticas de riesgo operacional
- Desarrollar e implementar herramientas de uso común
- Establecer indicadores de riesgo
- Elaborar programas de difusión y capacitación
- Analizar las vinculaciones con los riesgos de mercado y de crédito
- Desarrollar modelos de capital económico
- Construir bases de datos de eventos y pérdidas
- Asesorar y/o participar en la formulación de los planes de riesgo operacional de las unidades de negocio
- Consolidar la información sobre el portafolio de riesgo operacional de la entidad.

En el caso de las entidades que conforman el sistema financiero peruano, el Reglamento Para la Administración y Control de los Riesgos de Operación, referido en el acápite 2.7, en su artículo 5º, señala lo siguiente:

> *De conformidad con lo dispuesto en el Reglamento del Sistema de Control Interno, la Unidad de Riesgos será la encargada de la administración de los riesgos de operación que enfrenta la empresa, pudiendo comprender a alguna unidad especializada para la evaluación de dicho riesgo.*

Asimismo, para dicho fin, la unidad de riesgos o, de ser el caso, la unidad especializada, deberá contar con la infraestructura adecuada, así como con los recursos humanos, técnicos y logísticos que le permitan el apropiado cumplimiento de sus funciones, de acuerdo a la dimensión y estructura de la empresa, la naturaleza de sus operaciones y servicios y la complejidad de los mismos.

Entre las funciones de la referida unidad responsable se incluirán por lo menos las siguientes:

a. *Preparación y evaluación de políticas para la administración de los riesgos de operación.*
b. *Desarrollo de metodologías para la evaluación cuantitativa y/o cualitativa de los riesgos de operación.*
c. *Evaluación de los riesgos de operación, de forma previa al lanzamiento de nuevos productos y ante cambios importantes en el ambiente operativo o informático.*
d. *Consolidación y desarrollo de reportes e informes sobre la administración de los riesgos de operación por proceso, o unidades de negocio y apoyo.*
e. *Identificación de las necesidades de capacitación y difusión para una adecuada administración de los riesgos de operación.*
f. *Otras necesarias para el desarrollo de su función.*

CAPÍTULO 4: LOS PROCESOS

4. LOS PROCESOS

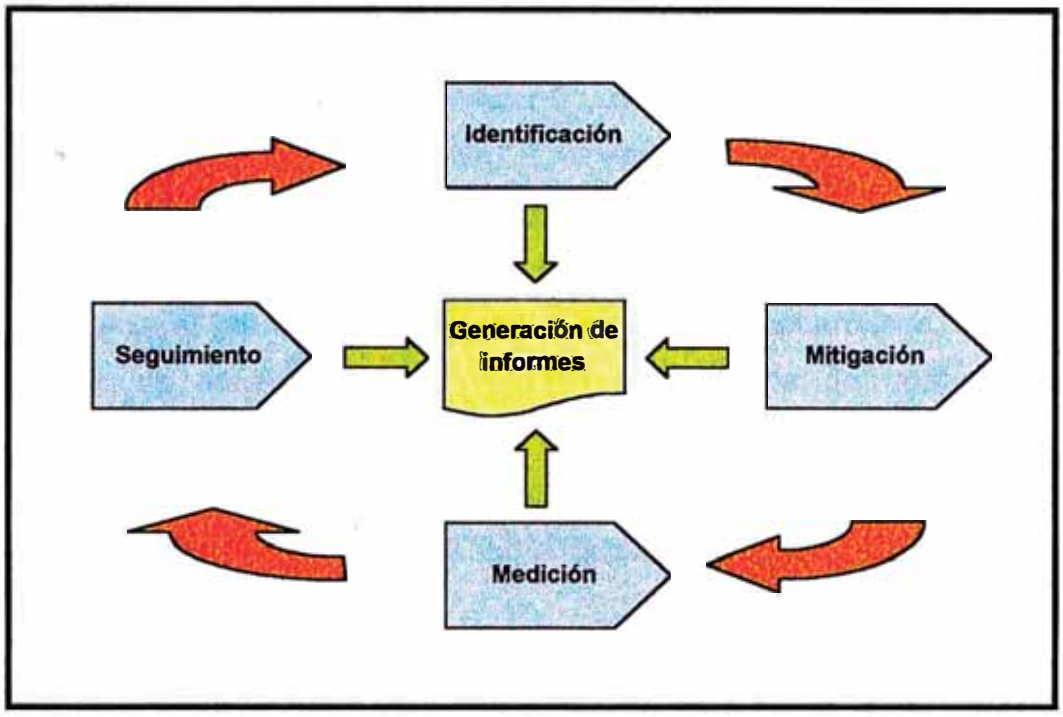
Los procesos de gestión del riesgo operacional son aquellas actividades que constituyen la administración cotidiana de este tipo de riesgos. Estos procesos pueden abarcar desde la observación de cómo se realiza determinada transacción, tal como el desembolso de un préstamo, para identificar las causas de posibles errores, hasta tareas más complejas como la construcción de bases de datos o la asignación de capital económico.

En este modelo estamos considerando que la gestión consta de cinco procesos, que deben ser llevados a cabo por cada unidad de negocio y de apoyo. Como ya se ha explicado anteriormente es fundamental que la unidad afectada por los riesgos esté directamente implicada en esta labor. La participación de la unidad central, como elemento de soporte técnico y asesoría, que valida los resultados del análisis, no implica trasladar a esta última la responsabilidad por la realización ni por los resultados del trabajo.

Estas cinco actividades deber ser consideradas, en su conjunto, como un proceso de mejora continua, que debe permitir a la organización el detectar y corregir las deficiencias de los procesos de negocio, de forma que se pueda minimizar el efecto adverso de los posibles eventos, siempre tomando en consideración que los elementos de costo implícitos en el proceso, no superen los beneficios de las menores pérdidas.

El Gráfico 8 ilustra la relación entre los procesos de gestión del riesgo operacional.

GRÁFICO 9: Procesos de gestión del Riesgo Operacional



4.1. IDENTIFICACIÓN

Consiste en determinar cuales son los factores de riesgo asociados a los procesos que realiza la unidad que se está analizando. Implica establecer, en el contexto de los objetivos del negocio, cómo puede asegurarse el logro de tales objetivos, a pesar de los riesgos implícitos.

Por proceso de negocio se entiende el conjunto de actividades necesarias para la transformación de las entradas (información o actividades) en salidas (información o actividades) destinadas a satisfacer los requerimientos de clientes o de otras unidades. Por ejemplo, en la cancelación de un préstamo, las entradas serían los datos del cliente (nombre, fecha, número del préstamo, importe del

pago) informados al momento de realizar la transacción. El proceso estará formado por todas las acciones que se realizan hasta que los fondos se aplican a la obligación respectiva. El producto final para el cliente será la confirmación de que su préstamo ha sido cancelado, mediante la emisión de un comprobante físico.

Como referencia para la identificación, es recomendable emplear la clasificación de eventos del NACB, referida en el acápite 1.3. Esto porque se trata de una clasificación estándar, que seguramente ha de ser adoptada por la SBS y porque su uso permitirá en algún momento el intercambio de información y el aprovechamiento de las bases de datos externas. Además de los tipos de riesgo ya señalados, otras fuentes como son el registro de eventos, la experiencia, la identificación de problemas y los indicadores clave, proveen información adicional sobre factores potenciales de riesgo.

Se entiende por factor de riesgo, toda aquella actividad o situación, cuyas características pueden dar lugar a que produzcan cualquiera de los tipos de eventos de riesgo definidos. Por ejemplo, la falta de capacitación o el exceso de carga de trabajo, son factores de riesgo porque pueden dar lugar a errores humanos; las demoras en la atención de reclamos pueden dar lugar a que el banco se pueda ver obligado a pagar multas e indemnizaciones; la falta de documentación de determinados programas informáticos pueden dar lugar a interrupciones en el servicio, por demoras en la detección de fallas.

La identificación es, esencialmente, un proceso de auto evaluación, llevado a cabo por la misma unidad de negocio para determinar:

- ¿Qué factores de riesgo existen?
- ¿Qué eventos de riesgo se pueden derivan de esos factores?
- ¿Qué pérdidas podrían ocasionar y con que frecuencia?

- ¿Cómo se controlan los riesgos?
- ¿Cuáles son los puntos débiles de los controles?
- ¿Qué se puede hacer para reforzarlos?
- ¿Quién es el responsable por las acciones de mejora?
- ¿Cómo se planea llevarlas a cabo?

Los riesgos deben ser identificados en base a la exposición inherente, es decir sin considerar ninguna medida de mitigación. Por ejemplo, si por demoras en el proceso de traslado de dinero, en la bóveda de una oficina hay siempre un promedio de USD100 000, la exposición al riesgo de robo es exactamente esa cantidad, independientemente de las medidas de seguridad que se hayan tomado.

Existen diferentes técnicas para llevar a cabo el proceso de identificación mediante auto evaluación. Entre las más utilizadas están:

- Cuestionarios estructurados, o *checklist*, en los que, a partir de una tipificación de los riesgos, se pide a la unidad involucrada que identifique aquellos que afectan a sus procesos, les asigne estimados de su frecuencia y severidad, detalle los controles que tiene implementados y haga sus propias sugerencias para mejorarlos.
- Entrevistas personales con las personas o equipos encargados de los procesos, en las que se les pide que describan los riesgos que ellos han detectado y sustenten la forma en que llevan a cabo sus controles. Esta es una modalidad que requiere de mayor esfuerzo pero que suele rendir mejores resultados que el llenado de un cuestionario, aunque también es usual que se combinen ambas técnicas.

- Talleres de trabajo, o *Workshops*, dirigidos por lo general por un consultor externo, o por la unidad central, en el que participan tanto la unidad afectada como representantes de otras unidades de negocio y de apoyo, que conozcan sobre el tema tratado, por ejemplo un proceso o grupo de procesos en particular. Esto tiene la ventaja de que la discusión entre personas con diferentes puntos de vista puede conducir a conclusiones consensuadas y por ende con mayor valor.

El resultado del proceso de identificación, es lo que se conoce como "mapa de riesgo", en el cual se indica qué clase de riesgos afectan a determinado negocio, proceso o unidad, y en que grado. El grado se expresa usualmente mediante la combinación de las características de frecuencia y severidad, que en esta etapa puede expresarse en forma cualitativa, por ejemplo como alta, media o baja, dejando las escalas cuantitativas para la etapa de medición.

Usualmente, la primera dificultad que se presenta es el número y la variedad de procesos que se deben analizar. Por ello lo recomendable es agrupar lo procesos por líneas de negocio, es decir agrupando procesos que corresponden a productos orientados a determinados segmentos de clientes, y luego agruparlos por familias de procesos similares entre sí en cuanto a sus características operativas. El mismo procedimiento se puede aplicar en el caso de los procesos realizados por las áreas de apoyo. Esta agrupación es útil porque permite identificar procesos con características de riesgo similares, lo cal simplifica el trabajo y reduce los tiempos de evaluación.

La identificación debe también extenderse a aquellos factores que tienen su origen en el ambiente externo y en las tendencias del sector. No debe limitarse a la situación actual sino que también debe enfocarse sobre los riesgos que pueden presentarse en el futuro

inmediato. Así como el desarrollo de productos lleva consigo nuevos riesgos, de la misma manera puede darse el caso de que riesgos ya existentes, que antes podían tener poca relevancia, adquieran nuevas dimensiones que hagan necesario tomarlos en cuenta. Por ejemplo, la banca por Internet ha ocasionado la aparición de tipos de riesgo que antes no existían.

4.2. MITIGACIÓN

El siguiente proceso consiste en establecer cuáles son las medidas de mitigación posibles, es decir aquellas que pueden contribuir a disminuir la frecuencia o la severidad de los eventos de riesgo. Algunas de estas medidas pueden ya existir al momento del análisis y otras tendrán que ser adoptadas. Entre las medidas de mitigación posibles tenemos:

- Rediseño de procesos: Consiste en añadir controles o reemplazarlos por otros más eficientes. Estos controles pueden estar incorporados en los sistemas automatizados, como por ejemplo las claves de acceso a los sistemas informáticos (seguridad lógica) o los filtros que impiden el ingreso de datos incompletos o incongruentes, o pueden consistir en sistemas alternativos de verificación, como es el caso de las conciliaciones de saldos contables.
- Sistemas de seguridad física: Comprenden todo aquello que actúa como barrera para impedir o disuadir el acceso no autorizado a edificios o ambientes, y para evitar la sustracción o el daño de bienes físicos. Por ejemplo el personal de vigilancia, las alarmas y sistemas de seguridad electrónicos, cristales blindados, cerraduras codificadas con claves, anclaje de equipos etcétera. También se refiere a los sistemas o dispositivos empleados para prevenir o para minimizar las consecuencias de accidentes o de desastres,

como por ejemplo los sistemas contra incendios, y la señalización de zonas de seguridad y vías de escape.

- Aumento / reemplazo de recursos: Dotar a las unidades con los recursos humanos, el equipo y los materiales, suficientes y adecuados, es una medida que evita los riesgos derivados de la sobrecarga de trabajo, que no sólo incluyen los errores sino también la baja en la calidad del servicio.
- Separación de funciones: Consiste en evitar que una misma persona ejerza funciones o tenga atribuciones que podrían dar lugar a actividades fraudulentas o no autorizadas, como por ejemplo autorizar una orden de compra y realizar el pago al proveedor, o tomar una posición en el mercado de valores y liquidarla.
- Rotación de puestos: La rotación periódica de puestos es una práctica que tiene por finalidad, aparte de contribuir a la transmisión de conocimientos y al desarrollo de capacidades y habilidades múltiples, a evitar la posibilidad de que surja la figura del empleado "indispensable" o de que se oculten deficiencias o irregularidades.
- Automatización: Reemplazar procesos manuales por automatizados es una medida que, al margen de los objetivos de mayor capacidad y velocidad de proceso, disminuye evita la posibilidad de errores humanos, evita las omisiones y favorece la integridad de los datos
- Capacitación y entrenamiento: El objetivo de estas actividades es el de asegurar que el personal tenga el nivel de conocimientos y la destreza necesarias para las labores del puesto que desempeña, incluyendo además todo lo relacionado con la gestión del riesgo operacional, en el ámbito de sus funciones.

- Diversificación: Esta es una medida importante para disminuir los riesgos derivados del incumplimiento de los proveedores. Concentrar las adquisiciones de determinado suministro en un solo proveedor, puede hacer que la empresa asuma un riesgo que desconoce, relativo a la continuidad del proveedor.

- Tercerización (*Outsoursing*): Consiste en contratar servicios de terceros, generalmente para aquellas actividades que no están en la línea de negocio de la empresa y que pueden ser realizadas más eficientemente por empresas especializadas. Un ejemplo puede ser el transporte de caudales, que traslada al proveedor los riesgos derivados de asaltos, fallas en los vehículos etc.

- Seguros: Es una de las modalidades de mitigación más conocidas, en las que se traslada el riesgo a una empresa aseguradora a cambio del pago de una comisión o prima, Se emplea para mitigar eventos de baja frecuencia y alta severidad, como es el caso de los fraudes, robos, incendios, responsabilidad por accidentes, desastres naturales etc.

- Planes de continuidad: Son aquellos que permiten mantener la continuidad de las operaciones, en caso que se presenten circunstancias que podrían interrumpir o dificultar su normal desarrollo por periodos más o menos cortos, por lo general de no más de un día, y casi siempre de manera localizada. Los planes de continuidad están referidos principalmente a los denominados "procesos críticos" del negocio, incluyendo aquellos en los que existe dependencia de terceros, para los que la rápida reanudación del servicio es fundamental. Ejemplos de estas medidas pueden ser los procedimientos de reemplazo del personal en caso de ausencia de los titulares, la disponibilidad de generadores

de energía eléctrica en caso de interrupción del servicio público, los procedimientos para el procesamiento de transacciones "fuera de línea", los programas de mantenimiento preventivo de equipos, la documentación de sistemas, la generación periódica de archivos de respaldo o *backups*, etcétera.

- Planes de contingencia: Son planes para hacer frente a eventos de consecuencias catastróficas, de muy baja frecuencia pero elevada severidad, como es el caso de desastres naturales, acciones terroristas, incendios, inundaciones, pérdidas masivas de datos por fallas de sistemas o a causa de virus informáticos, etcétera. Estos planes analizan las circunstancias que pudieran presentarse y las acciones que deben realizarse para mantener la continuidad de las operaciones, tratando de reducir al mínimo los periodos de interrupción, las pérdidas ocasionadas, y los costos de llevar a cabo tales acciones. Entre las medidas contempladas en los planes de continencia están, aparte de los seguros, los sistemas redundantes de almacenamiento de datos, la contratación de servicios alternativos de soporte informático y de comunicaciones, los planes para la evacuación de edificios, los sistemas contra incendio, etcétera.

Las medidas de mitigación pueden actuar sobre la frecuencia de los eventos, sobre la severidad o sobre ambos. Por ejemplo contratar un seguro o no afecta la frecuencia pero si disminuye la severidad; una mayor capacitación del personal no influye en la severidad de los errores pero puede disminuir la frecuencia.

La tarea de determinar las formas de mitigación, es una labor que corresponde realizar exclusivamente de las unidades de línea. Dado que en muchos casos la mitigación implica tomar medidas que

pueden estar fuera del ámbito de decisión de la unidad afectada, deben establecerse mecanismos para que un comité, con el nivel de autoridad suficiente, evalúe y autorice qué factores de riesgo deben ser mitigados y en qué forma. La consideración más importante será la de carácter económico, es decir que la mitigación debe generar beneficios superiores al costo de implementarla. Este análisis puede conducir a aceptar la presencia de un determinado riesgo sin realizar ninguna acción para mitigarlo, o a implementar una medida de mitigación que tal vez no sea la óptima en términos de efectividad, pero si la más eficiente en términos económicos.

4.3. MEDICIÓN

El proceso de medición tiene como principal objetivo el establecer medidas cuantitativas que permitan evaluar si la gestión está contribuyendo a los objetivos estratégicos de la empresa. Un segundo objetivo es la determinación de las necesidades de capital por riesgo operacional. Para cumplir estos propósitos, una vez concluida la identificación, el paso siguiente es realizar un análisis cuantitativo para estimar el impacto económico esperado como consecuencia de los riesgos que se han asumido. Existen seis tipos de mediciones para este efecto.

4.3.1. VARIABLES DE INFLUENCIA (*DRIVERS*)[16]

Son aquellas variables cuyos cambios, por lo general, están asociados con cambios en el perfil de riesgos de la empresa. Los cambios significativos en estas variables pueden implicar cambios en el nivel general de los riesgos o en el de riesgos específicos. Como ejemplos de este tipo de variables podemos citar:

[16] Aunque en las disciplinas relacionadas con la actividad financiera, la palabra inglesa *Driver*, se suele traducir como "Impulsor", el autor ha preferido el termino "Variable de Influencia" por considerarlo más apropiado para los fines de este trabajo.

- Volumen total de operaciones
- Número total de empleados
- Variedad / complejidad de productos
- Satisfacción de la clientela / calidad de servicio
- Tamaño de la red de oficinas
- Grado de automatización
- Nivel de satisfacción laboral

Muchas de estas variables son de tipo cualitativo y deben ser llevadas a escalas cuantitativas con el fin de analizar su influencia en el desempeño de las diferentes líneas de negocio. Debe también tenerse en cuenta que en muchos casos, los efectos del cambio en estas variables no suelen ser inmediatos sino que dejan sentir su efectúen en los riesgos, en el mediano y largo plazo.

4.3.2. INDICADORES CLAVE DE RIESGO

Los indicadores clave son variables cuantificables que permiten monitorear el desarrollo de una actividad o proceso, dentro de una determinada línea de negocio y para una categoría específica de riesgo. En la medida que estos indicadores hayan sido correctamente definidos, debe esperarse que sus variaciones indiquen que las probabilidades de pérdidas también están cambiando. Ejemplos de indicadores de riesgo son:

- Número de transacciones mal procesadas
- Número de horas de trabajo extra por empleado
- Duración promedio de las interrupciones del sistema
- Periodo promedio de rotación del personal

- % de empleados temporales
- Importe promedio de diferencias en cuadres de caja
- Tiempo promedio de atención de reclamos
- Nivel de preparación de los empleados

Los indicadores de riesgo constituyen las herramientas clave en el proceso de evaluación y control del riesgo operacional y para su determinación usualmente se requiere de la aplicación de técnicas para determinar las escalas apropiadas de medición y para expresarlos sobre bases de comparación uniformes (normalización).

La principal ventaja de los indicadores de riesgo es que por ser cuantitativos y objetivos, pueden ser generados automáticamente, o por lo menos su obtención es mucho más simple, comparada con el trabajo que implica el analizar las respuestas a cuestionarios cualitativos.

Los indicadores de riesgo pueden ser utilizados en primer lugar para calcular el nivel de riesgo real de cada unidad de negocio, y del conjunto de la empresa, para medir la eficacia de las medidas de mitigación, para generar señales de alerta y como herramienta de seguimiento. Por otra parte, su uso en técnicas para calcular las necesidades de capital económico, requiere que se disponga de datos históricos de pérdidas para poder determinar en qué forma los indicadores pueden relacionarse con las pérdidas futuras.

4.3.3. DATOS HISTÓRICOS DE EVENTOS Y PÉRDIDAS

Las empresas deben desarrollar bases de datos históricas que registren los eventos de riesgo operacional y las pérdidas ocasionadas por los mismos, si es que estas se hubieran

producido. La disponibilidad de datos históricos que cubran un periodo mínimo de cinco años, es un requisito que establece el NACB para las empresas que quieran aplicar los métodos de medición avanzados para determinar sus necesidades de capital.

Independientemente de las razones derivadas de las exigencias de la regulación, existen tres razones principales para acumular información sobre los eventos y las pérdidas:

- El registro de las experiencias pasadas ayuda a reforzar el sentido de prevención en todos los niveles de la empresa, favorece la comprensión de la importancia que tiene la gestión de estos riesgos y sirve de base para la evaluación y la mejora de los procesos.
- Los datos históricos sirven para la realización de análisis cualitativos, al proporcionar información sobre qué tipo de problemas ocurrieron, qué eventos se han repetido, con qué productos, en qué etapa del proceso y cuáles han sido las causas, todo lo cual ayuda a realizar acciones correctivas en los sistemas de control.
- Los datos constituyen la base para la realización de análisis cuantitativos que a su vez son el fundamento para la elaboración de modelos para la medición de los riesgos y para el cálculo de los requerimientos de capital económico. También sirven para estimar la "pérdida esperada", que es necesaria para la determinación de precios y la constitución de provisiones.

Las bases de datos deben contener información sobre todos los eventos de riesgo ocurridos, hayan o no producido finalmente pérdidas monetarias; deben identificar exactamente las unidades de negocio afectadas y el punto de

control en que se produjeron; deben estructurarse de manera que reflejen el esquema organizacional de la entidad y la clasificación de riesgos adoptada. Asimismo deben contener información descriptiva sobre las causas de los eventos, en un nivel de detalle que sea proporcional a la magnitud del evento y/o de la pérdida producida.

Es fundamental además que la implantación de la base de datos, su estructura, y las responsabilidades relacionadas con su mantenimiento sean comunicadas a toda la organización, y que todo el personal tenga conocimiento de las obligaciones que les compete en esta materia.

4.3.4. MODELOS CAUSALES

El propósito final de la gestión del riesgo operacional es poder predecir las pérdidas potenciales asociadas a los riesgos. Estas predicciones pueden formularse recurriendo al empleo de modelos causales, mediante los cuales se trata de establecer las relaciones que existen entre las variables de influencia, los indicadores clave de riesgo y la probabilidad de que se produzcan eventos de pérdida, probabilidad que puede ser estimada a partir de la data histórica.

Existen diferentes técnicas para la formulación de modelos causales. Las más utilizadas son las que utilizan el análisis estadístico multivariado para determinar qué indicador o indicadores están más estrechamente asociados con la ocurrencia de eventos de pérdida. Estos modelos pueden también utilizarse para analizar las causas de los eventos y para simular escenarios en de situaciones que podrían presentarse en el futuro.

Entre los métodos de análisis multivariado, los que tienen mayor aplicación en este campo son:

- Regresión Lineal Múltiple: tiene el mismo fundamento que la regresión lineal simple, pero la diferencia es que estudia la relación entre dos o más variables independientes, en este caso los factores o indicadores de riesgo, con una variable dependiente, por ejemplo la frecuencia o la severidad, estableciéndose así un modelo predictivo lineal.
- Regresión Logística. Se basa en una formula logarítmica que calcula la relación entre una o más variables independientes con una variable dependiente, de carácter dicotómico, como por ejemplo la ocurrencia o no de un evento de pérdida. Esta técnica también se emplea en la evaluación de los riesgos de crédito, para la elaboración de modelos de *scoring*, que permiten calificar las operaciones según su probabilidad de incumplimiento.
- Análisis Discriminante. Permite establecer la relevancia de los indicadores clave de riesgo, como elementos causales de los eventos, estableciendo las posibles correlaciones entre los indicadores y descartando aquellos factores que no son representativos al momento de predecir la probabilidad de ocurrencia del evento y/o de la pérdida consiguiente.

Además del requisito de contar con datos suficientes, las técnicas señaladas requieren conocimientos especializados y por lo tanto deben ser manejadas por profesionales con la formación adecuada, o por consultores experimentados, a fin de evitar que se pueda llegar a resultados incorrectos, al igual

que puede ocurrir con cualquier otra técnica estadística mal utilizada.

4.3.5. MODELOS DE CÁLCULO DE CAPITAL

La aplicación de los modelos causales para el cálculo de las pérdidas esperadas e inesperadas, por línea de negocio y por tipo de riesgo, conducen a la determinación de las necesidades de capital económico, es decir la máxima pérdida que en promedio debería esperarse, calculada con un nivel de confianza del 99.9%. El capital económico así calculado, al margen de las exigencias del NACB, y de las que el regulador local establezca en su momento, es un elemento de primera importancia para fines de fijación de precios y para obtener medidas de desempeño ajustadas por el riesgo.

Mientras que en el método del indicador básico y en el estándar, el calculo del capital está basado en indicadores relacionados con el tamaño de la entidad, lo cual significa que su requerimiento de capital será mayor mientras mayor sea el volumen de sus operaciones, en los métodos avanzados se reconoce que si una entidad tiene un nivel de controles consistente con el crecimiento de sus operaciones, entonces su nivel de riesgo tenderá a mantenerse constante y sus necesidades de capital no aumentarán, o por lo menos lo harán a un ritmo menor, con relación al volumen de sus negocios.

Por otra parte, adicionalmente a la eficiencia financiera derivada de menores requerimientos de capital, el análisis requerido para el desarrollo y la aplicación de los métodos avanzados, conjuntamente con la aplicación de las *Sound Practices*, favorece el conocimiento y la mejora constante de

los procesos internos, crea una cultura de responsabilidad para con el perfil de riesgos de la entidad y, como ya se ha señalado anteriormente, genera ventajas competitivas y contribuye a la creación de valor.

4.3.6. MEDIDAS DE DESEMPEÑO

A diferencia de las otras mediciones, las medidas del desempeño se caracterizan por ser de carácter más global y por lo general se enfocan sobre los periodos de tiempo para los que se han establecido las metas y objetivos de corto plazo, usualmente un año o un semestre; además suelen estar incorporadas en los reportes que registran la productividad de las distintas unidades y tienen una influencia cada vez más importante en los sistemas de retribución de los ejecutivos y del personal en general.

Mientras que las mediciones descritas en los acápites anteriores ayudan a la dirección de la entidad a entender y gestionar el perfil de riesgo sobre una base continua, las medidas de desempeño se utilizan al inicio del periodo de evaluación, para establecer las metas y al final del periodo para medir su cumplimiento. Como ejemplos de estas medidas de desempeño podemos citar:

- El avance en los procesos de auto evaluación
- El cumplimiento de los planes para implementar medidas de mitigación
- El nivel global de riesgo operacional de la unidad, medido como capital económico por riesgo
- El % de eventos no identificados, en número e importe, con relación a los identificados en la auto evaluación

Otras medidas de desempeño pueden tener un carácter más cualitativo, pero no por ello menos importante, como por ejemplo el nivel de participación o de implicación del personal en los proceso de auto evaluación, y en las medidas de mitigación, que no sólo son una medidas de desempeño sino que además constituye en si mismo factores de riesgo.

Debe tenerse presente que las medidas de desempeño deben reflejar fundamentalmente el resultado y la efectividad del trabajo realizado y no deben estar referidas a variables cuya volatilidad está fuera del control de las unidades o personas que están siendo evaluadas.

4.4. SEGUIMIENTO

El seguimiento es la parte del proceso de gestión que permite el entendimiento cabal del comportamiento del perfil de riesgo de la entidad, al mostrar qué cambios están ocurriendo y qué clase de riesgos deben ser objeto de atención. El seguimiento comprende el monitoreo de los factores de riesgo, variables de influencia e indicadores clave; analiza las tendencias, detecta las variaciones relevantes y las etapas de los procesos en donde estas ocurren, evalúa la efectividad de los controles, analiza las causas de los problemas y propone las medidas correctivas.

De la misma forma como el riesgo operacional es un aspecto inherente de cualquier proceso de negocio, el seguimiento de estos riesgos debe constituir parte inseparable de la gestión, debe estar incorporado en los planes de todas las unidades de la organización y así debe quedar establecido en las políticas, en los procedimientos y en las normas. El papel de la unidad central de riesgo operacional será el de proporcionar las herramientas, coordinar las tareas -en especial cuando se trata de riesgos que afectan a varias unidades-

facilitar el intercambio de experiencias y consolidar la información a nivel corporativo.

Un aspecto fundamental del seguimiento debe ser su enfoque preventivo. Su función no debe limitarse a un análisis *ex post* de los acontecimientos, sino que debe tratar de anticiparse a los mismos, detectando señales de alerta y evaluando las medidas correctivas según diferentes escenarios. En este contexto, el seguimiento no es sólo la labor de recoger y transmitir información, sino que debe dar un valor agregado a la misma, contribuyendo no sólo a corregir las deficiencias sino también a mejorar los procesos, de una manera eficiente en términos económicos.

4.5. GENERACIÓN DE INFORMES

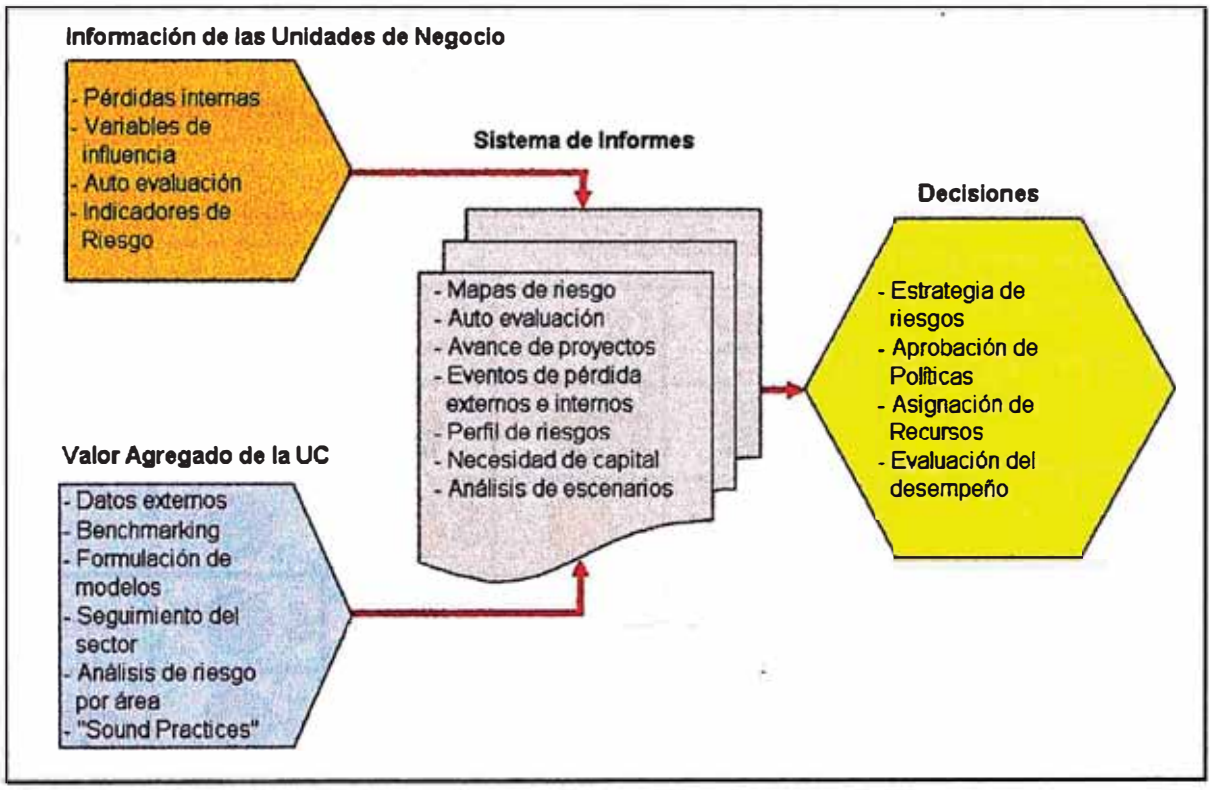
Este proceso comprende la implementación de un sistema que, partiendo de la información que las unidades de negocio y de apoyo deben proporcionar como parte de sus responsabilidades, y de la información que como valor añadido debe proporcionar la unidad central de riesgo operacional, la agrupe, la consolide y la presente en forma que sea útil para la toma de decisiones en los diferentes niveles de la organización.

El contenido y la frecuencia de estos reportes deben ajustarse a las necesidades de cada unidad de negocio. El nivel de detalle debe ser el suficiente para satisfacer los requerimientos de los responsables de las unidades de línea, pero también se debe proporcionar una visión consolidada del riesgo para uso de la alta dirección. Un esquema general de los principales reportes que debe proporcionar este sistema se muestra en el Grafico 10.

Dentro de los reportes que debe proporcionar el sistema están los mapas de riesgo, los cuales, como se ha mencionado anteriormente, son gráficos en los cuales los eventos de riesgo se plotean según

sus parámetros de frecuencia y severidad. La información para este fin puede provenir de los procesos de auto evaluación, o de las bases de datos de pérdidas. Los mapas pueden también mostrar los eventos según su riesgo inherente o después de las medidas de mitigación.

Grafico 10: Sistema de Informes de Riesgo Operacional[17]

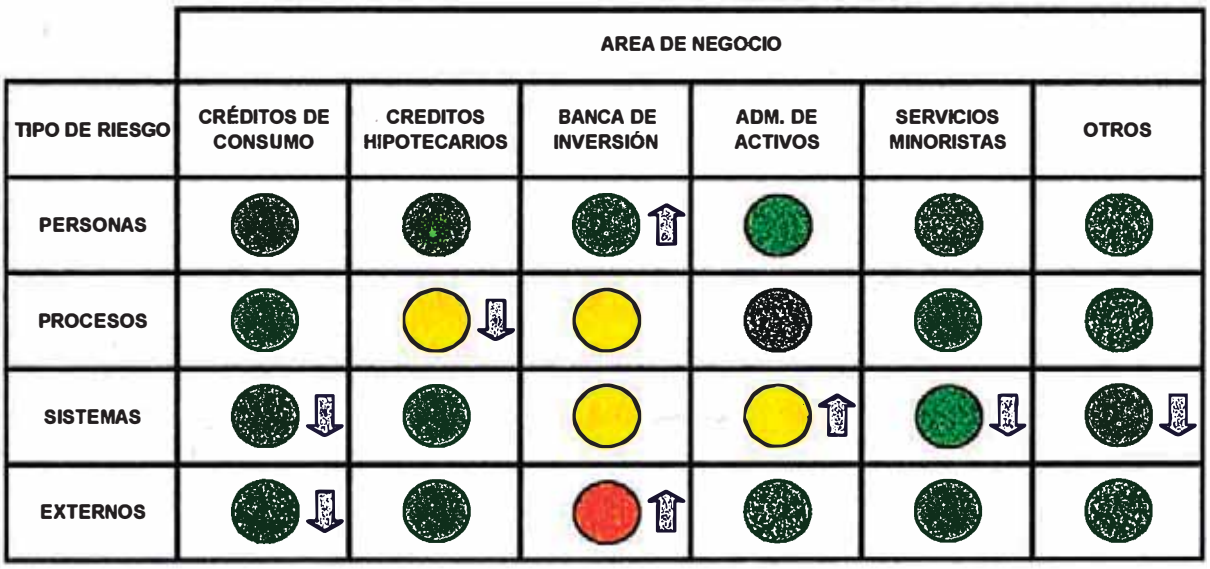


Otro tipo de reporte son los resultados de los procesos de auto evaluación, que también pueden ser mostrados en forma gráfica, por ejemplo empleando colores para identificar los diferentes niveles de riesgo, en una tabla que muestra los diferentes tipos de eventos y las líneas de negocio de la entidad mediante. Las tendencias del perfil de riesgo pueden ser señaladas mediante flechas.

[17] Adaptado de: Alexander, Carol (editora), op.cit. página 254

En el Gráfico 11 se ilustra una aplicación de este tipo. En ella los niveles de riesgo se representan mediante círculos de color, verde para el riesgo bajo, amarillo para un riesgo moderado y naranja para el riesgo alto. Al lado de cada círculo aparecen flechas que indican la tendencia observada: aumento si la flecha apunta hacia arriba, disminución si apunta hacia abajo. La ausencia de flechas indica una tendencia estable.

GRAFICO 11: Ejemplo de resumen de auto evaluación[18]



El sistema debe también proporcionar informes sobre los avances de proyectos en marcha. Estos proyectos pueden surgir como resultado del proceso de auto evaluación - por ejemplo implantar medidas de mitigación- de las revisiones de auditoria, cuando hay que corregir deficiencias, o de las exigencias de la regulación. Los planes de ejecución de estos proyectos definen las tareas a realizar, los tiempos y las responsabilidades. Los reportes pueden contener un

[18] Adaptado de: Alexander, Carol (editora), op. cit. página 255.

resumen de los proyectos más importantes, el estado de avance y las actividades que están retrasadas.

Los eventos de pérdida, ya sea que se hayan producido dentro de la entidad, o que hayan afectado a otra empresa del sector, proporcionan información valiosa para el análisis y la cuantificación del riesgo. Los reportes de eventos pueden contener resúmenes estadísticos de las bases de datos de pérdidas, mostrando promedios, variaciones y tendencias, por línea de negocio y tipo de pérdida. También se pueden hacer comparaciones con las pérdidas de otros periodos, o con el comportamiento del sector, elaborar diagramas de dispersión, mostrar el comportamiento de las recuperaciones y relacionar las pérdidas con las medidas de mitigación aplicadas.

En cuanto a los perfiles de riesgo, estos muestran como se distribuye el riesgo total de la empresa, por cada unidad de negocio y por tipo de eventos. El perfil de riesgo se determina como resultado del proceso de cuantificación y permite apreciar si los riesgos asumidos por cada área están en proporción con su contribución a los ingresos, o si esta distribución se ajusta a la política de tolerancia al riesgo establecida por la dirección. Los gráficos 11 y 12 muestran una forma de representar gráficamente el perfil de riesgos de una entidad, en base a la distribución de los porcentajes del riesgo total, por unidad de negocio y por tipo de eventos de pérdida. Alternativamente, el perfil puede estar referido a la necesidad de capital por riesgo, expresada en unidades monetarias.

GRÁFICO 12: Ejemplo de perfil de riesgo por tipo de evento[19]

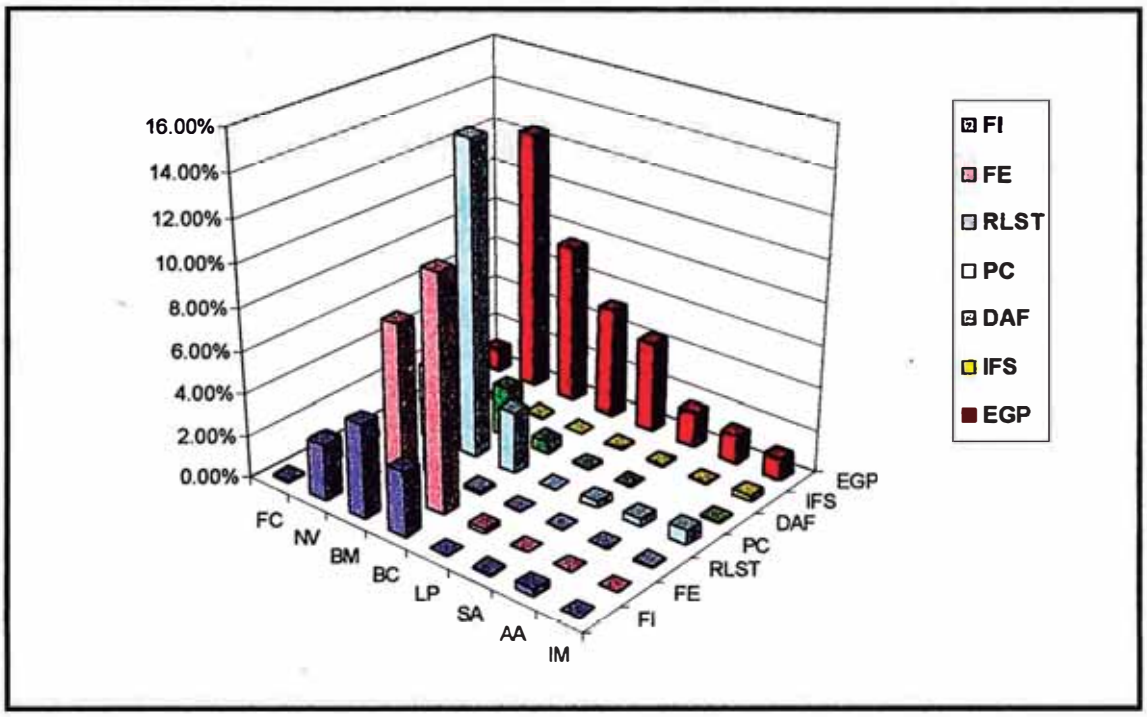
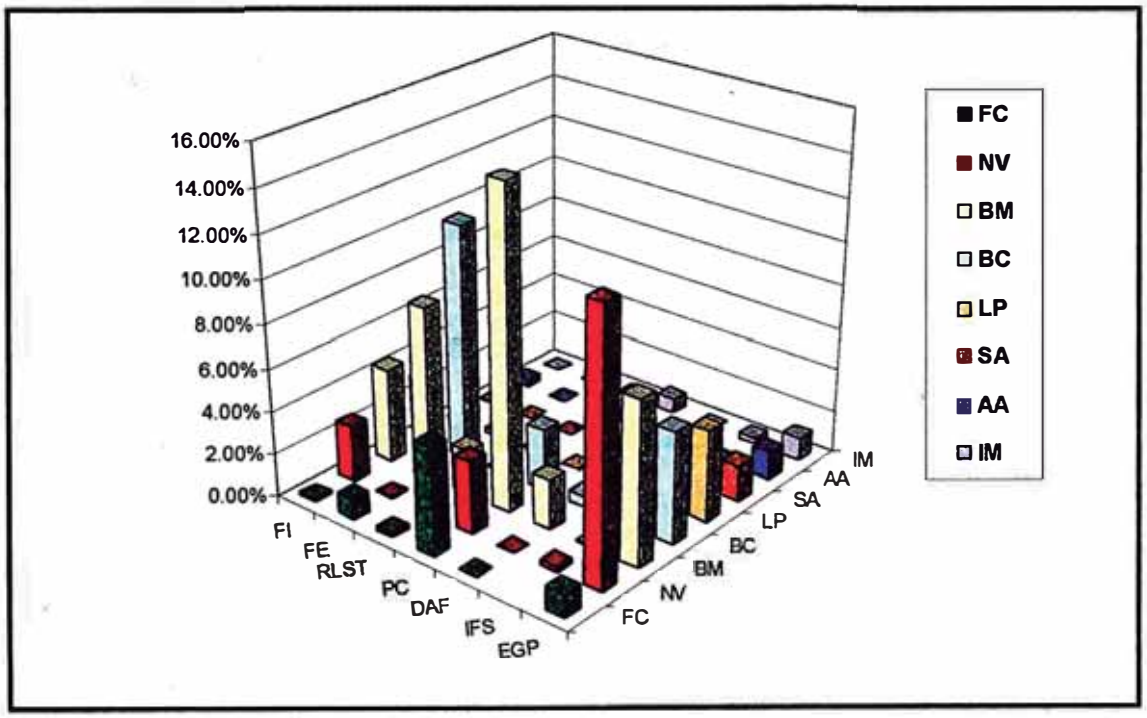


GRÁFICO 13: Ejemplo de perfil de riesgo por línea de negocio



[19] Gráficos elaborados con los datos del Anexo D

CAPÍTULO 5: LOS MEDIOS

5. LOS MEDIOS

Los medios o infraestructura son una de las dos partes que conforman la base del modelo de gestión del riesgo operacional. Loe medios comprenden la tecnología, incluyendo sus componentes tangibles e intangibles, los datos, las metodologías y los procedimientos, y los recursos humanos necesarios para llevar a cabo los procesos de gestión.

5.1. TECNOLOGÍA

Como en todos los campos, la tecnología es un instrumento indispensable para la gestión del riesgo operacional. Proporciona las herramientas necesarias para llevar a cabo los procesos de auto evaluación, para construir las bases de datos de eventos y pérdidas, para calcular los indicadores de riesgo, para operar los modelos causales y los de requerimientos de capital. Cada una de estas aplicaciones puede constituir un sistema separado, pero es recomendable que todas ellas trabajen sobre una base de datos y sobre definiciones comunes.

Al margen de su utilidad, no hay que perder de vista que la tecnología constituye un riesgo en si misma. De allí que se haya acuñado el término "Riesgo Tecnológico", para referirse al riesgo de pérdidas por desperfectos en el hardware, fallas de software, sistemas inadecuados o defectuosos y pérdidas de datos. El desarrollo interno de herramientas, aunque pueda parecer más económico, lleva implícito un elevado riesgo de este tipo, por ello es

indispensable compararlo con otras alternativas, como la adquisición a empresas especializadas, de sistemas "pre-fabricados", que puedan ser adecuados y parametrizados según las necesidades particulares de la empresa.

5.2. DATOS

Los datos constituyen el punto de partida y el objetivo central de los procesos de medición para la toma de decisiones. Esto que es cierto en todos los campos de la actividad empresarial, lo es más en el caso del sector financiero, en el que la información es su principal materia prima y producto. En la gestión del riesgo operacional las empresas recolectan datos de eventos de pérdidas, de factores y de indicadores y también recurren a bases de datos externas, pero los sistemas de cálculo más sofisticados no brindaran resultados útiles si es que los datos no son confiables o no han sido obtenidos oportunamente.

Aquí tenemos que tener claro que una cosa son los datos y otra el soporte o medio de almacenamiento de los mismos. Las empresas financieras pueden prescindir de un sistema de información propio (tanto el *hardware* como el *software*), hasta el punto de subcontratar con terceros la totalidad del servicio, pero no pueden prescindir de la información. La calidad de los datos radica en su confiabilidad, es decir en que sean fiel reflejo de la realidad, y en su disponibilidad, es decir en que puedan conseguirse cuando se necesitan.

La importancia de los datos como soporte del modelo de gestión, debe también reflejarse en la organización y en las políticas. La organización identifica a quienes tienen el encargo de proporcionar, registrar y velar por la integridad de los datos. Las políticas señalan las responsabilidades, las limitaciones y las pautas para el correcto uso de la información.

5.3. METODOLOGÍAS Y PROCEDIMIENTOS

Todo procedimiento orientado hacia la cuantificación requiere de metodologías detalladas y que estén apropiadamente documentadas. En el caso de los riesgos operacionales, las metodologías son especialmente necesarias para los procesos de medición y de manejo de los modelos causales y de cálculos de capital.

Los diferentes procesos de gestión también deben contar el apoyo de guías de procedimientos, para el correcto uso de las herramientas, y con manuales para la aplicación de las políticas, tanto de las que se refieren a los aspectos de riesgos como de las que corresponden a temas relacionados, como por ejemplo la prevención del lavado de dinero, la seguridad, los recursos humanos, contabilidad, compras etcétera.

La elaboración de metodologías y de manuales debe ser complementada con procedimientos para su adecuada divulgación y actualización permanente, estableciendo normas claras en cuanto a su alcance y confidencialidad.

5.4. RECURSOS HUMANOS

5.4.1. NECESIDADES

Las instituciones financieras deben asegurarse de asignar los recursos humanos necesarios para la gestión adecuada del riesgo operacional. También deben asegurarse que los responsables de los diferentes equipos de negocio y apoyo, tengan el perfil adecuado de experiencia y capacidad, y que estén plenamente identificados con los objetivos de la organización. Así mismo, debe asegurar que el personal responsable del seguimiento y control de la política de riesgos

de empresa tenga la autonomía y autoridad suficientes para llevar a cabo su misión y de que estás sean independientes de las líneas de negocio que supervisan.

Tal como se ha señalado en el apartado 3.5, el modelo organizativo más utilizado para la unidad central de riesgo operacional, comprende no más de cinco personas, incluyendo el ejecutivo responsable. Adicionalmente se considera un staff, con una o dos personas, en cada unidad de negocio, encargados de la supervisión de los procesos de gestión. Dependiendo de tamaño de la organización y de la complejidad de los procesos, el personal de las unidades de negocio puede llevar a cabo esta función a tiempo completo o compartiendo su tiempo con otras responsabilidades.

5.4.2. PERFILES

Las labores de identificación y de mitigación de los riesgos, en las unidades de línea y de apoyo, por lo general no requieren de conocimientos especializados distintos de los que proporciona la experiencia en las tareas propias de cada puesto, aunque siempre será necesario un entrenamiento en el uso de las herramientas que se provean para estos fines.

Tratándose del personal denominado de staff, referido en el acápite anterior, que eventualmente puede asignarse a funciones de soporte y control dentro de las unidades de negocio, es recomendable que estas sean personas con conocimientos y experiencia en todos los procesos de negocio que se realizan en la unidad, y que además hayan recibido entrenamiento en temas de análisis de flujos de procesos y programación de tareas. Asimismo, deberán contar con conocimientos básicos de estadística y probabilidades, de manera puedan comprender los

fundamentos de las técnicas cuantitativas que se utilizan en los métodos avanzados de medición, y actuar de manera consistente al momento de supervisar los trabajos de medición y de registro de datos.

En cuanto al personal de la unidad central de riesgo operacional, aquí será necesario contar con un equipo de profesionales, con formación académica orientada a aspectos cuantitativos, que incluyan conocimientos a nivel intermedio o avanzado de estadística, con formación en temas financieros y con un conocimiento de los procesos del negocio, a un nivel suficiente para poder realizar mediciones del riesgo confiables y para poder interpretar y transmitir los resultados, de manera que estos sean de utilidad para las unidades de negocio y para la dirección de la entidad.

CAPÍTULO 6: EL AMBIENTE

6. EL AMBIENTE

Tal como está señalado en las *sound practices*, tanto el directorio como la gerencia son responsables por la creación de una cultura organizacional que asigne la importancia debida a la gestión de los riesgos operacionales. La gestión de los riesgos será más efectiva en la medida que esta se desarrolle en un ambiente en el que haya una cultura consistente con los objetivos estratégicos, una dirección que demuestre con los hechos un alto grado de compromiso ético, y un sistema de comunicación que garantice la fluidez y la transparencia de la información.

6.1. LA CULTURA ORGANIZACIONAL

Según la definición propuesta por el profesor Stephen Robbins, "la cultura de una organización se refiere a un sistema de significado compartido entre sus miembros, que la distingue de otras organizaciones"[20]. Si aplicamos esta definición para establecer lo que es una Cultura del Riesgo, podemos decir que el significado compartido comprende las actitudes, creencias, valores, objetivos y prácticas, que caracterizan la forma como la empresa considera el riesgo en sus procesos de negocio.

La cultura del riesgo puede caracterizarse además por haber sido formulada de manera explícita, esto es de manera "formal", o ser el producto de un desarrollo a través del tiempo. Podemos decir

[20] Robbins, Stephen, *Comportamiento Organizacional*, 8va. edición, editorial Prentice Hall, México 1999, página 595.

entonces que la formulación de un modelo de gestión del riesgo operacional, es una forma de comunicar de manera explícita las características de la cultura que se desea para la organización.

Independientemente del modelo adoptado, la cultura del riesgo, formal o no, será la que finalmente defina los enfoques de gestión del riesgo operacional; por ejemplo si los criterios de medición serán cuantitativos o cualitativos, si las responsabilidades serán o no centralizadas, si los resultados de la gestión del riesgo afectarán, y en que grado, las medidas de desempeño, y también definirá el nivel de compromiso de la alta dirección.

El modelo de gestión del riesgo operacional será exitoso, si además de guiar la acción hacia el logro de los objetivos estratégicos, logra forjar una cultura del riesgo sólida que sirva de base para consolidar la aceptación y el perfeccionamiento del mismo modelo.

6.2. EL PAPEL DE LA DIRECCIÓN

El resultado de la gestión riesgo operacional es, en última instancia, responsabilidad del directorio y de la alta gerencia, ya que son ellos quienes determinan la estrategia y el nivel de riesgo que están dispuestos a asumir, asignan los recursos y evalúan el desempeño de los individuos. Para ello deben contar con un flujo de información continuo que les permita estar al tanto de la evolución del perfil de riesgos de la institución.

El directorio debe aprobar la implantación de un modelo que permita gestionar los riesgos de operación de manera explícita e independiente de los otros riesgos implícitos en el negocio. La gerencia es responsable de proponer los lineamientos generales del modelo y de desarrollar políticas, procesos y normas específicos para ser aplicados en las diferentes unidades de la organización.

Los responsables de la gestión del riesgo operacional a nivel corporativo, deben contar con el apoyo de la alta dirección, y esta debe estar involucrada activamente en el proceso. Los mensajes transmitidos acerca de la importancia del riesgo operacional deben ser consistentes con la atención que se brinde a todos los aspectos de la gestión, especialmente en lo que se refiere a la asignación de recursos y a la comunicación de los eventos.

También debe tenerse presente que la dirección de la empresa es en si misma una fuente de riesgos operacionales. En efecto, muchos de estos riesgos pueden tener su origen en decisiones tomadas por la alta dirección. Esto ocurre por ejemplo con la mayoría de los riesgos de naturaleza legal, los relacionados con el cumplimiento de las regulaciones, o aquellos que derivan de fallas en la estructura organizacional. Consecuentemente deben establecerse mecanismos para que la dirección evalúe y audite sus procesos de toma de decisiones y analice los eventos con un criterio amplio, que considere el papel que le puede tocar como factor de riesgo.

Es importante además que la dirección enfatice la necesidad de un alto nivel de comportamiento ético en todos los niveles de la institución y que este se refleje en un código de conducta cuyo principal medio de transmisión sea el ejemplo. Cualquier falla en este aspecto dará lugar a que la dirección se convierta en parte del problema en lugar de ser el principal protagonista de la solución.

6.3. LA COMUNICACIÓN

La misión y la estrategia de gestión debe ser comunicada en forma clara y oportuna a todos los niveles de la organización, de forma que todos entiendan los objetivos generales y el papel que a cada uno le corresponde para conseguirlos. La gerencia debe proveer canales

adecuados de comunicación para transmitir las políticas, las normas y los procedimientos, y para facilitar el flujo de realimentación.

La comunicación también debe favorecer el desarrollo de un lenguaje común, que al margen de las características particulares de las diferentes áreas de negocio, permita la comprensión de las definiciones contenidas en la estrategia de gestión, la comparación de objetivos y de resultados, la transmisión y el aprovechamiento de las experiencias y de buenas prácticas, y sirva de base para la consolidación de la cultura de riesgo.

El modelo de gestión debe apoyarse en sistemas de comunicación formales, ya sea que la información deba fluir de manera vertical u horizontal, y debe promover la apertura y la transparencia, de manera que todos se sientan motivados a compartir sus experiencias sin el temor de repercusiones negativas. Los eventos de pérdida deben ser vistos como oportunidades valiosas para mejorar los procesos y no como motivos para la búsqueda de responsables y para la aplicación de sanciones.

En este punto cabe mencionar lo señalado por Chorafas[21], en el sentido que la dirección de la empresa debe fomentar un ambiente en el cual los empleados no sólo tengan la libertad de hablar sobre cualquier aspecto del trabajo que pueda ser mejorado, o sobre cualquier cosa que a ellos les parezca que no marcha en forma correcta, sino que además se sientan cómodos haciéndolo. Esto es especialmente importante para la prevención de fraudes internos.

[21] Chorafas, Dimitris N., *OPERATIONAL RISK CONTROL WITH BASEL II; BASIC PRINCIPLES AND CAPITAL REQUIREMENTS*, Elsiever Butterworth-Heineman, Rochester, Reino Unido, 2004.

CAPÍTULO 7: CONSIDERACIONES ECONÓMICAS

7. CONSIDERACIONES ECONÓMICAS

7.1. NATURALEZA DE LOS COSTOS DE LA GESTIÓN DEL RIESGO OPERACIONAL

Es indudable que la implementación del NACB traerá consigo la necesidad de que las entidades financieras tengan que hacer frente a gastos significativos. Según una referencia del *ISMA CENTER – UNIVERSITY OF READING*[22], una encuesta a nivel mundial, realzada entre 3,000 bancos, reveló que será necesaria una inversión superior a los USD 23,000 millones, sólo para implementar las nuevas disposiciones de acuerdo, sin considerar el costo de mantenimiento de los sistemas. En el caso del riesgo operacional, tampoco se considera el costo asociado a cualquier cargo de capital exigido por los supervisores, como consecuencia de la aplicación de las nuevas normas.

La pregunta que surge aquí es si es posible llevar a cabo la cuantificación de los beneficios que obtendrán de la aplicación de estas medidas, y no sólo su identificación cualitativa, según se ha visto en el apartado 4.1, pero esta pregunta lleva implícita la suposición de que con dicha información será posible decidir si el esfuerzo se justifica o no en términos económicos, o en otras palabras si se debe o no efectuar la inversión. Para resolver esta interrogante es necesario primero analizar la naturaleza de los costos de gestionar el riesgo operacional.

[22] Información obtenida del sitio web: www.ismacentre.rdg.ac.uk/risk/rmg_brochure.pdf

Según refiere Chorafás[23], el esfuerzo de una empresa financiera, como el de cualquier otra organización, debe estar orientado hacia su propia supervivencia. Esto quiere decir que sus operaciones deben producir beneficios económicos. La obtención de beneficios económicos es una función esencial en cualquier sociedad, por lo que la rentabilidad debe ser el criterio que guíe la toma de decisiones de manera responsable. Pero es cierto también que la supervivencia de cualquier organización no depende sólo de su rentabilidad, sino de esta sea sostenible, y para ello es necesario que la empresa sea capaz de cumplir, y de superar, las expectativas de los grupos de interés relacionados y del conjunto de la sociedad.

Para garantizar su rentabilidad, y con ello su supervivencia, la administración de una empresa financiera debe ser capaz de cubrir todos los costos de su actividad, lo cual implica mucho más que los costos de realizar negocios, ello porque la actividad financiera, y también la industrial, deben estar enfocadas hacia el futuro. Siguiendo este criterio, Chorafas sugiere que la administración debe prestar especial atención a dos aspectos principales:

- Reducir sus costos fijos y hacer más eficientes sus operaciones
- Poner especial atención sobre los costos de "estar en el negocio"

Con respecto al segundo punto, es importante saber distinguir entre los costos de "hacer negocios" y los costos de "estar en el negocio". Los primeros son todos aquellos que están vinculados con el "día a día" de las operaciones. Por ejemplo, si hablamos de una empresa industrial, serían los costos de comprar, almacenar, producir, distribuir, vender y cobrar. Algunos de estos costos son fijos y otros son variables, pero su característica común es que todos pueden

[23] Chorafas, Dimitris N., op. cit.

incluidos en el precio del producto o servicio final. Estos son los costos que permiten la obtención de beneficios económicos.

Por su parte, los costos de "estar en el negocio" comprenden los gastos en investigación y desarrollo, y en aquellas actividades que tienen como propósito final, el garantizar que la empresa pueda tener un espacio en el mercado en el futuro. Muchas de estas actividades han tenido su origen en el ambiente académico, sin embargo hoy en día su aplicación es considerada como un elemento clave para el éxito de cualquier organización. Algunos ejemplos de estas actividades son:

- El planeamiento estratégico
- La gestión del conocimiento
- La gestión de las relaciones con los clientes (CMR)
- El aseguramiento de la calidad
- La responsabilidad social empresarial
- El cuidado del medio ambiente
- Las prácticas del buen "Gobierno Corporativo"

En el caso de la gestión del riesgo operacional, algunos costos pertenecen a la categoría de "estar en el negocio", como por ejemplo los de la investigación necesaria para la identificación de los riesgos, el desarrollo de modelos y herramientas de cálculo, la implementación de sistemas informáticos, el seguimiento del sector y, en general, las labores que están a cargo de la Unidad Central de Riesgo Operacional y las que involucran a la alta dirección. Otros costos, asociados con labores regulares de control, que se llevan a cabo en las unidades de línea, deben ser considerados como costos de "hacer negocios".

Una característica de los costos de "estar en el negocio" es que no están relacionados, o no tienen una relación clara, con un determinado periodo o ejercicio económico; tampoco pueden relacionarse con el volumen de producción, con las ventas, con el número de clientes, con la participación de mercado, etcétera. Por esta razón es que el costo de estas actividades difícilmente se podría asociar con algún tipo específico de ingreso, o con algún "periodo de recuperación", por lo que en estos casos no es aplicable, el concepto de "rentabilidad", en el sentido en que es empleado al evaluar las actividades que involucran costos de "hacer negocios".

Todo lo anterior no significa que los costos de "estar en el negocio" no sean un asunto relevante en la gestión del riesgo operacional. De hecho, como parte de la gestión siempre habrán decisiones económicas que tomar, por ejemplo para decidir entre el desarrollo interno de aplicativos o comprar soluciones "a la medida", realizar tareas con personal propio o subcontratar, alquilar equipos o comprarlos, automatizar o no ciertos procesos, etcétera. Todas estas decisiones deben ser consistentes con la necesidad de trabajar con bajos costos, pero estas serán decisiones puntuales, tomadas dentro del marco de una decisión de carácter estratégico que busca asegurar el desarrollo sostenible de la organización.

7.2. DIFICULTADES PARA LA CUANTIFICACIÓN DE LOS BENEFICIOS

La primera dificultad que se presenta para cuantificar los beneficios de implantar un modelo de gestión del riesgo operacional, así como de las otras actividades que implican costos de "estar en el negocio" radica en que, aunque está plenamente aceptado que estas actividades contribuyen a la creación de valor para el cliente y de ventajas competitivas para la empresa, las mismas no generan, por si solas, beneficios económicos fácilmente cuantificables, sino que

estos provienen de los mejores resultados que se obtienen en las actividades generadoras de ingresos, es decir en aquellas que incurren en los costos de "hacer negocios".

Un segundo problema es que la implantación del modelo implicará diseñar y poner en marcha los procesos de identificación, mitigación y medición de los riesgos, cuyos resultados sólo se conocerán en la medida que el modelo se encuentre operativo y que se puedan observar los resultados de su aplicación. Por otra parte, como ya se ha visto en el acápite 3.1, la dinámica actual de cambios en el sector financiero, con seguridad hará que aparezcan nuevos productos y servicios, y con ellos nuevos factores y tipos de riesgo, no conocidos actualmente.

En tercer lugar, la gestión del riesgo operacional es un campo de reciente desarrollo, por lo que es de esperarse que sus costos se vayan reduciendo, y que los beneficios aumenten, en la medida que tanto los desarrollos teóricos y la tecnología, aporten herramientas para un trabajo más productivo y eficiente, ello sin mencionar lo ahorros que cada empresa pueda obtener, derivados los conocimientos y destrezas que se adquieran como producto de la experiencia.

Debido a las dificultades señaladas, se recomienda que la evaluación económica del modelo de gestión se centre, al menos inicialmente, en el control de las inversiones y gastos que se realicen a nivel corporativo y por línea de negocio, dejando para más adelante la consideración de cualquier otro tipo de beneficio. La cifra así obtenida puede utilizarse entonces para establecer objetivos de reducción de las exigencias de capital por riesgo operacional, frente al 15% de los ingresos brutos que considera el NACB para el método del indicador básico, aunque por el momento esta exigencia no esté considerada en la normativa de la SBS.

7.3. EJEMPLO DE EVALUACIÓN DE LA INVERSIÓN INICIAL Y GASTOS ANUALES

Con el fin de que sirva como referencia al momento de estimar la inversión inicial y los gastos anuales para la implementación del modelo de gestión, a continuación expondremos la relación de rubros a considerar en la formación de la Unidad Central de Riesgo Operacional, así como un estimado de las cifras en dólares americanos. Seguidamente realizaremos un cálculo simplificado para establecer la inversión inicial equivalente que representa implementar esta Unidad.

Para efectos de esta estimación asumiremos una variante del esquema organizativo descrito en el acápite 4.5, para la unidad mencionada, considerando que la misma estará conformada por un responsable, o gerente de unidad, y tres analistas de riesgo. Para el caso del personal de apoyo, asignado a las unidades de negocio, no se consideran puestos de trabajo adicionales, por cuanto se asume que esta labor será realizada a tiempo parcial por personal que ya tiene otras responsabilidades.

En el caso de la inversión en equipos y software, teniendo en cuenta que se trata de la etapa inicial, no se consideran el desarrollo ni la compra de sistemas específicos, sino sólo de herramientas estándares de trabajo, a precios referenciales de venta al público; sin embargo, se entiende que estos precios podrían tener una reducción sustancial, en la medida que la empresa negocie con sus proveedores, precios especiales por su condición de cliente corporativo.

En cuanto a los nuevos procesos y metodologías, según la experiencia del autor de este trabajo, esta es una tarea que puede ser realizada por el personal especializado con el que cuentan la mayoría de empresas del sector, utilizando la infraestructura y

recursos ya disponibles, por lo que no se considera un gasto adicional en este rubro.

CUADRO 3: Inversión Inicial y Gastos Anuales Estimados
(Cifras en dólares)

	Inversión Inicial	Gasto Anual
Gastos de personal		250,000
Gastos generales		50,000
Capacitación	25,000	
Computadoras	10,000	
Software básico	3,000	
Software especial	20,000	
Muebles y equipo de oficina	7,500	
	65,500	300,000

En el Cuadro 3 se muestra un detalle de la inversión necesaria para implementar la Unidad Central de Riesgo Operacional, según las siguientes premisas:

El rubro de gastos de personal comprende las remuneraciones, beneficios y cargas sociales.

Los gastos generales se estiman en un 20% de los gastos de personal. Aquí se incluyen conceptos como son energía y agua, útiles de escritorio, suministros, espacio de trabajo, seguridad, seguros, etcétera. También se incluyen los cargos que corresponderán al reemplazo o renovación de los bienes comprendidos en la inversión inicial.

- Se estima que será necesaria un inversión en capacitación, por una sola vez, equivalente al 10% de los gastos de personal anuales.
- En el caso de las computadoras, se consideran 5 estaciones de trabajo, un servidor y una impresora compartida, más los gastos de instalación.
- El software básico se refiere a los programas para trabajo de oficina, comprendidos en productos como el *MS Office* o el *Lotus Smart Suite*.
- El software especial se refiere a programas para desarrollo de modelos estadísticos, como por ejemplo E-views o SPSS.
- Los muebles y el equipo de oficina, comprenden todo lo necesario para implementar el ambiente de trabajo de la Unidad.

Para efectos de poder calcular la inversión inicial equivalente, asumiremos que los gastos de personal, gastos generales y la capacitación tienen un escudo fiscal del 30% por efecto del menor impuesto a la renta; utilizaremos una tasa de rendimiento de 7% anual después de impuestos y, para simplificar el cálculo, consideraremos despreciable el efecto de la depreciación y amortización. De esta forma, aplicando el concepto de renta perpetua a los gastos anuales, tenemos que la inversión inicial equivalente será:

$$(300{,}000 * 0.7 \ / 0.07) + (25{,}000*0.7) + 40{,}500 = \text{USD } 3'058{,}000$$

Esto significa que sólo la implementación de la Unidad Central de Riesgo Operacional, representa una inversión inicial equivalente del orden de los tres millones de dólares, de manera que para efectos de realizar la evaluación económica de esta inversión, será necesario considerar que esta sólo estará justificada si es que el

trabajo realizado genera ahorros anuales después de impuestos, bajo el mismo esquema de renta perpetua y considerando la misma tasa de rendimiento de 7% anual, por una suma no menor a:

3'058,000 * 0.07 = USD 214,060

Según hemos visto anteriormente, el principal incentivo que plantea el NACB para adoptar métodos de medición de riesgos más sofisticados, es de las menores exigencias de capital. Así tenemos que, según el método del indicador básico, el capital mínimo por riesgo operacional se determina en base al promedio de los ingresos brutos anuales de los últimos tres años, al que se aplica el factor de 0.15. Este método no requiere la adopción de ninguna medida ni método especial de cálculo, consecuentemente podemos decir que representa el capital exigido en ausencia de un modelo de gestión.

Para utilizar un ejemplo extraído de la realidad, utilizaremos los datos que corresponden a los estados financiaros auditados de un banco local, correspondientes a los años 2000, 2001 y 2002, según se muestra en el Cuadro 4

CUADRO 4: Ingresos brutos anuales de un banco local [24]
(Cifras en miles de nuevos soles)

	2000	2001	2002	Promedio
Ingresos financieros	941,569	906,302	775,764	874,545
Gastos financieros	441,773	399,169	247,795	362,912
Margen financiero	499,796	507,133	527,969	511,633
Comisiones netas	186,531	201,440	205,904	197,958
Ingreso bruto	686,327	708,573	733,873	709,591

[24] Fuente: Memoria Anual de los años 2000, 2001 y 2002

Si asumimos un tipo de cambio promedio de S/.3.40 por dólar, entonces tendremos que, según el método del indicador básico, el capital mínimo por riesgo operacional será:

(709,591,000 / 3.40) * 0.15 = USD 31,305,485

Si consideramos el mismo costo del capital de 7% anual después de impuestos, utilizado en los cálculos anteriores, entonces el costo anual de mantener los 31 millones de dólares como capital por riesgo operacional será de:

31,305,485 * 0.07 = USD 2,191,384

Esto significa que la implementación de un modelo de gestión, cuyo único costo sea el de constituir y mantener operativa a la Unidad Central de Riesgo Operacional, estará justificado en la medida que se consiga que la nueva exigencia de capital, vía la aplicación de los métodos Estándar o de Medición Avanzada, sea como máximo de:

(2,191,384 - 214,060) / 0.07 = USD 28,247,485

Lo cual implica una menor exigencia de capital de:

31,305,485 – 28,247,485 = USD 3,058,000

Esta última cifra es precisamente la inversión equivalente inicial que representa la implantación y operación de la Unidad Central de Riesgo Operacional.

CAPÍTULO 8: EL NUEVO ROL DE LA AUDITORIA INTERNA

8. EL NUEVO ROL DE LA AUDITORIA INTERNA

Tradicionalmente el rol de la auditoria interna ha estado directamente vinculado con la realización de los controles necesarios para asegurar el cumplimiento por parte del personal, de las normas y procedimientos establecidos por la empresa y por las entidades supervisoras. También se ha identificado a esta unidad con la tarea de prevención de errores, detección e investigación de fraudes, verificación de la contabilidad, y en general de todo tipo de tareas que buscan resguardar el patrimonio de la empresa, tangible o intangible, contra los riesgos que no están relacionados con las actividades normales del negocio.

El nuevo enfoque que se le está dando a la gestión del riesgo operacional conduce a replantear el rol que le corresponde la auditora interna. En efecto, en el esquema presentado se ha visto que la responsabilidad por la evaluación de los diferentes procesos, está pasando directamente a las unidades que los llevan a cabo, con el apoyo y las herramientas proporcionadas por la unidad central de riesgo operacional. Es por esto que la auditora interna debe enfocarse ahora en analizar si el modelo de gestión del riesgo funciona apropiadamente, y en la realización de pruebas para verificar la eficacia de los controles.

La auditoria interna debe también ocuparse de evaluar la marcha de los diferentes procesos del modelo de gestión, así como la forma como estos han sido diseñados e implementados en las diferentes áreas de la empresa. Debe verificar si se están asumiendo riesgos en concordancia

con las políticas establecidas, como en el caso del lanzamiento de nuevos productos, verificar que todos los riesgos debidamente identificados en los procesos de auto evaluación y también controlar que todos lo eventos de pérdida se están registrando en las respectivas bases de datos. También debe evaluar la consistencia de los modelos para la medición de los riesgos y para los cálculos de capital económico y para ello debe contar con personal debidamente calificado.

Desde un principio el CSBB ha considerado el papel de la auditoria interna en la gestión del riesgo operacional, al establecer la necesidad de que los procesos de gestión sean objeto de revisiones y validaciones periódicas por parte de auditores externos y/o internos. El tercer documento consultivo del NACB indica que "*Los auditores externos y/o internos deberán llevar a cabo exámenes periódicos de los procesos de gestión y de los sistemas de medición del riesgo operativo. Estos exámenes deberán incluir tanto las operaciones de las unidades de negocio como las actividades de la unidad independiente de gestión del riesgo operativo*" [25].

[25] Comité de Supervisión Bancaria de Basilea, *EL NUEVO ACUERDO DE CAPITAL DE BASILEA. DOCUMENTO DE CONSULTA 3*, Banco de Pagos Internacionales, Basilea, Suiza, abril del 2003, página 129, www.bis.org

CAPÍTULO 9: CONCLUSIONES Y RECOMENDACIONES

9. CONCLUSIONES Y RECOMENDACIONES

Un modelo de gestión del riesgo operacional puede abarcar muchos componentes e involucrar a casi todos los integrantes de la organización, y puede tener muchas variantes según las características particulares de cada empresa. Existen sin embargo algunos aspectos que todos los modelos deben considerar para que el esfuerzo de desarrollo e implementación brinde los mejores resultados, los cuales se señalan a continuación, como conclusiones del presente trabajo.

La primera conclusión es que el papel protagónico de la alta dirección, y su confianza en que este proceso si genera valor, será lo que haga la diferencia con el enfoque tradicional de prevención. La gerencia debe estar convencida de que la gestión del riesgo operacional mejora la calidad del servicio, disminuye la volatilidad del riesgo y optimiza el uso del capital. Y este convencimiento, manifestado en un compromiso real, es lo que ayudará a que todos pongan su mejor esfuerzo en la nueva forma de gestión.

Un segundo aspecto tiene que ver con la actitud del personal de las líneas de negocio y especialmente con la de los responsables de las mismas. El modelo debe ser adoptado por todos de manera que cada uno se comprometa a aportar valor en la gestión y no limitarse a recolectar datos y a esperar que sean otros los que trabajen para lograr resultados. Para ello es necesario que todos entiendan que serán ellos los primeros

beneficiados con el resultado de su trabajo, y una forma de lograr esto es relacionar los progresos alcanzados con las medidas de desempeño.

El tercer aspecto se refiere a la necesidad de asegurarse que haya consistencia en los procesos. Para ello es fundamental la comunicación. Se debe proporcionar definiciones que sean entendidas por todos y propiciar el uso de un lenguaje común entre las diferentes áreas de la empresa, aunque las técnicas y los enfoques empleados en cada una de ellas sean diferentes. Ello permitirá que todos vean la importancia de su aporte al momento que se consoliden los resultados.

En cuarto lugar, se debe cuidar que en todos los puestos estén las personas adecuadas, en términos de conocimientos, motivación e identificación con la cultura del riesgo de la organización. El personal a cargo de las funciones corporativas del riesgo operacional debe tener los conocimientos y las habilidades necesarias en los campos de técnicas cuantitativas, mejora de procesos, sistemas de información y en las principales facetas del negocio bancario, y se debe autorizar los presupuestos suficientes para los recursos humanos y la tecnología necesarios.

Como quinto punto se debe tener en cuenta que el modelo de gestión del riesgo operacional debe ser dinámico, de la misma manera que lo son los riesgos que se trata de gestionar. Esta realidad exige que se cuestionen permanentemente los procesos, y la manera cómo estos se enfocan, y que haya un trabajo continuo de investigación, para identificar los riesgos que no han sido previstos y para desarrollar controles y formas de medición cada vez más efectivos.

Una sexta conclusión es que los resultados, sean positivos o adversos, deben compartirse con todas las áreas de negocio. Las pérdidas no deben ser vistas como errores sino como oportunidades para mejorar. De la misma manera, debe realizarse permanentemente procesos de *benchmarking*, tanto internos como externos, y estimular el desarrollo y la

comunicación de las "buenas prácticas", buscando que estas sean aplicadas en toda la organización.

Finalmente debemos señalar que el campo de la gestión de los riesgos operacionales, constituye una interesante área de trabajo para los profesionales de ingeniería, y especialmente de los ingenieros industriales, por su formación cuantitativa y por su orientación al análisis y mejora de procesos. Es por ello que el autor considera recomendable que se incorpore al plan de estudios de la carrera, bien sea como cursos complementarios o electivos, temas relacionados con la inferencia estadística, modelos econométricos, técnicas de análisis multivariado, y otras herramientas de la estadística utilizadas en la investigación, incidiendo en sus aplicaciones prácticas mediante el uso de programas informáticos como EVIEWS y SPSS.

BIBLIOGRAFÍA CONSULTADA

- Alexander, Carol (Editora), *OPERATIONAL RISK; REGULATION, ANALYSIS AND MANAGEMENT*, Pearson Education Limited, Prentice Hall – Financial Times, Londres, 2003.
- Chorafas, Dimitris N., *OPERATIONAL RISK CONTROL WITH BASEL II; BASIC PRINCIPLES AND CAPITAL REQUIREMENTS*, Elsiever Butterworth-Heineman, Rochester, Reino Unido, 2004
- Cruz, Marcelo G., *MODELING, MEASURING AND HEDGING OPERATIONAL RISK*, John Wiley & Sons Ltd., West Sussex, Reino Unido, 2002.
- Comité de Supervisión Bancaria de Basilea, *EL NUEVO ACUERDO DE CAPITAL DE BASILEA. DOCUMENTO DE CONSULTA 3*, Banco de Pagos Internacionales, Basilea, Suiza, abril del 2003, www.bis.org.
- Comité de Supervisión Bancaria de Basilea, *SOUND PRACTICES FOR THE MANAGEMENT AND SUPERVISION OF THE OPERATIONAL RISK*, Banco de Pagos Internacionales, Basilea, Suiza, febrero del 2003, www.bis.org.
- Comité de Supervisión Bancaria de Basilea, Risk Management Group, *THE QUANTITATIVE IMPACT STUDY FOR OPERATIONAL RISK, OVERVIEW OF INDIVIDUAL LOSS DATA AND LESSONS LEARNED*, Basilea, Suiza, enero del 2002, www.bis.org
- De Lara Haro, Alfonso, *MEDICIÓN Y CONTROL DE RIESGOS FINANCIEROS*, 2da. Edición, Editorial Limusa, México, 2002.

- Druker. Peter F., *LA SOCIEDAD POST CAPITALISTA*, Editorial Norma, Bogotá, 1994.
- Gómez Cáceres, Diego y López Zaballos, Jesús Miguel, *RIESGOS FINANCIEROS Y OPERACIONES INTERNACIONALES*, Editorial ESIC, Madrid, 2002.
- Gonzáles Mosquera, Luis, "Capital Regulatorio y Capital Económico: prociclicidad del nuevo Acuerdo de Capital y Análisis de Escenarios de Crisis", en: *ESTABILIDAD FINANCIERA, No. 2*, Banco de España, marzo del 2002, www.bde.es
- Hitt Michael, R. Duane Ireland y Robert E. Hoskinson, *ADMINISTRACIÓN ESTRATÉGICA, CONCEPTOS DE, COMPETITIVIDAD Y GLOBALIZACIÓN*, 3ra. Edición, International Thomsom Editores, México, 1999.
- Marrison, Chris, *THE FUNDAMENTALS OF RISK MEASUREMENT*, MacGraw-Hill, Nueva York, 2002.
- Porter, Michael E., *ESTRATEGIA COMPETITIVA, TECNICAS PARA EL ANÁLIS DE LOS SECTORES INDUSTRIALES Y DE LA COMPETENCIA*, Compañía Editorial Continental - CECSA, México, 1987.
- Robbins, Stephen P., *COMPORTAMIENTO ORGANIZACIONAL*, 8va. edición, Prentice Hall Hispanoamericana, México, 1999.
- Sebastián González, Altina y López Pascual, Joaquín, *GESTIÓN BANCARIA, LOS NUEVOS RETOS EN UN ENTORNO GLOBAL*, 2da. Edición, Mcgraw-Hill / Interamericana de España, Madrid, 2001.

ANEXO A

Resolución No. 006-2002. Superintendencia de Banca y Seguros del Perú*

* Documento disponible en el sitio web: www.sbs.gob.pe

Superintendencia de Banca y Seguros

Lima, 4 de enero de 2002

Resolución S.B.S.
No 006 -2002

El Superintendente de Banca y Seguros

CONSIDERANDO:

Que, es objetivo de esta Superintendencia propender a que las empresas supervisadas cuenten con un sistema de control de riesgos que les permita identificar, medir, controlar y reportar los riesgos que enfrentan con la finalidad de proteger los intereses del público de acuerdo a lo señalado en el artículo 347º de la Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros, Ley Nº 26702, y sus modificatorias, en adelante Ley General;

Que, entre los riesgos que enfrentan las empresas supervisadas en el desarrollo de sus actividades se encuentran los riesgos de operación, los cuales pueden generarse por deficiencias o fallas en los procesos internos, en la tecnología de la información, en las personas o por ocurrencia de eventos externos;

Que, resulta necesario establecer criterios mínimos prudenciales para que las empresas supervisadas realicen de manera adecuada la gestión de dichos riesgos;

Estando a lo opinado por las Superintendencias Adjuntas de Banca, Seguros y Asesoría Jurídica; y,

En uso de las atribuciones conferidas por los numerales 7 y 9 del artículo 349º de la Ley General y por la Resolución SBS N° 1028-2001 del 27 de diciembre de 2001;

RESUELVE:

Artículo Primero.- Aprobar el Reglamento para la Administración de los Riesgos de Operación, que forma parte integrante de la presente Resolución.

Artículo Segundo. - La presente Resolución entra en vigencia al día siguiente de su publicación en el Diario Oficial ¨ El Peruano".

Regístrese, comuníquese y publíquese,

SOCORRO HEYSEN ZEGARRA
Superintendente de Banca y Seguros (e)

Los Laureles Nº 214 - Lima 27 - Perú Telf. : (511)2218990 Fax: (511) 4417760

REGLAMENTO PARA LA ADMINISTRACION DE LOS RIESGOS DE OPERACION

CAPITULO I
DISPOSICIONES GENERALES

Alcance

Artículo 1º.- Las disposiciones de la presente norma son aplicables a las empresas señaladas en los artículos 16° y 17° de la Ley General, al Banco Agropecuario, a la Corporación Financiera de Desarrollo S.A. (COFIDE), al Banco de la Nación, a la Fundación Fondo de Garantía para Préstamos a la Pequeña Industria (FOGAPI) y a las derramas y cajas de beneficios que se encuentren bajo la supervisión de esta Superintendencia, en adelante empresas.

Definiciones

Artículo 2º.- Para los efectos de la presente norma deben considerarse los siguientes términos:

a. Administración de riesgos: Proceso que consiste en identificar, medir, controlar y reportar los riesgos que la empresa enfrenta.
b. Directorio: Toda referencia al directorio, entiéndase realizada también a cualquier órgano equivalente.
c. Información: Cualquier forma de registro electrónico, óptico, magnético o en otros medios, susceptible de ser procesada, distribuida y almacenada.
d. Proceso: Conjunto de actividades, tareas y procedimientos organizados y repetibles.
e. Proceso crítico: Proceso considerado indispensable para la continuidad de las operaciones y servicios de la empresa, y cuya falta o ejecución deficiente puede tener un impacto financiero significativo para la empresa.
f. Reglamento del Sistema de Control Interno: Reglamento del Sistema de Control Interno aprobado mediante la Resolución SBS Nº 1040-99 del 26 de noviembre de 1999.
g. Servicios críticos provistos por terceros: Servicios relacionados a procesos críticos provistos por terceros y cuya falta o ejecución deficiente puede tener un impacto financiero significativo para la empresa.
h. Superintendencia: Superintendencia de Banca y Seguros.
i. Tecnología de información: Incluye los sistemas informáticos y la tecnología asociada a dichos sistemas.

Riesgos de operación

Artículo 3º.- Las empresas deben administrar adecuadamente los riesgos de operación que enfrentan. Entiéndase por riesgos de operación a la posibilidad de ocurrencia de pérdidas financieras por deficiencias o fallas en los procesos internos, en la tecnología de información, en las personas o por ocurrencia de eventos externos adversos.

Responsabilidad del Directorio y la Gerencia

Artículo 4º.- El Directorio es responsable del establecimiento de políticas y procedimientos generales para identificar, medir, controlar y reportar apropiadamente los riesgos de operación. Asimismo, será también su responsabilidad el velar por el cumplimiento de las referidas políticas y procedimientos y de las disposiciones contenidas en el presente Reglamento. Corresponderá a la Gerencia General la implementación de las políticas y procedimientos generales establecidos por el Directorio.

Unidad de riesgos

Artículo 5º.- De conformidad con lo dispuesto en el Reglamento del Sistema de Control Interno, la Unidad de Riesgos será la encargada de la administración de los riesgos de operación que enfrenta la empresa, pudiendo comprender a alguna unidad especializada para la evaluación de dicho riesgo.

Asimismo, para dicho fin, la unidad de riesgos o, de ser el caso, la unidad especializada, deberá contar con la infraestructura adecuada, así como con los recursos humanos, técnicos y logísticos que le permitan el apropiado cumplimiento de sus funciones, de acuerdo a la dimensión y estructura de la empresa, la naturaleza de sus operaciones y servicios y la complejidad de los mismos.

Entre las funciones de la referida unidad responsable se incluirán por lo menos las siguientes:

a. Preparación y evaluación de políticas para la administración de los riesgos de operación.
b. Desarrollo de metodologías para la evaluación cuantitativa y/o cualitativa de los riesgos de operación.
c. Evaluación de los riesgos de operación, de forma previa al lanzamiento de nuevos productos y ante cambios importantes en el ambiente operativo o informático.
d. Consolidación y desarrollo de reportes e informes sobre la administración de los riesgos de operación por proceso, o unidades de negocio y apoyo.
e. Identificación de las necesidades de capacitación y difusión para una adecuada administración de los riesgos de operación.
f. Otras necesarias para el desarrollo de su función.

Manual de organización y funciones

Artículo 6º.- De conformidad con las disposiciones contenidas en la presente norma y en el Reglamento del Sistema de Control Interno, la empresa deberá disponer de una estructura organizacional y administrativa que le permita una adecuada administración de los riesgos de operación. Dicha estructura deberá establecerse de manera que exista independencia entre la unidad de riesgos y aquellas otras unidades de negocio, así como una clara delimitación de funciones, responsabilidades y perfil de puestos en todos sus niveles. Estos aspectos deberán encontrarse recogidos en el manual de organización y funciones de la empresa.

Manuales de políticas y procedimientos

Artículo 7º.- Las políticas y procedimientos establecidos para la administración de los riesgos de operación deberán estar claramente definidos en los manuales de políticas y procedimientos; asimismo, deberán ser consistentes con el tamaño y naturaleza de la empresa y con la complejidad de sus operaciones y servicios.

Manual de control de riesgos

Artículo 8º.- El manual de control de riesgos deberá contener una sección especial sobre los riesgos de operación. Dicha sección deberá contemplar por lo menos los siguientes aspectos:

a. Políticas para la administración de los riesgos de operación.
b. Funciones y responsabilidades de las unidades de negocio y de apoyo en la administración de los riesgos de operación.
c. Descripción de la metodología aplicada para la medición y evaluación de los riesgos de operación.
d. La forma y periodicidad con la que se deberá informar al Directorio y a la Gerencia General, entre otros, sobre la exposición a los riesgos de operación de la empresa y de cada unidad de negocio.

e. El proceso para la aprobación de propuestas de nuevas operaciones, productos y servicios que deberá contar, entre otros aspectos, con una descripción general de la nueva operación, producto o servicio de que se trate, los riesgos identificados y las acciones a tomar para su control.

CAPITULO II
ADMINISTRACION DE LOS ASPECTOS QUE ORIGINAN LOS RIESGOS DE OPERACION

Procesos internos

Artículo 9º.- Las empresas deberán administrar apropiadamente los riesgos asociados a los procesos internos implementados para la realización de sus operaciones y servicios, de tal forma que se minimice la posibilidad de pérdidas financieras relacionadas al diseño inapropiado de los procesos críticos, o a políticas y procedimientos inadecuados o inexistentes que puedan tener como consecuencia el desarrollo deficiente de las operaciones y servicios o la suspensión de los mismos.

En tal sentido, podrán considerarse entre otros, los riesgos asociados a las fallas en los modelos utilizados, los errores en las transacciones, la evaluación inadecuada de contratos o de la complejidad de productos, operaciones y servicios, los errores en la información contable, la inadecuada compensación, liquidación o pago, la insuficiencia de recursos para el volumen de operaciones, la inadecuada documentación de transacciones, así como el incumplimiento de plazos y costos planeados.

Tecnología de información

Artículo 10º.- Las empresas deberán administrar apropiadamente los riesgos asociados a la tecnología de información, de tal modo que se minimice la posibilidad de pérdidas financieras derivadas del uso de inadecuados sistemas informáticos y tecnologías relacionadas a ellos, que pueden afectar el desarrollo de las operaciones y servicios que realiza la empresa al atentar contra la confidencialidad, integridad y disponibilidad de la información.

Para este fin, las empresas podrán considerar los riesgos vinculados a las fallas en la seguridad y continuidad operativa de los sistemas informáticos, los errores en el desarrollo e implementación de dichos sistemas y la compatibilidad e integración de los mismos, problemas de calidad de información, la inadecuada inversión en tecnología, así como las fallas en la adecuación a los objetivos del negocio, entre otros aspectos.

Personas

Artículo 11º.- Las empresas deben administrar apropiadamente los riesgos asociados a las personas de la empresa, de tal modo que se minimice la posibilidad de pérdidas financieras asociadas a inadecuada capacitación del personal, negligencia, error humano, sabotaje, fraude, robo, paralizaciones, apropiación de información sensible, lavado de dinero y similares.

Eventos externos

Artículo 12º.- Las empresas deberán considerar en la administración de los riesgos de operación la posibilidad de pérdidas derivada de la ocurrencia de eventos ajenos al control de la empresa que pudiesen alterar el desarrollo de sus actividades, afectando los aspectos que dan origen a los riesgos de operación referidos en los artículos 9º, 10º y 11º del presente Reglamento. En tal sentido, entre otros factores, se podrán tomar en consideración los riesgos que implican las contingencias legales, las fallas en los servicios públicos, la ocurrencia de desastres naturales, atentados y actos delictivos, así como las fallas en servicios críticos provistos por terceros.

CAPITULO III
REQUERIMIENTOS DE INFORMACION

Informe anual a la Superintendencia

Artículo 13º.- Las empresas deberán presentar a la Superintendencia, dentro de los noventa (90) días calendario siguientes al cierre de cada ejercicio anual, un informe referido a la evaluación de los riesgos de operación que enfrenta la empresa por proceso o unidad de negocio y apoyo. Dicho informe deberá contemplar por lo menos los siguientes aspectos:

a. Metodología empleada para la administración de los riesgos de operación.
b. Identificación de los riesgos de operación por proceso o unidad de negocio y apoyo.
c. Evaluación de los riesgos de operación identificados.
d. Medidas adoptadas para administrar los riesgos de operación materiales identificados y plazos para su aplicación. Dichas medidas podrán ser, entre otras:
   - Evitar el riesgo
   - Reducir su probabilidad de ocurrencia
   - Reducir las consecuencias
   - Transferir el riesgo
   - Retener el riesgo
e. Funcionarios responsables de las actividades de control de riesgo identificadas.
f. Plan de actividades de la Unidad de Riesgos en lo referente a la administración de los riesgos de operación.

Información adicional

Artículo 14º.- La Superintendencia podrá requerir a la empresa cualquier otra información que considere necesaria para una adecuada supervisión de los riesgos de operación de la empresa.

Asimismo, la empresa deberá tener a disposición de esta Superintendencia todos los documentos a que hace mención el presente Reglamento, así como la información de auditoría o revisiones realizadas por la casa matriz en caso de las empresas cuya matriz no se encuentre en el país.

CAPITULO IV
COLABORADORES EXTERNOS

Auditoría Interna

Artículo 15º.- La Unidad de Auditoría Interna deberá evaluar el cumplimiento de los procedimientos utilizados para la administración de los riesgos de operación, así como de lo dispuesto en el presente Reglamento. Asimismo, la Unidad de Auditoría Interna deberá incluir la referida evaluación en las actividades permanentes del Plan Anual y deberá realizar los informes y recomendaciones que se deriven de la misma.

Auditoría Externa

Artículo 16º.- Las sociedades de auditoria externa deberán incluir en su informe sobre el sistema de control interno comentarios dirigidos a indicar si la entidad cuenta con políticas y procedimientos para la administración de los riesgos de operación, considerando el cumplimiento de lo dispuesto en el presente Reglamento.

Empresas Clasificadoras de Riesgo

Artículo 17º.- Las empresas clasificadoras de riesgo deberán tener en cuenta las políticas y procedimientos establecidos por la empresa para la administración de los riesgos de operación en el proceso de clasificación de las empresas supervisadas.

DISPOSICIONES FINALES Y TRANSITORIAS

Servicios provistos por terceros
Primera.- Las empresas son responsables de asegurar el cumplimiento de la normatividad emitida por la Superintendencia, aun en aquellos casos en que ciertas funciones sean realizadas por terceros. En este sentido, además del cumplimiento de lo dispuesto en la presente Resolución, las empresas deberán asegurarse de que los contratos suscritos con proveedores de servicios críticos a la empresa, incluyan cláusulas que faciliten una adecuada revisión de la respectiva prestación, por parte de las empresas, la Unidad de Auditoría Interna, la Sociedad de Auditoría Externa, así como por parte de la Superintendencia o la persona que ésta designe.

Medidas adicionales
Segunda.- La Superintendencia podrá disponer la adopción de medidas adicionales a las previstas en el presente Reglamento con el propósito de atenuar la exposición a los riesgos de operación que enfrentan las empresas.

Sanciones
Tercera.- En caso de incumplimiento de las disposiciones contenidas en el presente Reglamento la Superintendencia aplicará las sanciones correspondientes de conformidad con lo establecido en el Reglamento de Sanciones.

Plazo y Plan de Adecuación
Cuarta.- Las empresas contarán con un plazo de adecuación a las disposiciones de la presente norma que vencerá el 30 de junio de 2003. A dicha fecha las empresas deberán tener a disposición de este organismo de control los Manuales de Políticas y Procedimientos, el Manual de Organización y Funciones, el Manual de Control de Riesgos y los contratos de servicios críticos provistos por terceros a que se refiere la primera disposición final y transitoria del presente reglamento, adecuados a las disposiciones comprendidas en el mismo.

Para el ejercicio 2002 las empresas no se encuentran obligadas a presentar el informe anual a que se refiere el artículo 13º del presente reglamento. Sin embargo, en un plazo que no excederá del 30 de junio de 2002 deberán remitir a este organismo de control un plan de adecuación a las disposiciones contenidas en la presente norma. Dicho plan deberá incluir un diagnóstico preliminar de la situación existente en la empresa, las acciones previstas para la total adecuación y el cronograma de las mismas, así como los funcionarios responsables del cumplimiento de dicho plan.

Reglamento de Auditoría Interna
Quinta.- Toda referencia realizada al término riesgo informático en el Reglamento de Auditoría Interna, aprobado mediante la Resolución SBS Nº 1041-99, deberá ser entendida como referida a los riesgos de operación, de acuerdo con lo dispuesto en la presente norma.

ANEXO B

Asignación de las líneas de negocio*

* Comité de Supervisión Bancaria de Basilea: *El Nuevo Acuerdo de Capital de Basilea, Documento de Consulta*, Banco de pagos Internacionales, abril del 2003, anexo 6, página 204. Documento disponible en el sitio web: www.bis.org

Anexo 6

Asignación de las líneas de negocio

Nivel 1	Nivel 2	Grupos de Actividades
Finanzas corporativas	Finanzas corporativas	Fusiones y adquisiciones, suscripción de emisiones, privatizaciones, titulización, investigación, deuda (pública, alto rendimiento), acciones, sindicaciones, Ofertas Públicas Iniciales, colocaciones privadas en mercado secundario
	Finanzas de administraciones locales / públicas	
	Banca de inversión	
	Servicios de asesoramiento	
Negociación y ventas	Ventas	Renta fija, renta variable, divisas, productos básicos, crédito, financiación, posiciones propias en valores, préstamo y operaciones con pacto de recompra, intermediación, deuda, intermediación unificada *(prime brokerage)*
	Creación de Mercado	
	Posiciones Propias	
	Tesorería	
Banca minorista	Banca minorista	Préstamos y depósitos de clientes minoristas, servicios bancarios, fideicomisos y testamentarías
	Banca privada	Préstamos y depósitos a clientes privados, servicios bancarios, fideicomisos y testamentarías, asesoramiento de inversiones
	Servicios de tarjetas	Tarjetas de empresa / comerciales, de marca privada y minoristas
Banca comercial	Banca comercial	Financiación de proyectos, bienes raíces, financiación de exportaciones, financiación comercial, *factoring*, arrendamiento financiero, préstamos, garantías, letras de cambio
Liquidación y pagos[154]	Clientes externos	Pagos y recaudaciones, transferencia de fondos, compensación y liquidación
Servicios de agencia	Custodia	Cajas de seguridad, certificados de valores, préstamo de valores (Clientes), operaciones de sociedades
	Agencia de empresas	Agentes de emisiones y pagos
	Fideicomisos de empresas	
Administración de activos	Administración discrecional de fondos	Agrupados, segregados, minoristas, institucionales, cerrado, abierto, participaciones accionariales
	Administración no discrecional de fondos	Agrupados, segregados, minoristas, institucionales, de capital fijo, de capital variable
Intermediación minorista	Intermediación minorista	Ejecución y servicio completo

[154] Las pérdidas derivadas de las operaciones de liquidación y pagos relacionadas con las actividades propias del banco se incorporarán al historial de pérdidas de la línea de negocios afectada.

Principios para la asignación de las líneas de negocio[155]

(a) Todas las actividades deberán asignarse a las ocho líneas de negocio de nivel 1 de forma que a cada una de las actividades le corresponda una sola línea de negocio y no permanezca ninguna actividad sin asignar;

(b) Cualquier actividad bancaria o no bancaria que no pueda asignarse con facilidad al marco de las líneas de negocio, pero que represente una función auxiliar a una actividad incluida en dicho marco, deberá ser asignada a la línea de negocio a la que presta apoyo. Si la actividad auxiliar presta apoyo a más de una línea de negocio, deberá utilizarse un criterio de asignación objetivo;

(c) A la hora de asignar los ingresos brutos, si una actividad no puede ser asignada a una determinada línea de negocio, entonces deberá utilizarse la línea de negocio que genere el requerimiento de capital más elevado. Cualquier actividad auxiliar asociada deberá también asignarse a la misma línea de negocio;

(d) Los bancos podrán utilizar métodos internos de fijación de precios para asignar los ingresos brutos a las distintas líneas de negocio, siempre que los ingresos brutos totales del banco (conforme se registrarían utilizando el Método del Indicador Básico) continúen siendo iguales a la suma de los ingresos brutos para las ocho líneas de negocio;

(e) La asignación de actividades a líneas de negocio a los efectos de capital por riesgo operativo deberá ser coherente con las definiciones de líneas de negocio utilizadas en los cálculos de capital regulador en otras categorías de riesgo (es decir, riesgo de crédito y de mercado). Cualquier desviación de este principio deberá motivarse y documentarse con claridad;

(f) El proceso de asignación utilizado deberá documentarse con claridad. En particular, las definiciones por escrito de las líneas de negocio deberán ser suficientemente claras y detalladas para que la asignación de líneas de negocio realizada pueda ser reproducida por terceros. Entre otras cosas, la documentación deberá argumentar con claridad cualquier excepción o salvedad existente y deberá conservarse en registros;

---

[155] **Orientaciones complementarias para la asignación de las líneas de negocio**

Existe una diversidad de métodos válidos que los bancos podrán utilizar para asignar sus actividades a las ocho líneas de negocio, siempre que el enfoque utilizado satisfaga los principios para la asignación de las líneas de negocio. No obstante, el Comité reconoce que algunos bancos agradecerían orientaciones adicionales. En consecuencia, a continuación se presenta un ejemplo de un posible método a utilizar por un banco en la asignación de sus ingresos brutos.

Los ingresos brutos de la banca minorista están formados por los ingresos netos por intereses de préstamos y anticipos a clientes minoristas y a las PYME con tratamiento minorista, más las comisiones relacionadas con actividades minoristas tradicionales, los ingresos netos de *swaps* y derivados mantenidos para dar cobertura a la cartera de inversión minorista y los ingresos procedentes de los derechos de cobro adquiridos frente a minoristas. Al objeto de calcular los ingresos netos por intereses de la banca minorista, el banco detrae de los intereses percibidos en sus préstamos y anticipos a clientes minoristas el coste medio ponderado de la financiación de los préstamos (procedente de cualquier fuente: depósitos minoristas u otros).

De manera similar, los ingresos brutos de la banca comercial se componen de los ingresos netos por intereses de préstamos y anticipos a empresas (más a las PYME con tratamiento de empresas), interbancarios y soberanos, así como los ingresos procedentes de los derechos de cobro adquiridos frente a empresas, más las comisiones relacionadas con las actividades tradicionales de banca comercial, incluidos compromisos, garantías, letras de cambio, ingresos netos (por ejemplo, de cupones y dividendos) de valores mantenidos en la cartera de inversión y beneficios / pérdidas de *swaps* y derivados mantenidos para dar cobertura a la cartera de inversión comercial. De nuevo, el cálculo de los ingresos netos por intereses se basa en los intereses percibidos de los préstamos y anticipos a empresas, interbancarios y soberanos, menos el coste medio ponderado de la financiación de esos préstamos (procedente de cualquier fuente).

En el caso de la línea de negociación y ventas, los ingresos brutos consisten en los beneficios / pérdidas procedentes de los instrumentos mantenidos por motivos de negociación (es decir, en la cartera valorada a precios de mercado), netos de los costes de financiación, más las comisiones de la intermediación mayorista.

Por lo que respecta a las otras cinco líneas de negocio, los ingresos brutos consisten básicamente en las comisiones / cuotas netas obtenidas en cada uno de esos negocios. En el caso de la línea de liquidación y pagos, estos ingresos brutos se componen de las comisiones percibidas por la prestación de servicios de liquidación / pago a contrapartes mayoristas. En el caso de la administración de activos, se trata de la gestión de patrimonios por cuenta de terceros.

Los ingresos brutos no deben excluir los gastos de explotación.

ANEXO C

Clasificación detallada de tipos de eventos de pérdida*

* Comité de Supervisión Bancaria de Basilea: *El Nuevo Acuerdo de Capital de Basilea, Documento de Consulta*, Banco de pagos Internacionales, abril del 2003, anexo 7, página 207. Documento disponible en el sitio web: www.bis.org

Anexo 7

Clasificación detallada de tipos de eventos de pérdida

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 a 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 maliciosa de activos Falsificación Utilización de cheques sin fondos Contrabando Apropiación de cuentas / Fingimiento de personalidad / etc. Incumplimiento / evasión de impuestos (intencional) Sobornos / Cohechos 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 a soslayar la legislación, por parte un tercero	Hurto y fraude	Hurto/ Robo Falsificación Circulación de cheques sin fondos
		Seguridad de los sistemas	Daños por ataques informáticos Robo de información (con pérdidas pecuniarias)

Categorías de tipos de eventos (Nivel 1)	Definición	Categorías (Nivel 2)	Ejemplos de actividades (Nivel 3)
Relaciones laborales y seguridad en el puesto de trabajo	Pérdidas derivadas de actuaciones incompatibles con la legislación o acuerdos laborales, de higiene o seguridad en el empleo, del pago de reclamaciones por daños a las personas, o de eventos de diversidad / discriminación	Relaciones laborales	Cuestiones relativas a remuneración, beneficios sociales, extinción de contratos. Organización de la actividad laboral
		Salud y seguridad en el puesto de trabajo	Responsabilidad común (resbalones, etc.) Eventos relacionados con las normas de higiene y seguridad en el trabajo Indemnizaciones a los trabajadores
		Diversidad y discriminación	Todo tipo de discriminación
Prácticas con clientes, productos y negocios	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.) Quebrantamientos de la revelación de información sobre clientes minoristas Violación de privacidad Ventas agresivas Confusión de cuentas Abuso de información confidencial Responsabilidad del prestamista

Categorías de tipos de eventos (Nivel 1)	Definición	Categorías (Nivel 2)	Ejemplos de actividades (Nivel 3)
		Prácticas inadecuadas de negocio o de mercado	Prácticas ajenas a la competencia Prácticas inadecuadas de negociación / mercado Manipulación del mercado Abuso de información privilegiada (en favor de la empresa) Actividades no autorizadas Blanqueo de dinero
		Defectos del producto	Defectos del producto (no autorizado, etc.) Errores de los modelos
		Selección, patrocinio y exposición	Ausencia de investigación a clientes conforme a directrices Superación de los límites de exposición 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 los suministros

Categorías de tipos de eventos (Nivel 1)	Definición	Categorías (Nivel 2)	Ejemplos de actividades (Nivel 3)
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 carga Incumplimiento de plazos o de responsabilidades Funcionamiento erróneo de modelos / sistemas Error contable / atribución a entidades erróneas Errores en otras tareas Fallo en la entrega Fallo en la gestión colateral Mantenimiento de datos de referencia
		Seguimiento y comunicación de informes	Incumplimiento de la obligación de informar Inexactitud de informes externos (con generación de pérdidas)
		Admisión 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 por negligencia de activos de clientes
		Contrapartes comerciales	Prácticas inadecuadas de contrapartes distintas de clientes Otros litigios con contrapartes distintas de clientes
		Distribuidores y proveedores	Externalización Litigios con distribuidores

ANEXO D

Total de pérdidas por línea de negocio reportadas en el estudio de impacto cuantitativo realizado por el CSBB*

* Comité de Supervisión Bancaria de Basilea: *The Quantitative Impact Study for Operational Risk: Overview of Individual Loss Data and Lessons Lerned,* Banco de pagos Internacionales, junio del 2002, página 8. Documento disponible en el sitio web: www.bis.org

Table 4

Total Gross Loss Amounts by Business Line and Event Type
Thousands of Euros
30 Banks Reporting Data

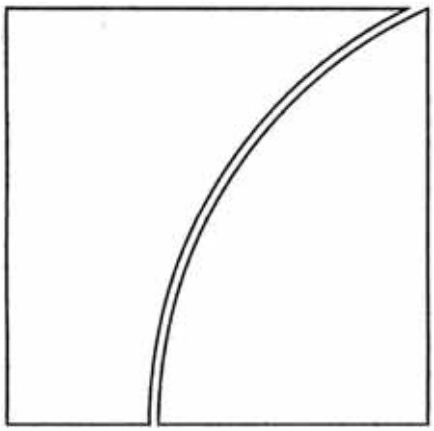
	Internal Fraud	External Fraud	Employment Practices and Workplace Safety	Clients, Products and Business Services	Damage to Physical Assets	Business Disruption and System Failures	Execution, Delivery, and Process Management	Total Across Event Types For Each Business Line
Corporate Finance	3,293	25,231	6,114	131,012	18		28,432	194,100
	0.13%	0.97%	0.23%	5.01%	0.00%		1.09%	7.43%
Trading and Sales	68,819	826	7,845	89,054	138	6,237	326,563	499,481
	2.63%	0.03%	0.30%	3.41%	0.01%	0.24%	12.50%	19.11%
Retail Banking	115,578	210,026	54,600	387,447	61,176	2,110	198,820	1,029,757
	4.42%	8.04%	2.09%	14.83%	2.34%	0.08%	7.61%	39.41%
Commercial Banking	78,869	287,855	3,662	76,217	14,033	1,424	136,659	598,717
	3.02%	11.02%	0.14%	2.92%	0.54%	0.05%	5.23%	22.91%
Payment and	750	5,447	719	1,144	2,061	2,705	112,468	125,295
Settlement	0.03%	0.21%	0.03%	0.04%	0.08%	0.10%	4.30%	4.79%
Agency and Custody	2,265	281	374	7,635	860	1,718	43,310	56,443
Services	0.09%	0.01%	0.01%	0.29%	0.03%	0.07%	1.66%	2.16%
Asset Management	8,566	603	1,075	8,978		664	34,841	54,728
	0.33%	0.02%	0.04%	0.34%		0.03%	1.33%	2.09%
Retail Brokerage	445	596	1,845	17,485	575	6,471	27,127	54,545
	0.02%	0.02%	0.07%	0.67%	0.02%	0.25%	1.04%	2.09%
Total Across	278,586	530,866	76,235	71,8971	78,860	21,329	908,219	2,613,066
Business Lines	10.66%	20.32%	2.92%	27.51%	3.02%	0.82%	34.76%	100.00%

ANEXO E

"Sound Practices for the Management and Supervision of Operational Risk" [•]

[•] Comité de Supervisión Bancaria de Basilea: *Sound Practices for the Management and Supervision of Operational Risk,* Banco de pagos Internacionales, febrero del 2003. Documento disponible en el sitio web: www.bis.org

Basel Committee
on Banking Supervision



Sound Practices for the Management and Supervision of Operational Risk

February 2003

BANK FOR INTERNATIONAL SETTLEMENTS

Risk Management Group of the Basel Committee on Banking Supervision

Chairman:
Mr Roger Cole – Federal Reserve Board, Washington, DC

Banque Nationale de Belgique, Brussels	Ms Dominique Gressens
Commission Bancaire et Financière, Brussels	Mr Jos Meuleman
Office of the Superintendent of Financial Institutions, Ottawa	Mr Jeff Miller
Commission Bancaire, Paris	Mr Laurent Le Mouël
Deutsche Bundesbank, Frankfurt am Main	Ms Magdalene Heid Ms Karin Sagner-Kaiser
Bundesanstalt für Finanzdienstleistungsaufsicht, Bonn	Ms Kirsten Straus
Banca d'Italia, Rome	Mr Claudio Dauria Mr Fabrizio Leandri Mr Sergio Sorrentino
Bank of Japan, Tokyo	Mr Satoshi Yamaguchi
Financial Services Agency, Tokyo	Mr Hirokazu Matsushima
Commission de Surveillance du Secteur Financier, Luxembourg	Mr Davy Reinard
De Nederlandsche Bank, Amsterdam	Mr Klaas Knot
Banco de España, Madrid	Mr Guillermo Rodriguez-Garcia Mr Juan Serrano
Finansinspektionen, Stockholm	Mr Jan Hedquist
Sveriges Riksbank, Stockholm	Mr Thomas Flodén
Eidgenössische Bankenkommission, Bern	Mr Martin Sprenger
Financial Services Authority, London	Mr Helmut Bauer Mr Victor Dowd
Federal Deposit Insurance Corporation, Washington, D.C.	Mr Mark Schmidt
Federal Reserve Bank of New York	Ms Beverly Hirtle Mr Stefan Walter
Federal Reserve Board, Washington, D.C.	Mr Kirk Odegard
Office of the Comptroller of the Currency, Washington, D.C.	Mr Kevin Bailey Ms Tanya Smith
European Central Bank, Frankfurt am Main	Mr Panagiotis Strouzas
European Commission, Brussels	Mr Michel Martino Ms Melania Savino
Secretariat of the Basel Committee on Banking Supervision, Bank for International Settlements	Mr Stephen Senior

Table of Contents

Sound Practices for the Management and Supervision of Operational Risk

Introduction

1. The following paper outlines a set of principles that provide a framework for the effective management and supervision of operational risk, for use by banks and supervisory authorities when evaluating operational risk management policies and practices.

2. The Basel Committee on Banking Supervision (the Committee) recognises that the exact approach for operational risk management chosen by an individual bank will depend on a range of factors, including its size and sophistication and the nature and complexity of its activities. However, despite these differences, clear strategies and oversight by the board of directors and senior management, a strong operational risk culture[1] and internal control culture (including, among other things, clear lines of responsibility and segregation of duties), effective internal reporting, and contingency planning are all crucial elements of an effective operational risk management framework for banks of any size and scope. The Committee therefore believes that the principles outlined in this paper establish sound practices relevant to all banks. The Committee's previous paper *A Framework for Internal Control Systems in Banking Organisations* (September 1998) underpins its current work in the field of operational risk.

Background

3. Deregulation and globalisation of financial services, together with the growing sophistication of financial technology, are making the activities of banks and thus their risk profiles (i.e. the level of risk across a firm's activities and/or risk categories) more complex. Developing banking practices suggest that risks other than credit, interest rate and market risk can be substantial. Examples of these new and growing risks faced by banks include:

- If not properly controlled, the greater use of more highly automated technology has the potential to transform risks from manual processing errors to system failure risks, as greater reliance is placed on globally integrated systems;
- Growth of e-commerce brings with it potential risks (e.g., internal and external fraud and system security issues) that are not yet fully understood;
- Large-scale acquisitions, mergers, de-mergers and consolidations test the viability of new or newly integrated systems;
- The emergence of banks acting as large-volume service providers creates the need for continual maintenance of high-grade internal controls and back-up systems;
- Banks may engage in risk mitigation techniques (e.g., collateral, credit derivatives, netting arrangements and asset securitisations) to optimise their exposure to market risk and credit risk, but which in turn may produce other forms of risk (e.g. legal risk); and

---

[1] *Internal operational risk culture* is taken to mean the combined set of individual and corporate values, attitudes, competencies and behaviour that determine a firm's commitment to and style of operational risk management.

- Growing use of outsourcing arrangements and the participation in clearing and settlement systems can mitigate some risks but can also present significant other risks to banks.

4. The diverse set of risks listed above can be grouped under the heading of 'operational risk', which the Committee has defined as 'the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events'.[2] The definition includes legal risk but excludes strategic and reputational risk.

5. The Committee recognises that operational risk is a term that has a variety of meanings within the banking industry, and therefore for internal purposes (including in the application of the Sound Practices paper), banks may choose to adopt their own definitions of operational risk. Whatever the exact definition, a clear understanding by banks of what is meant by operational risk is critical to the effective management and control of this risk category. It is also important that the definition considers the full range of material operational risks facing the bank and captures the most significant causes of severe operational losses. Operational risk event types that the Committee - in co-operation with the industry - has identified as having the potential to result in substantial losses include:

- Internal fraud. For example, intentional misreporting of positions, employee theft, and insider trading on an employee's own account.
- External fraud. For example, robbery, forgery, cheque kiting, and damage from computer hacking.
- Employment practices and workplace safety. For example, workers compensation claims, violation of employee health and safety rules, organised labour activities, discrimination claims, and general liability.
- Clients, products and business practices. For example, fiduciary breaches, misuse of confidential customer information, improper trading activities on the bank's account, money laundering, and sale of unauthorised products.
- Damage to physical assets. For example, terrorism, vandalism, earthquakes, fires and floods.
- Business disruption and system failures. For example, hardware and software failures, telecommunication problems, and utility outages.
- Execution, delivery and process management. For example, data entry errors, collateral management failures, incomplete legal documentation, unapproved access given to client accounts, non-client counterparty misperformance, and vendor disputes.

Industry Trends and Practices

6. In its work on the supervision of operational risks, the Committee has aimed to develop a greater understanding of current industry trends and practices for managing

---

[2] This definition was adopted from the industry as part of the Committee's work in developing a minimum regulatory capital charge for operational risk. While this paper is not a formal part of the capital framework, the Committee nevertheless expects that the basic elements of a sound operational risk management framework set out in this paper will inform supervisory expectations when reviewing bank capital adequacy, for example within the supervisory review process.

operational risk. These efforts have involved numerous meetings with banking organisations, surveys of industry practice, and analyses of the results. Based on these efforts, the Committee believes that it has a good understanding of the banking industry's current range of practices, as well as the industry's efforts to develop methods for managing operational risks.

7. The Committee recognises that management of specific operational risks is not a new practice; it has always been important for banks to try to prevent fraud, maintain the integrity of internal controls, reduce errors in transaction processing, and so on. However, what is relatively new is the view of operational risk management as a comprehensive practice comparable to the management of credit and market risk in principle, if not always in form. The trends cited in the introduction to this paper, combined with a growing number of high-profile operational loss events worldwide, have led banks and supervisors to increasingly view operational risk management as an inclusive discipline, as has already been the case in many other industries.

8. In the past, banks relied almost exclusively upon internal control mechanisms within business lines, supplemented by the audit function, to manage operational risk. While these remain important, recently there has been an emergence of specific structures and processes aimed at managing operational risk. In this regard, an increasing number of organisations have concluded that an operational risk management programme provides for bank safety and soundness, and are therefore making progress in addressing operational risk as a distinct class of risk similar to their treatment of credit and market risk. The Committee believes that an active exchange of ideas between the supervisors and industry is key to ongoing development of appropriate guidance for managing exposures related to operational risk.

9. This paper is organised along the following lines: developing an appropriate risk management environment; risk management: identification, assessment, monitoring and control/mitigation; the role of supervisors; and the role of disclosure.

Sound Practices

10. In developing these sound practices, the Committee has drawn upon its existing work on the management of other significant banking risks, such as credit risk, interest rate risk and liquidity risk, and the Committee believes that similar rigour should be applied to the management of operational risk. Nevertheless, it is clear that operational risk differs from other banking risks in that it is typically not directly taken in return for an expected reward, but exists in the natural course of corporate activity, and that this affects the risk management process.[3] At the same time, failure to properly manage operational risk can result in a misstatement of an institution's risk profile and expose the institution to significant losses. Reflecting the different nature of operational risk, for the purposes of this paper, 'management' of operational risk is taken to mean the 'identification, assessment, monitoring and control/mitigation' of risk. This definition contrasts with the one used by the Committee in previous risk management papers of the 'identification, measurement, monitoring and

[3] However, the Committee recognises that in some business lines with minimal credit or market risk (e.g., asset management, and payment and settlement), the decision to incur operational risk, or compete based on the ability to manage and effectively price this risk, is an integral part of a bank's risk/reward calculus.

control' of risk. In common with its work on other banking risks, the Committee has structured this sound practice paper around a number of principles. These are:

Developing an Appropriate Risk Management Environment

Principle 1: The board of directors[4] should be aware of the major aspects of the bank's operational risks as a distinct risk category that should be managed, and it should approve and periodically review the bank's operational risk management framework. The framework should provide a firm-wide definition of operational risk and lay down the principles of how operational risk is to be identified, assessed, monitored, and controlled/mitigated.

Principle 2: The board of directors should ensure that the bank's operational risk management framework is subject to effective and comprehensive internal audit by operationally independent, appropriately trained and competent staff. The internal audit function should not be directly responsible for operational risk management.

Principle 3: Senior management should have responsibility for implementing the operational risk management framework approved by the board of directors. The framework should be consistently implemented throughout the whole banking organisation, and all levels of staff should understand their responsibilities with respect to operational risk management. Senior management should also have responsibility for developing policies, processes and procedures for managing operational risk in all of the bank's material products, activities, processes and systems.

Risk Management: Identification, Assessment, Monitoring, and Mitigation/Control

Principle 4: Banks should identify and assess the operational risk inherent in all material products, activities, processes and systems. Banks should also ensure that before new products, activities, processes and systems are introduced or undertaken, the operational risk inherent in them is subject to adequate assessment procedures.

Principle 5: Banks should implement a process to regularly monitor operational risk profiles and material exposures to losses. There should be regular reporting of pertinent information to senior management and the board of directors that supports the proactive management of operational risk.

Principle 6: Banks should have policies, processes and procedures to control and/or mitigate material operational risks. Banks should periodically review their risk limitation and control strategies and should adjust their operational risk profile accordingly using appropriate strategies, in light of their overall risk appetite and profile.

---

[4] This paper refers to a management structure composed of a board of directors and senior management. The Committee is aware that there are significant differences in legislative and regulatory frameworks across countries as regards the functions of the board of directors and senior management. In some countries, the board has the main, if not exclusive, function of supervising the executive body (senior management, general management) so as to ensure that the latter fulfils its tasks. For this reason, in some cases, it is known as a supervisory board. This means that the board has no executive functions. In other countries, the board has a broader competence in that it lays down the general framework for the management of the bank. Owing to these differences, the terms 'board of directors' and 'senior management' are used in this paper not to identify legal constructs but rather to label two decision-making functions within a bank.

Principle 7: Banks should have in place contingency and business continuity plans to ensure their ability to operate on an ongoing basis and limit losses in the event of severe business disruption.

Role of Supervisors

Principle 8: Banking supervisors should require that all banks, regardless of size, have an effective framework in place to identify, assess, monitor and control/mitigate material operational risks as part of an overall approach to risk management.

Principle 9: Supervisors should conduct, directly or indirectly, regular independent evaluation of a bank's policies, procedures and practices related to operational risks. Supervisors should ensure that there are appropriate mechanisms in place which allow them to remain apprised of developments at banks.

Role of Disclosure

Principle 10: Banks should make sufficient public disclosure to allow market participants to assess their approach to operational risk management.

Developing an Appropriate Risk Management Environment

11. Failure to understand and manage operational risk, which is present in virtually all bank transactions and activities, may greatly increase the likelihood that some risks will go unrecognised and uncontrolled. Both the board and senior management are responsible for creating an organisational culture that places high priority on effective operational risk management and adherence to sound operating controls. Operational risk management is most effective where a bank's culture emphasises high standards of ethical behaviour at all levels of the bank. The board and senior management should promote an organisational culture which establishes through both actions and words the expectations of integrity for all employees in conducting the business of the bank.

Principle 1: The board of directors should be aware of the major aspects of the bank's operational risks as a distinct risk category that should be managed, and it should approve and periodically review the bank's operational risk management framework. The framework should provide a firm-wide definition of operational risk and lay down the principles of how operational risk is to be identified, assessed, monitored, and controlled/mitigated.

12. The board of directors should approve the implementation of a firm-wide framework to explicitly manage operational risk as a distinct risk to the bank's safety and soundness. The board should provide senior management with clear guidance and direction regarding the principles underlying the framework and approve the corresponding policies developed by senior management.

13. An operational risk framework should be based on an appropriate definition of operational risk which clearly articulates what constitutes operational risk in that bank. The framework should cover the bank's appetite and tolerance for operational risk, as specified through the policies for managing this risk and the bank's prioritisation of operational risk management activities, including the extent of, and manner in which, operational risk is transferred outside the bank. It should also include policies outlining the bank's approach to identifying, assessing, monitoring and controlling/mitigating the risk. The degree of formality and sophistication of the bank's operational risk management framework should be commensurate with the bank's risk profile.

14. The board is responsible for establishing a management structure capable of implementing the firm's operational risk management framework. Since a significant aspect of managing operational risk relates to the establishment of strong internal controls, it is particularly important that the board establishes clear lines of management responsibility, accountability and reporting. In addition, there should be separation of responsibilities and reporting lines between operational risk control functions, business lines and support functions in order to avoid conflicts of interest. The framework should also articulate the key processes the firm needs to have in place to manage operational risk.

15. The board should review the framework regularly to ensure that the bank is managing the operational risks arising from external market changes and other environmental factors, as well as those operational risks associated with new products, activities or systems. This review process should also aim to assess industry best practice in operational risk management appropriate for the bank's activities, systems and processes. If necessary, the board should ensure that the operational risk management framework is revised in light of this analysis, so that material operational risks are captured within the framework.

Principle 2: The board of directors should ensure that the bank's operational risk management framework is subject to effective and comprehensive internal audit by

operationally independent, appropriately trained and competent staff. The internal audit function should not be directly responsible for operational risk management.

16. Banks should have in place adequate internal audit coverage to verify that operating policies and procedures have been implemented effectively.[5] The board (either directly or indirectly through its audit committee) should ensure that the scope and frequency of the audit programme is appropriate to the risk exposures. Audit should periodically validate that the firm's operational risk management framework is being implemented effectively across the firm.

17. To the extent that the audit function is involved in oversight of the operational risk management framework, the board should ensure that the independence of the audit function is maintained. This independence may be compromised if the audit function is directly involved in the operational risk management process. The audit function may provide valuable input to those responsible for operational risk management, but should not itself have direct operational risk management responsibilities. In practice, the Committee recognises that the audit function at some banks (particularly smaller banks) may have initial responsibility for developing an operational risk management programme. Where this is the case, banks should see that responsibility for day-to-day operational risk management is transferred elsewhere in a timely manner.

Principle 3: Senior management should have responsibility for implementing the operational risk management framework approved by the board of directors. The framework should be consistently implemented throughout the whole banking organisation, and all levels of staff should understand their responsibilities with respect to operational risk management. Senior management should also have responsibility for developing policies, processes and procedures for managing operational risk in all of the bank's material products, activities, processes and systems.

18. Management should translate the operational risk management framework established by the board of directors into specific policies, processes and procedures that can be implemented and verified within the different business units. While each level of management is responsible for the appropriateness and effectiveness of policies, processes, procedures and controls within its purview, senior management should clearly assign authority, responsibility and reporting relationships to encourage and maintain this accountability, and ensure that the necessary resources are available to manage operational risk effectively. Moreover, senior management should assess the appropriateness of the management oversight process in light of the risks inherent in a business unit's policy.

19. Senior management should ensure that bank activities are conducted by qualified staff with the necessary experience, technical capabilities and access to resources, and that staff responsible for monitoring and enforcing compliance with the institution's risk policy have authority independent from the units they oversee. Management should ensure that the bank's operational risk management policy has been clearly communicated to staff at all levels in units that incur material operational risks.

20. Senior management should ensure that staff responsible for managing operational risk communicate effectively with staff responsible for managing credit, market, and other

---

[5] The Committee's paper, *Internal Audit in Banks and the Supervisor's Relationship with Auditors* (August 2001) describes the role of internal and external audit.

risks, as well as with those in the firm who are responsible for the procurement of external services such as insurance purchasing and outsourcing agreements. Failure to do so could result in significant gaps or overlaps in a bank's overall risk management programme.

21. Senior management should also ensure that the bank's remuneration policies are consistent with its appetite for risk. Remuneration policies which reward staff that deviate from policies (e.g. by exceeding established limits) weaken the bank's risk management processes.

22. Particular attention should be given to the quality of documentation controls and to transaction-handling practices. Policies, processes and procedures related to advanced technologies supporting high transactions volumes, in particular, should be well documented and disseminated to all relevant personnel.

Risk Management: Identification, Assessment, Monitoring and Mitigation/Control

Principle 4: Banks should identify and assess the operational risk inherent in all material products, activities, processes and systems. Banks should also ensure that before new products, activities, processes and systems are introduced or undertaken, the operational risk inherent in them is subject to adequate assessment procedures.

23. Risk identification is paramount for the subsequent development of a viable operational risk monitoring and control system. Effective risk identification considers both internal factors (such as the bank's structure, the nature of the bank's activities, the quality of the bank's human resources, organisational changes and employee turnover) and external factors (such as changes in the industry and technological advances) that could adversely affect the achievement of the bank's objectives.

24. In addition to identifying the most potentially adverse risks, banks should assess their vulnerability to these risks. Effective risk assessment allows the bank to better understand its risk profile and most effectively target risk management resources.

25. Amongst the possible tools used by banks for identifying and assessing operational risk are:

- Self- or Risk Assessment: a bank assesses its operations and activities against a menu of potential operational risk vulnerabilities. This process is internally driven and often incorporates checklists and/or workshops to identify the strengths and weaknesses of the operational risk environment. Scorecards, for example, provide a means of translating qualitative assessments into quantitative metrics that give a relative ranking of different types of operational risk exposures. Some scores may relate to risks unique to a specific business line while others may rank risks that cut across business lines. Scores may address inherent risks, as well as the controls to mitigate them. In addition, scorecards may be used by banks to allocate economic capital to business lines in relation to performance in managing and controlling various aspects of operational risk.
- Risk Mapping: in this process, various business units, organisational functions or process flows are mapped by risk type. This exercise can reveal areas of weakness and help prioritise subsequent management action.
- Risk Indicators: risk indicators are statistics and/or metrics, often financial, which can provide insight into a bank's risk position. These indicators tend to be reviewed on a periodic basis (such as monthly or quarterly) to alert banks to changes that may be indicative of risk concerns. Such indicators may include the number of failed

trades, staff turnover rates and the frequency and/or severity of errors and omissions.

Measurement: some firms have begun to quantify their exposure to operational risk using a variety of approaches. For example, data on a bank's historical loss experience could provide meaningful information for assessing the bank's exposure to operational risk and developing a policy to mitigate/control the risk. An effective way of making good use of this information is to establish a framework for systematically tracking and recording the frequency, severity and other relevant information on individual loss events. Some firms have also combined internal loss data with external loss data, scenario analyses, and risk assessment factors.

Principle 5: Banks should implement a process to regularly monitor operational risk profiles and material exposures to losses. There should be regular reporting of pertinent information to senior management and the board of directors that supports the proactive management of operational risk.

26. An effective monitoring process is essential for adequately managing operational risk. Regular monitoring activities can offer the advantage of quickly detecting and correcting deficiencies in the policies, processes and procedures for managing operational risk. Promptly detecting and addressing these deficiencies can substantially reduce the potential frequency and/or severity of a loss event.

27. In addition to monitoring operational loss events, banks should identify appropriate indicators that provide early warning of an increased risk of future losses. Such indicators (often referred to as key risk indicators or early warning indicators) should be forward-looking and could reflect potential sources of operational risk such as rapid growth, the introduction of new products, employee turnover, transaction breaks, system downtime, and so on. When thresholds are directly linked to these indicators an effective monitoring process can help identify key material risks in a transparent manner and enable the bank to act upon these risks appropriately.

28. The frequency of monitoring should reflect the risks involved and the frequency and nature of changes in the operating environment. Monitoring should be an integrated part of a bank's activities. The results of these monitoring activities should be included in regular management and board reports, as should compliance reviews performed by the internal audit and/or risk management functions. Reports generated by (and/or for) supervisory authorities may also inform this monitoring and should likewise be reported internally to senior management and the board, where appropriate.

29. Senior management should receive regular reports from appropriate areas such as business units, group functions, the operational risk management office and internal audit. The operational risk reports should contain internal financial, operational, and compliance data, as well as external market information about events and conditions that are relevant to decision making. Reports should be distributed to appropriate levels of management and to areas of the bank on which areas of concern may have an impact. Reports should fully reflect any identified problem areas and should motivate timely corrective action on outstanding issues. To ensure the usefulness and reliability of these risk and audit reports, management should regularly verify the timeliness, accuracy, and relevance of reporting systems and internal controls in general. Management may also use reports prepared by external sources (auditors, supervisors) to assess the usefulness and reliability of internal reports. Reports should be analysed with a view to improving existing risk management performance as well as developing new risk management policies, procedures and practices.

30. In general, the board of directors should receive sufficient higher-level information to enable them to understand the bank's overall operational risk profile and focus on the material and strategic implications for the business.

Principle 6: Banks should have policies, processes and procedures to control and/or mitigate material operational risks. Banks should periodically review their risk limitation and control strategies and should adjust their operational risk profile accordingly using appropriate strategies, in light of their overall risk appetite and profile.

31. Control activities are designed to address the operational risks that a bank has identified.[6] For all material operational risks that have been identified, the bank should decide whether to use appropriate procedures to control and/or mitigate the risks, or bear the risks. For those risks that cannot be controlled, the bank should decide whether to accept these risks, reduce the level of business activity involved, or withdraw from this activity completely. Control processes and procedures should be established and banks should have a system in place for ensuring compliance with a documented set of internal policies concerning the risk management system. Principle elements of this could include, for example:

- Top-level reviews of the bank's progress towards the stated objectives;
- Checking for compliance with management controls;
- Policies, processes and procedures concerning the review, treatment and resolution of non-compliance issues; and
- A system of documented approvals and authorisations to ensure accountability to an appropriate level of management.

32. Although a framework of formal, written policies and procedures is critical, it needs to be reinforced through a strong control culture that promotes sound risk management practices. Both the board of directors and senior management are responsible for establishing a strong internal control culture in which control activities are an integral part of the regular activities of a bank. Controls that are an integral part of the regular activities enable quick responses to changing conditions and avoid unnecessary costs.

33. An effective internal control system also requires that there be appropriate segregation of duties and that personnel are not assigned responsibilities which may create a conflict of interest. Assigning such conflicting duties to individuals, or a team, may enable them to conceal losses, errors or inappropriate actions. Therefore, areas of potential conflicts of interest should be identified, minimised, and subject to careful independent monitoring and review.

34. In addition to segregation of duties, banks should ensure that other internal practices are in place as appropriate to control operational risk. Examples of these include:

- Close monitoring of adherence to assigned risk limits or thresholds;
- Maintaining safeguards for access to, and use of, bank assets and records;
- Ensuring that staff have appropriate expertise and training;

[6] For more detail, see the *Framework for Internal Control Systems in Banking Organisations*, Basel Committee on Banking Supervision, September 1998.

- Identifying business lines or products where returns appear to be out of line with reasonable expectations (e.g., where a supposedly low risk, low margin trading activity generates high returns that could call into question whether such returns have been achieved as a result of an internal control breach); and
- Regular verification and reconciliation of transactions and accounts.

Failure to implement such practices has resulted in significant operational losses for some banks in recent years.

35. Operational risk can be more pronounced where banks engage in new activities or develop new products (particularly where these activities or products are not consistent with the bank's core business strategies), enter unfamiliar markets, and/or engage in businesses that are geographically distant from the head office. Moreover, in many such instances, firms do not ensure that the risk management control infrastructure keeps pace with the growth in the business activity. A number of the most sizeable and highest-profile losses in recent years have taken place where one or more of these conditions existed. Therefore, it is incumbent upon banks to ensure that special attention is paid to internal control activities where such conditions exist.

36. Some significant operational risks have low probabilities but potentially very large financial impact. Moreover, not all risk events can be controlled (e.g., natural disasters). Risk mitigation tools or programmes can be used to reduce the exposure to, or frequency and/or severity of, such events. For example, insurance policies, particularly those with prompt and certain pay-out features, can be used to externalise the risk of "low frequency, high severity" losses which may occur as a result of events such as third-party claims resulting from errors and omissions, physical loss of securities, employee or third-party fraud, and natural disasters.

37. However, banks should view risk mitigation tools as complementary to, rather than a replacement for, thorough internal operational risk control. Having mechanisms in place to quickly recognise and rectify legitimate operational risk errors can greatly reduce exposures. Careful consideration also needs to be given to the extent to which risk mitigation tools such as insurance truly reduce risk, or transfer the risk to another business sector or area, or even create a new risk (e.g. legal or counterparty risk).

38. Investments in appropriate processing technology and information technology security are also important for risk mitigation. However, banks should be aware that increased automation could transform high-frequency, low-severity losses into low-frequency, high-severity losses. The latter may be associated with loss or extended disruption of services caused by internal factors or by factors beyond the bank's immediate control (e.g., external events). Such problems may cause serious difficulties for banks and could jeopardise an institution's ability to conduct key business activities. As discussed below in Principle 7, banks should establish disaster recovery and business continuity plans that address this risk.

39. Banks should also establish policies for managing the risks associated with outsourcing activities. Outsourcing of activities can reduce the institution's risk profile by transferring activities to others with greater expertise and scale to manage the risks associated with specialised business activities. However, a bank's use of third parties does not diminish the responsibility of the board of directors and management to ensure that the third-party activity is conducted in a safe and sound manner and in compliance with applicable laws. Outsourcing arrangements should be based on robust contracts and/or service level agreements that ensure a clear allocation of responsibilities between external

service providers and the outsourcing bank. Furthermore, banks need to manage residual risks associated with outsourcing arrangements, including disruption of services.

40. Depending on the scale and nature of the activity, banks should understand the potential impact on their operations and their customers of any potential deficiencies in services provided by vendors and other third-party or intra-group service providers, including both operational breakdowns and the potential business failure or default of the external parties. The board and management should ensure that the expectations and obligations of each party are clearly defined, understood and enforceable. The extent of the external party's liability and financial ability to compensate the bank for errors, negligence, and other operational failures should be explicitly considered as part of the risk assessment. Banks should carry out an initial due diligence test and monitor the activities of third party providers, especially those lacking experience of the banking industry's regulated environment, and review this process (including re-evaluations of due diligence) on a regular basis. For critical activities, the bank may need to consider contingency plans, including the availability of alternative external parties and the costs and resources required to switch external parties, potentially on very short notice.

41. In some instances, banks may decide to either retain a certain level of operational risk or self-insure against that risk. Where this is the case and the risk is material, the decision to retain or self-insure the risk should be transparent within the organisation and should be consistent with the bank's overall business strategy and appetite for risk.

Principle 7: Banks should have in place contingency and business continuity plans to ensure their ability to operate on an ongoing basis and limit losses in the event of severe business disruption.

42. For reasons that may be beyond a bank's control, a severe event may result in the inability of the bank to fulfil some or all of its business obligations, particularly where the bank's physical, telecommunication, or information technology infrastructures have been damaged or made inaccessible. This can, in turn, result in significant financial losses to the bank, as well as broader disruptions to the financial system through channels such as the payments system. This potential requires that banks establish disaster recovery and business continuity plans that take into account different types of plausible scenarios to which the bank may be vulnerable, commensurate with the size and complexity of the bank's operations.

43. Banks should identify critical business processes, including those where there is dependence on external vendors or other third parties, for which rapid resumption of service would be most essential. For these processes, banks should identify alternative mechanisms for resuming service in the event of an outage. Particular attention should be paid to the ability to restore electronic or physical records that are necessary for business resumption. Where such records are backed-up at an off-site facility, or where a bank's operations must be relocated to a new site, care should be taken that these sites are at an adequate distance from the impacted operations to minimise the risk that both primary and back-up records and facilities will be unavailable simultaneously.

44. Banks should periodically review their disaster recovery and business continuity plans so that they are consistent with the bank's current operations and business strategies. Moreover, these plans should be tested periodically to ensure that the bank would be able to execute the plans in the unlikely event of a severe business disruption.

Role of Supervisors

Principle 8: Banking supervisors should require that all banks, regardless of size, have an effective framework in place to identify, assess, monitor and control/mitigate material operational risks as part of an overall approach to risk management.

45. Supervisors should require banks to develop operational risk management frameworks consistent with the guidance in this paper and commensurate with their size, complexity, and risk profiles. To the extent that operational risks pose a threat to banks' safety and soundness, supervisors have a responsibility to encourage banks to develop and use better techniques in managing those risks.

Principle 9: Supervisors should conduct, directly or indirectly, regular independent evaluation of a bank's policies, procedures and practices related to operational risks. Supervisors should ensure that there are appropriate mechanisms in place which allow them to remain apprised of developments at banks.

46. Examples of what an independent evaluation of operational risk by supervisors should review include the following:

- The effectiveness of the bank's risk management process and overall control environment with respect to operational risk;
- The bank's methods for monitoring and reporting its operational risk profile, including data on operational losses and other indicators of potential operational risk;
- The bank's procedures for the timely and effective resolution of operational risk events and vulnerabilities;
- The bank's process of internal controls, reviews and audit to ensure the integrity of the overall operational risk management process;
- The effectiveness of the bank's operational risk mitigation efforts, such as the use of insurance;
- The quality and comprehensiveness of the bank's disaster recovery and business continuity plans; and
- The bank's process for assessing overall capital adequacy for operational risk in relation to its risk profile and, if appropriate, its internal capital targets.

47. Supervisors should also seek to ensure that, where banks are part of a financial group, there are procedures in place to ensure that operational risk is managed in an appropriate and integrated manner across the group. In performing this assessment, co-operation and exchange of information with other supervisors, in accordance with established procedures, may be necessary. Some supervisors may choose to use external auditors in these assessment processes.

48. Deficiencies identified during the supervisory review may be addressed through a range of actions. Supervisors should use the tools most suited to the particular circumstances of the bank and its operating environment. In order that supervisors receive current information on operational risk, they may wish to establish reporting mechanisms, directly with banks and external auditors (for example, internal bank management reports on operational risk could be made routinely available to supervisors).

49. Given the general recognition that comprehensive operational risk management processes are still in development at many banks, supervisors should take an active role in

encouraging ongoing internal development efforts by monitoring and evaluating a bank's recent improvements and plans for prospective developments. These efforts can then be compared with those of other banks to provide the bank with useful feedback on the status of its own work. Further, to the extent that there are identified reasons why certain development efforts have proven ineffective, such information could be provided in general terms to assist in the planning process. In addition, supervisors should focus on the extent to which a bank has integrated the operational risk management process throughout its organisation to ensure effective business line management of operational risk, to provide clear lines of communication and responsibility, and to encourage active self assessment of existing practices and consideration of possible risk mitigation enhancements.

Role of Disclosure

Principle 10: Banks should make sufficient public disclosure to allow market participants to assess their approach to operational risk management.

50. The Committee believes that the timely and frequent public disclosure of relevant information by banks can lead to enhanced market discipline and, therefore, more effective risk management. The amount of disclosure should be commensurate with the size, risk profile and complexity of a bank's operations.

51. The area of operational risk disclosure is not yet well established, primarily because banks are still in the process of developing operational risk assessment techniques. However, the Committee believes that a bank should disclose its operational risk management framework in a manner that will allow investors and counterparties to determine whether a bank effectively identifies, assesses, monitors and controls/mitigates operational risk.