UNIVERSIDAD DE LOS ANDES
FACULTAD DE ADMINISTRACIÓN
MAESTRIA EN ADMINISTRACIÓN

MODELO DE IMPLEMENTACIÓN DE UN SISTEMA DE ADMINISTRACIÓN DE RIESGO OPERACIONAL PARA UNA LINEA DE NEGOCIO DE UN BANCO

Liliana Montenegro Maya

Director: Rafael Bautista

Santafé de Bogotá, Noviembre de 2005

TABLA DE CONTENIDO

INDICE DE TABLAS

INDICE DE ANEXOS

INTRODUCCIÓN

En los últimos años, la administración de riesgo operacional ha ganado gran importancia en el sector financiero. Aunque el riesgo operacional es inherente al negocio bancario tan sólo hasta ahora se reconoce que la importancia de este riesgo es similar a la que tienen el riesgo de crédito y el riesgo de mercado. Es así como, en un entorno financiero de gran competencia es muy probable que las entidades que logren una administración eficiente del riesgo operacional generen grandes ventajas competitivas, especialmente relacionadas con mejoras en eficiencia y disminución de pérdidas.

La mayor atención dedicada a este tema fue generada en parte por el acelerado proceso de modernización que adelanta el sector financiero, que involucra entre otros aspectos un mayor desarrollo de productos, un alto grado de automatización de operaciones, permanentes procesos de fusión o absorción de entidades y mayores posibilidades de operar en forma global. Estos aspectos exigen a las entidades financieras adecuar rápidamente todas sus actividades a los nuevos requerimientos, acción que de no hacerse adecuadamente puede generar importantes pérdidas a la entidad por causa de fallas en procesos, personas, tecnología o eventos externos, las cuales se denominan pérdidas generadas por riesgos operacionales.

Por otra parte, y teniendo en cuenta las pérdidas generadas en varias entidades financieras por causa del riesgo operacional, desde hace más de cinco años, el Comité de Basilea, organismo que emite los principales lineamientos de regulación bancaria, incluyó en los documentos preliminares del nuevo acuerdo de capitales el riesgo operacional. Es así como en el nuevo acuerdo de capitales, expedido oficialmente en junio de 2004, el Comité de Basilea incorporó el riesgo operacional otorgándole una importancia similar que la que tienen el riesgo de crédito y de mercado. El nuevo acuerdo exige que el capital mínimo exigido a las entidades financieras este afectado por un valor de riesgo operacional, buscando que las entidades cuantifiquen su exposición al riesgo por este concepto y cuenten con un capital adecuado de acuerdo con el riesgo operacional que estén asumiendo. Para tal fin presenta una serie de lineamientos a tener en cuenta para la administración de riesgo operacional, especialmente relacionados con los modelos a utilizar para el cálculo del nuevo requerimiento. Los países desarrollados deberán cumplir con las exigencias del nuevo acuerdo a más tardar en el 2007, mientras los demás países implementarán gradualmente el acuerdo según las fechas que el ente regulador de cada país determine.

Las entidades financieras que logren implementar en el corto plazo, sistemas efectivos de administración de riesgo operacional desarrollarán una ventaja competitiva, ya que esto les permitirá mejorar la eficiencia y disminuir los requerimientos de capital por concepto de riesgo operacional.

En Colombia, la Superintendencia Bancaria aún no se ha pronunciado al respecto, ya que actualmente concentra sus esfuerzos en la implementación de los sistemas de administración de riesgo de crédito (SARC) y riesgo de mercado (SEARM), y por lo tanto dejó a iniciativa de cada entidad financiera los temas relacionados con riesgo operacional. No obstante, varias entidades financieras ya están incursionando en la administración de riesgo operacional en parte motivadas por el mejoramiento de eficiencia y también buscando estar preparadas para un futuro requerimiento por parte del ente regulador.

Ante el reto que tienen las entidades financieras colombianas de desarrollar sistemas de riesgo operacional por iniciativa propia, este trabajo tiene como principal objetivo brindar una herramienta que permita a dichas entidades entender el manejo del riesgo operacional como un sistema integral y ofrecer una metodología a aplicar para la implementación de dicho sistema. Aunque no se busca dar un recetario de pasos a seguir, ya que cada entidad de acuerdo con sus necesidades determinará que aspectos le interesan o no, la metodología si busca dar unos lineamientos generales que faciliten la implementación del sistema. Además de sugerir una metodología a aplicar, se realizó una prueba piloto del diseño requerido para la implementación del sistema de administración de riesgo operacional en una línea de negocio de un banco, para lo cual se contó con la colaboración de algunos funcionarios relacionados con la línea de negocio objeto del estudio.

El trabajo esta dividido en cinco capítulos. En el primer capítulo se presenta un marco teórico general del riesgo operacional haciendo especial énfasis en los lineamientos del Comité de Basilea. En el segundo capítulo se hace una breve reseña de la administración de riesgos en Colombia. En capitulo tercero se presentan tres metodologías relacionadas con implementación de un sistema de administración de riesgo operacional sugeridas por diferentes autores. En el cuarto capitulo se presenta la metodología sugerida por este trabajo que en gran parte toma elementos de las metodologías presentadas en el capitulo tres. Por último en el capitulo cinco se presenta el diseño de un sistema de administración de riesgo para una línea específica del negocio bancario.

JUSTIFICACIÓN DEL PROYECTO

La necesidad de contar con una guía metodológica detallada que sirva como herramienta para el diseño de un sistema de administración de riesgo operacional de una entidad financiera se fundamenta en tres aspectos relevantes.

En primera instancia, la gran importancia que el tema de riesgo operacional viene ganando a nivel mundial, especialmente generada por las nuevas exigencias regulatorias expedidas por el Comité de Basilea. Como resultado de estas exigencias, varias entidades financieras, especialmente las originarias de países desarrollados han realizado importantes avances en el tema. No obstante, a nivel Latinoamericano aún son mínimas las acciones realizadas. En el caso específico de Colombia, la Superintendencia Bancaria aún no se ha pronunciado frente al tema, pero varias entidades financieras, por iniciativa propia, ya están adelantando esfuerzos en temas de riesgo operacional, buscando prepararse con anticipación para el futuro requerimiento por parte del ente regulador. Para estas entidades podría ser de gran ayuda contar con una guía metodológica frente al tema, así como tener acceso a una recopilación bibliográfica de aspectos relevantes de riesgo operacional que les permita profundizar en mayor medida la gestión de dicho riesgo.

Como segundo aspecto se destaca la importancia que tiene el generar conciencia en las entidades financieras sobre el manejo del riesgo operacional como un sistema integral y no como un modelo estadístico de estimación de pérdidas. Este aspecto es de gran relevancia y por lo tanto la metodología propuesta en este trabajo busca desarrollar una estructura de gestión de riesgo operacional dinámica fundamentada en gran medida en el desarrollo de una cultura de riesgo. El logro de los objetivos propuestos por cada entidad con la gestión de riesgo depende en gran medida del grado de cocientización que tengan todos los funcionarios frente a su responsabilidad en el manejo de este riesgo.

La tercera razón que justifica la propuesta de esta metodología está relacionada con el bajo nivel de detalle que presentan otras metodologías frente al desarrollo del sistema o la concentración en determinados puntos específicos, generalmente los modelos de medición, y los vacíos que quedan en los demás temas. Con la propuesta metodológica y con el diseño de la misma para una línea específica de negocio se busca en alguna medida brindar más claridad frente a varios aspectos que componen el sistema.

Por lo anterior, es necesario que las entidades financieras cuenten con una metodología que puede guiarlas en la implementación de un sistema de riesgo operacional y que puede ser de ayuda en la profundización de los distintos aspectos que conforman el sistema.

OBJETIVOS

Objetivo General

Diseñar un modelo de un sistema de administración de riesgo operacional para la línea de compra y venta de divisas de la tesorería de un banco, el cual pueda ser utilizado como base para implementar el sistema en la totalidad de líneas de negocio de una entidad financiera.

Objetivos Específicos

- Profundizar en los conceptos teóricos de riesgo operacional
- Conocer los requerimientos específicos que sobre el tema hace Basilea
- Conocer los avances en administración de riesgo operacional en Colombia
- Presentar una metodología a seguir para diseñar un sistema de riesgo operacional
- Proponer una metodología de identificación y cuantificación de riesgos operacionales
- Elaborar el mapa de riesgo para la línea a estudiar
- Diseñar los indicadores de control requeridos

CAPITULO 1

1 EL RIESGO OPERACIONAL Y BASILEA II

1.1. Generalidades de Riesgo Operacional

El riesgo operacional es inherente al negocio bancario y por lo tanto ha estado presente desde todos los tiempos. Aunque los administradores de las entidades financieras eran concientes de la existencia de este riesgo, la administración del mismo no se consideraba prioritaria y se trataba de manera reactiva. Una vez presente el problema se generaba una serie de correctivos *ex-post* para evitar o minimizar la ocurrencia del problema. En general, las entidades relacionaban este riesgo con el costo de hacer los negocios y buscaban administrarlo con controles estándar, diseñados para reducir la frecuencia y severidad de las pérdidas esperadas[1].

Si se tiene en cuenta la presencia permanente del riesgo operacional en las entidades financieras es posible afirmar que todas las entidades en alguna medida han implementado mecanismos de mitigación de este riesgo, los cuales, generalmente, están relacionados con controles y procedimientos de auditoria. Sin embargo, dado que el manejo es reactivo y que se realiza a través de esfuerzos aislados, no se logra tener un verdadero sistema para la administración de riesgo operacional (identificación, valoración, monitoreo y control[2]) y por lo tanto la mitigación del mismo es mínima.

Como lo afirma el Comité de Basilea en el documento "Sound pratices for the management and supervisión of operacional risk" la administración del riesgo operacional no es una practica nueva. En las entidades financieras, este riesgo siempre ha sido importante con el fin de intentar prevenir fraudes, mantener la integridad de los controles internos, reducir errores, entre otros. Sin embargo, lo que es relativamente nuevo es ver la administración de riesgo operacional como una practica comparable a la de administrar el riesgo de crédito y de mercado[3].

[1] FITCH RATINGS, FINANCIAL INSTITUTIONS. "The Oldest Tale but the Newest Store: Operacional Risk and the Evolution of its Measurement Under Basel II". / January 2004.
[2] BANK FOR INTERNACIONAL SETTLEMENTS. Basel Comité on Banking Supervisión. "Sound Practices for the management and supervision on operational Risk" Febrero de 2003.
[3] Idem.

Durante la segunda década de los años noventa, varias entidades financieras a nivel mundial registraron pérdidas significativas por aplicar un enfoque reactivo frente al riesgo operacional. Entre los casos destacados se encuentran[4]:

Tabla 1. Casos internacionales de pérdidas generadas por eventos de riesgo operacional

Entidad	USD millones	Causa
1991 BCCI	17,000	Fraude en un período de 20 años
1998 LTCM	4,000	Riesgo Modelo, Controles Internos
1996 Sumitomo Corp.	2,857	Excesivo Trading de Cobre
1994 Down Corning	2,000	Demandas de 18 mujeres
1991-93 Metallgesellschaft	1,800	Mal uso de futuros del petróleo
1994 Orange County	1,600	Inversiones demasiado riesgosas
1995 Barings	1,000	Pérdidas de Trading escondidas
Enron, Arthur Andersen, World Com, Xerox, Vivendi,.....		

Como consecuencia de todos estos casos de pérdidas, las entidades financieras tomaron mayor conciencia de la importancia de la administración de riesgo operacional.

Por otra parte, el alto nivel de competitividad existente en el negocio bancario obliga a las entidades financieras ha desarrollar permanentemente nuevos productos y mejorar niveles de eficiencia y tecnología. La mayor sofisticación de los productos y la velocidad con la cual deben ser implementados generan un mayor riesgo operacional que puede reflejarse en grandes pérdidas.

Teniendo en cuenta la importancia creciente de este riesgo y la necesidad de darle un tratamiento anticipado y cuantitativo, el Comité de Basilea incorporó una serie de lineamientos sobre el tema en el nuevo acuerdo de Basilea (Basilea II).

El Comité de Basilea es el encargado de determinar los principales lineamientos bajo los cuales deben operar las entidades financieras a nivel mundial y aquellos que deben controlar y adaptar las entidades de supervisión de cada país. Aunque el Comité de Basilea había mencionado levemente la existencia e importancia del riesgo operacional, sólo en el nuevo acuerdo se le otorga a este riesgo el atributo de ser cuantificado y de afectar el valor del capital requerido.

Por todo lo mencionado anteriormente se puede concluir que la mayor preocupación existente en el entorno financiero por la administración del riesgo operacional obedece principalmente a tres factores, algunos relacionados entre sí.

[4] KPMG. RISK ADVISORY SERVICES. Financial Risk Management. Basilea II. Training Series. Seminario Riesgo Operacional Bogotá, agosto de 2004.

En primer lugar, las pérdidas en que incurrieron varias entidades financieras por fallas generadas por factores relacionados con riesgo operacional, en segundo lugar por la mayor competencia de productos financieros que exige creatividad y rapidez en la implementación de los mismos y por último por las exigencias puntuales presentadas en el documento conocido como Basilea II, que tarde o temprano obligará a todas las entidades financieras ha implementar sistemas de administración de riesgo operacional.

1.2. Definición de riesgo operacional[5]

Aunque existen varias definiciones de riesgo operacional[6] para efectos de este trabajo se tomará como definición oficial la establecida por el Comité de Basilea: "El riesgo operativo se define como el riesgo de pérdida debido a la inadecuación o a fallos de los procesos, el personal y los sistemas internos o bien a causa de acontecimientos externos. Esta definición incluye el riesgo legal, pero excluye el riesgo estratégico y el de reputación".[7]

1.3 El Comité de Basilea

El Comité de Basilea perteneciente al Banco de Pagos Internacionales (BIS)[8] fue establecido en 1974 por los gobernadores de los bancos centrales de los diez países más importantes del Fondo Monetario Internacional, con el fin de generar enfoques de supervisión estándar para todas las entidades financieras y con esto fortalecer el adecuado funcionamiento de dichas entidades. Este Comité tiene aproximadamente 25 grupos de trabajo técnicos. Actualmente los miembros del Comité son de Bélgica, Canadá, Francia, Alemania, Italia, Japón, Luxemburgo, Holanda, España, Suecia, Suiza, Inglaterra y Estados Unidos. Este Comité formula lineamientos y estándares para la supervisión bancaria y recomienda a las entidades financieras mejores prácticas. Sin embargo, las exigencias legales encaminadas a cumplir con estos lineamientos son propias de la entidad supervisora de cada país[9].

En 1988, el Comité decidió introducir un sistema de medición de capital conocido

[5] KPMG, FINANCIAL SERVICES. Basilea II, una mirada más cercana. Administración de riesgo operacional.
[6] Ver otras definiciones en el trabajo realizado por RICARDO VARELA, María Cristina. Impacto de las Metodologías propuestas por el Comité de Basilea para el cálculo de los requerimientos de capital por riesgo operativo en el sector bancario colombiano. Universidad de los Andes. Tesis Ingeniería Industrial. Enero de 2004. Página 22.
[7] BANCO DE PAGOS INTERNACIONALES. Comité de Supervisión Bancaria de Basilea. Convergencia Internacional de Medidas y Normas de Capital. Junio de 2004. Capitulo V. Página 138.
[8] The Bank for International Settlements (BIS) es la organización internacional más antigua del mundo creada en Basilea Suiza en 1930. Esta entidad promueve la cooperación internacional y financiera y funciona como banco de bancos centrales.
[9] www.bis.org/about/index.htm

como el acuerdo de capital de Basilea. Este sistema buscaba la implementación de una estructura de medición de riesgo crediticio y relacionar este riesgo con el capital mínimo requerido para el funcionamiento de las entidades financieras[10]. Varios países adoptaron estos lineamientos. En junio de 1999, el Comité emitió una propuesta para una nueva estructura de capital para reemplazar el acuerdo de 1988. Esta propuesta fue revisada por las partes interesadas y en junio de 2004 el Comité publicó la versión definitiva del acuerdo de Basilea II.

El nuevo acuerdo de Basilea refleja mayor sensibilidad al riesgo y busca que las entidades estén mejor preparadas patrimonialmente para enfrentar los diferentes riesgos que asumen. Adicionalmente, busca fortalecer la disciplina de mercado a través de mayor transparencia en los reportes públicos de los bancos.

"Basilea II abarca un amplio enfoque de administración de riesgo y supervisión bancaria" explica Jean –Claude Trichet, presidente de grupo de gobernadores de bancos centrales del grupo de los diez y Presidente de Banco Central Europeo. "Este acuerdo mejorará la seguridad y solidez de los bancos, fortalecerá la estabilidad del sistema financiero como un todo y mejorará la habilidad del sector financiero para servir como una fuente sostenible de crecimiento para la economía"[11].

1.4 El nuevo acuerdo de Basilea[12]

La nueva propuesta de Basilea se fundamenta en tres pilares, los cuales se complementan uno a otro: requerimiento de capital en relación a los riesgos asumidos, revisión de la supervisión y disciplina de mercado.

El primer pilar presenta un fortalecimiento significativo de los capitales mínimos requeridos en 1988, mientras el segundo y el tercer pilar son aspectos nuevos.

El pilar I pretende alinear de una manera más precisa el mínimo valor de capital requerido con el riesgo asumido por cada banco. Basilea II propone establecer una relación directa entre el requerimiento de capital de un banco y el grado de riesgo en que éste incurra, más específicamente, que el capital de los bancos sea suficiente para protegerse contra los siguientes riesgos:
- Riesgo de Crédito: pérdida potencial por falta de pago de un acreditado
- Riesgo Operacional: pérdida potencial derivada de fallas en los procesos, sistemas, actuación del personal o eventos externos

[10] La relación mínima de solvencia establecida por el Comité es de 8%. La solvencia es la relación entre el patrimonio técnico (capital) y los activos ponderados por riesgo.
[11] G10 central bank governors and heads of supervision endorse the publication of the revised capital framework. Press Release. www.bis.org.
[12] BANK FOR INTERNACIONAL SETTLEMENTS. Basel Comité on Banking Supervisión. Internacional Convergente of Capital Measurement and Capital Standard. June 2004.

- Riesgo de Mercado: pérdida potencial por movimientos adversos en las tasas de interés, tipo de cambio, aprecio de los activos y pasivos.

Como aspecto novedoso, el nuevo acuerdo establece un requerimiento de capital por posibles pérdidas generadas por riesgo operacional. Al igual que en la estimación del riesgo de crédito, el acuerdo contempla tres alternativas para cumplir con la estimación del capital requerido por riesgo operacional. Frente a los requerimientos de capital por riesgo de crédito y operacional, el Comité anima a los bancos a adoptar modelos desarrollados, ya que estos les generarán menores requerimientos de capital. En lo relacionado con riesgo de mercado, el requerimiento no fue modificado.

El pilar II reconoce la necesidad de ejercer una supervisión efectiva de los bancos. El Comité espera que cuando los supervisores evalúen un banco puedan hacer evidente la ventaja de desarrollar un control sólido y del mejoramiento de procesos.

El pilar III busca que la disciplina del mercado pueda motivar una administración prudente a través del fortalecimiento de la transparencia de los reportes públicos de los bancos y al mayor desarrollo de la autodisciplina.

El Comité pretende que el nuevo enfoque este disponible para su implementación en los países miembros a principios del 2007. El acuerdo de Basilea II está más enfocado en los riesgos fundamentales y provee fuertes incentivos para quién mejore la administración de riesgo[13].

1.5 Metodologías de medición de riesgo operacional[14]

El acuerdo de Basilea II propone tres metodologías de medición del riesgo operacional. En orden creciente de sofisticación y sensibilidad al riesgo, estos métodos son:

(i) El Método del Indicador Básico
(ii) El Método Estándar
(iii) Los Métodos de Medición Avanzada (AMA)

Cada entidad financiera de acuerdo con su tamaño y complejidad podrá adoptar el enfoque que requiera. No obstante, el Comité busca estimular a las entidades a desarrollar modelos propios de medición, conocidos como avanzados, que permitan medir con mayor precisión el impacto del riesgo operacional y que se espera generen menores requerimientos de capital. Los Bancos internacionales y

[13] G10 central bank governors and heads of supervision endorse the publication of the revised capital framework. Press Release. www.bis.org.
[14] Bank For Internacional Settlements. Basel Comité on Banking Supervisión. "Internacional Convergente of Capital Measurement and Capital Standard". June 2004.

los que tienen exposición al riesgo operacional significativa están más interesados en usar un enfoque más sofisticado que el básico. Así mismo, un banco podrá utilizar el enfoque de indicador básico para algunos procesos y un enfoque más sofisticado para otros procesos.

1.5.1 El enfoque de indicador básico

Este es el enfoque más simple y está diseñado para entidades menos sofisticadas y generalmente de tamaño pequeño. Los bancos que adopten este enfoque deberán afectar el capital por riesgo operacional por un monto igual a la multiplicación de los ingresos brutos anuales positivos por un porcentaje fijo denominado alfa. Los ingresos brutos se definen como los ingresos netos por concepto de intereses más los ingresos ajenos a intereses[15]. Los ingresos brutos corresponden al promedio de los ingresos brutos de los últimos tres años. El cálculo del valor a cargar por riesgo operacional es el siguiente:

$K_{BIA} = [\Sigma (GI_{1\ldots n} \times \alpha)]/n$

Donde:

$K_{B/A}$ = Valor con el que se afecta el capital bajo el enfoque de indicador básico
GI = Ingresos anuales brutos (annual gross income)[16].
α = 15%. Este porcentaje es definido por el Comité de Basilea
n = numero de años que se va a tener en cuenta para el cálculo.

Se considera que las entidades que apliquen este enfoque registraran los mayores requerimientos de capital por concepto de riesgo operacional.

1.5.2 El enfoque estandarizado.

En este enfoque, las actividades de los bancos se dividen en ocho líneas de negocio: finanzas corporativas, negociación y ventas, banca minorista, banca comercial, pagos y liquidación, servicios de agencia, administración de activos e intermediación minorista. Por lo tanto, las entidades deben tener un mapa de sus principales líneas de negocio homologándolas con las propuestas por Basilea II. Este enfoque permite a las entidades reportar los riesgos totalmente relacionados

[15] Conforme a las definiciones de los supervisores nacionales y/o las normas contables nacionales. Se pretende que esta medida (i) sea bruta de cualquier provisión (por ejemplo, por impago de intereses); (ii) sea bruta de gastos de explotación, incluidas cuotas abonadas a proveedores de servicios de subcontratación15; (iii) excluya los beneficios / pérdidas realizados de la venta de valores de la cartera de inversión15; y (iv) excluya partidas extraordinarias o excepcionales, así como los ingresos derivados de las actividades de seguro.
[16] Sólo se tiene en cuenta si es positivo, de lo contrario el dato debe ser excluido del numerador y del denominador.

con cada una de las líneas del negocio y recolectar datos que son comparables de acuerdo con el riesgo operacional que generan.

Para calcular el valor con el cual se afecta el capital se multiplican los ingresos brutos de cada una de las líneas del negocio definidas anteriormente de los últimos tres años por un coeficiente específico para cada línea denominado Beta. Una vez se tiene el cálculo del valor en riesgo operacional de cada línea, el valor total se calcula como el promedio de la suma simple del valor en riesgo de cada línea de negocio para los últimos tres años. Si en uno de estos años el valor total es negativo, este se excluye del cálculo del promedio. El valor total con el que se afecta el capital se calcula de la siguiente manera:

$$K_{TSA}=\{\Sigma \text{ año } 1\text{-}3 \max[\Sigma (GI_{1\text{-}8} \times \beta_{1\text{-}8}),0]\}/3$$

Donde:
K_{TSA} = carga de capital por el enfoque estandarizado
$GI_{1\text{-}8}$ = ingreso anual bruto en una año determinado para cada una de las líneas del negocio
$\beta_{1\text{-}8}$ = un porcentaje fijo determinado por el Comité .

Tabla 2. Valor de los Betas para cada línea de negocio

Líneas de negocio	Factor β
Finanzas Corporativas (β 1)	18%
Negociación y Venta (β 2)	18%
Banca Minorista (β 3)	12%
Banca Comercial (β 4)	15%
Pagos y Liquidación (β 5)	18%
Servicios de Agencia (β 6)	15%
Administración de Activos (β 7)	12%
Intermediación Minorista (β 8)	12%

Adicionalmente cada una de estas clasificaciones se puede subdividir en otras categorías (ver anexo 1). El Comité de Basilea presenta una serie principios para la asignación de las líneas del negocio[17] y exige que exista una metodología clara de asignación la cual deberá ser aprobada por la Junta Directiva.

La autoridad supervisora de cada país podrá permitir a un banco la utilización del Método Estándar Alternativo (ASA), el cual es muy similar al Método Estándar excepto en dos líneas de negocio: banca minorista y banca comercial. En estas líneas de negocios se usará el valor de los créditos multiplicados por un factor fijo

[17] BANCO DE PAGOS INTERNACIONALES. COMITÉ DE BASILEA. "Principios para las líneas de asignación del negocio" Convergencia internacional de medidas y normas de capital. Basilea II. Junio de 2004, Versión en Español. Anexo 6, página 219.

"m" en reemplazo de los ingresos brutos. El valor total con el que se afecta el capital por concepto de estas líneas se calcula de la siguiente manera:

KRB = β RB x m x LARB

Donde:
KRB capital requerido por líneas de consumo o comercial
β RB beta para la líneas de consumo y comerciales
LARB valor de los préstamos de créditos de consumo o comerciales promedio de los últimos tres años
m = 0.035

Para que un banco pueda utilizar el Método Estándar o Estándar Alternativo debe satisfacer por lo menos los siguientes requerimientos[18]:

- La junta directiva y el presidente deben estar activamente involucrados en la supervisión de la estructura de riesgo operacional
- Tener un sistema de administración de riesgo que sea conceptualmente sólido y este implementado con integridad.
- Contar con los recursos requeridos para el uso de este enfoque en las principales líneas del negocio y en las áreas de control y auditoria.
- Criterios adicionales relacionados con la Unidad de Administración de Riesgo Operativo, recolección de datos, reportes, mecanismos de auditoria, entre otros.

1.5.3 El enfoque de medición avanzado

Bajo este enfoque, el requerimiento de capital regulatorio es igual a la medida de riesgo generada por el sistema interno de medición del riesgo operacional de cada banco, utilizando criterios cuantitativos y cualitativos. A través de este método, las entidades deberán estimar las pérdidas esperadas y no esperadas para el cálculo de la estimación del capital requerido. Si la entidad demuestra que tiene medidas de mitigación de riesgo, el capital requerido puede disminuir. El uso de este enfoque esta sujeto a la aprobación del ente supervisor de cada país.

Los bancos que decidan implementar este enfoque deberán cumplir como mínimo con los siguientes requerimientos:

- La junta directiva y el presidente deben estar activamente involucrados en la

[18] BANCO D E PAGOS INTERNACIONALES. COMITÉ DE BASILEA. Convergencia internacional de medidas y normas de capital. Basilea II. Junio de 2004, Versión en Español. Criterios de Admisión. Página 142.

- supervisión de la estructura de riesgo operacional
- Tener un sistema de administración de riesgo que sea conceptualmente sólido y este implementado con integridad.
- Contar con los recursos requeridos para el uso de este enfoque en las principales líneas del negocio y en las áreas de control y auditoria.
- Cumplir con los requerimientos adicionales cualitativos relacionados con: la Unidad de Administración de Riesgo Operacional, reportes, correctivos, documentación y auditoria entre otros.
- Tener un sistema interno para el cálculo del riesgo operativo acorde a la definición del riesgo operativo establecida por el Comité de Basilea y con los tipos de eventos de pérdida relacionados con fraude interno, fraude externo, daños a activos materiales, fallos en los sistemas, ejecución, entrega y gestión de procesos (ver Anexo 2).
- Cumplir con los requerimientos cuantitativos relacionados con la solidez del modelo.

1.5.3.1 Solidez del modelo

El modelo que se utilice y los supuestos estadísticos deben ser justificados técnicamente. Los procedimientos utilizados para el desarrollo del modelo deben ser rigurosos al igual que los utilizados para las validaciones del modelo. El valor por el cual se afecta el capital será la suma de la pérdida esperada y no esperada generada por riesgo operacional, a menos que la entidad demuestre que la pérdida esperada está totalmente medida y contabilizada en sus prácticas internas del negocio. La solidez de los modelos internos se fundamenta entre otras cosas en la utilización de datos internos y externos, de análisis de escenarios, de factores que reflejen el ambiente de negocios y de sistemas de control interno.

Los elementos considerados fundamentales son:

Datos internos

La recolección de datos internos es fundamental para desarrollar un modelo de medición de riesgo operacional. Estos datos son más relevantes si están relacionados directamente con las principales líneas del negocio, con procesos tecnológicos y con procedimientos de administración de riesgo. Para los modelos internos se requieren bases de datos que por lo menos tengan cinco años de historia. No obstante, cuando una entidad va a adoptar por primera vez este enfoque tres años de historia son suficientes, ya que la entidad de control exigirá que durante un tiempo se realicen cálculos paralelos. Los datos deberán estar categorizados de acuerdo con las líneas de negocio establecidas por Basilea. Así mismo, las entidades deberán determinar los datos que se van a recopilar

teniendo en cuenta el posible impacto que estos puedan generar. En lo posible los datos deben capturar el generador y la causa.

Datos externos
Los bancos pueden complementar sus bases de datos con datos externos, especialmente cuando se determine la posible generación de pérdidas por even43tos infrecuentes pero con probabilidad de ocurrencia. Se debe tener claramente definido el procedimiento de utilización de estos datos (en que casos se utilizan, si requieren ser adecuados, entre otros).

Análisis de escenarios
Un banco debe utilizar el análisis de escenarios apoyado en la opinión de un experto y con la utilización de los datos internos, para evaluar la exposición a eventos de alta severidad. Esta evaluación se fundamenta en el conocimiento de los administradores de las líneas de negocios y de administración de riesgo, que en conjunto determinaran la valoración de posibles pérdidas.

Ambiente de negocios y factores internos de control
Los bancos deben capturar elementos claves del ambiente de negocios y de los factores internos de control que pueden cambiar su perfil de riesgo. El tener en cuenta este aspecto hace que la valoración de riesgo tenga una visión a futuro y ayuda a alinear la asignación de capital con los objetivos de administración de riesgo.

Mitigación del riesgo
A las entidades que utilicen el modelo avanzado se les puede reconocer los seguros que utilicen para mitigar el riesgo, en la medición del capital requerido. El máximo reconocimiento de la mitigación está limitado al tipo de seguro o cobertura y será porcentaje del capital requerido para respaldar posibles pérdidas generadas por riesgo operacional.

1.5.3.2 Metodologías de medición avanzada utilizadas[19]

Frente al enfoque de medición avanzado, Basilea permite que cada entidad desarrolle una metodología propia, que posteriormente será avalada por el ente supervisor de cada país. No obstante, en un estudio preliminar, el Comité de Basilea pudo observar que varias entidades están desarrollando alguna de las siguientes metodologías: enfoque de medición interna, enfoque de distribución de pérdidas y enfoque *scorecard.* Las entidades pueden combinar aspectos de cada una de estas metodologías.

[19] BANK FOR INTERNACIONAL SETTLEMENTS. Basel Comité on Banking Supervisión. Working Paper on the Regulatory treatment of operational risk. September 2001. Annex 4. www.bis.org

Enfoque de medición interna

En este enfoque las entidades estiman el capital requerido por riesgo operacional basadas en medidas de pérdidas esperadas por riesgo operacional. Este enfoque asume una relación fija y estable entre pérdidas esperadas y pérdidas no esperadas, relación que puede ser lineal o no lineal. Generalmente, las pérdidas esperadas son calculadas por combinación de estimativos de frecuencia e impacto de las pérdidas. En general, para la utilización de esta metodología se realizan los siguientes pasos:

- Las actividades del banco son categorizadas en líneas de negocio y un conjunto de tipos de riesgo operacional son identificados para cada línea.
- Para cada combinación de línea y tipo de riesgo se específica un indicador de exposición (EI – Exposure Indicator) el cual es una aproximación del monto de riesgo al que esta expuesta cada línea.
- Para cada indicador de exposición, el banco mide, basado en sus datos internos de pérdida, un parámetro que representa la probabilidad de eventos de pérdida (PE – Probability event) así como un parámetro que representa la proporción del monto expuesto que podría perderse ante la ocurrencia de un evento (LGE – Average Loss Given that an event occurs)
- La pérdida esperada para la combinación de cada línea de negocio con un tipo de riesgo es igual a: EL = EI * PE * LGE
- El valor exigido de capital por riesgo operacional será igual a la suma de la pérdida esperada para cada línea de negocio multiplicada por un factor que será determinado por la entidad supervisora de cada país.

Enfoque de la distribución de pérdidas

Bajo este enfoque, para cada combinación de línea de negocio y tipo de riesgo, se identifica la distribución de pérdidas probable para un futuro horizonte de tiempo. Los datos utilizados para estimar la distribución están relacionados con la frecuencia de ocurrencia de los eventos de riesgo y la severidad de los mismos. La estimación de las distribuciones puede implicar asumir una distribución específica o determinar la distribución empíricamente a través de técnicas como simulación de Monte Carlo o *Boot-straping*. El valor de capital requerido será igual a la suma del riesgo operativo de cada línea de negocio.

Enfoque scorecard

Bajo este enfoque las entidades determinan un nivel inicial de capital requerido por

riesgo operacional para la entidad en total o para cada línea de negocios y modifican este valor en el tiempo con base en *scorecards* que intentan capturar las causas del perfil de riesgo y el ambiente de control de riesgo de varias líneas de

negocio. Este enfoque busca brindar un componente de visión futura en el cálculo del capital requerido, ya que refleja mejoras en el ambiente de control que se evidencia en reducción de frecuencia o impacto de los eventos de riesgo. Los scorecards pueden ser basados en medidas actuales de riesgo pero frecuentemente se identifican algunos indicadores como aproximaciones de un tipo particular de riesgo en una línea de negocio específica. Éstos se complementan periódicamente con apreciaciones de la administración de la entidad relacionada con el riesgo operacional.

1.6 Principios aclaratorios de manejo de riesgo operacional[20]

Conciente de la dificultad de enfrentar el tema de administración de riesgo operacional, el Comité de Basilea publicó un documento que aclara varios temas relacionados dicho riesgo. El documento se tituló "Sound practices for the management and supervisión of operacional risk[21]". En este documento el Comité reconoce que cada entidad es autónoma en la identificación de los generadores de riesgo operacional. Sin embargo, determinó algunos tipos de riesgo operacional que podrían reflejarse en altas pérdidas y se presentan en el Anexo 2. Adicionalmente, en el documento se presentan diez principios que las entidades deben tener en cuenta para manejar con altos estándares la administración de riesgo operacional. Los diez principios se pueden resumir así:

Desarrollo de un apropiado ambiente de manejo de riesgo

1. La Junta Directiva y el Presidente de la entidad son responsables de establecer la estrategia a seguir por la entidad en lo relacionado con la administración de riesgo operacional y de revisar periódicamente el cumplimiento de los lineamientos que dicha Junta halla definido.

2. La Junta Directiva y el Presidente de la entidad deben garantizar que el sistema de administración de riesgo operacional es sujeto de una efectiva auditoria interna, la cual deberá estar apropiadamente entrenada y contar con un staff competente. La auditoria interna no debe ser directamente responsable de la administración de riesgo operacional.

[20] BANK FOR INTERNACIONAL SETTLEMENTS. Basel Comité on Banking Supervisión. "Sound Practices for the Management and Supervisión of Operacional Risk". Febrero de 2003.
[21] Idem.

3. El Presidente de la entidad tiene la responsabilidad de implementar el sistema de administración de riesgo operacional aprobado por la Junta Directiva. El sistema debe ser implementado a través de toda la organización y todos los niveles de staff deberán entender su responsabilidad con respecto al riesgo operacional. El presidente deberá ser responsable de desarrollar las políticas, procesos y procedimientos para manejar el riesgo operacional en todos los productos, actividades procesos y sistemas.

Administración de riesgo (identificación, valoración, monitoreo y mitigación y control)

4. Los bancos deberán identificar y valorar el riesgo operacional inherente en todos los productos, actividades, procesos y sistemas, incluido el desarrollo de un nuevo producto.

5. Los bancos deberán monitorear periódicamente el riesgo operacional y enviar informes a la Junta Directiva y al Presidente que soporten una administración proactiva del riesgo operacional.

6. Los bancos deben implementar políticas, procesos y procedimientos para controlar y mitigar el riesgo operacional y analizar los beneficios y costos de las alternativas de mitigación y control de los riesgos operacionales.

7. Los bancos deben tener planes de contingencia y de continuación del negocio para asegurar la capacidad de operar con pérdidas limitadas ante un evento severo que afecte el normal funcionamiento del negocio.

Papel de los Supervisores

8. Los supervisores deberían exigir a los bancos tener implementado un sistema efectivo para identificar, medir, monitorear y controlar/ mitigar los riesgos operacionales, como parte de un sistema integral de administración de riesgo.

9. Los supervisores deben adelantar (directa o indirectamente) evaluaciones regulares e independientes de estos principios y asegurarse que un efectivo mecanismo de reporte existe.

Revelación de información

10. Los bancos deben tener una comunicación pública suficiente que permita a los participantes del mercado medir la exposición de riesgo operacional de la organización y la calidad de la administración de este riesgo operacional.

En los anteriores principios se evidencia el reconocimiento del riesgo operacional como un riesgo tan importante como el de crédito o el de mercado, ya que los lineamientos mencionados son similares a los exigidos para la implementación de sistemas de administración de estos riesgos. Se destaca la exigencia de un compromiso directo de la alta administración buscando principalmente generar una cultura de administración de riesgo operacional en la organización.

1.7 Posible impacto del nuevo acuerdo de Basilea

La implementación de los requerimientos del nuevo acuerdo de Basilea generará cambios en los esfuerzos de capitalización de los bancos. Las entidades que tengan mayor exposición del riesgo van a requerir capitalización y las de menor perfil de riesgo podrán tener un requerimiento de capital menor que el actual.

Un estudio del impacto de las normas, realizado por la firma de consultores Mercer Oliver Wyman y citado por el Financial Times concluyó que la puesta en vigor de la normativa costará a los bancos cinco puntos del total de sus activos durante cinco años, lo que para los grandes bancos del mundo, equivaldrá a entre 100 millones y 200 millones de dólares. Aún así, según el mismo informe, los bancos obtendrán compensaciones por el gasto en el cumplimiento de estas normas y los primeros en acatarlas tendrán ventajas. El estudio de Mercer Oliver Wyman también concluyó que los bancos británicos estarán en situación de reducir las reservas de capital, mientras que los de Alemania e Italia, tendrán que aportar los mayores incrementos. No se ha dado a conocer ningún estudio similar que mida el impacto en capital para América Latina. En Estados Unidos se ha calculado que algunos de los bancos "ganadores" podrán reducir su capital como un 30% mientras que otros tendrán que aumentarlo como en 40%, reveló un estudio dado a conocer por el Financial Times.

"Aunque el Acuerdo de Basilea solo es de obligatorio cumplimiento para los bancos de los países industrializados y, en principio, los bancos latinoamericanos tal vez no tengan que cumplir con sus normativas, plazas bancarias como Panamá, Venezuela, Colombia, que aspiran a seguir siendo plazas importantes, van a sentir presiones"[22]. México ya está bastante adelantado, básicamente, porque su sistema bancario se compone principalmente de bancos

[22] ESPARZA Rogelio, Gerente Senior, Financial Risk Management KPMG en México.

internacionales. Otros que le siguen los pasos son Panamá, Colombia y Venezuela, cuyas superintendencias están trabajando en la introducción de normas sobre administración de riesgos en sus respectivos países[23].

1.8 Críticas a Basilea II en lo relacionado con riesgo operacional

Antes de publicar el documento definitivo conocido como "Basilea II", el Comité de Basilea publicó desde 2001 tres documentos consultivos para que las partes interesadas a nivel mundial enviaran sus comentarios. El Comité recibió y estudio más de mil comentarios, algunos de los cuales se incorporaron en el documento definitivo[24]. Dentro de estos comentarios se identificaron varias críticas a la nueva propuesta. En la mayoría de los casos las críticas estaban relacionadas con el nuevo tratamiento del riesgo de crédito. Sin embargo, es posible rescatar algunos comentarios relacionados con el tratamiento que le da Basilea al Riesgo Operacional.

La complejidad en la aplicación del nuevo acuerdo. En lo relacionado con riesgo operacional, esta crítica está relacionada con la incorporación del mismo en el cálculo del capital requerido, en las diversas metodologías que se pueden utilizar para su cálculo, en la segmentación de las operaciones, entre otras. Sin embargo, de acuerdo con Herinch[25], el nuevo acuerdo es más complejo como consecuencia directa de la mayor complejidad del sector bancario. Adicionalmente, uno de los objetivos del nuevo acuerdo es generar mayor sensibilidad al riesgo y esto no es posible como enfoques simplificados.

Adicionalmente, las entidades no cuentan con bases de datos de riesgo operacional, que permitan medir de una manera objetiva este tipo de riesgo. Gran parte de las entidades deben acudir a valorar los posibles riesgos operacionales que se pueden presentar de una manera subjetiva, lo que generaría grandes diferencias entre los resultados de las entidades[26]. Por otra parte, la recolección de los datos (posibles fallas generadas por riesgo operacional) requiere un soporte

[23] ASOCIACIÓN DE BANCOS LATINOAMERICANOS. Centro de documentación. Basilea II: Una solución o un problema. Comentario de las ponencias presentadas en el "Segundo Encuentro Sector Público - Privado sobre el Nuevo Acuerdo de Capital de Basilea". Washington, D.C. BID, 30 de enero de 2004.
[24] HEINRICH Gregor. Representante para las Américas. Banco de Pagos Internacionales (BIS). Anales ALIDE 33. Tópico 2: Retos de Basilea II. Pagina 8.
[25] HEINRICH Gregor. Representante para la Américas. Banco de Pagos Internacionales (BIS). Anales ALIDE 33. Tópico 2: Retos de Basilea II. Pagina 5.
[26] FITHRATINGS FINANCIAL INSTITUTIONS. Special Report. Operacional Risk management & Basel II implementation: Survey results. Abril 21 de 2004. www.fitchratings.com

tecnológico óptimo que permita registrar estos eventos. En general pocas entidades cuentan con este soporte tecnológico especialmente en Latinoamérica, lo que dificultaría en mayor medida la recolección de los datos.

Posibles inconsistencias entre la metodología estándar y la metodología avanzada

La aplicación de estas metodologías conlleva a la multiplicación de unos factores de riesgo sugeridos por el Comité de Basilea por los ingresos brutos de la entidad. Esta metodología sugiere que si el tamaño de una entidad es mayor y genera altos ingresos, el riesgo operacional de la entidad sería alto. En opinión de Fitch Ratings, el tamaño de la entidad o de los ingresos de la misma no refleja necesariamente un mayor o menor riesgo operacional[27]. Adicionalmente, con base en un estudio realizado por Fitch Ratings a los cincuenta bancos más grandes a nivel mundial, se encontró que las entidades que aplican la metodología avanzada en algunos casos requieren un mayor valor de capital que si aplicaran la metodología básica. Lo anterior en razón a que en la aplicación de la metodología avanzada, Basilea aún no ha definido como tener en cuenta las herramientas de mitigación de riesgos en el cálculo del capital requerido[28].

Exigencias enfocadas en países desarrollados

La aplicabilidad de parámetros tan exigentes en sistemas financieros de países en desarrollo es lejana, ya que dichos sistemas aún se encuentran en desarrollo de exigencias anteriores. Adicionalmente, algunas entidades pequeñas con operaciones locales focalizadas, no están en capacidad de contar con la relación de solvencia exigida por Basilea. Frente a esta crítica, Heinrich menciona que si bien el acuerdo está dirigido en primer lugar a los bancos del G 10, dicho acuerdo generará los lineamientos a seguir por la banca mundial. Aunque algunos países de Latinoamérica participaron en los grupos de trabajo de Basilea II y otros enviaron comentarios a los documentos consultivos, se espera que éstos países adopten las nuevas exigencias de manera gradual y con plazos muchos mayores a los establecidos para los países del G 10.

Por otra parte y teniendo en cuenta que la valoración de riesgo operacional en un concepto nuevo en la banca, la implementación de un sistema de riesgo

[27] FITHRATINGS FINANCIAL INSTITUTIONS. Special Report. The Oldest Tal but the newest store: Operational risk and the evolution of its measurement under Basel II, Enero 7 de 2004.
[28] FITHRATINGS FINANCIAL INSTITUTIONS. Special Report. Operacional Risk management & Basel II implementation: Survey results. Abril 21 de 2004. www.fitchratings.com

operacional exige un amplio conocimiento de los procesos y de herramientas estadísticas y técnicas por parte de las personas que los deben aplicar como por parte de los que van a supervisar. Por lo anterior, los entes de control de los países en desarrollo deberán hacer grandes esfuerzos en capacitación especialmente en herramientas sofisticadas de medición y control de riesgos.

Un problema adicional es el de la hetereogeneidad de enfoques en países en desarrollo[29]. Los lineamientos de Basilea no son de cumplimiento obligatorio para todos los países. Es salvedad de cada ente supervisor acoger los lineamientos del Comité textualmente o adaptarlos a sus necesidades y limitaciones. Esto último es común en los países en desarrollo. Por lo anterior es muy probable que los bancos de cada país estén sujetos a distintos enfoques de acuerdo con la autoridad de supervisión que les corresponda. Bajo este escenario, los indicadores no son comparables y pueden generar discriminación de ciertas entidades.

1.9 Otras aproximaciones al riesgo operacional

El comité de Basilea ha afirmado, "La mayoría de los tipos importantes de riesgo operacional implican fallas en los controles internos y en el gobierno corporativo"[30]. En varios países, ya existen regulaciones específicas relacionadas con estos temas, que aunque tenga objetivos distintos, están perfectamente alineadas con algunos de los requerimientos de Basilea. Entre las regulaciones más importantes se destacan:

- The Committee of Sponsoring Organizations of the Treadway Commission (COSO). Es un marco de control interno creado en 1985 en Estados Unidos con el objetivo de estudiar las causas que conllevan a reportar la información financiera fraudulenta, además de desarrollar recomendaciones para las compañías y sus auditores. La aplicación de este marco permite a las entidades lograr objetivos relacionados con: Eficacia y eficiencia de las operaciones, confiabilidad de la divulgación financiera y conformidad con leyes y regulaciones.

- Control Objetives for Information and Related Tecnology (COBIT)[31]. Es un estándar publicado por la Asociación de Auditoria y Control de

[29] SALVATIERRA Ignacio. Basilea II: desafíos para la industria en América Latina. FELABAN. Julio de 2004.
[30] BANK FOR INTERNACIONAL SETTLEMENTS. Basel Comite on Banking Supervisión. "operacional Risk Management", september 1998.
[31] www.isaca.org/**cobit**.htm

Sistemas de Información (ISACA) cuyo objetivo es proveer un esquema para mantener una buena tecnología de la información y buenas practicas de seguridad y control de información.

- Sarbanes – Oxley Act[32]. Esta Ley fue aprobada por el Congreso de Estados Unidos en julio de 2002 y pretende introducir importantes cambios legislativos relacionados con prácticas financieras y con gobierno corporativo. El principal objetivo de esta Ley es proteger a los inversionistas a través del mejoramiento de la precisión y confiabilidad de la información corporativa revelada. El nombre de la Ley se deriva de los ponentes de la misma: el senador Paul Sarbanes y el Representante Michael Oxley y fue motivada por los diversos escándalos de corrupción que llevaron a la quiebra a algunas compañías. Entre otros temas, la Ley incluye normas relacionadas con el fortalecimiento de la responsabilidad corporativa y el fortalecimiento de la información financiera revelada. Esta ley está dividida en once títulos y a la vez estos en diferentes secciones. Entre los principales temas que trata se encuentran: La creación de una junta supervisora de la contabilidad de la compañías que tengan participación accionaria del público, aspectos relacionados con la independencia de los auditores, con responsabilidad Corporativa, el fortalecimiento de las revelaciones financieras, análisis de conflictos de interés, estudios y reportes requeridos, la responsabilidad corporativa y el fraude criminal, el fortalecimiento de la penalidad de crímenes de cuello blanco y el fraude corporativo y la responsabilidad, entre otros.

  En general la Ley busca mejorar los aspectos relacionados con gobierno corporativo, dedicando una sesión especial (404) a la evaluación gerencial de los controles internos. Teniendo en cuenta la importante relación existente entre este tema y el riesgo operacional se presentará un breve resumen del alcance de este tema.

  La sesión 404 exige que la SEC (Securities and Exchange Comisión) publique y fortalezca las reglas para implementar controles para asegurar la confiabilidad y transparencia de los datos financieros corporativos de las compañías con acciones en el mercado. Como respuesta a este requerimiento, la SEC propuso una regla que requerirá que el reporte anual de cada una de las compañías con acciones del público incorpore un reporte interno de control que:

  - Declare la responsabilidad de la administración de establecer y mantener adecuados controles internos sobre los reportes financieros de la compañía.

[32] www.sabarnes-oxley-forum.com

- Identifique la estructura utilizada por la administración para evaluar la efectividad de los controles internos
- Evalué la efectividad de los controles internos al final del año fiscal de la compañía.
- Declare que el auditor publicó un reporte testificando la evaluación realizada por la administración.

Los controles aplican a cada uno de los procesos, procedimientos, aplicaciones, sistemas y datos relacionados con el cálculo y la preparación de la información financiera de la entidad. Expertos manifiestan que esto implica que cada división de la compañía necesita tener un conjunto de reglas internas documentadas que controlen como los datos son generados, manipulados, grabados y reportados. La SEC determinó que los plazos para cumplir con este requerimiento son el 15 de abril de 2005 para pequeñas compañías y el 15 de junio para grandes compañías. Gran parte del éxito en la implementación de estos controles y por lo tanto de la confiabilidad de los informes financieros publicados radica en un adecuado soporte tecnológico.

- Otras aproximaciones[33]: En Canadá se encuentra el marco desarrollado por la Canadian Institute of Chartered Accountants' Criteria of Control Comité (CoCo), en Gran Bretaña los requisitos y el grupo de estándares de gobierno en un código combinado en The United Kingdom's Financial Services Authority (FSA), en Holanda la regulación incorporada en The Dutch Regulation on Organisation and Control (ROC) of the Dutch Central Bank and the Nadere Regeling 2002 of the Financial Markets Authority y en Alemania The German Corporate Sector Supervisión and Transparency Act (KonTraG) and Section 25a of the German Banking Act (KWG). Todas las anteriores regulaciones están relacionadas con el mejoramiento de los controles internos y de la administración de riesgos y el fortalecimiento del gobierno corporativo.

[33] KPMG FINANCIAL SERVICES. Basilea II, una mirada más cercana. Administración de riesgo operacional.

CAPITULO 2

2 Avances en la administración de riesgo en Colombia

2.1 Antecedentes

En Colombia el sistema financiero opera a través de entidades especializadas dentro de las cuales se destacan los siguientes grupos: establecimientos de crédito (Bancos, Corporaciones Financieras, Compañías de Financiamiento Comercial Tradicionales y especializadas en Leasing), Compañías de Seguros, y Sociedades Fiduciarias, entre otros. Durante la última década, todos los grupos de entidades registraron cambios significativos en su forma de operar generados por la mayor influencia de tendencias mundiales y por la crisis financiera registrada en los últimos años de la década de los noventa.

En el caso específico de los establecimientos de crédito es importante recordar que en 1998 enfrentaron una crisis financiera que se evidenció en la liquidación de 14 entidades, en la exigencia de capitalización a 16 entidades financieras, en el diseño de una línea especial de capitalización con recursos del gobierno a la cual accedieron 11 entidades financieras y en la disminución acelerada del número de entidades al pasar de 129 en 1997 a 58 en junio de 2004[34]. En lo relacionado con las entidades liquidadas, la principal causa de la liquidación estuvo relacionada con problemas de riesgo de crédito. No obstante, algunas también registraban deficiencias en la administración del riesgo operacional.

[34] BERMÚDEZ SALGAR Jorge - Delegado para Intermediación Tres de la Superintendencia Bancaria. El SARC: Un Cambio Cultural. Julio de 2003. El contenido del artículo es responsabilidad de la autor y no compromete a la Superintendencia Bancaria.

Tabla 3. Entidades liquidadas en Colombia crisis de 1998. Principales causas de liquidación[35].

Entidad	Causas	
	Relacionadas con riesgo de crédito y mercado	**Relacionadas con riesgo operacional**
1. Corporación financiera de Occidente	Deterioro calidad de cartera y de margen financiero	
2. Banco del Pacífico	Deterioro calidad de activos y margen financiero Problemas de liquidez	Incumplimiento reiterado de los requerimientos de Superbancaria sobre calificación de cartera y provisiones
3. Corporación Financiera del Pacífico		Realización de operaciones no autorizadas[36]
4. B. Andino	Deterioro calidad de activos y de liquidez	Inadecuada evaluación de clientes de crédito Prácticas inadecuadas de renovaciones y reestructuraciones desatendiendo la normatividad Calificación de cartera ineficiente Incumplimiento reiterado de las disposiciones de calificación de cartera y valoración de inversiones
5. CFC Findesarrollo	Deterioro calidad de activos y de liquidez	
6. Leasing Selfin	Deterioro calidad de activos y de liquidez	
7. Banco Selfin	Deterioro de liquidez	
8. CFC Banco del Pacífico	Deterioro calidad de activos, liquidez y rentabilidad	
9. CFC Bermudez y Valenzuela	Deterioro calidad de activos Deficientes indicadores de eficiencia	
10. L. Cauca	Deterioro de rentabilidad y solvencia	
11. Leasing Patrimonio	Deterioro de calidad de activos y de liquidez	

En varias entidades liquidadas se evidenció la presencia de fallas en los controles internos y externos, prácticas inseguras que comprometieron los intereses de las instituciones, falta de transparencia en la información, entre otros, factores relacionados con riesgo operacional.

[35] Tomado de las resoluciones de liquidación de cada una de las entidades.
[36] Descuento de títulos a cargo de los extrabajadores de Foncolpuertos.

Ante las graves consecuencias de la crisis, la Superintendencia Bancaria orientó todos sus esfuerzos hacia el fortalecimiento del manejo del riesgo en los intermediarios, a través de la modernización no solo de las normas sino de los sistemas de supervisión, buscando principalmente generar una mejor cultura de riesgo en los vigilados.

2.2 Administración de riesgos en Colombia

"La autoridad de supervisión colombiana ha seguido muy de cerca los planteamientos del Comité de Basilea expuestos en el Acuerdo de 1988. Se han implementado las principales directrices en lo que tiene que ver con márgenes de solvencia, cupos individuales de crédito, riesgo de mercado, de liquidez y aspectos relacionados con el gobierno corporativo en las diferentes actividades que desarrollan los intermediarios financieros"[37].

En concordancia con lo anterior es posible afirmar que desde hace más de diez años, la Superintendencia Bancaria de Colombia ha implementado una serie de normas cuyo objetivo principal es posicionar a la administración de riesgos como un elemento fundamental para el desarrollo de la actividad de intermediación. Gracias a las iniciativas del ente regulador colombiano, el sistema financiero es uno de los más avanzados de Latinoamérica en la implementación de las mejores prácticas internacionales en el tema de administración de riesgos.

Dentro de este contexto, se destacan los grandes avances en el tema de riesgo de crédito y en menor proporción, pero no menos importantes, los de riesgo de mercado. La normatividad relacionada con la administración de estos riesgos desarrollada en Colombia se fundamenta en el diseño e implementación de sistemas integrales de administración de riesgos. El sistema de administración de riesgo crediticio (SARC) y de riesgo de mercado (SEARM) exigieron a las entidades generar una mayor cultura de riesgo, asimilar la administración de riesgos como un mecanismo integral y generar un mayor fundamento técnico en las áreas de riesgos. Aunque en el tema específico de riesgo operacional aún no existe normatividad, algunos lineamientos presentados en los sistemas de administración de los otros tipos de riesgos se constituyen en un avance en el momento en el que se pretenda implementar un sistema de administración de riesgo operacional. Sin embargo, es importante tener en cuenta que estos avances son parciales y aislados, ya que solamente están relacionados con algunas áreas de la entidad. Además del SARC y el SEARM existen exigencias

[37] LEÓN OTERO Ricardo. Nuevo acuerdo de Basilea: Aspectos críticos y desafíos para su implementación en Colombia. II Congreso de Riesgo Financiero. Cartagena de Indias, agosto 1 de 2003. Pagina 3. Las opiniones expresadas por el autor de este artículo no comprometen el pensamiento de la Superintendencia Bancaria.

específicas frente al manejo del gobierno corporativo de cada entidad, las cuales tienen relación con la administración del riesgo operacional.

Las entidades de capital extranjero, ya están realizando adelantos en el tema de riesgo operacional, apoyadas en los lineamientos de la casa matriz. Así mismo, algunas entidades nacionales están incursionando en el tema concentrando los esfuerzos en la recopilación de datos que permitan identificar eventos generadores de pérdida por efecto del riesgo operacional. A pesar de estos avances, el tema aún tiene poco desarrollo en Colombia y se espera que en el mediano plazo, la Superintendencia Bancaria emita algunos requerimientos específicos con el fin de incentivar el interés de las entidades financieras en este tipo de riesgo.

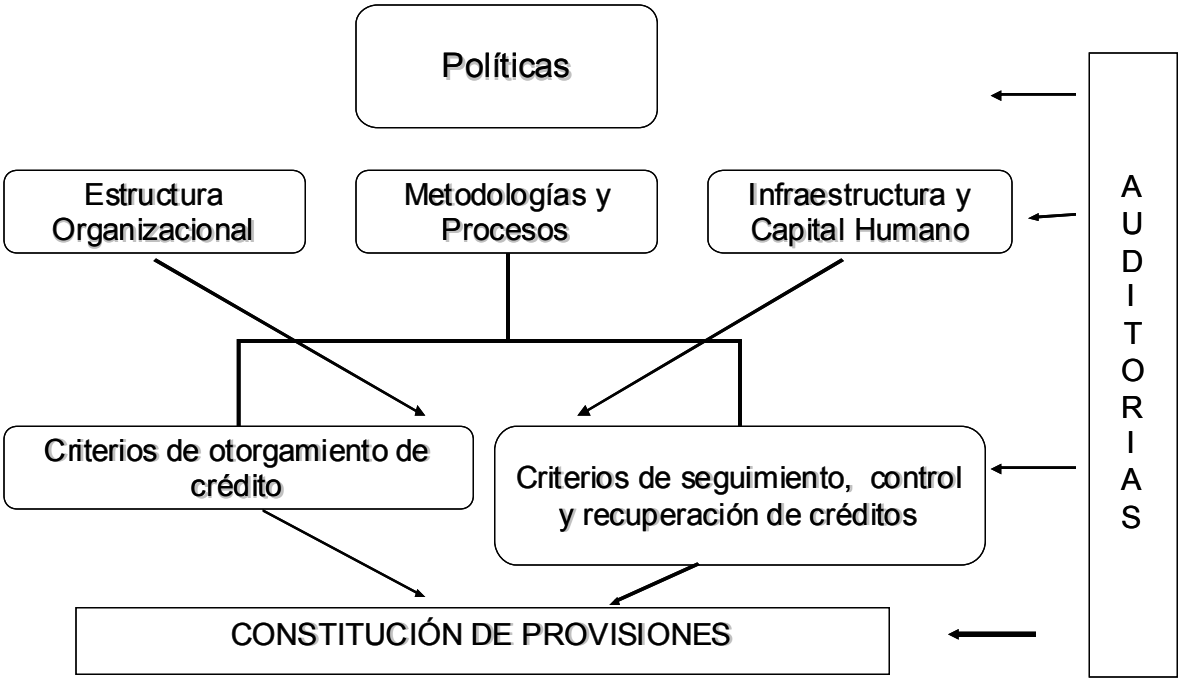
Aunque en la normatividad de riesgo de crédito y de mercado se mencionan algunos aspectos de riesgo operacional, en general el avance y la concientización de la importancia de ese riesgo en Colombia son mínimos. Los avances se limitan a mencionar algunos temas pero no existe un proceso definido para la identificación y control de estos riesgos y mucho menos para su medición.

2.2.1 Administración de riesgo de crédito (SARC)

En mayo de 2002, la Superintendencia Bancaria de Colombia expidió la Carta Circular Externa 11 y la Carta Circular 31 de marzo de 2002 con las cuales modificó radicalmente la gestión de riesgo de crédito de las entidades financieras en Colombia. A través de estas circulares, la Superintendencia Bancaria exige a las entidades financieras implementar en un determinado plazo un sistema de administración de riesgo crediticio (SARC) buscando fortalecer el autocontrol y la adecuada medición y control de riesgos. Es importante destacar la importancia que la Circular 11 otorga a la administración de riesgos. "el pilar fundamental de la supervisión bancaria está en la gestión interna de riesgo"[38]. Para la implementación de dicho sistema se definieron tres fases cada una de ellas con una fecha de finalización. El desarrollo del sistema debería terminarse en diciembre de 2003, no obstante esta fecha fue modificada[39].

El general, el sistema estaba conformado por los siguientes elementos: políticas, procedimientos, metodologías y mecanismos de control interno.

[38] Carta Circular Externa 11 de 2002 de la Superintendencia Bancaria.
[39] En diciembre 30 de 2004, la Superintendencia Bancaria a través de la circular externa 052 determinó que en junio de 2006 todas las entidades deberán calcular las provisiones a través del modelo propio y del modelo estándar que será publicado por la Superintendencia Bancaria. A partir de esta fecha las entidades pueden solicitar al ente regulador la aprobación del modelo propio.



Fuente: Carta Circular 31 de 2002. Superintendencia Bancaria.

La implementación de este sistema generó grandes cambios en la administración de riesgo de crédito entre los que se destacan, un cambio cultural frente a la administración de riesgo, una visión de riesgo como un sistema integral en el que participa toda la organización, una mejor definición de responsabilidades, el compromiso de la alta gerencia, la mayor conciencia del concepto riesgo-rentabilidad, la evolución de las entidades hacia un manejo más técnico del riesgo y la constitución de provisiones basadas en posibles hechos futuros.

Adicionalmente, la implementación del SARC requirió una definición por parte de cada entidad del "apetito de riesgo" de acuerdo con el cual se determina que tipo de mercados o productos son de interés. Así mismo, el desarrollo de los modelos propios de estimación de pérdida esperada, exige que las entidades cuenten con una amplia base de datos del comportamiento crediticio de los deudores[40].

En los dos últimos años, todas las entidades financieras colombianas concentraron los esfuerzos en el desarrollo de las exigencias del SARC. Este hecho ayuda en gran medida a preparar el terreno para una próxima implementación de un sistema de riesgo operacional, ya que las entidades están familiarizadas con el proceso y ya han desarrollado una mayor cultura de riesgo.

[40] BERMÚDEZ SALGAR Jorge - Delegado para la Intermediación Financiera Tres de la Superintendencia Bancaria. Tomado del artículo: El SARC: un cambio cultural escrito por 80 años Superintendencia Bancaria de Colombia. Las opiniones expresadas por el autor de este artículo no comprometen el pensamiento de la Superintendencia Bancaria. julio de 2003.

Es así como los temas de políticas, compromiso de la alta gerencia, procedimientos, bases de datos y modelos propios son temas comunes para el riesgo de crédito, riesgo de mercado y en el futuro para la implementación de un sistema de riesgo operacional.

2.2.2 Administración de riesgo de mercado

Al igual que con el manejo del riesgo de crédito, desde hace varios años, la Superintendencia Bancaria trata de adoptar las prácticas internacionales, lineamientos de Basilea, en lo relacionado con la administración del riesgo de mercado. En el artículo publicado por Esperanza Hernández Avendaño "Esquemas de Supervisión por Riesgos: El caso Colombiano[41]" la autora presenta un recorrido general a través de las normas que regulan el riesgo de mercado. Es así como en 1996, el ente regulador expidió la Resolución 1 de 1996 relacionada con metodologías de medición de los gaps de liquidez, tasa de interés y tasa de cambio. En el año 2000, expidió la Circular 88 en la cual se establecen los requisitos mínimos de administración de riesgos que deben tener las entidades financieras para realizar sus operacionales de tesorería, a la vez que introdujo algunos conceptos del buen gobierno corporativo, en concordancia con los lineamientos de Basilea. En septiembre de 2001 se expidió la Circular 42 sobre la medición de riesgo de mercado. Adicionalmente, se estableció el cálculo de un VAR por riesgo de merado y se incorporó este valor en el cálculo del patrimonio mínimo exigido. En agosto de 2002 se expidió la Circular 33, en la cual se modifican los lineamientos sobre clasificación, valoración y contabilización de inversiones.

Complementado las normas presentadas por Esperanza Hernández, en el año 2004, a través de la Circular externa 31, se modificaron las reglas aplicables a la gestión de riesgos de mercado y se presento el tema de una manera más integral a través de la presentación y exigencia en las entidades de un Sistema Especial de Administración de Riegos (SEARM), el cual comprende varios aspectos. Entre los principales aspectos a tener en cuenta están: determinación de políticas, definición de procesos, diseño e implementación de metodologías de medición de riesgo y establecimiento de controles. Debido a que varios de estos aspectos ya eran exigencias realizadas por en ente regulador en normatividad anterior, la Superintendencia Bancaria exigió que el SEARM entrara en funcionamiento desde la fecha en la cual se expidió la Circular (agosto 9 de 2004).

[41] Esperanza Hernández Avendaño. Directora de Intermediación Financiera uno de la Superintendencia Bancaria. Esquema de Supervisión por Riesgos: El caso Colombiano: julio de 2003. El contenido del artículo es responsabilidad de la autora y no compromete a la Superintendencia Bancaria.

Bajo este nuevo requerimiento las entidades tendrán que desarrollar un sistema integral de administración de riesgos y no contar únicamente con diferentes mediciones y estimaciones aisladas que no permiten a la entidad dimensionar la medida real del riesgo que podría enfrentar. Al igual que con el SARC, la implementación del SEARM permitirá a las entidades avanzar en mayor la manera de desarrollar un sistema de riesgo y contribuirá con el mayor desarrollo de una cultura de riesgo.

2.2.3 Administración de riesgo operacional

En lo relacionado específicamente con el riesgo operacional, algunos requerimientos de SARC y el SEARM contribuyen con una mejor administración de riesgo operacional, como por ejemplo:

Procesos
Revisión detallada de procesos y documentación de los mismos.
Conocimiento del proceso por parte de los involucrados.

Personas
Separación de funciones entre back, middle y front office.
Clara asignación de atribuciones y responsabilidades.
Permanente control de la alta dirección.
Revisión de criterios de selección de personal.
Actividades permanentes de capacitación.

Sistemas
Almacenamiento de datos en aplicativos más seguros.
Desarrollo de programas que permitan operar en línea con todos los aplicativos.
Accesos restringidos a los aplicativos.
Existencia de copias de seguridad.

Eventos externos
Ninguna

Adicionalmente, la a Superintendencia de Colombia ha evidenciado su interés en algunos temas relacionados riesgo operacional, a través de sus pronunciamientos sobre gobierno corporativo:

- En el año 2003, a través de la Circular 7 impartió instrucciones acerca de la composición de las Juntas Directivas, posesión de los oficiales de cumplimiento y exigencia de la designación de un defensor del cliente.
- En la Ley 795 de 2003 menciona las reglas de conducta y obligaciones legales de las entidades vigiladas, de sus administradores, directores, representantes

legales, revisores fiscales y funcionarios[42]. Este artículo enumera las actividades prohibidas para los funcionarios enumerados anteriormente, entre estas se encuentra: exceder los límites legales de riesgo, realizar negocios con personas vinculadas excediendo los límites legales, no suministra la información adecuada al público o a los clientes, no llevar la contabilidad de acuerdo con las normas, utilizar indebidamente o divulgar información sujeta a reserva, entre otras.

- En el artículo 200 de la Ley 222 de 1995 se menciona que los administradores responderán solidaria e ilimitadamente de los perjuicios que por dolo o culpa ocasionen en la sociedad a los socios o terceros.
- En la Circular Externa 14 de 1998 de la Superintendencia Bancaria[43] relacionada con valoración y contabilización de derivados se exige que las entidades adopten los controles internos que les permita administrar los riesgos propios de estas operaciones (establecimiento de políticas, límites, procedimientos y programa de seguimiento), existencia de un área independiente que controle el cumplimiento de límites de estas operaciones, existencia de un manual de ética
- En la Circular 88 de 2000 de la Superintendencia Bancaria[44] referente a parámetros mínimos que deben cumplir las entidades vigiladas para la realización de las operaciones de tesorería se mencionan algunos aspectos de riesgo operacional. Entre los principales temas que trata se destacan: la responsabilidad de la Junta Directiva y la Gerencia, el establecimiento de límites, las exigencias para desarrollar nuevos mercados y nuevos productos, responsabilidades y reportes de control de riesgos, los requisitos del sistema de control y gestión de riesgos, entre otros. Esta Circular menciona específicamente el riesgo operacional abordando entre otros temas: líneas de autoridad y procedimientos claros, independencia de funciones, existencia documentada de procedimientos de negociación, medición y control de las operaciones y divulgación de los riesgos, correspondencia entre el soporte tecnológico y la complejidad y volumen de las operaciones, adecuado registro y documentación de las operaciones, existencia de planes de contingencia ante eventuales fallas de los sistemas, planes de contingencia ante excesos de límites y formalización de operaciones a través de contratos.

Sin perjuicio de los avances que genera la implementación del SARC y el SEARM en algunos temas de riesgo operacional es importante tener en cuenta que mientras no se cree una conciencia clara de la importancia de la administración de riesgo operacional, los avances serán aislados y el logro de los objetivos principales de este sistema, mejorar eficiencia y rentabilidad y minimizar pérdidas, serán difícilmente alcanzables.

[42] RÉGIMEN FINANCIERO Y CAMBIARIO. Agosto de 2003. Parágrafo 1601.
[43] RÉGIMEN FINANCIERO Y CAMBIARIO. Parágrafo 14157 - 14165
[44] RÉGIMEN FINANCIERO Y CAMBIARIO. Parágrafo 14236 – 14256.

Teniendo en cuenta que actualmente la Superintendencia Bancaria está concentrada en la implementación del SARC, y que aún faltan algunas etapas importantes por culminar y ajustar, es muy probable que las exigencias frente al riesgo operacional no se presenten en el corto plazo. Esta afirmación es confirmada por el pronunciamiento del Superintendente Bancario en el II Congreso de Riesgo Financiero "Finalmente, y para responder otra inquietud formulada en este muy importante foro me permito recordar que cada día trae su afán, y que se dice que el tiempo se venga de las cosas que se hacen sin su concurso. Por eso sólo una vez que se haya consolidado el sistema SARC comenzará la Superintendencia a abordar con todo rigor y contando de antemano con los mejores aportes de la entidades vigiladas, la medición y prevención de riesgos operativos y tecnológicos"[45] Sin embargo, las entidades que avancen en los temas de riesgo operacional, por lo menos en la recolección de los datos, tendrán una ventaja competitiva importante y difícilmente igualable por las otras entidades, en el momento de la implementación de este sistema.

2.3 Posible impacto de la incorporación del riesgo operacional en el cálculo de solvencia para el sistema financiero colombiano

A diciembre de 2003, en Colombia existían 28 entidades bancarias cuyos activos totales ascendían a COP 84.9 billones. Aunque la Superintendencia Bancaria aún no se ha pronunciado frente a los requerimientos por riesgo operacional es posible realizar un cálculo preliminar siguiendo los lineamientos del Comité de Basilea.

El estudio realizado por María Cristina Ricardo Varela[46] estima el impacto que tendría en las instituciones bancarias colombianas, la incorporación del requerimiento de capital por riesgo operacional. En dicho estudio se estima el impacto del riesgo operacional en el cálculo del indicador a través del enfoque básico con un α del 15% que es el propuesto por Basilea y con α del 12.2% calculado con datos de bancos colombianos. Adicionalmente se estima el impacto a través del enfoque estándar utilizando los factores β propuestos por Basilea. En general los resultados de aplicar el enfoque básico o estándar son similares para la mayor parte de los bancos con excepción de las entidades especializadas en determinada línea de negocio.

[45] PINZÓN SÁNCHEZ Jorge. Asunción de Riesgos, deberes de los administradores de las entidades financieras y funciones del supervisor. Palabras del Superintendente Bancario, en el II Congreso de Riesgo Financiero. Cartagena, agosto 1 de 2003. Página 15.

[46] RICARDO VARELA María Cristina. Impacto de las Metodologías propuestas por el Comité de Basilea para el cálculo de los requerimientos de capital por riesgo operativo en el sector bancario colombiano. Tesis para optar el título de Ingeniera Industrial de la Universidad de los Andes. Enero de 2004.

En lo referente a la aplicación del enfoque básico, el cual es el que probablemente utilicen en principio la mayor parte de entidades por la facilidad de aplicación, utilizando un α del 15% y con cifras a diciembre de 2003, el requerimiento de capital por riesgo operacional para los bancos colombianos sería de COP 879.045 millones cifra superior a la reportada en diciembre de 2003 para el riesgo de mercado (COP 374.732 millones). Este requerimiento de capital se reflejaría en un cambio del margen de solvencia del grupo de entidades bancarias (utilizando la mediana) del 11.6% sin riesgo operacional al 10.1% con riesgo operacional. Adicionalmente, el estudio menciona que bajo este escenario, siete entidades bancarias registrarían un margen de solvencia inferior al mínimo legal exigido. Las entidades son: B. Bogotá (8.4%), B. Popular (8.1%), Lloysd TSB Bank (8.6%), B. de Occidente (8.4%), B. Superior (8.8%), Megabanco (8.8%) y B. Colmena (8.7%).

Frente a este resultado se puede afirmar que el impacto del riesgo operacional medido en el cálculo del margen de solvencia es alto, mayor que el del riesgo de mercado, más si se tiene en cuenta que varios bancos registran indicadores de solvencia cercanos al mínimo exigido (9%). Respecto a las entidades que registrarían un margen de solvencia menor al 9% con la incorporación del riesgo operacional se puede afirmar que algunas de estas entidades por política interna mantienen un margen de solvencia muy cercano al mínimo exigido con el fin de utilizar al máximo nivel el patrimonio para apalancar sus operaciones pero realizan inyecciones de capital en la medida en que se requiera (B. Bogotá, B. Occidente y B. Popular).

Por otra parte, es importante tener en cuenta que en el 2005, el sistema financiero colombiano adelanta un agresivo proceso de reacomodamiento que se reflejará en entidades de mayor tamaño tanto en activos como en patrimonio e ingresos. Es así como dos de los bancos que en el estudio quedaron con un indicador de solvencia menor al mínimo requerido adelantan procesos de fusión (B. Superior y B. Colmena)[47]. Por otra parte, el Lloysd Bank fue adquirido por el grupo financiero de Banco del Istmo y probablemente adecuará su capital a los nuevos requerimientos de su negocio. Dado el alto dinamismo relacionadas con fusiones y adquisiciones anunciadas en el 2005 es muy probable que los resultados del estudio realizado con cifras a 2003 cambien significativamente. Sin embargo, se debe destacar que sin importar cuales entidades en particular puedan registrar problemas de solvencia todas registrarán disminuciones importantes en este indicador, lo que unido a un periodo de alto crecimiento de operaciones podría generar importantes requerimientos de capital a varias entidades.

Estos resultados deberán constituirse en un motivador adicional para que las entidades bancarias colombianas inicien el proceso de desarrollo de un Sistema de Administración de Riesgo Operacional con miras a implementar metodologías

[47] Banco Superior fue adquirido por B. Davivienda y B. Colmena se fusionó con B. Caja Social.

avanzadas que se espera se reflejen en menores requerimientos de capital por riesgo operacional.

CAPITULO 3

3 Metodologías para la implementación de un sistema de administración de riesgo operacional

En la década de los ochenta, las entidades bancarias fueron pioneras en la administración del riesgo como respuesta a las pérdidas en que incurrieron por una deficiente gestión de riesgos. En esa época, las entidades financieras se concentraron en la administración de riesgo de crédito y mercado y desarrollaron estrategias para reducir el impacto negativo de estos riesgos en las utilidades. No obstante, a pesar de los controles implementados, algunas entidades continuaron registrado grandes pérdidas y detectaron que éstas eran generadas por elementos relacionados con riesgo operacional como errores en los procesos y en los sistemas y fallas en los controles[48].

De lo anterior es posible afirmar que las entidades financieras deberán identificar la administración del riesgo operacional como una herramienta generadora de valor. El principal objetivo de una entidad financiera al implementar un sistema integral de administración de riesgo operacional debe ser la generación de valor agregado, ya sea a través de menores costos por la optimización de los procesos, menores pérdidas, mejor servicio al cliente y/o mayor eficiencia.

Teniendo en cuenta que los documentos preliminares del acuerdo de Basilea II fueron publicados a partir de 1998, y que éstos ya incluían el tema de riesgo operacional, algunos autores y algunas entidades han desarrollado metodologías para la implementación del sistema de administración de riesgo operacional. Si bien existen algunas metodologías generales y otras detalladas, todas presentan aspectos comunes relacionados con: la definición de políticas, la identificación de riesgos y controles y la medición y modelación de dichos riesgos. A continuación se presentará en forma resumida tres metodologías que pueden ser utilizadas como guía para la implementación de un sistema de administración del riesgo operacional. Posteriormente se presentará la propuesta metodológica que será utilizada en este trabajo.

[48] KING Jack L. Operacional Risk. Pagina 3. Editorial John Wiley & Sons Ltda. 2001.

3.1 Metodología de King[49]

King inicia su propuesta afirmando que el riesgo operacional está relacionado con la desviación adversa del desempeño de la firma debido a cómo opera la firma y no a cómo se financia la firma. Por lo anterior, la administración del riesgo operacional se debe concentrar en los principales procesos generadores de valor y buscar responder a la pregunta: ¿cuáles son las causas que generan la volatilidad en las operaciones fundamentales de la entidad?

De acuerdo con la propuesta de King, la administración del riesgo operacional se fundamenta en tres aspectos:

- Implementación de lineamientos de gobierno corporativo
- Definición de controles operacionales
- Medición del riesgo operacional

3.1.1. Implementación de lineamientos de gobierno corporativo

Los lineamientos de gobierno corporativo inician por la determinación de los objetivos de riesgo, es decir por definir "el apetito de riesgo" de la entidad. Los objetivos generalmente se determinan subjetivamente pero paralelamente se deben diseñar medidas para controlar el logro de los mismos.

3.1.2. Definición de controles operacionales

La definición de los controles es inherente a la identificación de los riesgos y busca asegurar el cumplimiento de los objetivos propuestos. Jack King presenta tres posibles formas de implementar los controles: la primera es a través de la identificación de relaciones causa efecto de los riesgos, la segunda utiliza datos estadísticos cuando no es posible determinar la relación causa efecto y la tercera utiliza escenarios evidenciando los riesgos que podría enfrentar la entidad.

3.1.3. Medición del riesgo operacional

De acuerdo con la metodología propuesta por King, para la medición del riesgo operacional se requiere la identificación del modelo del negocio y un conjunto de asunciones de la relación entre los indicadores de riesgo operacional y los de desempeño. La medición se concentra en la estimación de las posibles variaciones entre el desempeño esperado y el obtenido, generadas por riesgo

[49] Idem.

operacional. El autor afirma que existen dos fuentes de riesgo operacional: variaciones en las actividades del proceso y presencia de eventos extremos. Las primeras generan desviaciones pequeñas y son parte de la operación de la firma. Los segundos se presentan rara vez pero generan grandes desviaciones del desempeño de la firma. Así mismo, afirma que los riesgos pueden clasificarse en riesgos con causas controlables y riesgos con causas incontrolables. No obstante, los dos pueden mitigarse.

Para la medición del riesgo operacional, el autor sugiere diseñar:
- La estructura de medición
- La metodología de medición
- Los modelos predictivos

3.1.3.1. Estructura de medición

La estructura de medición busca alinear las medidas de riesgo con las de desempeño de la entidad. Esta estructura deberá contener las definiciones básicas, las metas, las asunciones utilizadas para la medición del riesgo operacional. Esta estructura servirá de base para la implementación de los indicadores de medición en todas las unidades de negocio.

De acuerdo con el autor, una estructura efectiva deberá permitir:
- Identificar los riesgos importantes de la firma
- Clasificar los riesgos en controlables e incontrolables
- Identificar las causas de los riesgos controlables
- Asignar a los riesgos incontrolables posibles estrategias de mitigación
- Proveer medidas de retroalimentación sobre cambios en los riesgos que permitan a la administración tomar las respectivas acciones.

King presenta unos lineamientos generales para el diseño de la estructura de medición que incluye:
- Asunciones
- Definiciones
- Estructura de medición
- Modelo del negocio

Asunciones
El autor propone seis asunciones básicas, las cuales pueden disminuir o aumentar de acuerdo con cada entidad.

1. La administración del riesgo operacional beneficia a todo los

"Stakeholders[50]"

2. Un sistema de medición de riesgo operacional debe incluir las relaciones de causalidad de las operaciones de la firma con la volatilidad de las ganancias.
3. Una medida de riesgo operacional debe estar en capacidad de reflejar la variabilidad de las ganancias como resultado de pérdidas debido a errores u omisiones y controlar las caídas o los eventos ocasionales.
4. La cantidad de control en una firma está reflejada en la combinación de pérdidas controlables resultantes de errores y omisiones y de pérdidas incontrolables resultantes de excepciones, inoperancia de controles y eventos ocasionales.
5. Las pérdidas operacionales son el resultado de factores de causalidad en las actividades del proceso que adicionan valor y su predicción requiere una técnica que incorpore este factor en el modelo.
6. Las pérdidas excesivas resultan de eventos esporádicos y caída de controles y no están relacionados con factores de causalidad de las actividades de los procesos que agregan valor. Éstas deben ser analizadas usando un enfoque que combina eventos internos actuales, eventos externos y errores cercanos en escenarios probables de eventos extremos.

Definiciones

King sugiere que se presente una serie de definiciones básicas que permitan a la organización tener una efectiva comunicación en lo relacionado con el sistema de medición de riesgo operacional. Entre otros aspectos define: factores de causalidad, factores de riesgo, procesos de adición de valor, pérdidas, ganancias, pérdidas controlables, pérdidas incontrolables, fallas de controles, entre otras.

Estructura para la medición del riesgo operacional

La estructura propuesta por King combina un enfoque de modelo de negocio con una metodología de medición. El modelo de negocio define las unidades de análisis y los factores a medir y la metodología de medición provee la forma de calcular la medida de riesgo.

El modelo de negocio

Este modelo utiliza los procesos que agregan valor en cada una de las unidades de negocios como las unidades de análisis para medir el riesgo operacional. Cada unidad de negocio tiene la obligación de reportar ganancias y pérdidas, al igual que los procesos que la integran. Para cada proceso que agrega valor se identifican factores de riesgo bajo el análisis de causalidad.

King menciona que la metodología sólo permite incorporar las pérdidas asignables ya que éstas están relacionadas con un factor de riesgo. Estas pérdidas generadas por factores de riesgo son relacionadas a las ganancias a través de

[50] Todas las partes relacionadas con la organización: accionistas, empleados, proveedores, clientes, etc.

una función de ganancias. A las pérdidas no asignables, generalmente de baja ocurrencia pero de alto impacto, no se les puede asociar un factor de riesgo debido a que este es desconocido o depende de un evento externo. Por lo tanto no tienen una función de pérdidas asignada, pero el modelo las tiene en cuenta a través de la adición de fuentes de pérdidas no explicables por factores de riesgo.

3.1.3.2. Metodología de medición

La metodología de medición debe estar en capacidad de medir dos fuentes de riesgo operacional: variaciones en el proceso y eventos extremos. El autor presenta la metodología Delta – EVT^{TM} que permite medir riesgo operacional generado por las dos fuentes y es el resultado de la combinación de dos metodologías[51]. La metodología Delta se utiliza para determinar pérdidas generadas en el proceso por los factores de riesgo (pérdidas asignables) y la metodología EVT para determinar grandes pérdidas generadas por eventos extremos (pérdidas no asignables). Para la utilización de estas metodologías se debe definir el umbral a partir del cual se deberá utilizar una u otra metodología. Esta metodología se presenta en detalle en el libro Operational Risk de Jack King, pero a continuación se presenta un breve resumen de la misma.

La metodología Delta que asume que las utilidades son una función de factores causales que pueden ser constantes y variables, siendo los variables los factores de riesgo. A través de esta metodología la función de utilidad se sensibiliza de acuerdo con cambios en el factor de riesgo para generar la distribución de pérdidas en cada línea de negocio. Para la aplicación de esta metodología se deben seguir los siguientes pasos:

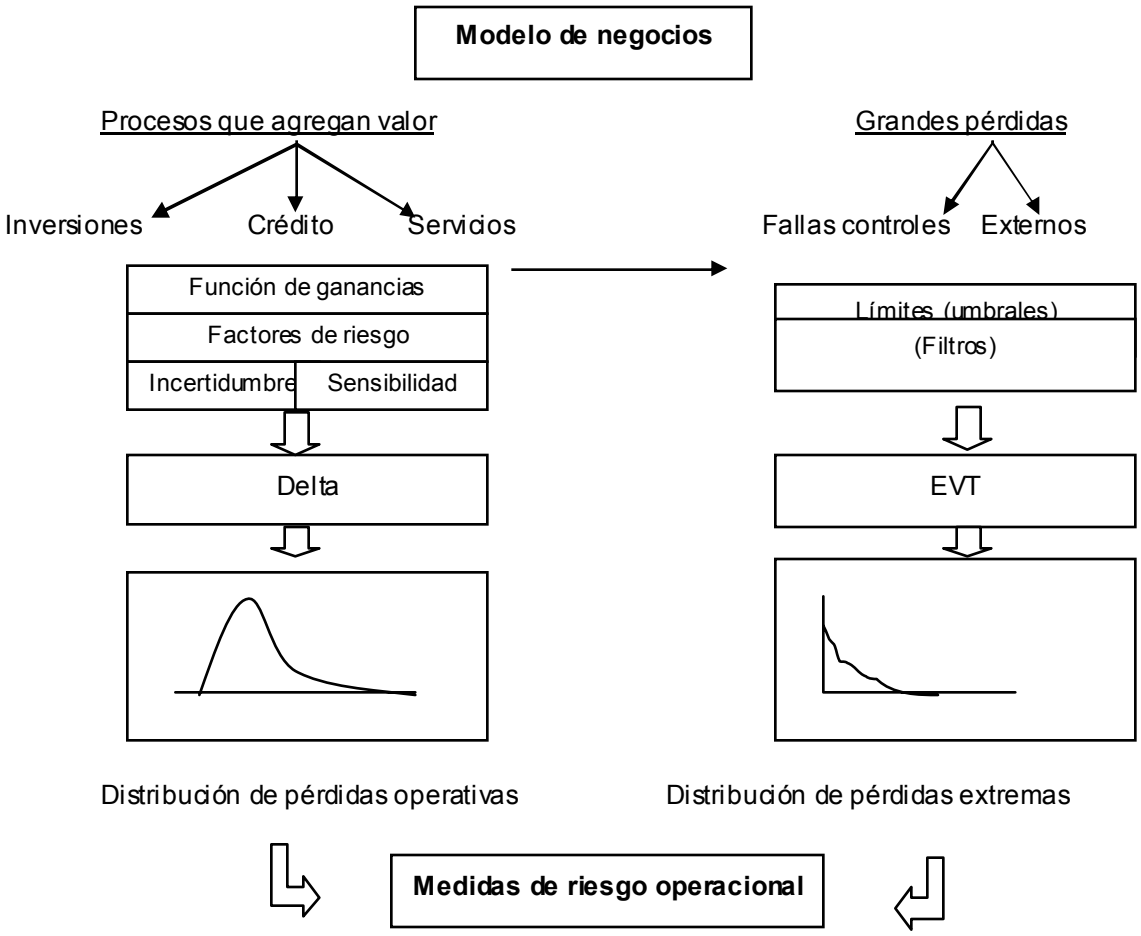
- Identificar los principales factores de riesgo que afectan las utilidades y los factores de volatilidad de los mismos (varianza esperada de un determinado grupo de errores).
- Determinar la función de utilidad que relaciona cada factor de riesgo con las utilidades y la sensibilidad de las utilidades a cada factor.
- Calcular y combinar las medidas de incertidumbre para riesgo operacional.

Esta metodología presenta ventajas en la medición de riesgo operacional ya que puede estimar el comportamiento de las utilidades (pérdidas) frente a la ocurrencia de determinados factores de riesgo, aún sin que estos se encuentren presentes en los datos históricos. Adicionalmente, permite relacionar el riesgo operacional directamente con el comportamiento de las líneas del negocio, a través de la sensibilización. La principal limitante es que sólo puede ser usada para riesgos asignables y no aplica para eventos extremos.

[51] Ver detalle de la metodología en el libro de Jack King " Operacional Risk", capítulos 5, 6 y 7.

Para el tratamiento de eventos extremos se utiliza la metodología EVT (Extrema Value Theory) que mide la severidad de los eventos extremos y extrapola el impacto de los mismos en largos periodos. La metodología utiliza los datos de pérdidas para construir un modelo de distribución de pérdidas separando la severidad de la frecuencia. Las distribuciones de la severidad y de frecuencia son combinadas en una simulación de Montecarlo para generar la distribución de pérdidas excesivas. Los datos requeridos para esta metodología se pueden obtener de datos históricos, externos, estimados, escenarios o simulaciones. Esta distribución junto con la distribución de pérdidas de la operación del método Delta se utilizan para determinar el valor del riesgo operacional.

King presenta un resumen de la metodología de implementación de la estructura de medición de riesgo operacional a través del siguiente diagrama:



Fuente: Operacional Risk. Jack King. Pag.66

3.1.3.3. El desarrollo de modelos predictivos

King afirma que los modelos son utilizados para predecir y tomar acciones. Los modelos causales utilizados para medir riesgo operacional permiten tener un enlace entre las fluctuaciones en el desempeño y sus causas. El conocimiento de las causas del riesgo es esencial para tomar acciones apropiadas para controlar y manejar el riesgo. El autor sugiere que con el fin de realizar modelos de predicción, el impacto en las operaciones debe ser separado en riesgo controlable e incontrolable. El riesgo controlable es aquel que tiene identificadas las causas y éstas causas pueden ser modificadas. El riesgo incontrolable es aquel que no tiene un factor causal que pueda ser influenciadas y el impacto de este riesgo debe ser determinado a través de modelos de pérdidas. El tener en cuenta la causalidad permite la administración adecuada del riesgo operacional.

La metodología propuesta por King brinda una serie de herramientas técnicas para la implementación de un sistema de riesgo operacional y presenta una guía detallada de la implementación de la misma. Esta metodología se caracteriza por el sólido fundamento técnico que ofrece para la medición y el desarrollo de modelos para la estimación de las posibles pérdidas generadas por riesgo operacional.

3.2 Metodología de KPMG[52]

Como resultado del trabajo continuo con entidades financieras, especialmente con entidades que operan en países desarrollados, la firma de consultaría y auditoria KPMG desarrolló un esquema detallado para la implementación de un sistema de administración de riesgo operacional.

[52] KPMG. FINANCIAL SERVICES. Basel II – A Closer Look: Managing Operacional Risk. Pag 12 – 21.

3.2.1. Elementos del proceso de administración de riesgo operacional

Fuente: KPMG, 2003

Los componentes de la estructura de administración de riesgo operacional propuesta por KPMG son:

3.2.1.1. Estrategia de riesgo

Al igual que para la administración de riesgo de crédito y riesgo de mercado, los organismos de dirección deberán emitir unas políticas generales que reflejen la tolerancia al riesgo operacional de la entidad. La tolerancia al riesgo está relacionada con la estrategia de la entidad frente a este tema y se busca que todas las unidades de negocio funcionen de acuerdo con esta estrategia. La Junta Directiva deberá establecer los límites máximos de riesgo tolerables. Teniendo en cuenta que la cuantificación de este riesgo aún es limitada, la tarea de establecer límites es compleja. Generalmente, las entidades establecen límites aplicando umbrales por unidades de negocio de acuerdo con la información disponible (estimaciones de riesgo, reportes de control, indicadores claves de riesgo y reportes de los incidentes de riesgo operacional o pérdidas).

3.2.1.2. Estructura organizacional

El banco debe asignar roles y responsabilidades para las distintas unidades de negocio, funciones e individuos. Dos grandes objetivos clave deben ser alcanzados en una estructura de riesgo operacional:

1. El manejo del riesgo operacional no puede ser restringido a una unidad organizacional específica (como el riesgo de mercado) sino que la mayor responsabilidad está en los administradores y se apoya en áreas de soporte.
2. Se recomienda crear un área independiente para la administración de riesgo, distinta a la auditoria interna, que coordine la información que envíen los diferentes administradores de la entidad y las áreas de soporte.

La estructura organizacional también comprende líneas de reporte, tanto a nivel de toda la entidad como en las unidades de negocio. La estructura organizacional une el desempeño de la administración de riesgo operacional con las unidades claves y las metas de desempeño del negocio. Se busca que los procesos, procedimientos y políticas estén totalmente alineados con la estrategia de riesgo operacional.

La experiencia ha mostrado que es importante el tratamiento del riesgo por funciones especializadas y la existencia de un Comité de Riesgo Operacional que podría pertenecer a un Comité de Administración Integral del Riesgo.

3.2.1.3. Reportes

Debido a que el riesgo operacional afecta a todas las unidades de negocio, los reportes tienen alcance en toda la organización. Estos reportes deben cubrir dos aspectos:

1. Entrega de información relevante a la administración y a control de riesgo
2. Reportes de información agregada por categoría para la administración de líneas de negocio, la Junta y el Comité de riesgo.

El primero está relacionado con datos tales como pérdidas, equivocaciones recurrentes, indicadores y resultados de valoración de riesgo. El segundo refleja información agregada, estructurada y frecuentemente diseñada para proveer a cada nivel de administración lo que necesita para estar en capacidad de mejorar la administración de riesgo operacional.

Un ejemplo de los reportes que se deberían enviar a cada área es el siguiente:

Tabla 4. Reportes de riesgo operacional

Destinatario	Tipo de información recibida
Junta Directiva	Información agregada de las datos de pérdidas de todo el banco Valoración del riesgo y resultados de indicadores claves Capital económico y regulatorio Los reportes que se requieran en caso de mayores eventos
Comité de Administración de Riesgo Operacional	Información agregada de las datos de pérdidas de todo el banco Los reportes detallados que se requieran en caso de mayores eventos Valoración del riesgo y resultados de indicadores claves Capital económico y regulatorio
Líderes de las unidades de negocios	Información agregada de datos de pérdidas de la unidad correspondiente Valoración del riesgo y resultados de indicadores claves Capital económico y regulatorio Los reportes que se requieran en caso de mayores eventos
Unidad de Riesgos	Información detallada de datos de pérdidas de todo el Banco Valoración de Riesgo Indicadores claves de riesgo
Departamentos especializados	Información detallada de la respectiva área
Comité de Auditoria	Acorde con los actuales requerimientos de información
Unidad de auditoria interna	Acorde con los actuales requerimientos de información
Auditoria Externa	Acorde con los actuales requerimientos de información

Fuente: KPMG, 2003

3.2.1.4. Definiciones, uniones y estructura

Los bancos necesitan un lenguaje común para describir el riesgo operacional y los tipos de eventos de pérdida, las causas y los efectos. Ellos también necesitan el mapa de reglas necesarias para cumplir con los requerimientos regulatorios. El desarrollo de definiciones, uniones y estructuras permite al banco la identificación eficiente, valoración y reportes de los riesgos operacionales. Esto ayuda a clarificar el alcance del riesgo operacional y evita diferentes interpretaciones, también permite identificar subcategorías y límites con otros riesgos.

3.2.1.5. Datos de pérdidas

Una vez se ha establecido un lenguaje común en la entidad frente al riesgo operacional se requiere definir los procesos para recolección, evaluación, monitoreo y reporte de los datos que generan riesgo de pérdida operacional. Esta

será la herramienta para la lograr cuantificar los riesgos y lograr una buena estimación de la implicación de dichos riesgos. Si la entidad lo considera pertinente puede complementar los datos internos con bases de datos externas.

En la recolección de datos están involucradas todas las áreas del Banco. Los eventos que superen los límites establecidos necesitan se almacenados en una base de datos de pérdidas y ser verificados. Las políticas y los procedimientos establecidos son necesarios para ayudar a dar consistencia al proceso. Pérdidas definidas de baja frecuencia y alto impacto, dada su baja ocurrencia no van a contar con datos en la entidad y por lo tanto en este caso podría tomarse datos externos.

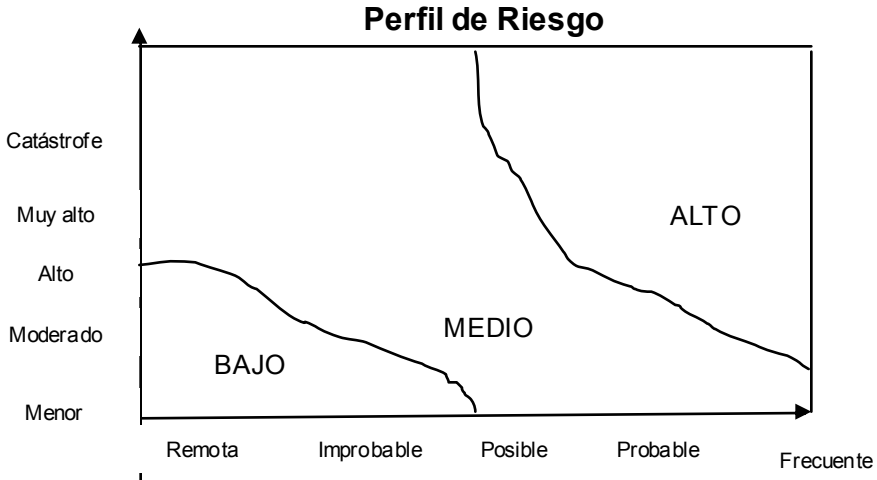
La disponibilidad y calidad de los datos son generalmente uno de los mayores problemas, debido a que hasta que la cultura de administración de riesgos no esté completamente arraigada, la colaboración de todos los funcionarios de la entidad no es óptima. Por lo tanto este proceso toma tiempo. Una vez se haya determinado la estructura del sistema de administración de riesgo operacional y se proceda a la recolección de los datos se presenta un tiempo de ajuste en el que la cantidad de errores puede disminuir o puede incrementarse, lo importante es analizar los resultados teniendo en cuenta que el sistema se está ajustando. También se debe tener en cuenta que en este proceso de implementación algunas pérdidas sólo se pueden detectar meses o años después de su ocurrencia.

Un proceso de recolección de datos internos deberá tener incentivos y controles que aseguren un alto grado de calidad y cobertura de los datos. Los datos internos deben ser complementados periódicamente con datos externos, los cuales deben ajustarse a la realidad de cada entidad.

3.2.1.6. Valoración del riesgo

La valoración del riesgo provee un enfoque cuantitativo para identificar los riesgos potenciales de naturaleza severa a través de la estructuración de escenarios en los cuales se representan todas las unidades de negocios. Esto ayuda a generar grados de sensibilidad frente a los riesgos y busca encontrar un equilibrio entre los datos históricos y los posibles riesgos futuros de la entidad.

La estructura básica de la valoración del riego operacional comprende: un conjunto de matrices de identificación y valoración del riesgo operacional y sus sub componentes en términos de probabilidad e impacto de ocurrencia, basado en un apetito por el riesgo definido. Esta valoración se puede presentar para toda la entidad o por área y también se puede incluir el valor del riesgo inherente a la operación versus el valor del riesgo una vez se ha mitigado y sólo queda el riesgo residual.



Fuente: KPMG. BAsel II. A Closer Look: Managing Operacional Risk. Pag-16.

3.2.1.7. Indicadores claves de riesgo

Estos indicadores permiten a la entidad conocer rápidamente la situación frente al riesgo operacional. Contienen señales de alerta de sistemas, procesos, productos, personas y aspectos externos.

Los indicadores líderes incluyen datos observables de pérdidas y no datos estimados de futuras pérdidas. Inicialmente es complejo determinar los indicadores líderes y mucho más establecer la correlación entre los mismos debido a la carencia de datos. De todas maneras las entidades inician con unos indicadores básicos. Buscando que la información sea de fácil comprensión y por lo tanto es importante que el número de indicadores sea limitado. Adicionalmente cada indicador debe incluir la urgencia de la acción a seguir dependiendo del nivel en el cual se ubique.

3.2.1.8. Mitigación

Una vez la entidad identificó y cuantificó los riesgos pueden diseñarse mecanismos de mitigación relacionados con políticas, procedimientos, sistemas y controles. Para esto es fundamental que la entidad haya definido la tolerancia al riesgo y frente a este limite se determina que porcentaje del riesgo se asume y cual se transfiere.

La mitigación de riesgo es totalmente interactiva y de avances, cuando una táctica es implementada otra debe ser revalorada. Para la determinación de las tácticas se debe tener presente la valoración costo beneficio y tener en cuenta que variar permanentemente estas tácticas puede afectar el desempeño de la entidad.

3.2.1.9. Modelación de capital requerido

Esta relacionado con el cálculo del capital económico requerido. Estos modelos requieren: la base de datos adecuada, una definición de medidas estadísticas y supuestos, la implementación del modelo y la validación del mismo.

En el enfoque de Basilea de 2004, se presentan varias alternativas, entre las que se encuentra la posibilidad de diseñar un modelos propios. El objetivo es estimar las pérdidas no esperadas, las cuales se deben tener en cuenta en el capital económico requerido legalmente a la entidad y también pueden tenerse en cuenta para la determinación del precio de los productos.

En los modelos de estimación de capital requerido la clave es la validación de los datos de entrada, de la estructura del modelo, de los supuestos y concentrar esfuerzos en la validación de los resultados.

3.2.1.10. Información tecnológica

Es la base y la facilitadora de la administración de riesgo operacional. Debe adecuarse para incorporar los datos, los controles y los indicadores requeridos y desarrollar las interfaces que se necesiten

3.2.2. Pasos para la implementación de un sistema de administración de riesgo operacional

Además de presentar los elementos del sistema, el documento elaborado por KPMG presenta en forma resumida los pasos requeridos para diseñar e implementar un sistema de riesgo operacional:

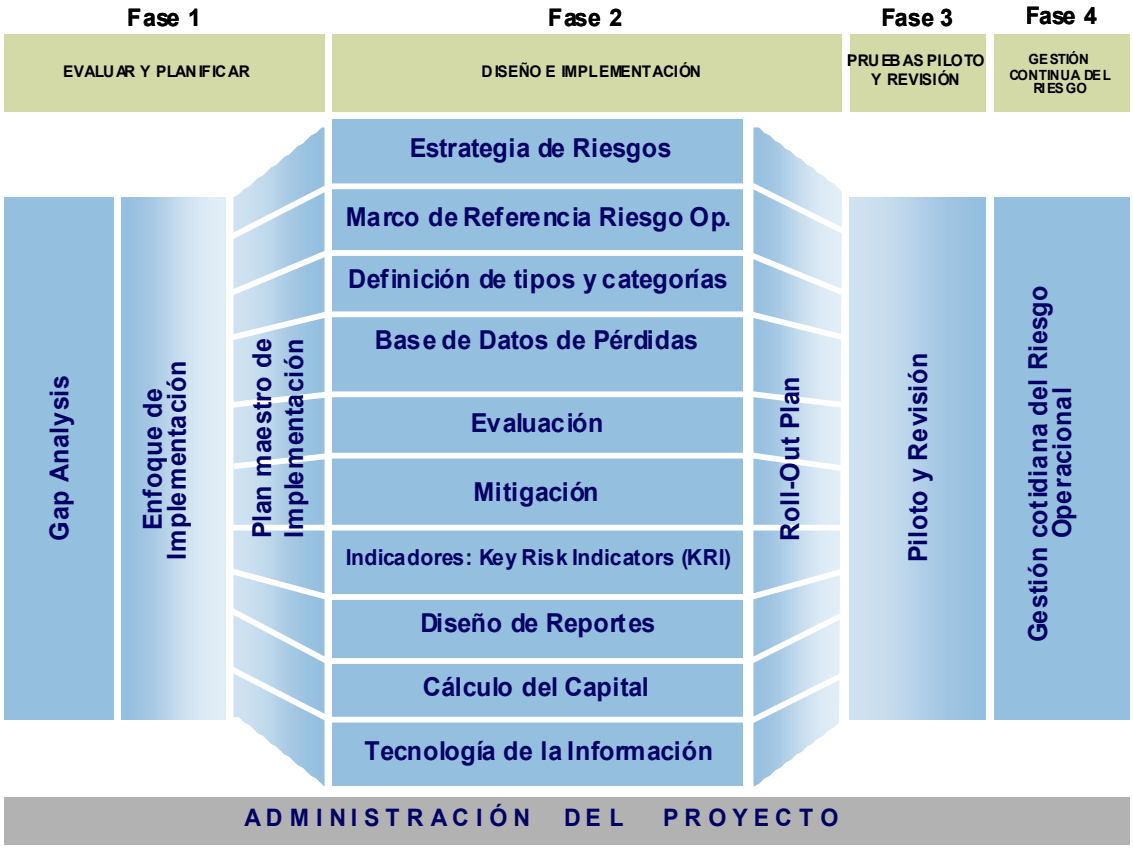
Fase I: es un análisis general de los riesgos operacionales que enfrenta la entidad. En esta fase la entidad puede analizar como está actualmente la administración de riesgo operacional y asignar las respectivas tareas y responsabilidades. Se puede revisar la estructura, contenido y criterios del enfoque de riesgo actual. También se debe revisar la frecuencia de los eventos de riesgo, la estructura de reportes y los límites actuales. El análisis de los indicadores de riesgo existentes y los procesos que soportan la recolección de datos también hacen parte de esta fase.

Fase II: La entidad puede establecer varios grupos para desarrollar aspectos específicos de riesgo operacional como: estructura organizacional, definiciones,

uniones y estructuras, recolección de datos, valoración de riesgo, indicadores líderes, reportes, modelos de capital requerido e información y tecnología. Estos grupos definen las necesidades de datos, diseñan estructuras organizacionales, procesos y sistemas, mejoran la administración de riesgo operacional y diseñan un plan. Desarrollar un plan lleva a los grupos a tener en cuenta la comunicación y entrenamiento.

FASE III: La entidad puede llevar a cabo una prueba piloto.

FASE IV: El sistema se retroalimenta tanto a través de la evaluación por parte de los directivos como a través de la comparación con exigencias legales.



Fuente: KPMG. BAsel II. A Closer Look: Managing Operacional Risk. Pag-20.

La duración de la implementación de un proyecto de riesgo operacional depende de la entidad pero en general puede tomar dos o más años.

Teniendo en cuenta que KPMG ofrece servicios de asesoría en el tema de riesgo operacional, el esquema sugerido por esta entidad es muy didáctico y detallado y

se constituye en una herramienta importante para una entidad que quiere incursionar en la administración de riesgo operacional. Sin embargo, y comparada con la metodología propuesta por King, éste esquema no profundiza en la herramientas técnicas de medición y modelación del riesgo.

3.3 Metodología de Fithratings Financial Institutions[53].

El análisis y calificación de riesgo de entidades financieras es una de las tareas realizadas por Fitchratings. Dentro de este análisis, la calificadora evalúa todos los riesgos a los que está expuesta la entidad, incluyendo los riesgos operacionales. De las evaluaciones realizadas a varias entidades financieras Fitch observó cómo cada entidad diseñaba e implementaba una estructura que le permitiría administrar el riesgo operacional. De acuerdo con estas observaciones Fitch presenta una metodología de diseño de un sistema de administración de riesgo operacional que contempla las siguientes etapas:

1) Definiciones básicas
2) Identificación
3) Estructura organizacional y cultura
4) Recolección de datos
5) Medición
6) Administración.

Adicionalmente, Fitch realizó una investigación de las experiencias que han tenido algunas entidades en la implementación de un sistema de riesgo operacional[54], cuyos resultados fueron utilizados para sugerir la metodología. Es esta investigación, la firma calificadora de riesgo estudio a los 42 mayores bancos a nivel mundial que se encuentran implementando el sistema de administración de riesgo operacional.

3.3.1 Definiciones básicas

Antes de iniciar el diseño del sistema de administración de riesgo operacional es de gran importancia que la entidad defina claramente a que se refiere cuando menciona riesgo operacional. Varias entidades adoptan la definición de Basilea II, sin embargo, cada entidad puede incluir los aspectos que considere convenientes.

El análisis realizado por Fitch evidenció que todas las entidades están orientando esfuerzos hacia el cumplimiento de los requerimientos de Basilea II. En este

[53] FITHRATINGS FINANCIAL INSTITUTIONS. Special Report. The Oldest Tal but the newest store: Operational risk and the evolution of its measurement Ander Basel II. Enero 7 de 2004. www.fitchratings.com

[54] FITHRATINGS FINANCIAL INSTITUTIONS. Special Report. Operacional Risk management & Basel II implementation: Survey results. Abril 21 de 2004. www.fitchratings.com

sentido estas entidades han logrado determinar límites entre el riesgo de crédito y operacional y han evolucionado conceptualmente en el tema. Varias entidades incluyeron en el riesgo operacional el riesgo reputacional y el riesgo estratégico, los cuales no se tienen en cuenta en el acuerdo de Basilea, debido a la dificultad de valoración de estos riesgos. Las entidades que involucraron estos riesgos buscan por ahora identificarlos para posteriormente determinar su cuantificación.

3.3.2 Identificación

Para la identificación de los riesgos las instituciones pueden utilizar las siguientes técnicas:

- Realizar la recolección, análisis y mapeo de los datos de pérdidas de riesgo operacional generados por fuentes internas y determinar la frecuencia y severidad de dichas pérdidas.
- Diseñar indicadores claves de riesgo derivados de agregar datos internos y de asignar valores límites, los cuales proveen un nivel del perfil de riesgo a la administración de la entidad.
- Utilizar scorecards que permiten trasladar las valoraciones cualitativas de las unidades de negocios en medidas cuantitativas.
- Implementar metodologías de auto valoración que recopilan la información de los empleados reflejando riesgos que están presentes en la organización.

Independientemente de la metodología que se utilice, lo importante es capturar el mayor número de riesgos a los que está expuesta la entidad y lograr incorporar factores de proyección de los mismos.

De acuerdo con el estudio realizado por la calificadora, todos los bancos analizados adoptaron una combinación de procedimientos para identificar los riesgos. El 65% de los bancos utilizaron autovaloración del riesgo[55] y el autocontrol y el 32.5% indicadores claves de riesgo[56] como las principales herramientas para identificar el riesgo operacional. Un 37.5% uso mapas de riesgo y un 10% scorecards como herramientas adicionales. Todas las entidades manifestaron interés en aumentar el uso de otras herramientas de identificación de riesgos. Fitch recomienda utilizar varias metodologías con el fin que el sistema puede identificar todos los generadores de riesgo.

[55] Para esta valoración se realizaron ejercicios con los administradores de las unidades de negocio y se les solicitó identificar todos los riesgos operacionales que éstos enfrentan. Esta metodología permitió integrar a toda la organización en el tema y otorgó gran responsabilidad a estos administradores por el monitoreo y administración del riesgo de su unidad.
[56] Este es un enfoque de alto nivel, a través los riesgos se identifican y se agrupan en grandes categorías y así permiten observar problemas que posiblemente no son visibles a nivel de unidades de negocios.

3.3.3 Estructura organizacional y cultura

Para la exitosa implementación del sistema se requiere que este haga parte de todo el sistema de administración de riesgo de la entidad. El sistema no tiene objetivos propios sino que refuerza los objetivos de cada unidad de negocio. El sistema requiere el apoyo y compromiso de la alta gerencia y de todas y cada una de las áreas del negocio.

Adicionalmente es importante crear una cultura de riesgo operacional, que logre que el tema esté presente en las conversaciones cotidianas de los empleados y que permita a dichos empleados informar sobre todos los problemas presentados por riesgo operacional y no ha esconder dichos problemas a la administración. En este proceso es importante la estructura del grupo de riesgo operacional, ya que se requiere un responsable de la visión global del riesgo operacional de la entidad, pero también se requiere la presencia de una persona de cada área del negocio que esté en contacto directo con los riesgos.

3.3.4 Recolección de datos

Una vez identificados los riesgos se requiere hacer seguimiento a las pérdidas internas generadas por riesgo operacional y relacionarlas a las áreas de negocio. Aunque los datos de pérdidas registradas son importantes en la construcción del perfil de riesgo de la entidad, también se debe tener en cuenta que estos datos reflejan la situación pasada y deben ser analizados cuidadosamente para determinar el perfil de riesgo actual de cada entidad. Es importante precisar que la recolección de datos internos permite identificar pérdidas que se presentan recurrentemente con bajo impacto. Para el caso de pérdidas esporádicas de alto impacto se complementan las bases de datos con análisis de escenarios y con bases externas que permite determinar todos los posibles riesgos a los que está expuesta la entidad. La utilización de datos externos, análisis de escenarios y opiniones de expertos permiten a la administración ser proactiva en el manejo del riesgo.

Fitch afirma que para la administración del riesgo operacional la entidad no sólo deberá concentrarse en los factores que generan pérdidas, sino que debe analizar cada uno de los procesos de la entidad identificando los riesgos potenciales, las causas y las posibles consecuencias.

Adicionalmente, en la recolección de datos pueden presentarse problemas por la ocurrencia de un evento que afecta el riesgo de crédito, de mercado y operacional. Fitch afirma que en estos casos se pueden adoptar dos procedimientos: reportar el evento en riesgo de mercado o crédito para los propósitos de medición, pero rastrear la ocurrencia simultanea de un problema de riesgo operacional o el

segundo enfoque es determinar eventos en los que varios riesgos se presentan y diseñar una metodología para la medición de los mismos.

Fitch afirma que la efectividad de un proceso de recolección de datos está afectada por los sistemas utilizados para la recolección de los datos, la calidad de los datos, la cultura de riesgo de la organización, la calidad de los reportes, entre otros. No obstante recomienda empezar lo más pronto posible con la recolección de datos, ya que con la experiencia se mejora la calidad de este proceso.

Los bancos analizados en el estudio realizado por Fitch presentan diferencias en el número de años que llevan de recolección de datos y en la calidad de los mismos. El 43% de los bancos ha registrado datos por un periodo entre uno y dos años, otro 43% ha registrado datos por más de 2 años y el 13% cuenta con menos de un año de recolección de datos. En general la mayor parte de los bancos estaría en capacidad de adoptar el modelo avanzado en términos de disponibilidad de bases de datos. No obstante, varias entidades manifestaron preocupación frente a la calidad de los datos, especialmente los recolectados en los primeros periodos. Por otra parte, el 69% de los bancos muestran preocupación frente a la doble contabilidad de un evento cuando este se puede relacionar con varios tipos de riesgo. Frente a esta inquietud, los bancos adoptaron los lineamientos del Comité de Basilea que sugiere registrar el evento como riesgo de mercado o crédito y simultáneamente rastrear las causas relacionadas con riesgo operacional para tenerlo en cuenta en la administración de este riesgo.

3.3.5 Medición

En los últimos años las entidades han desarrollados modelos de medición de riesgo operacional que combinan datos cualitativos y cuantitativos, provenientes de datos internos, opiniones de expertos, autovaloración y análisis de escenarios. Dentro de los modelos propuestos se destacan los mencionados en el acuerdo de Basilea II[57].

De acuerdo con el estudio realizado por la firma calificadora Fitch, el 75% de las entidades del estudio están tratando de desarrollar modelos avanzados. Los cálculos preliminares muestran que el capital requerido calculado a través de este método es, en algunos casos, mayor que el requerido utilizando el enfoque estándar, esto sin tener en cuenta las correlaciones. Estos resultados son contrarios a la intención de Basilea de incentivar a los bancos a desarrollar modelos avanzados, ya que al medir con mayor precisión el riesgo se esperaba menores requerimientos de capital.

[57] Los enfoques propuestos por Basilea II se presentaron en el capitulo 1.

La mayor parte de los bancos va ha utilizar una distribución de pérdidas para calcular el requerimiento de capital. Este enfoque permite calcular las pérdidas esperadas y las no esperadas[58] usando una función de distribución de las pérdidas. El insumo básico para determinar la distribución son los datos, los cuales se obtienen de fuentes internas, fuentes externas, análisis de escenarios, entre otros.

De acuerdo con el estudio realizado por Fitch, los bancos analizados incorporaron los datos externos de tres maneras posibles: complemento directo de datos internos, instrumento de validación para asumir la distribución y ayuda para el análisis de escenarios. Las entidades que los utilizan para complementar los datos internos deben identificar los cambios requeridos a los datos para incorporarlos en los modelos propios. La manipulación de los datos externos para adaptarlos a los requerimientos internos de cada banco necesita alto nivel de conocimiento y cuidado. La incorporación de datos externos genera grandes dudas en el momento de tener en cuenta los mecanismos de control. Dado que la probabilidad de ocurrencia de una pérdida tiene relación directa con el diseño y efectividad de los mecanismos de control, en el caso de la incorporación de datos externos se requiere determinar para cada banco cual sería el requerimiento de capital, si los controles a estos eventos existieran e implementar los mecanismos de control que sean necesarios.

Por otra parte, la utilización de análisis de escenarios para determinar una aproximación a la exposición por riesgo operacional de una entidad se está incrementando, ya que esta permite incorporar las la perspectivas futura de la entidad. Por naturaleza este enfoque es subjetivo en la aplicación. Cada administrador determina que posibles escenarios puede llegara a enfrentar la entidad. Para la determinación de los escenarios algunas entidades utilizan los datos externos y otras tratan de identificar las pérdidas de acuerdo con la frecuencia de ocurrencia.

Una vez las entidades cuentan con los datos, utilizan una distribución estadística para modelar los datos. Debido a la poca disponibilidad de datos muchos bancos manifiestan que un alto grado de criterio es necesario para construir la distribución con mejor ajuste. Puede ser posible que una entidad tenga diferentes distribuciones de pérdidas todas con un nivel de ajuste aceptable pero con grandes diferencias en el resultado de requerimiento de capital. Por lo tanto, las entidades adoptaran algunos supuestos los cuales deberán ser razonables. Fitch considera que el proceso de cuantificación del riesgo operacional mejorará a medida que las entidades avancen en la evaluación y control de este riesgo.

[58] La pérdida esperada se define como la media de la distribución y la no esperada como la diferencia entre la media y el nivel de capital requerido para asegurar que las pérdidas potenciales sean cubiertas por dicho capital para un determinado nivel de confianza.

Los bancos analizados afirman que al tener en cuenta las correlaciones entre los diferentes eventos y riesgos se reduciría significativamente el requerimiento de capital, pero encuentran grandes dificultades en la demostración de estas correlaciones. Frente a este tema el Comité de Basilea publicó un documento[59] en el cual permite a los bancos que adopten el enfoque avanzado incorporar los efectos de la diversificación siempre que estos se fundamenten en estimaciones razonables.

El 83% de los bancos analizados utilizan seguros para mitigar el riesgo. Algunas entidades la restan todo el valor de la cobertura al valor requerido de capital para riesgo operacional, mientras otras analizan cada una de las coberturas y solo disminuyen el valor de capital requerido en una proporción.

3.3.6 Administración

Una vez identificados y medidos los riesgos estos requieren ser administrados. Para esta administración se pueden utilizar controles de la organización, el desarrollo de procesos para medir e implementar estos controles y el uso de programas de seguros para transferir el riesgo. No obstante, Fitch recomienda tener especial cuidado con los seguros utilizados para mitigar el riesgo revisando si en realidad cubre todas las eventualidades posibles o de lo contrario incluir el valor descubierto en el requerimiento de capital.

En el estudio realizado por Fitch se observó que en varios bancos se concentraron en las mediciones del riesgo pero no en el desarrollo de una cultura de riesgo. Fitch afirma que sin este elemento, el éxito de un sistema de administración de riesgo es mínimo. Estos sistemas requieren entidades participativas y abiertas y no estructuras rígidas y de permanentes juicios.

El esquema metodológico presentado por Fitch ofrece un elemento adicional a las metodologías anteriores, ya que complementa la teoría con la experiencia. Conocer las prácticas de entidades financieras líderes en el tema de riesgo operacional puede ser utilizado como una guía a seguir por las entidades que apenas van a incursionar en este tema.

Existen otras propuestas metodológicas que pertenecen principalmente a grupos financieros o a consultores expertos en el tema que presentan algunos elementos nuevos o profundizan en determinados temas, pero en general trabajan sobre los

[59] BANK FOR INTERNACIONAL SETTLEMENTS. Basel Comité on Banking Supervisión. Principles for the home-host recognition of AMA operacional risk capital. www.bis.org

puntos tratados por las tres propuestas metodológicas anteriores.

CAPITULO 4

4 Propuesta metodológica para la implementación de un sistema de administración de riesgo operacional

Teniendo en cuenta que un sistema de administración de riesgo operacional involucra aspectos cuantitativos y cualitativos y que estos últimos permiten incorporar una parte importante de subjetividad, una metodología para la implementación de un sistema de administración de riesgo operacional puede ser tan sencilla o compleja como se quiera. Con una propuesta metodológica de implementación de un sistema de administración de riesgo operacional se busca brindar una herramienta que pueda ser utilizada como guía por las entidades que están incursionando en el manejo del riesgo operacional. La metodología propuesta toma elementos de las tres metodologías expuestas anteriormente y en algunos casos los complementa con propuestas de otros autores.

Aunque la subjetividad del tema, y por lo tanto la complejidad del mismo, no permite presentar un recetario a seguir, si se busca generar una guía general de acción y presentar algunas herramientas que pueden ayudar a las entidades en la implementación del sistema.

Antes de presentar los aspectos que se deberían desarrollar para la implementación del sistema se requiere definir quien o quienes serán los responsables de la implementación del sistema. Es importante tener en cuenta que toda la organización está relacionada con el tema de riesgo operacional y por lo tanto todas las áreas son responsables de la implementación de dicho sistema. Sin embargo, siguiendo las recomendaciones de KPMG y Fitchratings se sugiere tener un área independiente que lidere la implementación y vele por el adecuado funcionamiento del sistema de administración de riesgo operacional. Adicionalmente, para la implementación del sistema es conveniente crear grupos de trabajo responsables de los diferentes aspectos que requiere el sistema. El coordinador de todos los grupos de trabajo deberá ser el funcionario responsable de la administración del riesgo operacional en la entidad.

Aspectos a desarrollar para la implementación de un sistema de administración de riesgo operacional:

1. Definiciones básicas
2. Lineamientos de gobierno corporativo
3. Definición de la estructura de medición de riesgos
4. Análisis de riesgos (Identificación, clasificación por frecuencia y por impacto, determinación de causas)
5. Recolección de datos

6. Monitoreo (diseño de reportes e identificación de indicadores líderes)
7. Mitigación de riesgos
8. Determinación de la infraestructura tecnológica requerida
9. Definición de la metodología para medición del riesgo operacional

4.1. Definiciones básicas

Las tres metodologías presentadas en el capitulo anterior mencionan en algún momento este aspecto. La propuesta metodológica de este trabajo considera que este debe ser el primer paso para la implementación de un sistema de administración de riesgo operacional, ya que es primordial definir unos conceptos básicos que permitan a todos los funcionarios de la entidad entender los aspectos principales del sistema y crear un lenguaje único sobre el tema. Cada entidad, de acuerdo con la cultura de riesgo operacional que tenga, determinará que definiciones considera relevantes. Como un primer paso se sugiere que inicialmente se realice una presentación a la Junta Directiva y a la alta Gerencia por parte de la unidad responsable de la administración del riesgo operacional, que induya un marco teórico general sobre riesgo operacional haciendo especial énfasis en la definición de este riesgo y en las ventajas generadas por la implementación del sistema. Una vez se realice esta presentación se puede crear un grupo de trabajo para proponer las definiciones básicas del sistema.

En la metodología propuesta no se incorpora el tema de asunciones propuesto por King buscando simplificar la implementación del sistema. No obstante, una vez la entidad haya avanzado en los distintos aspectos del sistema y en la asimilación de la cultura de riesgo operacional es posible complementar dicho sistema con este aspecto.

4.2. Lineamientos de gobierno corporativo

En este aspecto coinciden las tres metodologías presentadas en el capitulo anterior. Aunque algunas metodologías separan en varios puntos los temas relacionados con este aspecto todas coinciden en que el éxito de la implementación del sistema radica en gran medida en el grado de compromiso que tenga la Junta Directiva y el nivel superior de la administración con la implementación de dicho sistema. Una vez la entidad ya cuenta con las definiciones básicas sobre riesgo operacional y tenga un conocimiento del tema, es esencial que la Junta Directiva y la administración de primer nivel generen los principales lineamientos para la administración del riesgo y evidencien su total compromiso con la implementación de dicho sistema. En este aspecto se deben tener en cuenta los siguientes puntos:

- Definición de políticas generales

- Definición de la estructura organizacional
- Definición de funciones
- Diseño de mecanismos de control de cumplimiento de las políticas

Para la definición de políticas, estructura organizacional y funciones relacionadas con el sistema de administración de riesgo operacional, siguiendo las recomendaciones de KPMG, se sugiere crear un grupo de trabajo conformado por representantes de las distintas áreas de la entidad, que tengan conocimiento sobre riesgo operacional y una visión general de los procesos que se desarrollan en cada área. Este grupo será responsable de elaborar los lineamientos generales sobre el sistema. Una vez elaborado el primer documento se presenta a un segundo grupo conformado por los administradores de primer nivel de la entidad para su revisión. Por último la propuesta se presenta a la Junta Directiva para aprobación y/o comentarios. En todos los grupos deberá participar el responsable de la administración de riesgo operacional de la entidad.

Definición de políticas. La Junta directiva debe determinar claramente los lineamientos generales frente al tema. La definición de políticas debe tener en cuenta por lo menos lo siguiente: política general que incorpore el apetito de riesgo de la entidad, política de mitigación de riesgos, política de evaluación y monitoreo del riesgo, límites de clasificación de riesgos, instancias de decisión, entre otros. Como lo menciona KPMG, en principio la definición de límites será subjetiva ya que no se cuenta con datos históricos sobre la incidencia de los eventos generadores de riesgo operacional en la entidad.

Definición de la estructura organizacional. Auque toda la organización está relacionada con el sistema de administración de riesgo operacional y todos en alguna medida son responsables del adecuado funcionamiento del mismo, es importante que la entidad defina el área líder para la implementación del sistema, la cual debe tener independencia frente a las demás áreas. Adicionalmente es importante definir los responsables del sistema en cada una de las áreas. Por otra parte, la estructura organizacional se complementa con los comités relacionados con riesgo operacional que la entidad considere se requieran.

Definición de funciones. Tanto en la etapa de implementación, como en el funcionamiento normal del sistema es importante que la Junta Directiva y la administración determinen las funciones específicas de cada área y funcionario relacionadas con el sistema de riesgo operacional. En estas funciones se encuentran: elaboración de reportes, implementación de controles y ejecución de los mismos, clasificación y valoración de riesgos, elaboración de metodologías y modelos, monitoreos, entre otros.

Diseño de mecanismos de control del cumplimiento de políticas. El compromiso de la Junta Directiva y de la administración debe ser permanente y evidenciarse en un seguimiento continuo al funcionamiento del sistema. Las diferentes unidades relacionadas con el sistema, especialmente la unidad responsable de la administración de riesgo operacional deberán presentar reportes periódicos a las máximas instancias de decisión de la entidad.

Una vez definidas las políticas, estructura organizacional y funciones se deberá iniciar un programa de capacitación y divulgación de la información en todos los niveles de la organización. Esto contribuye con la generación de la cultura de riesgo operacional, la cual es imprescindible para que el sistema de administración de riesgos funcione.

4.3. Definición de la estructura de medición de riesgos

Este aspecto se menciona con mayor detalle en la metodología de King, ya que para este autor es muy importante que la estructura de medición de riesgo operacional siga una estructura similar a la utilizada para el análisis de generación de valor del negocio, buscando que los objetivos del sistema sea coincidentes con los objetivos generales de la entidad. El grupo de trabajo deberá levantar un mapa de los procesos estratégicos de la entidad, identificando cuales son los procesos y actividades que se consideran mayores generadores de valor. De cada uno de los procesos se levanta un mapa de actividades y se identifican las áreas involucradas en cada uno. Cada entidad determinará si va ha implementar el sistema de manera simultanea en todos los procesos o escoge un proceso piloto. Para el análisis de cada uno de los procesos se sugiere crear un grupo de trabajo especializado que cuente con representantes de cada una de las áreas involucradas y sea liderado por el responsable de la administración de riesgo operacional.

4.4. Análisis de riesgos (Identificación, clasificación por frecuencia y por impacto, determinación de causas)

Este es una de los aspectos más importantes para la implementación del sistema y por lo tanto King, KPMG y Fitch tratan este aspecto, siendo la metodología de KPMG la que presenta mayor detalle.

Debido a que los riesgos operacionales incorporan un importante grado de subjetividad es posible que las entidades presenten confusión o hagan esfuerzos innecesarios en la identificación y evaluación de los riesgos, por lo que se presentan unos lineamientos generales que ayuden a las entidades en esta tarea.

4.4.1 Identificación

Para la identificación de los riesgos se sugiere un enfoque de abajo hacia arriba, en el cual la entidad identifica y cuantifica los riesgos operacionales de las líneas de negocio para posteriormente proceder a medir el riesgo operacional de toda la entidad. Esta aproximación permite tener información más detallada de la entidad, lo que podría facilitar la gestión de riesgo. Tomando las recomendaciones de Fitch, la identificación de los riesgos se puede realizar a través de una o varias de las siguientes metodologías: recolección, análisis y mapeo de los datos de pérdidas de riesgo operacional, diseño de indicadores claves de riesgo, utilización de scorecards, implementación de metodologías de auto valoración que recopilan la información de los empleados, entre otros.

4.4.3 Clasificación

Además de la identificación de los riesgos, las entidades deben clasificarlos en distintas categorías con el fin de relacionarlos con las causas que los generan. Existen varios esquemas de clasificación de los riesgos, aún uno sugerido por el Comité de Basilea (anexo 2). No obstante, en las metodologías mencionadas en el capitulo anterior se deja en libertad a la entidad para determinar la clasificación que más se adecue a sus necesidades. Es importante que los grupos en los que se clasifiquen los riesgos sean excluyentes entre ellos.

Para efectos de este trabajo se utilizará como base la clasificación propuesta por Zurch IC Squared[60]. Esta clasificación se fundamenta en la propuesta por Gene Alvarez[61], solo que le agrega una mayor nivel de detalle. Se propone esta clasificación debido a que se considera más sencilla de implementar y entender que la propuesta por Basilea. La clasificación propuesta es la siguiente[62]:

Riesgo de personal: pérdidas intencionales o no intencionales causadas por un empleado o relacionadas con los empleados. Las subdivisiones de esta categoría son:

- Errores de los empleados: errores en las transacciones, procedimientos inadecuados.
- Problemas de recursos humanos: poca disponibilidad de empleados, contratación, despidos.
- Lesiones físicas al personal: Lesiones corporales, salud y seguridad.
- Lesiones no físicas al personal: difamación, discriminación, hostigamiento.
- Actos ilícitos: fraude, sobornos, falsificaciones.

[60] ZURCH IC SQUARED, www.ic2.zurich.com
[61] Alvarez Gene. A rigorous way for Quantifying Data – GARP Risk Review-Issue 4 dec-01/jan-02
[62] Basado en los trabajos de : ALVAREZ Gene. Operational Event Clasification. www.garp.com/library/Articles/Operational%20RiskEventClassification.pdf. y RICARDO VARELA María Cristina: Impacto de las Metodologías propuestas por el Comité de Basilea para el cálculo de los requerimientos de capital por riesgo operativo en el sector bancario colombiano. Tesis Ingeniería Industrial. Universidad de los Andes. Enero de 2004. Página 37.

Riesgo de procesos: pérdidas generadas por aspectos relacionados con la ejecución y mantenimiento de las transacciones y funcionamiento de un negocio, incluyendo productos y servicios. En general sólo se incluyen aspectos que afecten únicamente a la entidad y no a terceros. Las subdivisiones de esta categoría son:

- Procesos del negocio: falta de diligencia, problemas contables.
- Riesgos del negocio: fusiones, nuevos productos o mercados.
- Errores y omisiones: seguridad y control de calidad inadecuados.
- Responsabilidades específicas: de los empleadores, directores y gerentes.

Tecnología: pérdidas causadas por piratería, robos, fallas, interrupciones, tecnología inadecuada para las necesidades del negocio. Se divide en las siguientes categorías:

- Problemas generales de tecnología: errores operativos, uso indebido o no autorizado.
- Hardware: fallas de los equipos, hardware inadecuado o no disponible.
- Seguridad: intromisión de personas ajenas a los sistemas, interrupciones externas.
- Software: virus, fallas en la ejecución de programas.
- Sistemas: fallas, negligencia en el mantenimiento.
- Comunicaciones: fallas con teléfono, fax, internet.

Externalidades: pérdidas generadas por daños en la propiedad física por causas naturales o no naturales. Incluye acciones cometidas por personas externas.

- Desastres: naturales o no naturales.
- Alteraciones externas: fraude, lavado de dinero.
- Regulación: control de capital, cambios regulatorios.

4.4.3 Determinación de frecuencia e impacto

Una vez identificados los riesgos y clasificados de acuerdo con el esquema que la entidad diseñe sigue la evaluación de los mismos. King, KPMG y Fitch coinciden en que la etapa de evaluación se concentra en dos aspectos específicos: la frecuencia de ocurrencia de los eventos y el impacto de los mismos en la entidad.

La frecuencia de ocurrencia se refiere a la cantidad de veces que un evento generador de riesgo operacional se presenta en la entidad en un determinado intervalo de tiempo. El impacto se mide en dinero y está relacionado con el monto de capital que la entidad puede llegar a perder por la ocurrencia de uno de los eventos.

Teniendo en cuenta que la mayoría de las entidades que van a incursionar en el tema no cuentan con datos históricos de los efectos del riesgo operacional es

necesario utilizar herramientas técnicas que permitan traducir criterios y experiencia en variables cuantitativas.
Para la determinación de la probabilidad de ocurrencia y el impacto se pueden utilizar los siguientes análisis:
Top-down: Análisis cualitativo (entrevistas, escenarios Delphi)
Bottom-up: Análisis cuantitativo (Análisis de tendencia y regresión, análisis actuariales, distribución de pérdidas)

Para la determinación de la probabilidad de ocurrencia y del impacto se pueden utilizar tablas de calificación cuyos rangos serán definidos por la Junta Directiva de cada entidad, como los que se presentan a continuación:

Tabla 5. Propuesta general clasificación de frecuencia

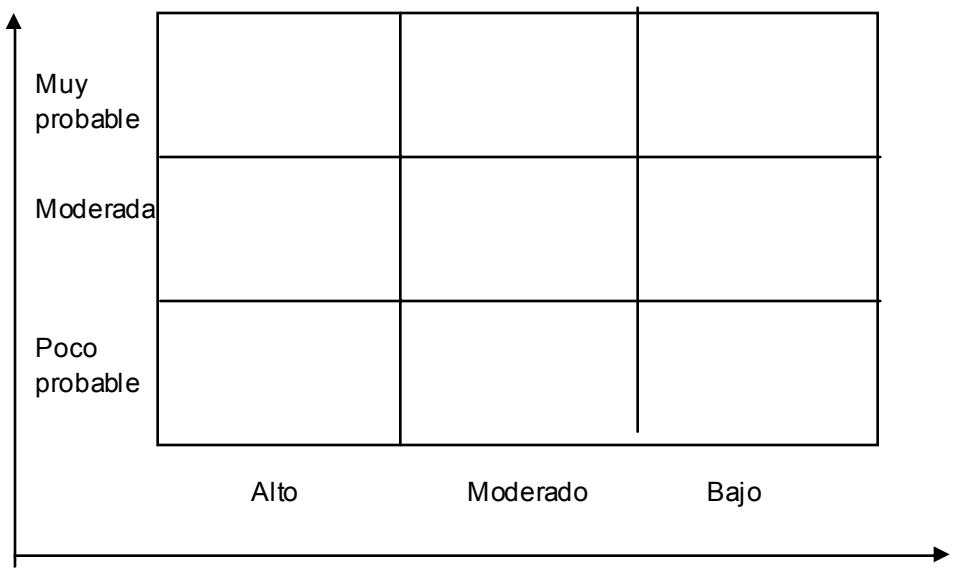
Probabilidad de ocurrencia	**N. mínimo de eventos**
Muy probable	Uno en x mes(es)
Moderado	Uno en x mes(es)
Poco probable	Uno en x año(s)

Tabla 6. Propuesta general clasificación de impacto

Incidencia	**Valor de las pérdidas**
Alta	Pérdidas mayores al x millones
Moderada	Pérdidas menores a x millones
Baja	Costo de reprocesamiento o ganancias no generadas

De acuerdo con KPMG, una vez se identifique la frecuencia y el impacto de cada uno de los eventos de riesgo se puede generar una matríz de riesgos que permite jerarquizar los eventos, donde los eventos de mayor frecuencia y mayor impactos son los de mayor riesgo.

Frecuencia



La matríz de riesgos permite a la entidad clasificar los eventos de riesgo en niveles con el fin de definir las acciones a seguir con cada uno de ellos. Cada entidad deberá adecuar el número de categorías de riesgo a sus necesidades. Sin embargo, como ilustración se presenta la siguiente clasificación:

Tabla 7. Ejemplo de acciones a seguir de acuerdo con la clasificación de riesgo

Riesgo	Acción a seguir
Alto	Requiere atención inmediata, investigación, planificación y toma de decisiones por parte de la Junta Directiva y el Comité de Riesgos
Severo	Requiere atención y acción por parte de la Alta Gerencia y el Comité de Riesgos
Moderado	Responsabilidad gerencial debe ser específica
Bajo	No hay mayor preocupación por el evento y se puede estar manejando con procedimientos rutinarios

Fuente: Leonardo Buniak y Asociados. Riesgo Operacional.

4.5. Recolección de datos

KPMG y Fitch tratan como un aspecto particular la labor de recolección de datos destacando que la realización de esta labor deberá apoyarse en gran medida en los aplicativos tecnológicos con los que cuente la entidad, los cuales deberán ser adecuados para permitir capturar la ocurrencia de eventos relacionados con riesgo operacional. En etapas preliminares del sistema y mientras se adecuan los aplicativos tecnológicos es posible diseñar plantillas que deberán ser diligenciadas por los funcionarios responsables. El éxito en el proceso de recolección de datos depende del grado de desarrollo de la cultura de riesgo que tenga la entidad, lo que permitirá la colaboración de los funcionarios. La organización deberá desarrollar una cultura de aprendizaje frente al error, en la cual, la ocurrencia de un evento de riesgo deberá ser vista como una oportunidad para mejorar y no como un error que se debe castigar.

El diligenciamiento diario del formato de registro de eventos de riesgo deberá incorporarse en el manual de funciones de los funcionarios designados como responsables. El grupo responsable de la implementación del sistema de administración del riesgo operacional será el responsable del diseño de las plantillas de registro de eventos. Adicionalmente se requiere la implementación de controles periódicos que permitan verificar si se están registrando todos los eventos de riesgo ocurridos. Para la implementación de los modelos de estimación de pérdidas esperadas es necesario contar con bases de datos que por lo menos tengan tres años de datos históricos. No obstante, las bases de datos se pueden complementar con datos externos y con información generada por análisis de escenarios. Cada uno de los responsables de las actividades críticas de cada proceso deberá recolectar los datos de los eventos que evidencien la ocurrencia del riesgo operacional. El funcionario responsable de cada área reportará a la unidad de riesgo operacional todos los datos y verificará periódicamente que los eventos se registren. El funcionario de la unidad de riesgo operacional también deberá realizar controles esporádicos para verificar que los eventos de riesgo se estén registrando.

4.6. Monitoreo de riesgos

La metodología propuesta por KPMG incluye como un aspecto particular la elaboración de reportes, mientras Fitch profundiza en el tema de indicadores líderes. La propuesta metodológica de este trabajo busca combinar estos dos aspectos en uno solo denominado monitoreo de riesgos. La unidad responsable de la administración de riesgos deberá diseñar los informes necesarios para mantener actualizada a la administración de la entidad. Los informes deben

tener claramente definido un objetivo, una periodicidad y un responsable de la elaboración del mismo. Para el monitoreo es importante identificar los indicadores claves de riesgo, con los cuales se revisará el desempeño de cada una de las áreas frente al riesgo operacional.

4.7. Mitigación de riesgos

La metodología propuesta por KPMG presenta este aspecto como un tema particular. El grupo de trabajo de cada proceso sujeto a análisis deberá determinar para cada riesgo el posible mecanismo de mitigación. Adicionalmente deberá realizar un análisis de costo beneficio de la implementación de dicho mecanismo.

Los mecanismos de mitigación se definen una vez la entidad identificó y cuantificó los riesgos. Estos mecanismos están relacionados con políticas, procedimientos, sistemas y controles. Cada entidad debe definir su tolerancia al riesgo y los límites hasta los cuales asume los riesgos o los transfiere. Los lineamientos presentados por KPMG se pueden complementar con las principales opciones de mitigación que se puede utilizar[63]:

- **Asumir:** Aceptar el riesgo potencial
- **Evitar**: Evitar el riesgo eliminando la causa del riesgo y/o la consecuencia.
- **Limitar:** Implementar controles que minimicen el impacto adverso de una amenaza (Uso de controles preventivos y detectivos).
- **Transferir:** Transfiriendo el riesgo usando otras opciones para compensar las pérdidas, tales como la compra de seguros.

Dentro de las estrategias de mitigación se encuentra la implementación de controles, aspecto que es mencionado en las tres metodologías. Los controles son mecanismos que permiten autorregular los procesos y a la vez ser indicadores de riesgos que enfrenta la entidad. Los controles deben ser diseñados en paralelo con el proceso y deben cumplir por lo menos con las siguientes características: nombre, descripción, ubicación, responsable, método de realización (manual o automático), categorías (preventivo o detectivo) y frecuencia. Adicionalmente todos los controles deben estar documentados y deben ser monitoreados y divulgados adecuadamente[64].

[63] BUNIAK Leonardo y Asociados. Curso Avanzado para el Análisis, Evaluación y Gestión de Riesgo Operacional. Miami, octubre de 2004.
[64] Idem.

4.8. Determinación de la infraestructura tecnológica requerida

Aunque las tres metodologías presentadas en capitulo anterior reconocen la importancia de la tecnología en el desarrollo de un sistema de administración de riesgo operacional, sólo KPMG menciona este aspecto de manera específica.

Uno de los aspectos claves para el funcionamiento del sistema es contar con un soporte tecnológico idóneo que permite recolectar los eventos generadores de riesgo operacional de manera automática y registrar las características específicas de los mismos. Para este efecto, una vez revisados los puntos anteriores es importante hacer un diagnóstico del estado actual del soporte tecnológico frente al requerido y definir los plazos para la adecuación del mismo. Sin embargo, mientras la plataforma tecnológica se actualiza se deberá diseñar un plan de transición que permita lo antes posible iniciar la recolección de datos.

4.9. Definición de la metodología de medición de riesgos

En este punto se busca determinar el monto de capital requerido por la entidad para cubrir las posibles pérdidas generadas por riesgo operacional y es un aspecto primordial para el sistema, razón por la cual todas las metodologías mencionan este aspecto, pero solo King lo profundiza.

Para la implementación de los modelos de medición se debe contar con datos históricos propios de la entidad, los cuales se deben complementar con datos externos y análisis de escenarios. Para la realización del cálculo se pueden aplicar las metodologías sugeridas por Basilea II mencionadas en el capitulo uno de este trabajo: el método del indicador básico, el método estándar y los métodos de medición avanzados o modelos internos. Con el fin de familiarizarse con estos modelos, la entidad podrá inicialmente adoptar el método del indicador básico o el método estándar, los cuales se caracterizan por se de menor complejidad pero así mismo por exigir un mayor monto de capital[65]. No obstante, en el mediano plazo, una vez se cuente con los datos necesarios, la entidad deberá desarrollar modelos internos avanzados.

Además de las metodologías presentadas en capitulo uno[66] se encuentran las siguientes metodologías[67]:

- El método *proxy*, análogo o sustitutivo
- El método de escenarios o estimación directa
- El método Delta - EVT

[65] Ver detalle de aplicación de estos modelos en el capítulo 1.
[66] Método básico, método estandarizado y metodologías internas.
[67] www.austega.com. Operacional Risk Mesurement Methods.

4.9.1 El método *proxy*, análogo o sustitutivo.

Este método se utiliza por entidades de gran tamaño con varias líneas de negocio, las cuales funcionan de manera independiente. Los pasos a seguir para la aplicación de este método son:

- Identificar entidades que cuentan con líneas de negocio similares a las de la compañía de estudio.
- Identificar el capital requerido por riesgo operacional y otras variables financieras claves para cada línea de negocio y analizar la relación entre el capital y las variables claves identificadas (se puede utilizar análisis de regresión).
- Utilizar la relación para calcular el capital requerido por cada división de la entidad según sus variables financieras claves.

Los principales problemas que presenta este método son: la subjetividad para seleccionar las entidades similares, el nivel de juicio requerido para la formación del algoritmo, la dificultad de proyección de datos, la separación entre el capital de riesgo medido y la gestión de riesgo de la entidad, entre otros.

4.9.2 El método de escenarios o estimación directa

Este método complementa el análisis histórico de datos de pérdidas con el juicio de los administradores para estimar la distribución de riesgo. Aunque incorpora un cierto grado de subjetividad, también permite ajustar los modelos proactivamente anticipándose a los cambios que enfrentará la entidad. La distribución seleccionada puede afinarse en la medida en que se cuente con más datos. El detalle de estimación de los riesgos depende de cada entidad. El principal problema que presenta este método es el alto grado de subjetividad.

4.9.3 El método Delta – EVT

Esta metodología se presentó en el capitulo anterior (numeral 5.1.1.3.2.)

Es importante tener en cuenta que el sistema de administración de riesgo operacional se debe caracterizar por su dinamismo. Por lo tanto, una vez aplicada la metodología de implementación se debe realizar una evaluación periódica al sistema y actualizar y afinar los aspectos que se requieran siempre en concordancia con las necesidades del negocio.

CAPITULO 5

5 Diseño del sistema de administración de riesgo operacional

De acuerdo con la propuesta del capitulo cuatro se realizará el diseño de un sistema de administración de riesgo operacional para una banco, tomando como línea piloto el proceso de compra y venta de divisas forward.

5.1. Línea de negocio escogida para el estudio

La implementación de un sistema de administración de riesgo operacional en una entidad puede realizarse simultáneamente para todas las líneas de negocio o inicialmente para una línea piloto. Para efecto de este trabajo se utilizará el segundo enfoque, buscando minimizar la complejidad de la implementación del sistema al concentrar todos los esfuerzos en una sola línea, la cual será utilizada como modelo para la implementación en las demás líneas del negocio. Adicionalmente, en la fecha de este estudio, la entidad está desarrollando varios proyectos estratégicos distintos a los relacionados con administración de riesgo que no permitirían orientar los esfuerzos de toda la organización al desarrollo del sistema de administración de riesgo operacional en todas las líneas de negocio.

Para definir la línea piloto se identificaron las principales líneas del negocio, específicamente todas aquellas que generan valor a la entidad. Para esta identificación se utilizó la cadena de valor que hace parte de la planeación estratégica. Dentro de este contexto se identificaron varias líneas de negocio, entre las que se encuentran, crédito, tesorería, captación, asesoría, comercio exterior, entre otras. Dentro de cada línea de negocio se deben identificar sublíneas específicas que permitan hacer más precisa la identificación y valoración de los riesgos.

Para efecto de este trabajo se seleccionó la línea de negocio de tesorería como piloto para la aplicación del sistema. Lo anterior en razón a que la experiencia internacional muestra que las mayores pérdidas generadas por riesgo operacional se han presentado en la áreas de tesorería, en gran medida por la inmediatez con la que se deben realizar las operaciones y por la gran cantidad de productos nuevos que permanentemente están generando estas áreas. Por otra parte, debido a que dentro de esta línea existen gran variedad de posibles negocios (sublíneas) y cada uno cuenta con un proceso detallado y presenta diversos eventos generadores de riesgo se decidió limitar el alcance del trabajo exclusivamente a la línea de compra y venta de divisas forward.

Operaciones de compra y venta de divisas forward

Estas operaciones hacen parte de las operaciones de mercado cambiario permitidas en Colombia y consisten en la compra o venta de divisas a futuro a alguno de los agentes del mercado cambiario[68]. Estas operaciones de realizan a través del sistema electrónico de transacciones de la Bolsa de Valores de Colombia y los plazos de las mismas oscilan, principalmente, entre un día y 360 días.

Dentro del ejercicio permanente de planeación estratégica que realiza la entidad objeto del estudio, desde 1999 se redefinió el papel del área de Tesorería, la cual hasta hace poco tiempo concentraba su labor en la consecución de recursos y en el manejo de los excedentes de liquidez, y ahora se busca convertirla en un área generadora de ingresos. Para este fin, la entidad viene trabajando en varios frentes entre los cuales se destacan la reorganización organizacional (nuevos cargos, cambios en funciones y responsabilidades, nuevo personal, capacitaciones), la adecuación de aplicativos de operación y de administración de riesgo, el desarrollo de nuevos productos, entre otros. El producto de compra y venta de divisas *forward* fue uno de los primeros en implementarse y es uno de los que mayor dinámica registra, razón por la cual fue seleccionado como línea piloto. A la fecha de este trabajo, esta línea de negocio era objeto de varias modificaciones especialmente relacionadas con modernización tecnológica y capacitación de funcionarios. El monto máximo de operación de la entidad en esta línea de negocio es determinado por la Junta Directiva de acuerdo con la exposición al riesgo calculada mediante el VAR[69].

5.2. Implementación del Sistema de Administración de Riesgo Operacional para la línea de negocio de compra y venta de divisas (forward)

De acuerdo con la propuesta del capitulo cuatro, los aspectos a desarrollar para la implementación de un sistema de administración de riesgo operacional son:

1. Definiciones básicas
2. Lineamientos de gobierno corporativo
3. Definición de la estructura de medición de riesgos
4. Análisis de riesgos (Identificación, clasificación por frecuencia y por impacto, determinación de causas)
5. Recolección de datos

[68] Los intermediarios del mercado cambiario colombiano son: los Bancos, las Corporaciones Financieras, las Compañías de Financiamiento Comercial, la FEN, Bancóldex, Cooperativas Financieras, Comisionistas de Bolsa y Casas de Cambio.
[69] Metodología de cálculo de valor en riesgo Value at Risk.

6. Monitoreo (diseño de reportes e identificación de indicadores líderes)
7. Mitigación de riesgos
8. Determinación de la infraestructura tecnológica requerida
9. Definición de la metodología para medición del riesgo operacional

En la medida en que se van desarrollando cada uno de los aspectos que conforman el sistema se requiere de un eficiente ejercicio de divulgación del mismo al interior de la entidad.

5.2.1 Definiciones básicas

Aunque la entidad cuenta con un sistema de administración de riesgo de crédito, está implementando un sistema de administración de riesgo de mercado y tiene una dirección independiente de administración de riesgos, aún se requiere un gran esfuerzo en el desarrollo de la cultura organizacional de riesgo. Específicamente el conocimiento y avances en riesgo operacional son mínimos. Por lo anterior se sugiere que antes de iniciar con la implementación del sistema, la entidad realice una capacitación general sobre el tema a toda la organización preferiblemente con la colaboración de consultores externos. Uno de los objetivos más importantes de esta capacitación es que todos los funcionarios de la entidad tomen conciencia de que el cada uno tiene responsabilidad en el adecuado funcionamiento del sistema y no se vea como un tema exclusivo del área de riesgos o netamente relacionado con la elaboración de modelos. Una vez se realice este ejercicio, se sugiere constituir un grupo de trabajo de riesgo operacional, liderado por el responsable de riesgo operacional (funcionario de la dirección de riesgo) y conformado por funcionarios de cada una de las áreas involucradas en los procesos de línea de negocio. Este grupo deberá iniciar su labor con la propuesta de definiciones básicas del sistema de administración de riesgo operacional, para lo cual puede tener en cuenta las sugeridas en el apéndice de este trabajo.

5.2.2 Lineamientos de gobierno corporativo (políticas, estructura organizacional y funciones)

De acuerdo con la experiencia de la entidad en la implementación de los sistemas de administración de riesgo de crédito y riesgo de mercado, entre los aspectos que el grupo de trabajo de riesgo operacional podría proponer a la alta gerencia y posteriormente a la Junta Directiva relacionadas con políticas, estructura organizacional y funciones se encuentran:

5.2.2.1 Políticas generales

- La administración de riesgo operacional se constituye en un pilar fundamental de la administración integral de riesgos y por lo tanto se considera como elemento primordial en la generación de valor del Banco.
- Todas las líneas de negocio del Banco hacen parte del sistema de administración de riesgo operacional.
- La entidad deberá cuenta con procesos y procedimientos claros, revisados periódicamente en función de las nuevas necesidades, y con líneas de responsabilidad bien definidas.
- La entidad tiene claramente identificados todos los eventos de riesgo operacional que puedan generar una pérdida significativa. El Comité de Administración de Riesgos definirá que se considera pérdida significativa.
- La Junta Directiva del Banco es el ente responsable del cumplimiento de lo establecido en el sistema de administración de riesgo operacional y apoyará su labor en el Presidente, el Comité de Administración de riesgos, el Comité de Riesgo Operacional y en la Gerencia de Riesgos.
- La entidad incluye la variable riesgo operacional en las decisiones de negocio en todos los ámbitos, estratégico, táctico y operativo.
- El Banco realiza un monitoreo mensual de los eventos de pérdida generados por riesgo operacional cuyos resultados se presentan en el Comité de Administración de Riesgo Operacional por la Gerencia de Riesgo. Adicionalmente, en forma trimestral se presentará un informe de seguimiento al Comité de Administración de Riesgos y a la Junta Directiva con los eventos de riesgo registrados y que tengan impacto alto o moderado para la organización.
- El Banco buscará mecanismos de mitigación de riesgo utilizando siempre un criterio costo-beneficio. Todos los eventos de riesgo operacional que generen impacto alto a la organización serán considerados prioritarios en la adopción de mecanismos de mitigación. El Comité de Administración de Riesgo Operacional es el ente responsable de proponer los mecanismos de mitigación requeridos y el Comité de Administración de Riesgos el ente que los aprueba para su implementación.
- El Comité de Administración de Riesgo Operacional tiene la atribución de exceder los límites de exposición establecidos por la Junta Directiva frente a este tipo de riesgo, en los casos en los cuales se demuestre que el no hacerlo generaría mayores riesgos o pérdidas a la entidad. Estos casos deben ser informados al Comité de Administración de Riesgos y a la Junta Directiva.

5.2.1.2. Políticas específicas (aplican únicamente para la línea de negocios de compra y venta de divisas – forward):

- Clasificación de eventos de riesgo:
  Por frecuencia de ocurrencia:
  Para efectos de la administración de riesgo operacional del Banco se considera la siguiente clasificación:

Tabla 8. Clasificación de frecuencia para el caso de estudio

Probabilidad de ocurrencia	N. mínimo de eventos[70]
Muy probable	Uno en un mes
Moderado	Uno en seis meses
Poco probable	Uno en un año

Por impacto:
Para efectos de la administración de riesgo operacional del Banco se considera la siguiente clasificación:

Tabla 9. Clasificación de impacto para el caso de estudio

Incidencia	Valor de las pérdidas[71]
Alta	Pérdidas mayores o iguales a COP[72] 500 millones
Moderada	Pérdidas menores a COP 500 millones
Baja	Costo de reprocesamiento o ganancias no generadas

- *Límites de riesgo operacional que asumirá la entidad*
  Sólo se pueden definir una vez la entidad esté en capacidad de valorar la exposición en cada operación por riesgo operacional. Este limité será propuesto por la Gerencia de Riesgos y la Junta Directiva decidirá el valor de acuerdo con el perfil de riesgo que quiera que tenga el Banco.

- *Mitigación:*
  La entidad implementará las diferentes estrategias de mitigación de acuerdo con los siguientes criterios:

[70] Los intervalos de tiempo se proponen a manera de ejemplo y fueron definidos por los funcionarios involucrados en la línea de negocio.
[71] El valor definido como límite se propone a manera de ejemplo y está relacionado con el volumen de operaciones de compra y venta de divisas forward que la entidad puede realizar diariamente para cumplir con los límites establecidos internamente por el Comité de Administración de Riesgos
[72] Nomenclatura internacional para referirse a pesos colombianos.

Evitar*: eventos de riesgo que generen pérdidas mensuales mayores a COP 1.000 millones*[73]*.*
Transferir o limitar*: eventos de riesgo que generen pérdidas mensuales menores o iguales a COP 1.000 millones.*
Asumir*: eventos de riesgo que generen costos de reprocesamiento.*

- *Seguimiento:*
  La Gerencia de Riesgos realizará un monitoreo diario de los eventos de pérdida generados por riesgo operacional en la línea de negocio compra y venta de divisas forward.

5.2.1.3. Estructura organizacional

Actualmente, la estructura de administración de riesgo (crédito y mercado) de la entidad está conformada por la Junta Directiva, el Comité de Administración de Riesgos, la Gerencia de Planeación y Riesgo (de la cual depende la dirección de riesgos) y los Comités de apoyo (Comités de Activos y Pasivos y Comité de Crédito). Para la estructura organizacional del sistema de administración de riesgo operacional se requiere proponer funciones a la Junta Directiva, al Comité de Administración de Riesgos y a la Gerencia de Planeación y Riesgos relacionadas con riesgo operacional y crear un Comité de Riesgo Operacional. Dada la actual estructura organizacional de la entidad, en la cual existe un área independiente responsable exclusivamente de la administración de riesgos se recomienda que dicha área sea la que asuma las funciones de administración del riesgo operacional.

Junta Directiva: máxima instancia de decisión de la entidad y responsable de las pérdidas que se puedan generar por una inadecuada administración del riesgo operacional. Apoyará su labor relacionada con riesgo operacional en el Comité de Administración de Riesgos, en el Comité de Riesgo Operacional y en la Gerencia de Riesgos.

Funciones:

- Aprobar las políticas generales y específicas de riesgo operacional.
- Delegar en las distintas instancias las atribuciones que se requieran.
- Aprobar los límites de clasificación de riesgos.
- Aprobar la periodicidad de evaluación de riesgo operacional.
- Propender por el desarrollo de la cultura de riesgo en la entidad.

[73] El valor definido como límite se propone a manera de ejemplo y está relacionado con el volumen de operaciones de compra y venta de divisas forward que la entidad puede realizar para cumplir con los límites establecidos internamente por el Comité de Administración de Riesgos

- Hacer seguimiento periódico del adecuado funcionamiento del sistema de riesgo operacional.

Comité de Administración de Riesgos: A esta instancia llegan los informes de los diferentes tipos de riesgo (crédito, mercado, liquidez, operacional) con el fin de que tenga una visión integral de los riesgos a los cuales está expuesta la entidad y pueda definir las acciones a realizar para que la entidad tenga el perfil de riesgo deseado. Está conformado por representantes de la Junta Directiva y algunos miembros de la administración de la entidad.

Funciones[74]:

- Garantizar el adecuado funcionamiento del Sistema de Administración de Riesgo Operacional.
- Definir acciones a seguir cuando el impacto de riesgo operacional sea muy alto
- Aprobar estrategias de administración de riegos que involucre todos los tipos de riesgo.
- Revisar periódicamente los reportes generados por el Sistema de Administración de Riesgo Operacional.
- Aprobar las metodologías propuestas por la Gerencia de Riesgos para identificar, medir, controlar, monitorear y valorar los diversos riesgos asumidos por la entidad.
- Aprobar límites de exposiciones al riesgo dentro de las políticas globales aprobadas por la Junta Directiva
- Propender por la difusión de la cultura de riesgo en la entidad.

Comité de Administración de Riesgo Operacional: Este Comité estará integrado por los funcionarios que se designen como líderes del Sistema de Administración de Riesgo Operacional y deberá contar con la participación de las distintas áreas de la entidad: Financiera, Tecnológica, Jurídica, Administrativa, Operativa, Contraloría y Riesgo.

Funciones:

- Proponer las políticas de riesgo operacional, de acuerdo con los lineamientos que fije la Junta Directiva.
- Diseñar las estrategias de administración del riesgo operacional.
- Establecer los mecanismos adecuados para la gestión de los riesgos asociados a nuevas operaciones.

[74] Algunas funciones fueron tomadas de la Resolución N° 136-03 de la Superintendencia de Bancos y Otras Instituciones Financieras (SUDEBAN). Gaceta Oficial de la república Bolivariana de Venezuela N° 37.703 del 3 de junio de 2003. Normas para una adecuada Administración de Riesgos.

- Generar valor agregado para la entidad como resultado de una adecuada administración del riesgo.

Gerencia de Administración de Riesgos: unidad independiente que reporta directamente al Presidente de la entidad y es la responsable de identificar, medir, evaluar y monitorear los diferentes riesgos que enfrente la entidad. En el tema de riesgo operacional apoya su labor en los responsables de riesgo operacional de cada una de las áreas de la entidad.

Funciones[75]:

- Velar por el cumplimiento de los límites de exposición al riesgo y los niveles de autoridad delegados.
- Revisar de forma sistemática la exposición por riesgo operacional.
- Informar periódicamente al Comité de Riesgo Operacional y al Comité de Administración de Riesgos acerca del cumplimiento de metas, así como sobre cualquier asunto que por su implicación o importancia amerite ser hecho del conocimiento de dicha instancia superior.
- Establecer los procedimientos y líneas de comunicación con los líderes de riesgo operacional de cada una de las áreas.
- Elaborar y someter a la consideración y aprobación del Comité de Riesgos las metodologías para identificar, medir, monitorear y valorar el riesgo operacional en la entidad.
- Presentar a la instancia respectiva los resultados obtenidos en la cuantificación de la exposición al riesgo.
- Elaborar los reportes que la Junta Directiva, el Comité de Administración de Riesgos y la Administración requieran.

5.2.3 Definición de la estructura de medición de riesgos

El proceso de compra y venta de divisas forward se dividió en tres grandes subprocesos:

- Negociación
- Valoración
- Cumplimiento

En cada uno de estos subprocesos se encuentran diversas actividades realizadas por distintas áreas de la organización. En el anexo 3 se presenta el flujograma del proceso en estudio.

[75] Idem.

Elaborar el flujograma del proceso es un requisito indispensable para la identificación de los eventos de riesgo operacional. En la elaboración del mismo participaron funcionarios de todas las áreas involucradas en el proceso y el levantamiento del mismo hizo parte de la formalización de la operación de nuevos productos que actualmente desarrolla la entidad. El nivel de detalle del flujograma depende de cada entidad, pero se debe buscar que todas las actividades que generen ganancia o pérdida de valor hagan parte del flujograma.

5.2.4. Análisis de riesgos (Identificación, clasificación por frecuencia y por impacto, determinación de causas) a través de la utilización de la metodología Delphi

Para el desarrollo de este punto se sugiere que una vez se haya identificado la línea de negocio a estudiar y se cuente con el flujo detallado del proceso se desarrolle un esquema de identificación y clasificación de los riesgos.

Para la identificación y evaluación de los eventos de riesgo operacional en la línea de compra y venta de divisas forward se utilizará la metodología Delphi. Lo anterior en razón a que la entidad no cuenta con registros históricos de pérdidas generadas por este riesgo, pero si cuenta con funcionarios con amplia experiencia en el manejo de las operaciones. A continuación se presentará una descripción detallada de la metodología y luego la aplicación de la misma.

5.2.4.1 Presentación Método Delpi[76]

Definición

El método Delphi es una herramienta que permite construir juicios colectivos a través de juicios individuales. Este método puede ser utilizado para identificar eventos importantes que pueden ocurrir en el futuro, de los cuales no se tiene información histórica.

El método Delphi fue elaborado en los años cincuenta por Olaf Helmer y Norman Dalkey en el Centro de Investigación Rand Corporation (California) para la fuerza área norteamericana, con el fin de seleccionar un sistema industrial

[76] La mayor parte de la teoría del método Delphi presentada en este capitulo fue tomada del documento Métodos y Técnicas de Investigación Prospectiva para la Toma de Decisiones" elaborado por KONOW Irene y PÉREZ Gonzalo. Universidad de Chile. 1990.

norteamericano óptimo y la estimación del número de bombas A requeridas para reducir la producción de municiones en cierto monto [77].

Este método se fundamenta en la aplicación de una serie de cuestionarios individuales a expertos. Una vez se aplica el primer cuestionario se obtiene información que posteriormente será incorporada en el siguiente cuestionario, y así sucesivamente. A través de estos cuestionarios se identifican puntos de convergencia y divergencia sobre los cuales se trabaja. El método se caracteriza por el anonimato, la interacción y la retroalimentación, lo que permite aprovechar la sinergia del debate en el grupo y eliminar las interacciones sociales indeseables que existen dentro de todo grupo. Gran parte del éxito de la aplicación de la metodología depende del diseño de los cuestionarios y de la selección de los expertos.

Aunque el método Delphi pueda parecer una técnica simple y de muy fácil uso, es necesario considerar cuidadosamente los problemas en su aplicación: composición del panel, deficiente formulación del cuestionario, falta de conocimiento del tema, existencia de prejuicios en la persona que lidera el ejercicio, exceso de simplificación, manipulación de los datos, entre otros.

5.2.4.2 Etapas para la aplicación del método Delphi[78]

La aplicación del método se puede dividir en seis etapas:

1. Etapa Exploratoria
En esta etapa se deben desarrollar los siguientes aspectos:
a) Definición de objetivos: Antes de diseñar el ejercicio, es necesario definir claramente los objetivos que se persiguen con la realización de un determinado Delphi.
b) Estudio del tema y búsqueda de información: Es necesario acotar la investigación hasta el punto de dejar claramente especificadas las variables que presentan el mayor interés el grupo investigador.
c) Programación de Recursos Humanos y Materiales: elaborar un cronograma definiendo al 0tiempo de aplicación del método y las horas requeridas de cada uno de los participantes.

2. Selección de grupo coordinador
La aplicación de la metodología exige la selección de una o varias personas responsables de coordinar el ejercicio. Esta o estas personas deberán conocer

[77] KONOW Irene y PÉREZ Gonzalo. Métodos y Técnicas de Investigación Prospectiva para la toma de decisiones. Ed. Fundación de Est. Propectivos (FUNTURO). Universidad de Chile. 1990. Eneko Astigarraga. El método Delphi. Universidad de Deusto.
[78] Idem.

detalladamente la metodología Delphi, conocer el tema que se quiere estudiar y tener gran imaginación y creatividad.

El grupo monitor deberá definir los objetivos de la aplicación de la metodología, reunir la información requerida relacionada con el tema de estudio, fijar los criterios de selección de los panelistas y determinar su número y composición, elaborar un cronograma detallado del tiempo que se requerirá para la realización del ejercicio, diseñar los cuestionarios y evaluar la información obtenida.

3. Selección del panel de expertos
Son los responsables de proveer la información requerida para el estudio. La selección de los expertos la realiza el grupo monitor. El número óptimo de panelistas depende del tema, objetivos del estudio y los recursos con que se cuenta.

4. Elaboración y aplicación de los cuestionarios
La elaboración de las preguntas y la forma de presentar la información son aspectos determinantes para el éxito de la metodología.

En lo relacionado con las preguntas del cuestionario, éstas deben ser elaboradas cuidadosamente, presentar claridad de conceptos y conformar un cuestionarlo que no sea demasiado extenso. La información de las preguntas puede presentarse en series, histogramas u otras gráficas. Por otra parte, las preguntas deben incluir el grado de certeza de la respuesta (escalas de respuesta). Dichas preguntas pueden ser abiertas, de ranking (ordenar información), de votación, de fechas y de probabilidades, entre otros.

5. Evaluación del primer cuestionario
Para la evaluación de la información obtenida en el primer cuestionario se deberán tener en cuenta aspectos como: elaborar un resumen de la información obtenida, identificar los sesgos y corregir los mismos, identificar consensos y discrepancias, identificar fallas en el cuestionario, elaborar la retroalimentación, entre otros.

6. Evaluación de los siguientes cuestionarios y presentación de resultados
En el segundo cuestionario se investigan las discrepancias identificadas en la evaluación del primer cuestionario. Se somete a la consideración de los panelistas aquellas ideas que son de interés al tema y que fueron planteadas por algún panelista en especial. En general la técnica para elaborar este cuestionario es la misma descrita para el primero. En esta vuelta muchas de las preguntas requieren especificar la justificación de la respuesta, con el fin de investigar las razones de las discrepancias presentadas en la primera vuelta. Esta etapa es necesario además evaluar el impacto de la retroalimentación sobre las opiniones de los panelistas. El efecto de la retroalimentación sobre las respuestas de los panelistas se evalúa midiendo el grado y velocidad que se tiende al consenso en

las vueltas sucesivas. Por último, una vez se logra un grado adecuado de consenso se procede a presentar los resultados del ejercicio.

5.2.4.3 Aplicación del método Delphi en la identificación, clasificación, determinación de impacto y frecuencia de eventos de riesgo operacional

Es importante tener en cuenta que la aplicación del método Delphi ofrece una herramienta para la facilitar y complementar la toma de decisiones, pero no sustituye el análisis y las decisiones que deben tomar la alta administración y los distintos comités que operen en la entidad.

La metodología se aplicará para el análisis del proceso de compra y venta de divisas forward.

Los objetivos específicos del estudio son:

1. Identificar los posibles eventos generadores de riesgo operacional que se presentan en todo el proceso.
2. Clasificar estos eventos por causas generadoras.
3. Determinar la posible frecuencia de ocurrencia de los eventos.
4. Determinar la posible incidencia de la ocurrencia de los eventos en los resultados de la entidad (impacto).

Para la selección de los expertos se identificaron todos los funcionarios de la entidad que están relacionados con el proceso de estudio. En este proceso están involucradas seis áreas [79] y 10 funcionarios. Tomando como criterio básico constituir el grupo con personas de diferentes áreas que cuenten con experiencia en las distintas actividades del proceso de estudio se determinó que el grupo de expertos estaría compuesto por seis funcionarios[80].

La aplicación del método se realizó a través de dos encuestas.

5.2.4.3.1 Primera encuesta

En el anexo 4 se presenta la primera encuesta entregada a los funcionarios. En esta encuesta se presentan generalidades sobre el riesgo operacional y sobre el funcionamiento del método Delphi. Adicionalmente, los cuestionarios incorporan

[79] Tesorería, Riesgo, Contabilidadad, Contraloría, Operaciones y Sistemas.
[80] Tesorero, trader operaciones moneda extranjera, gerente de Riesgo, analista de procesos, analista de operaciones y ejecutivo de contraloría.

un diagrama del proceso objeto de estudio y las tablas de clasificación de los riesgos requeridas para desarrollar la encuesta.

5.2.4.3.2 Resultados primera encuesta

En la aplicación de la primera encuesta, los funcionarios identificaron 19 posibles eventos generadores de riesgo operacional, clasificados en tres segmentos determinados por las etapas principales del proceso:
Etapa de negociación: 10
Etapa de valoración: 5
Etapa de cumplimiento: 4

En la tabla 10 se presentan los resultados de la primera encuesta incluyendo los eventos de riesgo, la vulnerabilidad, la amenaza, la clasificación por tipo de riesgo y el número de encuestados que identificaron cada riesgo.

Tabla 10 Identificación de eventos de riesgo operacional

Proceso de compra y venta de divisas (Forward)						
Resultados primera encuesta						
	Riesgo	**Vulnerabilidad**	**Amenaza**	**Clasificación**		**Número de encuestados que identificó este riesgo**
				Tipo	**Subtipo**	
Etapa 1: Negociación						
1	Problemas en estrategias de cobertura por errores de cálculo en posición propia[81]. Este dato es fundamental para la definición de estrategias de cobertura.	Cálculos manuales. Errores en la alimentación de datos requeridos para el cálculo de posición propia. Pocos mecanismos de verificación o control de datos.	Cambios periódicos en normatividad legal de cálculo. El cálculo deber realizarse diariamente.	1	B	2
2	Exceder los cupos de negociación aprobados por la Junta Directiva.	No existe interfaz entre los aplicativos de negociación de operaciones. Las modificaciones del valor o condiciones de los cupos son manuales y deben realizarse en varios aplicativos	Presión de tiempo para realizar operaciones.	3	C	6

[81] Es un indicador de riesgo cambiario de los intermediarios financieros que se calcula sumando los derechos en moneda extranjera menos las obligaciones en moneda extranjera que tenga cada intermediario dentro y fuera del balance.

	Riesgo	Vulnerabilidad	Amenaza	Clasificación		Número de encuestados que identificó este riesgo
3	Problemas por fallas en sistemas transaccionales.	Se depende de fuentes externas y no existe plan de contingencia formal.	Caída o servicio deficiente de los sistemas de transacción	3	E	3
4	Problemas por errores en la inclusión de las operaciones en los aplicativos	El aplicativo no cuenta con mecanismos de verificación del adecuado registro de las operaciones.	Presión de tiempo para realizar operaciones	3	C	3
5	Problemas generados por inconsistencia entre las operaciones constituidas y las gestiones (papeletas) recibidas	En el front office, no se verifican datos ingresados en aplicativo contra ticket	Presión de tiempo.	2	C	2
6	Incumplimiento por parte del Banco de las condiciones de negociación definidas en el contrato marco	El contrato no se recibe oportunamente. El proceso no tiene explicita la etapa de revisión detallada por parte del área de cumplimiento de los datos contrato	Presión de tiempo.	2	E	1
7	Errores en la toma de decisiones por falta de información del portafolio global del Banco.	No se cuenta con un sistema de administración y control de portafolios adecuado. Las operaciones se manejan en distintos aplicativos.	Permanentemente se deben tomar decisiones de portafolio. Presión de tiempo	3	C	2
8	Imposibilidad de operar por factores externos como cortes de electricidad, problemas de acceso a las oficinas, etc.	No existe plan de contingencia formal para dar continuidad al negocio en estos casos	Algunas veces se presentan cortes de electricidad, problemas de acceso al edificio	4	B	1
9	Exceder límites o realizar operaciones no aprobadas por desconocimiento de políticas	Falta de capacitación. Desconocimiento del producto	Presión de tiempo al realizar las operaciones. Nuevas operaciones para la entidad. Nuevos funcionarios	1	C	1

	Riesgo	Vulnerabilidad	Amenaza	Clasificación		Número de encuestados que identificó este riesgo
10	Se pierden oportunidades de negocio porque no existen atribuciones internas para exceder límites. Todo debe ser aprobado por Junta Directiva.	El proceso no muestra las acciones alternativas a seguir en caso de requerirse exceder un límite, la línea de responsabilidad o atribución	En algunas ocasiones las condiciones de mercado puede requerir el exceso eventual de límites y la respuesta debe ser inmediata	2	A	1
Etapa 2: Cumplimiento						
11	En caso de incumplimiento de operaciones de un tercero hacia el Banco se presentan demoras en la toma de acciones requeridas,	No se tiene claridad de las acciones inmediatas a realizar en caso de incumplimiento. No se tiene un proceso definido para estos casos	El posible incumplimiento de operaciones hace parte del riesgo asumido en este negocio	2	E	2
12	Girar a los terceros valores diferentes a los pactados o incumplimiento de compromisos	Error del trader en la digitación de la operación. El aplicativo no valida datos. Varios datos se digitan. Errores en la papeleta que soporta la operación. Controles escasos	Presión de tiempo	1	B	5
13	Incumplimiento de operaciones por fallas de los sistemas operacionales en los cuales se registran las operaciones.	No existe plan de contingencia formalizado	Caída o servicio deficiente de los sistemas	3	C	2
14	Incumplimiento de operaciones por demora en flujo de información interna	El funcionario que cumple las operaciones recibe por mail la información de vencimientos con demoras	El cumplimiento de operaciones es un proceso diario	1	B	1
15	Registro contable distinto al de la negociación	Proceso de registro manual. Pocos controles	Elevado número de operaciones y de terceros	3	C	2
Etapa 3: Valoración						
16	Errores en decisiones de negociación por falta de oportunidad de los reportes de valoración (tasas requeridas para valorar las operaciones)	No se tiene fuente de información alterna para obtener tasas de valoración. Las tasas no se encuentran en el sistema de información en tiempo real	Presión de tiempo	3	E	2

	Riesgo	Vulnerabilidad	Amenaza	Clasificación		Número de encuestados que identificó este riesgo
17	Discrepancias entre registros contables y el aplicativo central frente a datos de valoración	Fallas de digitación, aproximaciones o redondeo de cifras	No existe interfaz que comunique los aplicativos	3	D	2
18	Error humano en la valoración de operaciones	Gran parte del proceso es manual. No existe manual de procesos detallado	Presión de tiempo	1	B	2
19	La información sobre el portafolio valorado es mínima, lo que no permite una administración integral del mismo.	Ausencia de políticas claras de valoración financiera. No se cuenta con aplicativo que permita valorar financieramente las operaciones. Gran manejo manual de cálculos. Aplicativos no vinculados	Algunas estrategias tienen como insumo el portafolio valorado y por lo tanto pueden ser erradas	3	C	4

Aspectos a destacar en los resultados de la primera encuesta:

- Aunque algunos eventos de riesgo fueron identificados por más de un encuestado, en general los funcionarios identificaron en mayor medida eventos de riesgo relacionados con sus tareas reflejando especialización de funciones.
- 9 de los 19 eventos de riesgo identificados fueron atribuidos a problemas con tecnología, 5 con personal, 4 con procesos y 1 con eventos externos. Este resultado evidencia que la mayoría de las personas entrevistadas relacionan el riesgo operacional, en mayor medida, con modernización tecnológica y por otra parte tienen requerimientos frente a este aspecto, que de implementarse podrían disminuir la ocurrencia de posibles eventos de riesgo.
- El mayor número de eventos de riesgo se identificó en la etapa de negociación, hecho que se explica por la inmediatez con la que se deben realizar las operaciones en esta etapa. Adicionalmente, todos los funcionarios están más familiarizados con esta etapa del proceso que con el resto de las etapas.
- En los casos en que varios encuestados identificaron el mismo evento de riesgo, todos los encuestados otorgaron una clasificación de riesgo operacional igual.
- En contraste con lo anterior, la asignación de la frecuencia, incidencia e importancia difería en muchos casos, lo que podría explicarse por la

mayor dificultad que evidenciaron los encuestados en asignar características numéricas a eventos de riesgo de los cuales no se tienen datos históricos. Por lo anterior, en la segunda encuesta se solicitó a los encuestados otorgar nuevamente estas características a cada evento de riesgo.

- En la fecha del estudio, la línea de compra y venta de divisas forward era objeto de varias modificaciones relacionadas con modernización tecnológica, de procesos y capacitación de funcionarios y por lo tanto algunos eventos de riesgo identificados podrían eliminarse en el corto plazo.

5.2.4.3.3 Segunda encuesta

Con los resultados de la primera encuesta se desarrolló una segunda encuesta que básicamente presentaba los eventos de riesgo operacional identificados en la primera encuesta, con el fin de que los encuestados manifestaran su acuerdo o desacuerdo con los mismos y asignaran las características de frecuencia, impacto e importancia. La segunda encuesta entregada se presenta en el anexo 5.

5.2.4.3.4 Resultados segunda encuesta

Los resultados de la segunda encuesta se presentan en la tabla 11

Tabla 11. Resultados segunda encuesta aplicación método Delphi

Tabla 11. RESULTADOS SEGUNDA ENCUESTA APLICACIÓN MÉTODO DELPHI
IDENTIFICACIÓN DE EVENTOS DE RIESGO OPERACIONAL
PROCESO DE COMPRA Y VENTA DE DIVISAS (FORWARD)
RESULTADOS SEGUNDA ENCUESTA

Etapa 1: Negociación

	Riesgo	Vulnerabilidad	Amenaza	Clasificación		Frecuencia			Impacto			Importancia			De acuerdo	En desacuerdo
				Tipo	Subtipo	Muy	Moderado	Poco	Alta	Moderada	Bajo	1	2	3		
						Número de encuestados										
1	Problemas en estrategias de cobertura por errores de cálculo en posición propia	Cálculos manuales. Errores en la alimentación de datos requeridos para el cálculo. Pocos mecanismos de verificación o control de datos.	Cambios periódicos en normatividad legal de cálculo. El cálculo deber realizarse diariamente.	1	B	1	5	-	-	4	2	5	1	-	6	-
2	Exceso en cupos de negociación aprobados	No existe interfaz entre los aplicativos de negociación. Las modificaciones de cupos son manuales y deben realizarse en varios aplicativos	Presión de tiempo para realizar operaciones.	3	C	-	-	6	1	1	4	6	-	-	6	-
3	Problemas por fallas en sistemas transaccionales.	Se depende de fuentes externas y no existe plan de contingencia formal.	Caída o servicio deficiente de los sistemas de transacción	3	E	-	4	2	2	4	-	4	2	-	6	-
4	Problemas por errores en la indusión de operaciones en los aplicativos	El aplicativo actual no permite registrar adecuadamente las operaciones ni tener un control automático de las mismas. Falta de capacitación del producto.	Presión de tiempo para realizar operaciones	3	C	2	4	-	-	3	3	2	4	-	6	-

Tabla 11. RESULTADOS SEGUNDA ENCUESTA APLICACIÓN MÉTODO DELPHI
IDENTIFICACIÓN DE EVENTOS DE RIESGO OPERACIONAL
PROCESO DE COMPRA Y VENTA DE DIVISAS (FORWARD)
RESULTADOS SEGUNDA ENCUESTA

	Riesgo	Vulnerabilidad	Amenaza	Clasificación		Frecuencia			Impacto			Importancia			De acuerdo	En desacuerdo
				Tipo	Subtipo	Muy	Moderado	Poco	Alta	Moderada	Bajo	1	2	3		
Etapa 1: Negociación																
	Riesgo	**Vulnerabilidad**	**Amenaza**	**Clasificación**											**De acuerdo**	**En desacuerdo**
				Tipo	**Subtipo**											
5	Problemas generados por incosistencia entre las operaciones constituidas y las gestiones recibidas	No se verifican datos ingresados en aplicativo contra ticket. El aplicativo no permite hacer modificaciones	Presión de tiempo.	2	C	-	6	-	1	5	-	2	4	-	6	-
6	Incumplimiento de condiciones de negociación definidas en el contrato marco	Falta verificación de datos del contrato	Presión de tiiempo. El contrato no se recibe oportunamente	2	E	-	1	5	1	1	4	6	-	-	6	-
7	Errores en la toma de decisiones por falta de información	No se cuenta con un sistema de administración y control de portafolios adecuado	Permanentemente se deben tomar decisiones de portafolio. Presiòn de tiempo	3	C	-	4	2	1	5	-	5	1	-	6	-
8	Imposibilidad de operar por factores externos	No existe plan de contingencia formal para continuar con las negociaciones	Cortes de electricidad, problemas de acceso al edficio	4	B	-	6	-	2	4	-	6	-	-	5	1
9	Exceder límites o realizar operaciones no aprobadas por desconocimiento de políticas	Falta de capacitación. Desconocimiento del producto	Presión de tiempo al realizar las operaciones. Nuevas operaciones para la entidad. Nuevos funcionarios	1	C	-	4	2	-	5	1	6	-	-	6	-
10	Se pierden oportunidades de negocio porque no existen atribuciones para exceder límites	El porceso no muestra las acciones alternativas a seguir en caso de requerirse exceder un límite, la línea de responsabilidad o atribución	En algunas ocasiones las condiciones de mercado puede requerir el exceso eventual de límites	2	A	-	6	-	-	6	-	5	1	-	6	-

Tabla 11. RESULTADOS SEGUNDA ENCUESTA APLICACIÓN MÉTODO DELPHI
IDENTIFICACIÓN DE EVENTOS DE RIESGO OPERACIONAL
PROCESO DE COMPRA Y VENTA DE DIVISAS (FORWARD)
RESULTADOS SEGUNDA ENCUESTA

Etapa 2: Cumplimiento

	Riesgo	Vulnerabilidad	Amenaza	Clasificación		Frecuencia			Impacto			Importancia			De acuerdo	En desacuerdo
				Tipo	Subtipo	Muy	Moderado	Poco	Alta	Moderada	Bajo	1	2	3		
11	Demora en toma de acciones requeridas, en caso de incumplimiento de operaciones hacia el Banco	No se tiene claridad de las acciones inmediatas a realizar en caso de incumplimiento. No se tiene un proceso definido para estos casos	Posible incumplimiento de operaciones	2	E	-	2	4	5	1	-	5	1	-	6	-
12	Girar valores diferentes a los pactados o incumplimiento de compromisos	Error del trader en la digitación de la operación. El aplicativo no valida datos. Varios datos se digitan. Errores en la papeleta que soporta la operación. Controles escasos	Presión de tiempo	1	B	-	6	-	2	4	-	5	1	-	6	-
13	Incumplimiento de operaciones por fallas de los sistemas operacionales	No existe plan de contingencia formal	Caída o servicio deficiente de los sistemas	3	C	-	5	1	5	1	-	6	-	-	6	-
14	Registro contable distinto al de la negociación	Proceso de registo manual. Pocos controles	Elevado núimero de operaciones y de terceros	3	C	5	1	-	1	-	5	5	-	1	6	-

Tabla 11. RESULTADOS SEGUNDA ENCUESTA APLICACIÓN MÉTODO DELPHI
IDENTIFICACIÓN DE EVENTOS DE RIESGO OPERACIONAL
PROCESO DE COMPRA Y VENTA DE DIVISAS (FORWARD)
RESULTADOS SEGUNDA ENCUESTA

Etapa 3: Valoración de operaciones

	Riesgo	Vulnerabilidad	Amenaza	Clasificación		Frecuencia			Impacto			Importancia			De acuerdo	En desacuerdo
				Tipo	Subtipo	Muy	Moderado	Poco	Alta	Moderada	Bajo	1	2	3		
15	Errores por falta de oportunidad en reportes de valoración	No se tiene fuente de información alterna para obtener tasas de valoración. Estas tasas no se encuentran en el sistema de información del banco en tiempo real	Presión de tiempo	3	E	-	1	5	-	1	5	-	1	5	6	-
16	Discrepancias entre registros contables y el aplicativo central	Fallas de digitación, aproximaciones o redondeo de cifras	No existe interfaz que comunique los aplicativos	3	D	5	1	-	1	-	5	2	4	-	6	-
17	Deficiente información sobre el portafolio valorado	Ausencia de políticas claras de valoración financiera. No se cuenta con aplicativo que permita valorar financieramente las operaciones. Gran manejo manual de cálculos. Aplicativos no vinculados	Algunas estrategia tienen como insumo el portafolio valorado y por lo tanto pueden ser erradas	3	C	-	2	4	-	-	6	2	-	4	6	-

Aspectos a destacar en los resultados de la segunda encuesta:

- Como resultado de la segunda encuesta se eliminaron dos eventos de riesgo, ya que los funcionarios relacionados directamente con la etapa del proceso en la cual se presentan estos eventos manifestaron que los factores generadores de dichos riesgos ya fueron eliminados. Los eventos de riesgo eliminados fueron: incumplimiento de operaciones por demora de información, ya que se implementó un procedimiento en el cual el vencimiento de operaciones se informa con un día de anticipación y el evento de error en valoraciones generado por error humano ya que este procedimiento se sistematizó.

5.2.4.3.6 Resultados de la aplicación del la metodología Delphi

- Como resultado de la aplicación de la primera y segunda encuesta se identificaron 17 eventos de riesgo los cuales se encuentran distribuidos por etapas del proceso de la siguiente manera:
  Etapa de negociación: 10
  Etapa de cumplimiento: 4
  Etapa de valoración: 3
- Aunque varios eventos de riesgo solo fueron mencionados por un encuestado, el funcionario que mayor relación tiene con la parte del proceso en la cual se presenta el evento, se decidió incorporarlos como posibles eventos de riesgo, ya que en la segunda encuesta no fueron rechazados por los demás encuestados.
- El mayor número de eventos de riesgo se identificó en la etapa de negociación, en gran medida como resultado de la inmediatez con la que se deben realizar las actividades de esta etapa del proceso. No obstante, ninguno de los eventos de riesgo identificados en esta etapa se ubicó en la zona de mayor riesgo de la matriz de riesgo (muy probable y alto impacto).
- De acuerdo con los encuestados, la causa generadora de riesgo que afecta en mayor medida el proceso es la deficiencia en tecnología. Es así como de los 17 eventos de riesgo identificados, nueve son generados por problemas de tecnología, cuatro por riesgos de procesos tres por riesgo de personal y uno por externalidades.
- En general, las calificaciones de frecuencia, impacto e importancia registraban tendencias hacia determinada categoría de calificación. Tanto para frecuencia, impacto e importancia, la categoría con menor votación tenía más de tres de los seis encuestados a favor. Con base en este resultado, para la presentación de resultados del estudio, se asignó a cada evento de riesgo una calificación de frecuencia, impacto e

importancia correspondiente a la categoría que mayor número de encuestados registró. Adicionalmente se verificó que la calificación otorgada por el funcionario que mayor relación tuviera con el evento de riesgo estuviera en la categoría seleccionada.

- En algunos eventos de riesgo las calificaciones otorgadas por alguno o algunos de los encuestados eran opuestas a las de la mayoría de encuestados, lo que podría reflejar que algunas personas conocen detalladamente la parte que manejan del proceso pero tienen vacíos frente al resto de actividades del proceso.
- En la calificación de frecuencia se observa un cierto grado de consenso, ya que en varios casos todos los encuestados votaron a favor de una misma calificación o en algunos casos las diferencias eran solo de una categoría. En contraste, en la calificación de impacto se presentaron las mayores diferencias, ya que en varios eventos de riesgo todas las posibles calificaciones tenían votos a favor. Esto se puede explicar por la gran dificultad que se presenta al tratar de asignar valores de impacto en dinero sobre eventos de riesgo que no han ocurrido en la historia. Aunque los resultados obtenidos sobre impacto pueden ser utilizados como una primera aproximación para la clasificación de los eventos de riesgo se requiere que a medida que se recolecten datos de eventos de riesgo esta clasificación se ajuste.
- En la etapa de cumplimiento, en la cual se realiza el pago de las operaciones se registraron los eventos de mayor frecuencia e incidencia, dado que en esta etapa se materializa la negociación y por lo tanto es evidente la incidencia de los errores.
- La categoría de frecuencia seleccionada en mayor medida fue moderado. De los 17 eventos de riesgo: diez fueron categorizados en moderado, cinco en poco y dos en muy frecuentes (uno en la etapa de valoración y uno en la etapa de cumplimiento)
- Así mismo, la categoría de impacto que mayor número de veces fue seleccionada fue moderado. De los 17 eventos de riesgo nueve fueron categorizados en moderado, seis en bajo y dos en alto (los dos en la etapa de cumplimiento).
- La clasificación de importancia fue una característica adicional que se le asignó a los riesgos destacándose la categoría de muy importante, la cual fue asignada a 12 eventos de riesgo, moderadamente importante a tres y levemente importante a dos.

Utilizando los resultados de la primera y segunda y asignando las características a cada evento de riesgo de acuerdo con la clasificación que más votos a favor registraba dentro de las categorías posibles, se presentan los resultados definitivos del estudio en la tabla 12:

Tabla 12. Identificación de eventos de riesgo operacional

Proceso de compra y venta de divisas (Forward)

Resultados aplicación método Delphi

Etapa 1: Negociación

	Riesgo	Vulnerabilidad	Amenaza	Clasificación		Frecuencia	Impacto	Importancia
				Tipo	Sub tipo			
1	Problemas en estrategias de cobertura por errores de cálculo en posición propia[82]. Este dato es fundamental para la definición de estrategias de cobertura.	Cálculos manuales. Errores en la alimentación de datos requeridos para el cálculo. Pocos mecanismos de verificación o control de datos.	Cambios periódicos en normatividad legal de cálculo. El cálculo deber realizarse diariamente.	1	B	Moderado	Moderado	1
2	Exceder los cupos de negociación aprobados por la Junta Directiva.	No existe interfaz entre los aplicativos de negociación. Las modificaciones de cupos son manuales y deben realizarse en varios aplicativos	Presión de tiempo para realizar operaciones.	3	C	Poco	Bajo	1
3	Problemas por fallas en sistemas transaccionales.	Se depende de fuentes externas y no existe plan de contingencia formal.	Caída o servicio deficiente de los sistemas de transacción	3	E	Moderado	Moderado	1
4	Problemas por errores en la inclusión de operaciones en los aplicativos	El aplicativo no cuenta con mecanismos de verificación del adecuado registro de las operaciones.	Presión de tiempo para realizar operaciones	3	C	Moderado	Moderado	2
5	Problemas generados por inconsistencia entre las operaciones constituidas y las gestiones (papeletas) recibidas	En el front office, no se verifican datos ingresados en aplicativo contra ticket	Presión de tiempo.	2	C	Moderado	Moderado	2
6	Incumplimiento por parte del Banco de las condiciones de negociación definidas en el contrato marco	El contrato no se recibe oportunamente. El proceso no tiene explicita la etapa de revisión detallada por parte del área de cumplimiento de los datos contrato	Presión de tiempo.	2	E	Poco	Bajo	1

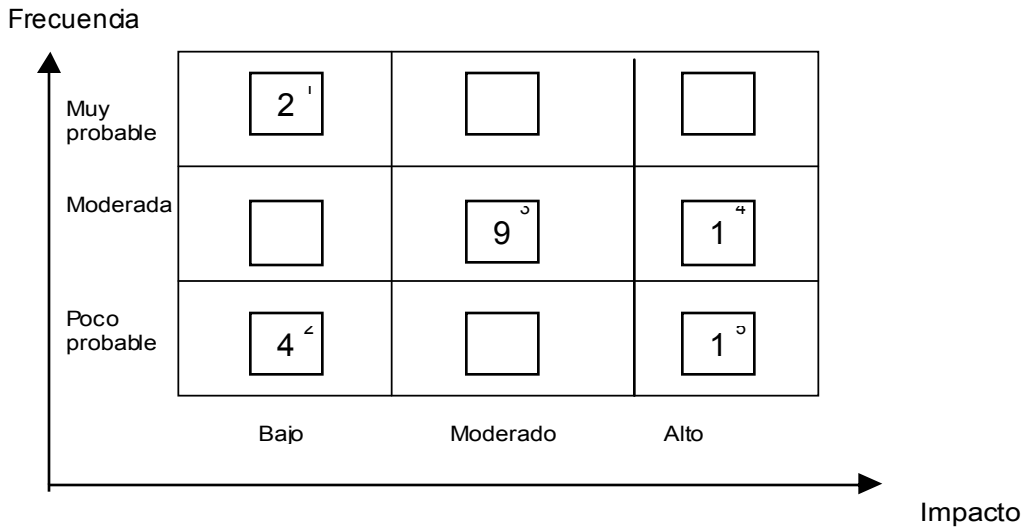
[82] Idem.

	Riesgo	Vulnerabilidad	Amenaza	Clasificación		Frecuencia	Impacto	Importancia
				Tipo	Sub tipo			
7	Errores en la toma de decisiones por falta de información del portafolio global del Banco.	No se cuenta con un sistema de administración y control de portafolios adecuado. Las operaciones se manejan en distintos aplicativos.	Permanentemente se deben tomar decisiones de portafolio. Presión de tiempo	3	C	Moderado	Moderado	1
8	Imposibilidad de operar por factores externos como cortes de electricidad, problemas de acceso a las oficinas, etc.	No existe plan de contingencia formal para dar continuidad al negocio en estos casos	Algunas veces se presentan cortes de electricidad, problemas de acceso al edificio	4	B	Moderado	Moderado	1
9	Exceder límites o realizar operaciones no aprobadas por desconocimiento de políticas	Falta de capacitación. Desconocimiento del producto	Presión de tiempo al realizar las operaciones. Nuevas operaciones para la entidad. Nuevos funcionarios	1	C	Moderado	Moderado	1
10	Se pierden oportunidades de negocio porque no existen atribuciones internas para exceder límites. Todo debe ser aprobado por Junta Directiva.	El proceso no muestra las acciones alternativas a seguir en caso de requerirse exceder un límite, la línea de responsabilidad o atribución	En algunas ocasiones las condiciones de mercado puede requerir el exceso eventual de límites y la respuesta debe ser inmediata	2	A	Moderado	Moderado	1
Etapa 2: Cumplimiento								
11	En caso de incumplimiento de operaciones de un tercero hacia el Banco se presentan demoras en la toma de acciones requeridas,	No se tiene claridad de las acciones inmediatas a realizar en caso de incumplimiento. No se tiene un proceso definido para estos casos	El posible incumplimiento de operaciones hace parte del riesgo asumido en este negocio	2	E	Poco	Alto	1
12	Girar valores diferentes a los pactados o incumplimiento de compromisos	Error del trader en la digitación de la operación. El aplicativo no valida datos. Varios datos se digitan. Errores en la papeleta que soporta la operación. Controles escasos	Presión de tiempo	1	B	Moderado	Moderado	1

	Riesgo	Vulnerabilidad	Amenaza	Clasificación		Frecuencia	Impacto	Importancia
				Tipo	Sub tipo			
13	Incumplimiento de operaciones por fallas de los sistemas operacionales en los cuales se registran las operaciones.	No existe plan de contingencia formal	Caída o servicio deficiente de los sistemas	3	C	Moderado	Alto	1
14	Registro contable distinto al de la negociación	Proceso de registro manual. Pocos controles	Elevado número de operaciones y de terceros	3	C	Muy	Bajo	1
Etapa 3: Valoración								
15	Errores en decisiones de negociación por falta de oportunidad de los reportes de valoración (tasas requeridas para valorar las operaciones)	No se tiene fuente de información alterna para obtener tasas de valoración. Estas tasas no se encuentran en el sistema de información del Banco en tiempo real	Presión de tiempo	3	E	Poco	Bajo	3
16	Discrepancias entre registros contables y el aplicativo central frente a datos de valoración	Fallas de digitación, aproximaciones o redondeo de cifras	No existe interfaz que comunique los aplicativos	3	D	Muy	Bajo	2
17	La información sobre el portafolio valorado es mínima, lo que no permite una administración integral del mismo	Ausencia de políticas claras de valoración financiera. No se cuenta con aplicativo que permita valorar financieramente las operaciones. Gran manejo manual de cálculos. Aplicativos no vinculados	Algunas estrategia tienen como insumo el portafolio valorado y por lo tanto pueden ser erradas	3	C	Poco	Bajo	3

5.2.4.3.6 Matriz de riesgos

De acuerdo con estos resultados se obtuvo la siguiente matriz de riesgos:



1. Corresponde a los riesgos 14 y 16 de la tabla 12
2. Corresponde a los riesgos 2,6,15 y 17 de la tabla 12
3. Corresponde a los riesgos 1, 3, 4, 5, 7, 8, 9, 10 y 12 de la tabla 12
4. Corresponde al riesgo 13 de la tabla 12
5. Corresponde al riesgo 11 de la tabla 12

5.2.4.3.7 Propuesta acción a seguir con los eventos de riesgo identificados

Siguiendo la propuesta del capitulo cuatro y con el fin de definir la acción a seguir con cada evento de riesgo se sugiere la siguiente clasificación:

Tabla 13. Propuesta acción a seguir con los eventos de riesgo identificados

Impacto	Frecuencia	Riesgo	Número de eventos en el proceso	Acción a seguir
Alto	Muy probable	Riesgo alto	0	Atención inmediata
Alto	Moderado	Riesgo severo	1	Implementar en el corto plazo mecanismos que eliminen o minimicen los factores de riesgo
Alto	Poco probable	Riesgo severo	1	"
Moderado	Muy probable	Riesgo severo	0	"
Moderado	Moderado	Riesgo moderado	9	Implementar en el mediano plazo mecanismos que eliminen o minimicen los factores de riesgo
Moderado	Poco probable	Riesgo moderado	0	"
Bajo	Muy probable	Riesgo moderado	2	"
Bajo	Moderado	Riesgo bajo	0	Administración con controles
Bajo	Poco probable	Riesgo bajo	4	"

Como resultado de la aplicación del método Delphi, la entidad logró identificar los principales eventos de riesgo que afectan la línea de negocio (17), identificar la principal causa que los genera y asignarles una calificación de frecuencia e impacto. Con esta información, el grupo de trabajo de riesgo operacional procederá a diseñar mecanismos para la recolección de datos y determinará el tratamiento que se le dará a cada uno de los eventos de riesgo identificados. Los resultados de este ejercicio deberán complementarse con eventos de riesgo adicionales que se presenten en adelante en la línea de negocio y no hayan sido contemplados dentro de los 17 eventos de riesgo.

5.2.5 Recolección de datos

La implementación de un sistema de administración de riesgo operacional tiene entre sus objetivos mejorar la eficiencia de la entidad y por lo tanto dentro de su filosofía no está la generación de mayores tareas a los funcionarios a través del diligenciamiento permanente de formatos. No obstante, hasta que la entidad cuente con los aplicativos tecnológicos adecuados la recolección inicial de datos requiere la colaboración de cada uno de los funcionarios involucrados en el proceso a través del registro de los eventos generadores de pérdida.

El diseño de formatos de registro se constituye en una herramienta importante para la recolección de datos. Estos formatos deben tener claramente asignado un responsable y el diligenciamiento de los mismos deberá ser revisado periódicamente.

En la tabla 14 se presenta el registro requerido para cada uno de los eventos de riesgo identificados.

	Tabla 14. Datos que se deben registrar de los eventos de riesgo		
	Proceso de compra y venta de divisas (Forward)		
	Etapa 1: Negociación		
	Riesgo	**Datos a registrar**	**Responsable**
1	Problemas en estrategias de cobertura por errores de cálculo en posición propia	Corrección del valor de posición propia	Analista de Contabilidad
2	Exceso en cupos de negociación aprobados	Exceso de cupos de negociación sin previa autorización	Analista de Riesgo
3	Problemas por fallas en sistemas transaccionales.	Fallas en sistemas transaccionales	Trader
4	Problemas por errores en la inclusión de operaciones en los aplicativos	Corrección de valor de operaciones registradas por el trader.	Trader
5	Problemas generados por inconsistencia entre las operaciones constituidas y las gestiones recibidas	Corrección de valor de operaciones registradas por el trader o corrección de tickets.	Trader
6	Incumplimiento de condiciones de negociación definidas en el contrato marco	Eventos de incumplimiento de condiciones de contrato	Funcionario de Operaciones
7	Errores en la toma de decisiones por falta de información	Eventos de pérdida de dinero o de oportunidades de negocios por falta de información del portafolio	Trader
8	Imposibilidad de operar por factores externos	Ocurrencia de eventos externos que no permitan operar	Trader
9	Exceder límites o realizar operaciones no aprobadas por desconocimiento de políticas	Realización de operaciones no autorizadas en tipo o en monto	Analista de Riesgo
10	Se pierden oportunidades de negocio porque no existen atribuciones para exceder límites	Pérdida de negocios por carencia de políticas o procedimientos	Trader

	Riesgo	Datos a registrar	Responsable
	Etapa 2: Cumplimiento		
11	Demora en toma de acciones requeridas, en caso de incumplimiento de operaciones hacia el Banco	Incumplimiento de operaciones por parte de terceros	Funcionario de Operaciones
12	Girar valores diferentes a los pactados o incumplimiento de compromisos	Pérdida por errores en cumplimiento de operaciones Incumplimiento de operaciones	Funcionario de Operaciones
13	Incumplimiento de operaciones por fallas de los sistemas operacionales	Fallas en sistemas operacionales	Funcionario de Operaciones
14	Registro contable distinto al de la negociación	Correcciones a la información contable	Funcionario de Operaciones
	Etapa 3: Valoración		
	Riesgo	**Datos a registrar**	**Responsable**
15	Errores por falta de oportunidad en reportes de valoración	Pérdidas de dinero o de negocios por demoras en valoración	Trader
16	Discrepancias entre registros contables y el aplicativo central	Correcciones a los registros contables por no coincidir con aplicativo valoración	Analista de Riesgo
17	Mínima información sobre el portafolio valorado	Pérdidas de dinero o de negocios por deficiente información de portafolio valorado	Trader

Teniendo en cuenta que actualmente los aplicativos tecnológicos que operan en la entidad no permiten guardar automáticamente los eventos de riesgo operacional es necesario apoyar dicha labor en el diligenciamiento de formatos. En la tabla 15 se presenta una propuesta del formato que podría utilizarse para el registro de los eventos de riesgo.

Tabla 15. Formato registro de eventos de riesgo operacional

Ejemplo: Problemas por fallas en sistemas transaccionales

Fecha evento	Línea de negocio	Descripció evento	Factor de riesgo	Áreas afectadas	Conse-cuencias				Monto recupera-ción
					Valor de las pérdidas ($)	Tiempo reprocesa miento	Detalle pérdida negocios	Otras	

La recolección de datos en forma manual requiere contar con la colaboración de los funcionarios que participan en el proceso y para esto es imprescindible que la organización cuente con una cultura de riesgo desarrollada.

Diariamente, el analista de riesgo operacional deberá recibir las plantillas de registro de eventos de cada una de las áreas relacionadas con el proceso con el fin de consolidar toda la información en una sola base de datos y realizar los reportes que correspondan. El analista de riesgo es el único funcionario autorizado para cargar los reportes de cada una de las áreas a la base de datos previa revisión de la información.

En el corto plazo, es conveniente que la entidad adecué los aplicativos tecnológicos con herramientas que permitan registrar la ocurrencia de eventos de riesgo, ya que esto le dará mayor confiabilidad a la recolección de datos. En todos los casos, la dirección de cada área involucrada deberá realizar una auditoria periódica a los formatos de registro de eventos de riesgo frente a la realidad de la entidad y posteriormente a los informes que resulten de los aplicativos.

5.2.6 Monitoreo de riesgos

El monitoreo de los eventos de riesgo operacional permite a los distintos niveles de la organización estar informados del desempeño del sistema de administración

de riesgo operacional con el fin de que se tomen las acciones que correspondan. El monitoreo se realiza a través de distintos informes cuyo nivel de detalle depende de la instancia a la cual se presenta.

Teniendo en cuenta la estructura organizacional de la entidad se sugiere que para la línea de estudio se diseñen tres tipos de informes:

- Gerencial: dirigido a Junta Directiva, Comité de Administración de Riesgo
- Detallado: Comité de Riesgo Operacional
- De control: Área de Riesgo

El responsable de la elaboración de estos informes es el analista de riesgo operacional. No obstante, la confiabilidad y oportunidad de los datos utilizados para los informes dependen de los funcionarios responsables de riesgo operacional de cada una de las áreas.

El informe gerencial deberá incluir la información consolidada de todas las líneas de negocio, la periodicidad es mensual y se sugiere incorpore la siguiente información:

- Evolución mensual número de eventos de riesgo operacional registrados.
- Evolución mensual número de eventos de riesgo operacional registrados que generan pérdida.
- Evolución mensual de las pérdidas generadas por riesgo operacional.
- Distribución de las pérdidas generadas por riesgo operacional en el mes por línea de negocio.
- Distribución de las pérdidas generadas por riesgo operacional en el mes por factor de riesgo.
- Mejoras de eficiencia registradas en las diferentes líneas en el mes.
- Reporte de incumplimiento de políticas determinando responsable, causa y acción tomada.

El informe detallado podría incluir el informe gerencial y adicionalmente presentar un informe individual de cada una de las líneas de negocio. La periodicidad es mensual. Para la línea de estudio, el informe complementario podría incluir la siguiente información:

- Evolución de las pérdidas generadas por riesgo operacional en el mes.
- Evolución el número de reprocesos realizados en el mes.
-

- Distribución de las pérdidas generadas en el mes por factor de riesgo.
- Reporte de incumplimiento de políticas
- Reporte de mejoras realizadas al proceso
- Número de negocios perdidos por problemas de riesgo operacional
- Indicadores detallados: se elaboran de acuerdo con los riesgos identificados en cada línea y con los datos disponibles. Para la línea de estudio se identificaron 17 posibles generadores de eventos de riesgo y por lo tanto el informe deberá incluir para cada uno de los eventos de riesgo el número de veces que se registró en el mes y el impacto generado.

El informe de control es consolidado y se deberá realizar diariamente. Este informe deberá incluir cada uno de los eventos de riesgo registrados durante el día, con la línea de negocio correspondiente, el impacto y el factor de riesgo asociado.

Además de entregar los informes a las instancias respectivas es importante que éstos sean divulgados periódicamente a través de capacitaciones a todos los funcionarios de la entidad. Adicionalmente estos informes deberán incluirse en el sistema de información gerencial del Banco.

5.2.7 Mitigación de riesgos

Las estrategias de mitigación se diseñan siguiendo la política específica establecida por la Junta Directiva frente al tema. Adicionalmente se asume que la entidad realizó todas las acciones necesarias para cumplir con las políticas generales y específicas establecidas y por lo tanto ya se cuenta con manuales de procesos y funciones revisados y actualizados.

Para cada uno de los 17 eventos de riesgo identificados por los encuestados se propone una estrategia de mitigación del mismo. Teniendo en cuenta que la entidad aún no cuenta con datos históricos sobre las pérdidas generadas por riesgo operacional, la valoración de pérdidas es subjetiva y por lo tanto, el efecto de la mitigación no se puede cuantificar de manera exacta hasta tanto se cuente con los datos históricos.

Para efectos de este estudio se asume que ningún evento de riesgo generaría pérdidas mayores a COP 1.000 millones y por lo tanto ningún evento quedó categorizado como evento de riesgo a evitar.

Cada evento de riesgo tiene asignada una clasificación de riesgo específica con el fin de facilitar la administración del mismo, no obstante es muy usual que un evento de riesgo se pueda clasificar en varias categorías (personas, procesos, tecnología y externalidades), en cuyo caso se diseñan planes de mitigación relacionados con cada una de las categorías. Se destaca que la mayor parte de los eventos de riesgo identificados tienen vinculado una estrategia de mitigación relacionada con tecnología, ya que un aplicativo tecnológico adecuado permite reducir riesgos de personal, de procesos, de tecnología y hasta externalidades. Por lo anterior es muy común que las entidades financieras consideren al soporte tecnológico como uno de los grandes pilares de un sistema de administración de riesgo operacional

En la tabla 16 se presentan los eventos de riesgo identificados con la correspondiente estrategia de mitigación incluyendo los controles que se sugiere implementar:

Tabla 16. Propuesta estrategias de mitigación

Proceso de compra y venta de divisas (forward)					
Etapa 1: Negociación					
	Riesgo	**Causa**	**Estrategia de mitigación**		
			Corto plazo	**Controles**	**Largo plazo**
1	Problemas en estrategias de cobertura por errores de cálculo en posición propia	Personas	Implementación mecanismos de control. Definición clara de funcionario responsable de la actualización de la normatividad.	Verificación de principales cifras utilizadas para calcular la posición propia	Mayor sistematización del proceso
2	Exceso en cupos de negociación aprobados	Tecnología	Implementación de controles	Verificación cupos aprobados vs cupos alimentados en los aplicativos	Implementación tecnológica que permita interfaz entre los distintos aplicativos
3	Problemas por fallas en sistemas transaccionales.	Tecnología	Diseño de plan de contingencia (acuerdos con otras entidades para utilizar sus aplicativos, definición clara de acciones a seguir en estos casos)		
4	Problemas por errores en la inclusión de operaciones en los aplicativos	Tecnología	Capacitación periódica y detallada del proceso y del producto. Adquisición de pólizas de seguros	Verificación diaria aleatoria de operaciones por parte del Director.	Implementación de sistema tecnológico adecuado
5	Problemas generados por inconsistencia entre las operaciones constituidas y las gestiones recibidas	Procesos	Implementación de controles	Verificación de ticket vs operaciones en aplicativo	Implementación interfaz entre aplicativo operacional, de control de cupos y emisor del ticket

	Riesgo	Causa	Estrategia de mitigación		
			Corto plazo	**Controles**	**Largo plazo**
6	Incumplimiento de condiciones de negociación definidas en el contrato marco	Procesos	Capacitación periódica y detallada del proceso y del producto. Diseño de mecanismos efectivos de comunicación de condiciones del contrato		Parametrización en el aplicativo de las condiciones de cada contrato
7	Errores en la toma de decisiones por falta de información	Tecnología	Diseño de informes que integren todas las operaciones		Implementación de un aplicativo tecnológico que permita un manejo integral del portafolio
8	Imposibilidad de operar por factores externos	Externalidades	Diseño de plan de contingencia (acuerdos con otras entidades para utilizar sus aplicativos, definición clara de acciones a seguir en estos casos). Adquisición de póliza de seguros.		
9	Exceder límites o realizar operaciones no aprobadas por desconocimiento de políticas	Personas	Capacitaciones periódicas sobre políticas, productos y procedimientos. Diseño de instructivo interactivo y claro sobre políticas	Verificación de operaciones vs límites	Implementación de aplicativo tecnológico que no permita realizar operaciones no aprobadas por Junta Directiva
10	Se pierden oportunidades de negocio porque no existen atribuciones para exceder límites	Procesos	Diseño de proceso de exceso de límites. Los distintos aplicativos deben bloquear automáticamente exceso de límites. Sólo determinados perfiles tendrán la atribución de autorizar exceder dichos límites previa realización del procedimiento que se defina.	Verificación de cumplimiento de protocolo en caso exceso de límites	Implementación de aplicativo tecnológico que sólo permita exceder operaciones previa autorización de determinados perfiles
Etapa 2: Cumplimiento					
11	Demora en toma de acciones requeridas, en caso de incumplimiento de operaciones hacia el Banco	Procesos	Diseño del proceso requerido. Implementación de sistemas de información que en tiempo real comunique el incumplimiento a todos los interesados		

	Riesgo	Causa	Estrategia de mitigación		
			Corto plazo	Controles	Largo plazo
12	Girar valores diferentes a los pactados o incumplimiento de compromisos	Personas	Implementación de controles	Verificación de operaciones a cumplir vs ticket	Implementación aplicativo tecnológico que integre el cargue de la operación, la elaboración del ticket, el control de cupos y el registro del cumplimiento
13	Incumplimiento de operaciones por fallas de los sistemas operacionales	Tecnología	Diseño de plan de contingencia (acuerdos con otras entidades para utilizar sus aplicativos, definición clara de acciones a seguir en estos casos),		
14	Registro contable distinto al de la negociación	Tecnología	Implementación de controles	Verificación de operaciones registradas vs ticket	Implementación aplicativo tecnológico que integre todos los procesos requeridos para el producto en tiempo real.
Etapa 3: Valoración					
15	Errores por falta de oportunidad en reportes de valoración	Tecnología	Mejoras al sistema de información		Implementación de aplicativo tecnológico que permita valorar las operaciones en tiempo real
16	Discrepancias entre registros contables y el aplicativo central	Tecnología	Implementación de controles	Verificación datos valoración vs datos contabilidad	Implementación aplicativo tecnológico que integre todos los procesos requeridos para el producto en tiempo real.
17	Deficiente información sobre el portafolio valorado	Tecnología			Implementación de aplicativo tecnológico que permita valorar el portafolio integral en tiempo real

Aunque se proponen estrategias de mitigación para todos los eventos de riesgo, la velocidad de implementación de las mismas depende de la categoría de riesgo que generen (alto, severo, moderado y bajo). Por esta razón los eventos de riesgo identificados con los números 11 (demora en toma de acciones requeridas, en caso de incumplimiento de operaciones hacia el Banco) y 13 (incumplimiento de operaciones por fallas de los sistemas operacionales clasificados como riesgo) clasificados como riesgo severo requieren implementar las estrategias de mitigación en el corto plazo.

Dentro de las estrategias de mitigación de largo plazo se destaca la relacionada con la implementación de un aplicativo tecnológico adecuado para el manejo de portafolio del Banco y que opere en línea con los demás aplicativos. La

implementación de este aplicativo permitiría minimizar la ocurrencia de 12 de 17 eventos generadores de riesgo.

Como parte de las estrategias de mitigación se encuentra la implementación de controles. Estos mecanismos se diseñaron tanto para realizar autocontrol como para realizar controles externos. Aunque en el proceso, la entidad aplica algunos controles estos son esporádicos y no están debidamente formalizados. Para que los controles sean realmente efectivos se requiere que estén debidamente documentados, claramente asignado un responsable, efectivamente divulgados, periódicamente monitoreados y revisados[83]. En la tabla 17 se presentan los controles requeridos. A cada uno de los controles se le asignó una descripción, ubicación, responsable, método de control, categoría y frecuencia.

Tabla 17. Propuesta controles

Proceso de compra y venta de divisas (Forward)							
Etapa 1: Negociación							
	Controles	**Descripción**	**Ubicación**	**Responsable**	**Método**	**Categoría**	**Frecuencia**
1	Verificación de principales cifras utilizadas para calcular la posición propia	Antes de reportar el valor, el analista de contabilidad deberá verificar diariamente las principales cifras utilizadas para el cálculo (apoyado en planilla de control y en el aplicativo tecnológico que detecta importantes variaciones diarias). El Director de Contabilidad deberá realizar este control quincenalmente y verificar aleatoriamente el diligenciamiento e la plantilla de control.	Etapa de Negociación. Subproceso: Cálculo de posición propia	Analista de Contabiliad. Director de Contabilidad	Manual	Preventivo por parte del analista. Detectivo por parte del Director	Diaria
2	Verificación cupos aprobados vs cupos alimentados en los aplicativos	Al inicio de cada día, el analista de riesgo deberá verificar los cupos aprobados frente a los cupos cargados en los distintos aplicativos con la ayuda de un programa. El Director de riesgo deberá realizar este control por lo menos una vez a las semana.	Etapa: Negociación Subproceso: Alimentación de cupos	Analista de Riesgo. Director de Riesgo	Automático	Detectivo (ya que la información se consolida el día siguiente)	Diaria

[83] Tomado de: . Buniak Leonardo y Asociados. Curso Avanzado para el Análisis, Evaluación y Gestión de Riesgo Operacional Miami, octubre de 2004.

	Controles	Descripción	Ubicación	Responsable	Método	Categoría	Frecuencia
4	Verificación diaria aleatoria de operaciones por parte del Director.	El trader deberá verificar algunos datos principales de la operación antes de grabarla. El Tesorero verificará aleatoriamente que el cargue de las operaciones sea correcto	Etapa: Negociación. Subproceso: Inclusión de la operación en el aplicativo	Trader. Tesorero	Manual	Detectivo	Diaria
5	Verificación de ticket vs operaciones en aplicativo	El trader deberá verificar que todos los datos del ticket sean iguales a los ingresaos en el aplicativo. El Tesorero deberá realizar diariamente en forma aleatoria este control.	Etapa: Negociación. Subproceso: elaboración de ticket	Trader. Tesorero	Manual	Preventivo por parte del trader. Detectivo por parte del Tesorero	Diaria
9	Verificación de operaciones vs límites	El Director de Riesgo deberá verificar diariamente el tipo de operaciones realizadas vs los límites permitidos	Etapa: Negociación. Subproceso: generación informe de cupos	Director de Riesgo	Automático	Detectivo	Diaria
10	Verificación de cumplimiento de protocolo en caso exceso de límites	El Director de Riesgo diariamente deberá identificar los casos de exceso de límites y verificar si se realizó el procedimiento requerido.	Etapa: Negociación. Subproceso: generación informe de cupos	Director de Riesgo	Manual	Detectivo	Diaria
Etapa 2: Cumplimiento							
12	Verificación de operaciones a cumplir vs ticket	El funcionario de operaciones deberá diligenciar la plantilla de control en la cual se verifican los principales datos de la operación a cumplir vs el ticket para cada una de las operaciones a cumplir. El Director de Operaciones deberá verificar aleatoriamente el adecuado diligenciamiento de la plantilla por lo menos una vez por semana.	Etapa: Cumplimiento. Subproceso: verificación liquidación del día	Funcionario de Operaciones Director de Operaciones	Manual	Preventivo por parte del funcionario de operaciones. Detectivo por parte del Director de Operaciones	Etapa: Cumplimiento. Subproceso: verificación liquidación del día
14	Verificación de operaciones registradas vs ticket	El funcionario de operaciones deberá diligenciar la plantilla de control en la cual se verifican los principales datos con los cuales registra la operación vs el ticket. El Director de Operaciones deberá verificar aleatoriamente el adecuado diligenciamiento de la plantilla por lo menos una vez por semana.	Etapa: Cumplimiento. Subproceso: verificación liquidación del día	Funcionario de Operaciones Director de Operaciones	Manual	Preventivo por parte del funcionario de operaciones. Detectivo por parte del Director de Operaciones	Diaria
Etapa 3: Valoración							
16	Verificación datos valoración vs datos contabilidad	El analista de riesgo deberá verificar diariamente que las cifras del aplicativo de valoración y las del aplicativo central coincidan. El Director de Riesgo deberá realizar semanalmente verificación.	Etapa: Valoración. Subproceso: valoración de operaciones	Analista de Riesgo Director de Riesgo	Automático	Preventivo	Diaria

5.2.8 Determinación de la infraestructura tecnológica requerida

La infraestructura tecnológica de una entidad se constituye en una herramienta que permite alcanzar los objetivos de cada negocio. El Banco objeto de estudio adelanta un proceso de transformación estratégica en el cual se busca desarrollar nuevos negocios. Por esta razón el área de tecnología está adecuando los aplicativos a los nuevos requerimientos. Dentro de este contexto, y como se mencionó al principio de este capitulo la Tesorería del Banco está pasando de ser un área de consecución de recursos a ser un área que genere importantes utilidades. Para este efecto, el Banco está desarrollando varios productos de tesorería nuevos cada uno de los cuales requiere un apoyo tecnológico específico.

Actualmente, el soporte tecnológico de la Tesorería se caracteriza por contar con varios aplicativos cada uno especializado en el manejo de una parte del proceso (registro, cupos, valoración, contabilidad, etc), los cuales no operan en línea. Por otra parte, dada la baja dinámica de operaciones que tenía anteriormente el Banco en este unidad de negocio, son aplicativos básicos que se han adecuado en la medida de lo posible, pero que no se constituyen en una herramienta de apoyo de decisiones estratégicas de portafolio debido a la fragmentación de información.

Por lo anterior, y aunque el Banco ya adelanta un proyecto de modernización del soporte tecnológico de la Tesorería, se sugiere que el nuevo aplicativo incluya las siguientes características:

- Integración de todas las etapas del proceso
- Operación en línea
- Implementación de controles automáticos
- Registro automático de eventos de riesgo operacional
- Cada dato sólo debe registrarse una vez
- Información consolidada y reportes gerenciales de administración de portafolio
- Valoración en tiempo real
- Sistema de alarmas por incumplimiento de políticas

En lo relacionado con los procesos de recolección de datos, monitoreo y control relacionados exclusivamente con riesgo operacional, la entidad requiere el diseño de una base de datos de riesgo operacional parametrizada que hará parte del *data warehouse* del Banco. Esta base de datos se alimentará automáticamente con los datos de los reportes diarios de riesgo diligenciados por cada área, pero cargados únicamente por el analista de riesgo operacional. En el mediano plazo gran parte de los eventos de riesgo deberán ser detectados por el aplicativo tecnológico y

pasarán directamente a alimentar la base de datos. Por otra parte, la entidad deberá contar con un manejador de datos que se alimente de la base de datos y permita realizar los monitoreos requeridos (cálculo de indicadores y elaboración de reportes).

5.2.9 Definición de la metodología para medición de riesgos

Inicialmente y con el fin el de dimensionar el capital requerido por riesgo operacional, se sugiere que la entidad aplique el enfoque básico sugerido por el Comité de Basilea para lo cual puede utilizar los lineamientos presentados en el trabajo de María Cristina Ricardo Varela[84].

Una vez se cuente con datos históricos, por lo menos de tres años, la entidad podrá aplicar alguna de los modelos internos sugeridos en el capitulo cuatro, teniendo presente las exigencias que hace Basilea para la utilización de este enfoque y que se presentaron en el capitulo uno. Para la entidad de estudio se sugiere utilizar la metodología Delta EVT propuesta por King, ya que está permite modelar tanto las pérdidas generadas por el proceso como por eventos extremos y adicionalmente no requiere gran cantidad de datos. El detalle de la metodología se encuentra en el capitulo tres.

[84] RICARDO VARELA María Cristina. Impacto de las Metodologías propuestas por el Comité de Basilea para el cálculo de los requerimientos de capital por riesgo operativo en el sector bancario colombiano. Tesis de ingeniería Industrial. Universidad de los Andes. Enero de 2004

CONCLUSIONES

Las pérdidas registradas en los últimos años por entidades financieras internacionales generadas por eventos de riesgo operacional dejan como enseñanza la urgente necesidad que tienen las entidades financieras de implementar un sistema de administración de riesgo operacional que minimice el impacto de este riesgo.

El nuevo acuerdo de Basilea, aún con todas las críticas que ha recibido, obligará a las entidades financieras ha implementar rápidamente sistemas de administración de riesgo operacional y destinar parte de su capital a cubrir este riesgo. Esto fortalecerá la gestión de riesgo de dichas entidades y permitirá tener sistemas financieros más sólidos.

La gestión de riesgo operacional no es solamente una moda o una norma que se debe cumplir. En el mediano plazo, las entidades que cuenten con un sistema de administración de riesgo operacional desarrollarán ventajas competitivas generadas por la disminución de pérdidas, los mayores índices de eficiencia y la mayor capacidad de respuesta ante cambios sin generar grandes traumas a la operación.

La gestión de riesgo operacional no se limita exclusivamente a la implementación de un modelo de medición de pérdidas. Al igual que la gestión de riesgo de crédito y de mercado requiere el diseño e implementación de un sistema integral y dinámico que involucre a todas las áreas de la organización.

El éxito del proceso de mitigación, y en general la gestión de riesgos está fundamentado en la cultura que la organización haya desarrollado frente al riesgo. El desarrollo de esta cultura es el principal reto que tienen las entidades financieras.

Ante el reto de la gestión de riesgo operacional, los avances del sector financiero colombiano aún son mínimos. Sin embargo, se viene desarrollando un proceso de concientización que se evidencia en el interés que varias entidades manifiestan por el tema y en la creación de unidades especializadas para administrar este riesgo. Lo anterior con el fin de competir en igualdad de condiciones con sus competidores extranjeros, los cuales ya están adoptando las prácticas de sus casas matrices frente a este tema.

El diseño de un sistema de riesgo operacional es propio de cada entidad y de las necesidades de la misma. No obstante, existen algunos lineamientos generales en gran parte tomados de las mejores prácticas internacionales que todas las

entidades deberán atender. Es importante iniciar por un esquema de baja complejidad que permita avanzar en la implementación para posteriormente, y en la medida en que se tenga mayor experiencia y mayor desarrollo de la cultura de riesgo, se complemente.

La implementación del sistema requiere de grandes esfuerzos económicos especialmente relacionados con modernización tecnológica, capacitación de personal y dedicación de tiempo por parte de todos los funcionarios, especialmente de la alta dirección. Por lo anterior, las entidades deben definir claramente los objetivos de la implementación del sistema con el fin de evaluar la relación costo–beneficio de las estrategias que se van a desarrollar.

El riesgo operacional a diferencia del riesgo de crédito y mercado involucra a toda la organización y tiene inmerso un alto grado de subjetividad. Lo anterior incrementa la complejidad de la implementación del sistema y fundamenta en gran medida el éxito de la implementación en el factor humano.

La carencia de datos de eventos de riesgo operacional se constituye en uno de los mayores obstáculos para la medición de dicho riesgo. Este es un proceso complejo ya que requiere la colaboración de todos los funcionarios. De la calidad de los datos recolectados dependerán los resultados de la medición. Por lo anterior es importante que las entidades financieras colombianas inicien lo más pronto posible este proceso.

El apoyo tecnológico es uno de los pilares de un adecuado sistema de administración de riesgo operacional, ya que minimiza la ocurrencia de eventos de riesgo, permite implementar controles, facilita la recolección de datos y el manejo posterior de modelos y permite mantener informada permanentemente a la organización. En este aspecto es relevante que el desarrollo tecnológico de cada entidad sea acorde con las necesidades del negocio y se modernice de acuerdo con los nuevos requerimientos.

En el ejercicio de diseño del sistema de administración de riesgo operacional para la línea de compra y venta de divisas forward se detectó que los aspectos desarrollados que presentaron mayor complejidad fueron la definición de políticas y la identificación y cuantificación de eventos de riesgo. El primero por la urgente necesidad de contar con el compromiso real de la alta administración y por la dificultad en determinar límites ante la ausencia de datos históricos. El segundo por la alta subjetividad que encierra igualmente por la carencia de datos históricos.

La utilización de la metodología Delphi para la identificación y clasificación de los eventos de riesgo se constituyó en una herramienta valiosa que permitió realizar dicha identificación a través de un proceso participativo y ordenado. Para la utilización de esta metodología se requiere compromiso por parte de los

encuestados. La inexistencia de datos históricos hace que en algunos casos las respuestas de los encuestados sean opuestas, principalmente las relacionadas con calificaciones cuantitativas. Por lo anterior se requiere utilizar los resultados como una guía inicial y depurarlos en la medida en que se cuente con datos históricos.

Teniendo en cuenta lo novedoso del tema para la mayoría de entidades financieras se sugiere realizar al final de la aplicación de la metodología Delphi reuniones de discusión de resultados que permitan tener mayor claridad de las respuestas de los encuestados y realizar ajustes periódicos a los resultados que se obtengan en la medida en que la organización gana mayor experiencia en el tema.

En el caso específico de la entidad utilizada para el estudio, los resultados de este trabajo se constituyen en un marco general ha seguir cuando se decida desarrollar el sistema de administración de riesgo operacional para toda la entidad. En el corto plazo, los resultados permitieron observar que se presentan importantes requerimientos en tecnología y por lo tanto la entidad en la que se realizó el estudio está concentrando grandes esfuerzos en la adecuación de dicha tecnología a las necesidades actuales.

Los resultados del trabajo también permiten concluir que el conocimiento de la organización frente al riesgo operacional es mínimo, lo que se evidencia en algunas respuestas contradictorias frente a la clasificación de dicho riesgo. Lo anterior sugiere que antes de desarrollar un plan de implementación del sistema se requiere capacitar a los funcionarios con el fin de lograr el compromiso de los mismos.

Mantener permanente informada a la organización frente a los avances del sistema de riesgo operacional es fundamental para desarrollar y fortalecer la cultura de riesgo y tomar acciones oportunas frente a los resultados del mismo. Los distintos reportes que se sugieren en la metodología apoyan esta labor.

BIBLIOGRAFIA

1. http:\www.sabarnes-oxley-forum.com

2. http:\www.isaca.org.

3. http:\www.austega.com. Operacional Risk Mesurement Methods.

4. ASTIGARRAGA Eneko, El Método Delphi, Universidad de Deusto.

5. BASEL COMITÉ ON BANKING SUPERVISIÓN. Sound Practices for the Management and Supervisión of Operacional Risk. Bank for Internacional Settlenments. Febrero de 2003. http:\www.bis.org

6. _____ Internacional Convergente of Capital Measurement and Capital Standard. A Revised Framework". Bank for Internacional Settlenments.June 2004. http:\www.bis.org

7. BERMUDEZ SALGAR Jorge. El SARC: Un Cambio Cultural. Julio de 2003.

8. BUNIAK Leonardo y Asociados. Curso Avanzado para el Análisis, Evaluación y Gestión de Riesgo Operacional. Miami, octubre de 2004

9. CORREA Patricia. Presentación Desarrollo del Nuevo Esquema de Supervisión. Convención Bancaria 2002. Cartagena Agosto 29 de 2002.

10. FITHRATINGS FINANCIAL INSTITUTIONS. Special Report. "The Oldest Tale but the newest story: Operational risk and the evolution of its measurement under Basel II". Enero 7 de 2004. http:\www.fitchratings.com

11. _____ Special Report. "Operacional Risk management & Basel II implementation: Survey results". Abril 21 de 2004. http:\www.fitchratings.com

12. HEINRICH Gregor. Representante para las Américas Banco de Pagos Internacionales (BIS). Anales de ALIDE 33.

13. HERNÁNDEZ AVENDAÑO Esperanza. Esquema de Supervisión por Riesgos: El caso Colombiano. Julio de 2003.

14. JACK L. KING. Operacional Risk. Editorial John Wiley & Sons Ltda. 2001.

15. KONOW Irene y PÉREZ Gonzalo. Métodos y Técnicas de Investigación Prospeciva para la toma de decisiones. Ed. Fundación de Est. Propectivos (FUNTURO). Universidad de Chile. 1990.

16. KPMG. FINANCIAL SERVICES. "Basel II – A Closer Look: Managing Operacional Risk".

17. LEÓN Ricardo. Nuevo Acuerdo de Basilea: Aspectos críticos y desafíos para su implantación en Colombia. II Congreso de Riesgo Financiero. Cartagena, agosto 1 de 2003.

18. PINZÓN SÁNCHEZ JORGE. Asunción de Riesgos, deberes de los administradores de las entidades financieras y funciones del supervisor. II Congreso de Riesgo Financiero. Cartagena, agosto 1 de 2003.

19. PRICE WATERHOUSE COOPERS, Gestión del Riesgo Operacional en las entidades Financieras Españolas Acuerdo de Basilea. Madrid 2 de octubre de 2002. . http:\ www.pwcglobal.com

20. _____El Riesgo Operacional en Latinoamerica. http:\ www.pwcglobal.com

21. RICARDO VARELA María Cristina. Tesis de grado de Ingeniería Industrial "Impacto de las Metodologías propuestas por el Comité de Basilea para el cálculo de los requerimientos de capital por riesgo operativo en el sector bancario colombiano". Universidad de los Andes. Enero de 2004.

22. SUESCÚN Fernando. La auditoria frente a la administración de riesgos de tesorería. FELABAN. La Habana, mayo 20 de 2004.

23. SUPERINTENDENCIA BANCARIA DE COLOMBIA. Carta Circular Externa 11 de 2002

24. _____ Carta Circular Externa 31 de marzo de 2002

25. SUPERINTENDENCIA DE BANCOS Y OTRAS INSTITUCIONES FINANCIERAS. Resolución N° 136-03 - Normas para una adecuada Administración de Riesgos. Gaceta Oficial de la República Bolivariana de Venezuela N° 37.703 del 3 de junio de 2003.

APENDICE

Definiciones básicas para la implementación del sistema de riesgo operacional

Riesgo:
Posibilidad de que se produzca un acontecimiento, que conlleve a pérdidas materiales en el resultado de las operaciones y actividades que desarrollen las instituciones financieras[85].

Administración Integral de Riesgos:
Es un conjunto de objetivos, políticas, procedimientos y acciones que se implementan para identificar, medir, monitorear, limitar, controlar, informar y revelar los distintos tipos de riesgos a que se encuentran expuestas las instituciones financieras[86].

Riesgo Operacional:
El riesgo operacional se define como el riesgo de pérdida debido a la inadecuación o a fallos de los procesos, el personal y los sistemas internos o bien a causa de acontecimientos externos. Incluye el riesgo legal, pero excluye el riesgo estratégico y el de reputación"[87].

Sistema de Administración de Riesgo Operacional
Conjunto de elementos relacionados con riesgo operacional que permiten una administración integral de este riesgo y que involucra a toda la organización. El sistema de Riesgo Operacional está conformado por las políticas de riesgo, los límites, las responsabilidades, los procesos de identificación, valoración y mitigación de riesgos, las metodologías de medición y los mecanismos de control.

Beneficios generados por la implementación de un Sistema de Riesgo Operacional:

- Mejora índices de eficiencia
- Minimiza el riesgo de grandes pérdidas por este concepto
- Mejora percepción por parte de calificadoras de riesgo y del mercado en general

[85] Superintendencia de Bancos y Otras Instituciones Financieras (SUDEBAN). Resolución N° 136-03 - Normas para una adecuada Administración de Riesgos. Gaceta Oficial de la república Bolivariana de Venezuela N° 37.703 del 3 de junio de 2003.
[86] Idem.
[87] Se adopta la definición presentada por el Banco de Pagos Internacionales. Comité de Supervisión Bancaria de Basilea. Convergencia Internacional de Medidas y Normas de Capital. Junio de 2004. Capitulo V. Página 138.

Responsables del funcionamiento del Sistema de Riesgo Operacional
Todos los funcionarios de la organización tienen responsabilidades relacionadas con el Sistema de Riesgo Operacional. No obstante esta responsabilidad está en cabeza de la Junta Directiva, el Comité de Administración de Riesgos, el Comité de Riesgo Operacional y la alta Gerencia de la entidad.

Generadores de riesgo operacional:
Riesgo de personal: pérdidas intencionales o no intencionales causadas por un empleado o relacionadas con los empleados. Ejemplo: errores en las transacciones, procedimientos inadecuados, poca disponibilidad de empleados, alta rotación del personal, lesiones físicas o psicológicas del personal, actos ilícitos, entre otros.
Riesgo de procesos: pérdidas generadas por aspectos relacionados con la ejecución y mantenimiento de las transacciones y funcionamiento de un negocio, incluyendo productos y servicios. Ejemplo: fusiones, nuevos productos o mercados, seguridad y control de calidad de procesos inadecuados, definición poco clara de responsabilidades, incumplimiento de contratos legales, entre otros.
Tecnología: pérdidas causadas por piratería, robos, fallas, interrupciones, tecnología inadecuada para las necesidades del negocio. Ejemplos: errores operativos, uso indebido o no autorizado, fallas de los equipos, hardware inadecuado o no disponible, intromisión de personas ajenas a los sistemas, interrupciones externas, virus, fallas en la ejecución de programas, negligencia en el mantenimiento, fallas con teléfono, fax, internet, entre otros.
Externalidades: pérdidas generadas por daños en la propiedad física por causas naturales o no naturales. Incluye acciones cometidas por personas externas. Ejemplo: desastres naturales o no naturales, fraude externo, lavado de dinero, cambios regulatorios, entre otros.

Indicadores de riesgo operacional:
Índices numéricos que a través de la relación de variables permiten conocer la situación de la entidad frente al riesgo operacional Estos indicadores permiten a la administración determinar controles y acciones correctivas a implementar.

Mecanismos de control de riesgo operacional:
Acciones de control sobre los procesos que conforman las líneas de negocio generalmente apoyados en los resultados de los indicadores de riesgo operacional. Estas acciones requieren una revisión periódica y buscan disminuir la frecuencia de ocurrencia de eventos generadores de riesgo operacional.

Esquemas de mitigación del riesgo operacional:
Mecanismos diseñados para minimizar o mantener controladas las posibles pérdidas que se pueden generar por la presencia de un evento generador de riesgo operacional (sistematización de procesos, adquisición de seguros, aplicación de mayores controles, etc.)

Modelos propios de medición de riesgo operacional:
Modelos generalmente estadísticos que con la ayuda de datos históricos permiten determinar el valor en riesgo de la entidad por concepto de riesgo operacional para un intervalo de tiempo determinado. De acuerdo con Basilea, el resultado de esta medición afectará el capital requerido a cada entidad.

ANEXOS

Anexo 1. Asignación de las líneas de Negocio

Asignación de la líneas de Negocio[88]		
Nivel 1	**Nivel 2**	**Grupos de actividades**
Finanzas corporativas	Finanzas corporativas	Fusiones y adquisiciones, suscripción de emisiones, privatizaciones, titularización, servicio de estudios, deuda (pública, alto rendimiento), acciones, sindicaciones, Ofertas Públicas Iniciales, colocaciones privadas en mercados secundarios
	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 de particulares, servicios bancarios, fideicomisos y testamentarías, y asesoramiento de inversión
	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, préstamo, garantías, letras de cambio
Pago y liquidación[89]	Clientes externos	Pagos y recaudaciones, transferencia de fondos, compensación y liquidación
Servicios de agencia	Custodia	Contratos de replica, certificados de depósito, operaciones de sociedades (clientes) para préstamo de valores
	Agencia para empresas	Agentes de emisiones y pagos
	Fideicomisos de empresas	
Administración de activos	Administración Discrecional de fondos	Agrupados, segregados, minoristas, institucionales, cerrados, abiertos, 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

[88] BANCO D E PAGOS INTERNACIONALES. Comité de Basilea. Convergencia internacional de medidas y normas de capital. Basilea II. Junio de 2004, Versión en Español. Anexo 6, página 218.

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

Anexo 2. Clasificación detallada de tipos de eventos de pérdida

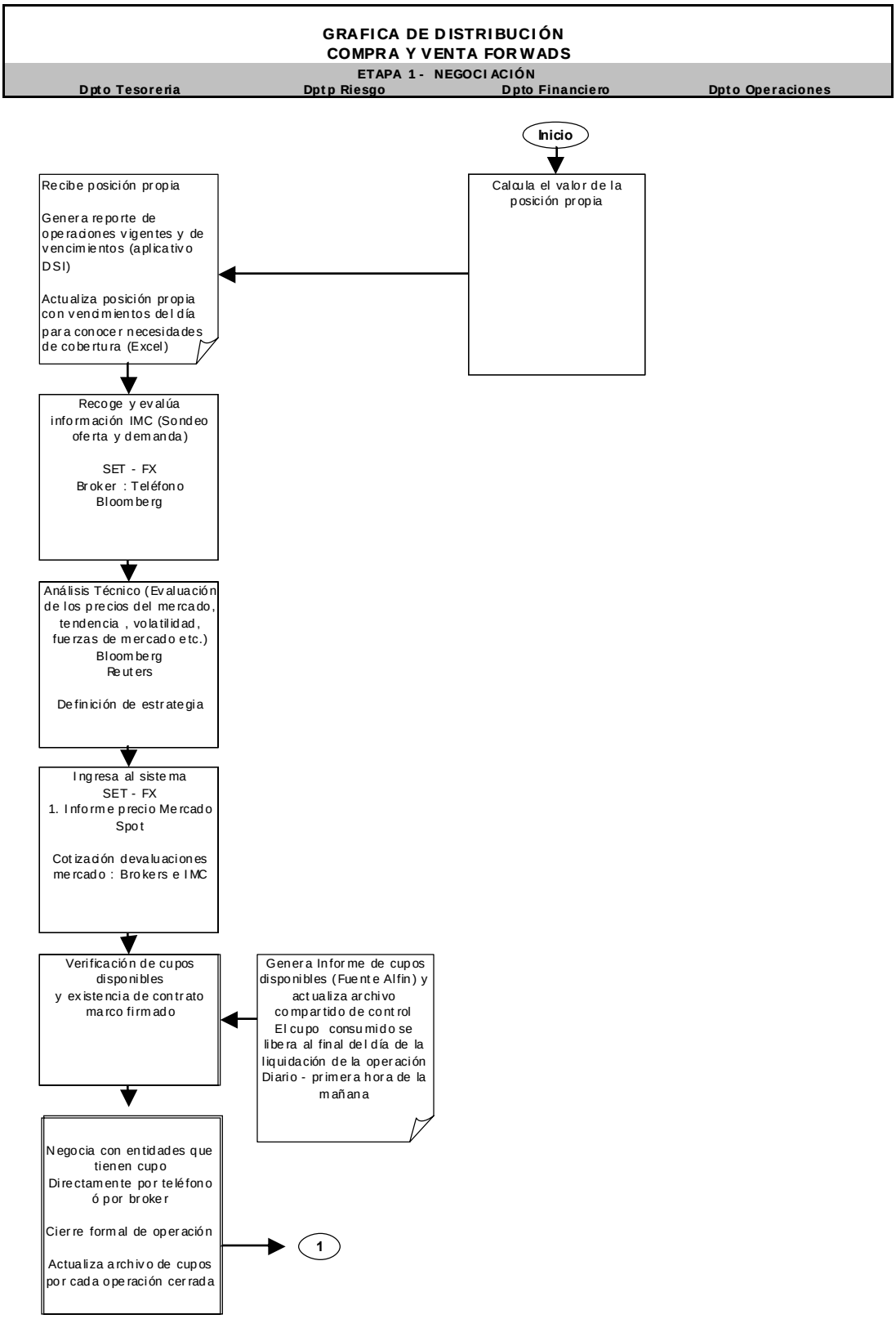
Categorías de tipos de eventos (Nivel 1)	Definición	Categorías (Nivel 2)	Ejemplos de actividades (Nivel 3)
Fraude Interno	Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o soslayar regulaciones, leyes o políticas empresariales (excluidos los eventos de diversidad / discriminación) en las que se encuentra implicada, al menos, una parte interna a la empresa	Actividades no autorizadas	Operaciones no reveladas (intencionalmente) Operaciones no autorizadas (con pérdidas pecuniarias) Valoración errónea de posiciones (intencional)
		Hurto y fraude	Fraude / fraude crediticio/ depósitos sin valor Hurto / extorsión / malversación / robo Apropiación indebida de activos Destrucción dolosa de activos Falsificación Utilización de cheques sin fondos Contrabando Apropiación de cuentas, de identidad, etc. Incumplimiento / evasión de impuestos (intencional) Soborno / cohecho Abuso de información privilegiada
Fraude Externo	Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o soslayar la legislación, por parte un tercero	Hurto y fraude	Hurto/ robo Falsificación Utilización de cheques sin fondos
		Seguridad de los sistemas	Daños por ataques informáticos Robo de información (con pérdidas pecuniarias)
Relaciones laborales y seguridad en el puesto de trabajo	Pérdidas derivadas de actuaciones incompatibles con la legislación o acuerdos laborales, sobre higiene o seguridad en el trabajo, sobre el pago de reclamaciones por daños personales, o sobre casos relacionados con la diversidad / discriminación	Relaciones laborales	Cuestiones relativas a remuneración, prestaciones sociales, extinción de contratos. Organización laboral
		Higiene y seguridad en el trabajo	Responsabilidad en general (resbalones, etc.) Casos relacionados con las normas de higiene y seguridad en el trabajo Indemnización a los trabajadores
		Diversidad y discriminación	Todo tipo de discriminación

Categorías de tipos de eventos (Nivel 1)	Definición	Categorías (Nivel 2)	Ejemplos de actividades (Nivel 3)
Clientes, productos y prácticas empresariales	Pérdidas derivadas del incumplimiento involuntario o negligente de una obligación profesional frente a clientes concretos (incluidos requisitos fiduciarios y de adecuación), o de la naturaleza o diseño de un producto	Adecuación, divulgación de información y confianza	Abusos de confianza / incumplimiento de pautas Aspectos de adecuación / divulgación de información Quebrantamiento de la privacidad de información sobre clientes minoristas Quebrantamiento de privacidad Ventas agresivas Confusión de cuentas Abuso de información confidencial Responsabilidad del prestamista
		Prácticas empresariales o de mercado improcedentes	Prácticas restrictivas de la competencia Prácticas comerciales / de mercado improcedentes Manipulación del mercado Abuso de información privilegiada (en favor de la empresa) Actividades no autorizadas Blanqueo de dinero
		Productos defectuosos	Defectos del producto (no autorizado, etc.) Error de los modelos
		Selección, patrocinio y riesgos	Ausencia de investigación a clientes conforme a las directrices Superación de los límites de riesgo frente a clientes
		Actividades de asesoramiento	Litigios sobre resultados de las actividades de asesoramiento
Daños a activos materiales	Pérdidas derivadas de daños o perjuicios a activos materiales como consecuencia de desastres naturales u otros acontecimientos	Desastres y otros acontecimientos	Pérdidas por desastres naturales Pérdidas humanas por causas externas (terrorismo, vandalismo)
Incidencias en el negocio y Fallos en los sistemas	Pérdidas derivadas de incidencias en el negocio y de fallos en los sistemas	Sistemas	Hardware Software Telecomunicaciones Interrupción / incidencias en el suministro

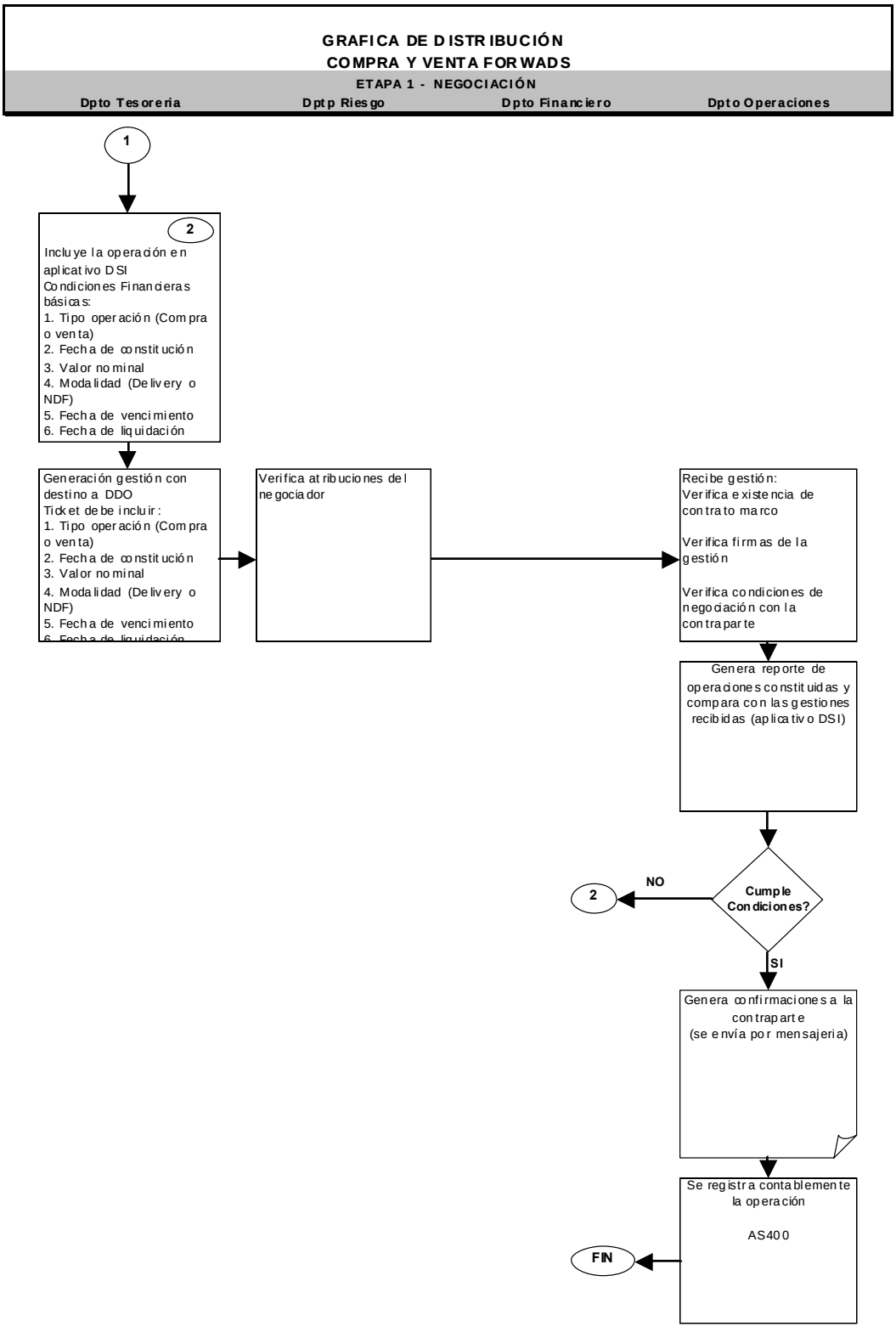
Categorías de tipos de eventos (Nivel 1)	Definición	Categorías (Nivel 2)	Ejemplos de actividades (Nivel 3)
Ejecución, entrega y gestión de procesos	Pérdidas derivadas de errores en el procesamiento de operaciones o en la gestión de procesos, así como de relaciones con contrapartes comerciales y proveedores	Recepción, ejecución y mantenimiento de operaciones	Comunicación defectuosa Errores de introducción de datos, mantenimiento o descarga Incumplimiento de plazos o de responsabilidades Ejecución errónea de modelos / sistemas Error contable / atribución a entidades erróneas Errores en otras tareas Fallo en la entrega Fallo en la gestión del colateral Mantenimiento de datos de referencia
		Seguimiento y presentación de informes	Incumplimiento de la obligación de informar Inexactitud de informes externos (con generación de pérdidas)
		Aceptación de clientes y documentación	Inexistencia de autorizaciones / rechazos de clientes Documentos jurídicos inexistentes /incompletos
		Gestión de cuentas de clientes	Acceso no autorizado a cuentas Registros incorrectos de clientes (con generación de pérdidas) Pérdida o daño de activos de clientes por Negligencia
		Contrapartes comerciales	Fallos de contrapartes distintas de clientes Otros litigios con contrapartes distintas de clientes
		Distribuidores y proveedores	Subcontratación Litigios con distribuidores

Anexo 3. Diagrama de proceso de compra y venta de divisas forward

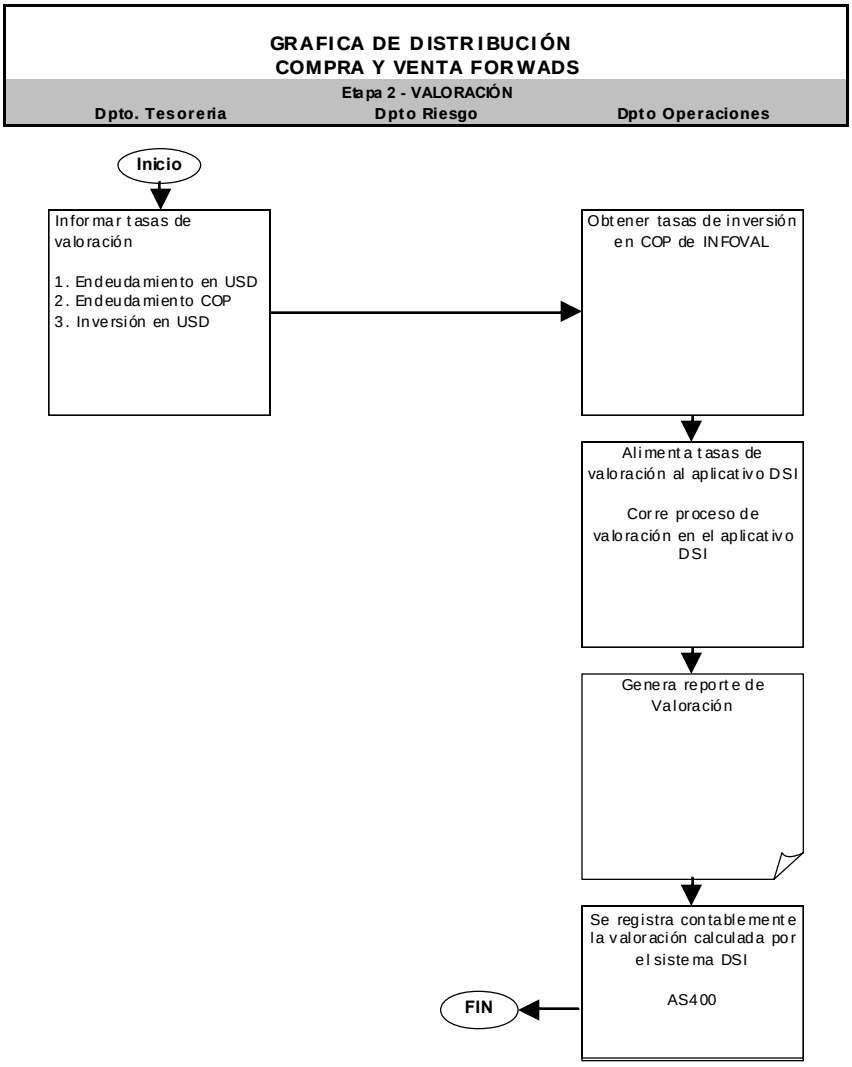
Anexo 3 Diagrama de procesos de compra y venta de divisas forward



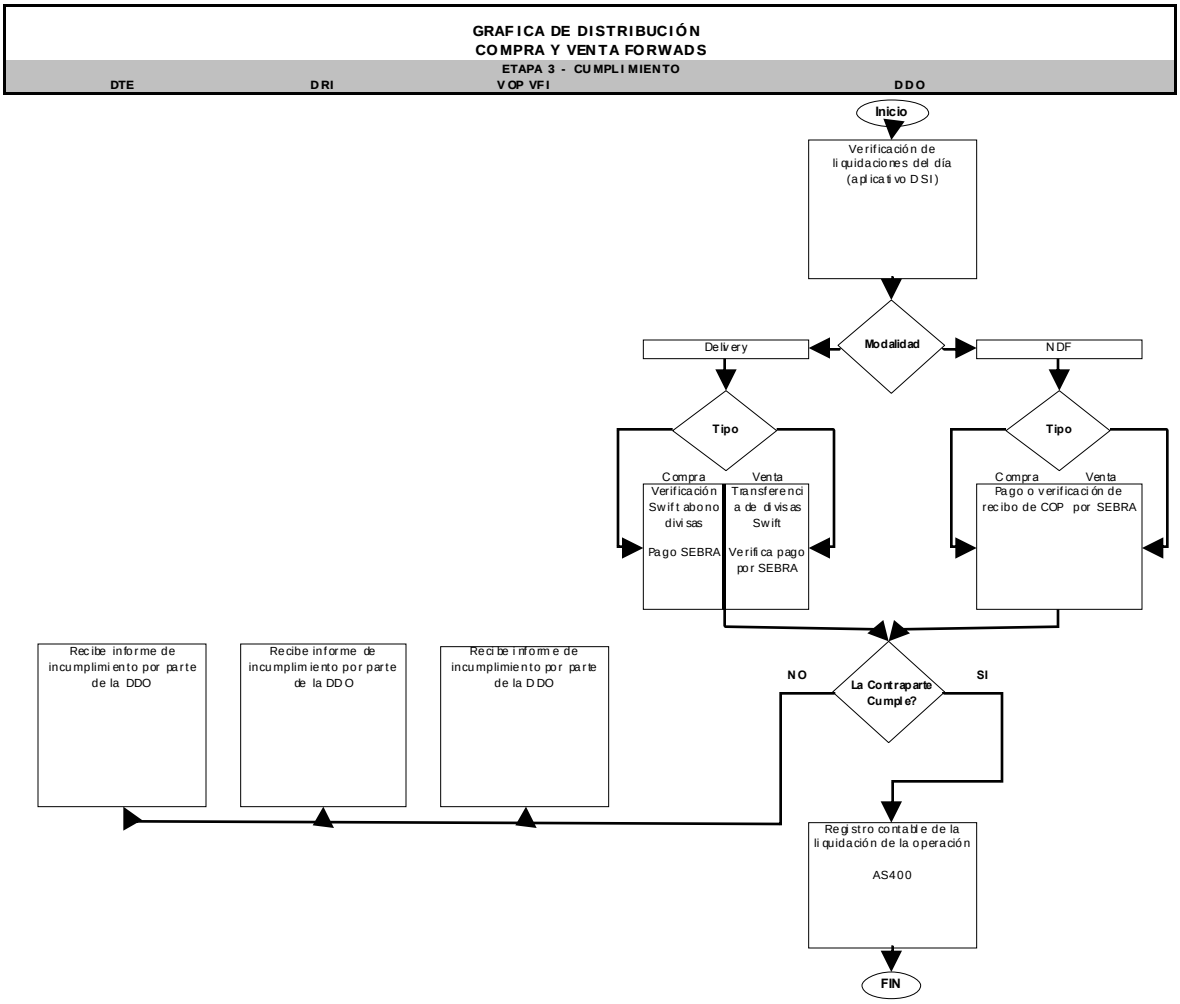
Anexo 3 Diagrama de procesos de compra y venta de divisas forward



Anexo 3 Diagrama de procesos de compra y venta de divisas forward



Anexo 3 Diagrama de procesos de compra y venta de divisas forward



Anexo 4. Encuesta entregada primera vuelta

IDENTIFICACIÓN DE EVENTOS DE RIESGO OPERACIONAL EN EL PROCESO DE COMPRA Y VENTA DE DIVISAS

PRIMERA ENCUESTA

I. Objetivo del ejercicio:

1. Identificar los posibles eventos generadores de riesgo operacional que se presentan en todo el proceso.
2. Clasificar estos eventos por causas generadoras.
3. Determinar la posible frecuencia de ocurrencia de los eventos.
4. Determinar la posible incidencia de la ocurrencia de los eventos en los resultados de la entidad.

II. Información general requerida:

Generalidades riesgo operacional

Aunque la administración del riesgo operacional ha estado presente desde hace varios años en el sector bancario, se requiere que se reconozca que este riesgo es tan importante como el riesgo de crédito y de mercado. Lo anterior en razón a que cada vez son mayores las pérdidas registradas a nivel mundial por eventos relacionados con este tipo de riesgo. El alto nivel de competitividad existente en el negocio bancario obliga a las entidades financieras a desarrollar permanentemente nuevos productos y mejorar niveles de eficiencia y tecnología. La mayor sofisticación de los productos y la velocidad con la cual deben ser implementados generan un mayor riesgo operacional que puede reflejarse en grandes pérdidas.

Por otra parte, y en respuesta a lo mencionado anteriormente, el Comité de Basilea[90] incorporó el requerimiento de capital por riesgo operacional en el nuevo documento conocido como Basilea II[91]. Por lo anterior es muy probable que en el mediano plazo, el ente regulador colombiano se pronuncie frente a este riesgo.

Basilea define el riesgo operacional como: "El riesgo de pérdida debido a la inadecuación o fallos de los procesos, el personal y los sistemas, o como resultado de acontecimientos externos". Dentro de este riesgo, Basilea incluye el riesgo legal y excluye el riesgo estratégico y reputacional.

Dentro del proceso de implementación de un sistema de administración de riesgo operacional, la identificación y valoración de los riesgos se constituye en una etapa crucial, ya que del exitoso desarrollo de esta labor dependerá en gran medida la posibilidad de contrarrestar el efecto negativo de los eventos de riesgo operacional.

Método Delphi

Para la identificación y clasificación de los riesgos se utilizará el método Delphi, el cual es una herramienta que permite construir juicios colectivos a través de juicios individuales. Este método se fundamenta en la aplicación de una serie de cuestionarios individuales a expertos. Una vez se aplica el primer cuestionario se obtiene información que posteriormente será incorporada en el siguiente cuestionario, y así sucesivamente. A través de estos cuestionarios se identifican puntos de convergencia y divergencia sobre los cuales se trabaja. El método se caracteriza por el anonimato, la interacción y la retroalimentación.

[90] Este Comité formula lineamientos y estándares internacionales para la supervisión bancaria y recomienda a las entidades financieras las mejores prácticas.
[91] El documento final fue publicado en junio de 2004.

Proceso de compra y venta de divisas

Se seleccionó el proceso de compra y venta de divisas como línea de negocio piloto para identificar y clasificar los eventos generadores de riesgo operacional. En el anexo 1 se presenta el flujograma del proceso.

III. Desarrollo de la encuesta

Esta es la primera de tres encuestas que se pretenden realizar. Por favor entregar esta encuesta diligenciada antes del día **1 de abril de 2005**.

1. De acuerdo con su experiencia identifique los eventos de riesgo operacional que se han presentado o podrían presentarse en el proceso de compra y venta de divisas (ver flujograma).

Diligencie la respuesta en el formato anexo especificando para cada uno de los eventos de riesgo la vulnerabilidad y la amenaza que tengan relacionadas.
Vulnerabilidad: deficiencias que se presentan en el proceso que permiten que el evento de riesgo ocurra.
Amenaza: hecho interno o externo que al presentarse permite que ocurra el evento de riesgo.

2. Cada uno de los eventos de riesgo identificados deben ser clasificados de acuerdo con las siguientes categorías:
Esquema de clasificación de eventos de riesgo operacional

1. Riesgo de personal	2. Riesgos procesos	3. Tecnología	4. Externalidades
A. B. Errores de empleados C. Problemas de recursos humanos D. Lesiones físicas al personal E. Lesiones no físicas al persona F. Actos ilícitos	A. Procesos del negocio B. Riesgos del negocio C. Errores y omisiones D. Responsabilidades específicas E. Incumplimientos legales	A. Problemas generales B. Hardware C. Software D. Sistemas E. Comunicaciones	A. Desastres B. Alteraciones externas C. Regulación

Riesgo de personal: pérdidas intencionales o no intencionales causadas por un empleado o relacionadas con los empleados. Las subdivisiones de esta categoría son:

- Errores de los empleados: errores en las transacciones, procedimientos inadecuados.
- Problemas de recursos humanos: poca disponibilidad de empleados, contratación, despidos.
- Lesiones físicas al personal: Lesiones corporales, salud y seguridad.
- Lesiones no físicas al personal: difamación, discriminación, hostigamiento.
- Actos ilícitos: fraude, sobornos, falsificaciones.

Riesgo de procesos: pérdidas generadas por aspectos relacionados con la ejecución y mantenimiento de las transacciones y funcionamiento de un negocio, incluyendo productos y servicios. En general sólo se incluyen aspectos que afecten únicamente a la entidad y no a terceros. Las subdivisiones de esta categoría son:

- Procesos del negocio: falta de diligencia, problemas contables.
- Riesgos del negocio: fusiones, nuevos productos o mercados.
- Errores y omisiones: seguridad y control de calidad inadecuados.
- Responsabilidades específicas: de los empleadores, directores y gerentes.
- Incumplimiento de contratos legales

Tecnología: pérdidas causadas por piratería, robos, fallas, interrupciones, tecnología inadecuada para las necesidades del negocio. Se divide en las siguientes categorías:

- Problemas generales de tecnología: errores operativos, uso indebido o no autorizado.

- Hardware: fallas de los equipos, hardware inadecuado o no disponible.
- Seguridad: intromisión de personas ajenas a los sistemas, interrupciones externas.
- Software: virus, fallas en la ejecución de programas.
- Sistemas: fallas, negligencia en el mantenimiento.
- Comunicaciones: fallas con teléfono, fax, internet.

Externalidades: pérdidas generadas por daños en la propiedad física por causas naturales o no naturales. Incluye acciones cometidas por personas externas.

- Desastres: naturales o no naturales.
- Alteraciones externas: fraude, lavado de dinero.
- Regulación: control de capital, cambios regulatorios.

Si se identifican eventos generados por riesgo operacional que puedan ser clasificados en varias casillas de la tabla se solicita clasificarlos en el aspecto que se considere tiene mayor relación y se incluya en la parte de comentarios, los otros aspectos relacionados.

3. Determinación de la frecuencia de ocurrencia:

Probabilidad de ocurrencia	N. mínimo de eventos
Muy probable	Uno en un mes
Moderado	Uno en seis meses
Poco probable	Uno en un año

4. Incidencia para el Banco en términos económicos

Incidencia	Valor de las pérdidas
Alta	Pérdidas mayores al $ 500 millones
Moderada	Pérdidas menores a $ 500 millones
Baja	Costo de reprocesamiento o ganancias no generadas

5. Calificación de la importancia del evento de riesgo otorgada por el encuestado

Calificación	El encuestado considera el riesgo
1	Muy importante
2	Moderadamente importante
3	Levemente importante

Ejemplo:

Etapa 1 del proceso: Negociación

Riesgo	Vulnerabilidad	Amenaza	Clasificación		Frecuencia	Impacto	Importancia
			Tipo	Subtipo			
Se exceden los límites de negociación aprobados por la entidad	El aplicativo no permite controlar los límites máximos de negociación	El trader debe realizar las negociaciones con gran presión de tiempo	3	C	Muy probable	Moderado	1
La entidad no puede operar	No existen planes operativos de contingencia	Fallas de la energía eléctrica por un lapso de tiempo importante	4	A	Moderada	Alta	2

Anexo 5. Encuesta entregada segunda vuelta

IDENTIFICACIÓN DE EVENTOS DE RIESGO OPERACIONAL EN EL PROCESO DE COMPRA Y VENTA DE DIVISAS - FORWARD
SEGUNDA ENCUESTA

Fecha de entrega: 10 de mayo de 2005

En el desarrollo de la primera encuesta se contó con la colaboración de seis funcionarios del Banco que laboran en las distintas áreas relacionadas con el proceso de estudio. Como resultado de estas encuestas se identificaron 22 eventos generadores de riesgo operacional.

En esta segunda encuesta se presentarán los resultados a los encuestados con el fin de que éstos manifiesten si están de acuerdo o en desacuerdo con los eventos de riesgo identificados. En los casos en los que el encuestado esté en desacuerdo deberá presentar la justificación en la casilla de comentarios.

Adicionalmente, se busca contar con la opinión de todos los encuestados frente a tres características de los eventos de riesgo identificados. Por esta razón los encuestados deberán asignar a cada uno de los riesgos identificados las características de **frecuencia, impacto e importancia.** A continuación se presentan las tablas de ayuda para la asignación de estas características.

Esquema de clasificación de eventos de riesgo operacional (informativa)

1. Riesgo de personal	2. Riesgos procesos	3. Tecnología	4. Externalidades
A. Errores de empleados B. Problemas de recursos humanos C. Lesiones físicas al personal D. Lesiones no físicas al personal E. Actos ilícitos	A. Procesos del negocio B. Riesgos del negocio C. Errores y omisiones D. Responsabilidades específicas E. Incumplimientos legales	A. Problemas generales B. Hardware C. Software D. Sistemas E. Comunicaciones	A. Desastres B. Alteraciones externas C. Regulación

Determinación de la frecuencia de ocurrencia:

Probabilidad de ocurrencia	N. mínimo de eventos
Muy probable	Uno en un mes
Moderado	Uno en seis meses
Poco probable	Uno en un año

Incidencia para el Banco en términos económicos

Incidencia	Valor de las pérdidas
Alta	Pérdidas mayores al $ 500 millones
Moderada	Pérdidas menores a $ 500 millones
Baja	Costo de reprocesamiento o ganancias no generadas

Calificación de la importancia del evento de riesgo otorgada por el encuestado

Calificación	El encuestado considera el riesgo
1	Muy importante
2	Moderadamente importante
3	Levemente importante