Universidad Andina Simón Bolívar
Sede Ecuador

Área de Gestión

Programa de Maestría
en Finanzas y Gestión de Riesgos

Formulación de una metodología para la administración de riesgo operativo, aplicado a FINCA S.A.

David Herrera Salazar

2007

Al presentar esta tesis como uno de los requisitos previos para la obtención del grado de magíster de la Universidad Andina Simón Bolívar, autorizo al centro de información o a la biblioteca de la universidad para que haga de esta tesis un documento disponible para su lectura según las normas de la universidad.

Estoy de acuerdo en que se realice cualquier copia de esta tesis dentro de las regulaciones de la universidad, siempre y cuando esta reproducción no suponga una ganancia económica potencial.

Sin perjuicio de ejercer mi derecho de autor, autorizo a la Universidad Andina Simón Bolívar para la publicación de esta tesis, o de parte de ella, por una sola vez dentro de los treinta meses después de su aprobación.

David Herrera Salazar
Diciembre 2007

Universidad Andina Simón Bolívar
Sede Ecuador

Área de Gestión

Programa de Maestría
en Finanzas y Gestión de Riesgos

Formulación de una metodología para la administración de riesgo operativo, aplicado a FINCA S.A.

Autor: David Herrera Salazar

Tutor: Econ. Roberto Andrade

Quito, 2007

Resumen

Por medio del presente estudio se pretende realizar la formulación de una metodología para la administración del riesgo operacional, de acuerdo a las normas vigentes emitidas por la Superintendencia de Bancos y Seguros, y las recomendaciones realizadas por el Comité de Basilea.

Se ha tomado como eje del estudio a la Sociedad Financiera FINCA S.A., por medio de la cual se ha realizado un seguimiento de cómo se encuentra estructurada la gestión de riesgo operacional, y en base a los resultados obtenidos se ha podido realizar ciertas recomendaciones que pueden ayudar a una mejor gestión de acuerdo a la metodología recomendada por el Comité de Basilea y adicionalmente a los lineamientos del ente de Control.

Para poder realizar las recomendaciones pertinentes para la gestión de riesgo operacional se ha tomado en cuenta los diversos temas concernientes a la implementación y requisitos que se debe tener para la gestión de este riesgo en particular, el mismo que tiene la misma importancia y su propia metodología como lo son el riesgo de mercado y liquidez, y el riesgo de crédito.

Dentro del estudio se indica la base conceptual inicial por medio de la que se parte como punto directriz, siguiendo con los requisitos indispensables para una adecuada gestión de riesgo operacional, tales como la elaboración de auto evaluaciones, mapas de riesgos, bases de datos, entre otras.

Es así que una vez conocida la base conceptual que se encuentra detrás de una correcta gestión de riesgo operacional, se estará en capacidad de conocer cuales son las principales amenazas reales o potenciales que afectan a la entidad en su conjunto (Identificación), de igual forma se podrá determinar cuál es el impacto ocasionado por los riesgos identificados en la entidad, el cual se podrá determinar por medio criterios cualitativos o cuantitativos (Evaluación), para luego poder verificar la evolución de los riesgos que han sido identificados (Seguimiento) y finalmente poder realizar las acciones que se encaminen a reducir el impacto del riesgo evaluado (Control y Mitigación).

A mis padres, por su amor y sacrificio. Por impulsarme cada día con su ejemplo y apoyo incondicional para la culminación de esta meta que es enriquecedora tanto a nivel personal como profesional. A mis hermanas por su amistad y cariño porque han sabido ser una fuente de motivación muy importante para esforzarme cada día más y poderles demostrar que los sueños se alcanzan con esfuerzo y dedicación constante.

Deseo expresar mi agradecimiento al Econ. Roberto Andrade, quien con sus valiosos conocimientos y dedicación supo dirigir la realización de esta investigación. De igual forma a Sociedad Financiera para la Asistencia Comunitaria FINCA S.A. por permitirme realizar el presente estudio y proporcionarme de la manera más efectiva la información necesaria. También a mis amigos y amigas, y a todas aquellas personas que de una u otra forma participaron en el desarrollo de esta disertación, mis sentimientos de gratitud más profundos.

INDICE

INDICE DE CUADROS

LISTADO DE ANEXOS

ANEXO 7.

Sección III, capitulo I, Subtitulo VI, Titulo VII " De los Activos y de los Límites de Crédito", de la Codificación de Resoluciones de la Superintendencia de Bancos y Seguros y Junta Banacaria

ANEXO 8.

Descripción de procesos, subprocesos y eventos de riesgos.

ANEXO 9.

Bitacora de Captura de Datos

ANEXO 10.

Actividades generadoras de pérdidas

GLOSARIO

El presente glosario recoge las equivalencias de los términos de origen inglés, así como de ciertos términos técnicos utilizados en el presente estudio. En algunos casos se han incluido los significados de las siglas en inglés entre paréntesis.

AMA	Método de Medición Avanzado
CEO	Consejero Delegado
CFO	Director Financiero
Correlación	Es el grado de asociación lineal entre dos variables
COSO	Committe of Sponsoring Organizations of the Treadway Commission
COSO – ERM	COSO conjuntamente con la gestión de riesgos corporativos
CRO	Chief Risk Officer
Diversificación	Reducción del riesgo de una cartera de inversión mediante la combinación de distintas clases de activos o instrumentos, con el propósito de compensar con activos poco correlacionados un posible descenso en el precio de alguno de ellos
FASB	Financial Accounting Standards Board
LDA	Modelo de Distribución de Pérdidas
OpVar	Capital at Risk – Capital en riesgo

Outsourcing	Es el proceso en el cual una firma identifica una porción de su proceso de negocio que podría ser desempeñada más eficientemente y/o más efectivamente por otra corporación, la cual es contratada para desarrollar esa porción de negocio.
PCAOB	Public Company Accounting Oversight Board
Probabilidad	Es la proporción de veces que un evento ocurrirá en ensayos repetidos de un experimento.
Rendimiento	Retorno de una inversión en un periodo determinado, incluyendo las ganancias por intereses, dividendos y fluctuaciones de precio
Riesgo	Es la posibilidad de que se produzca un hecho generador de pérdidas que afecten al valor económico de las instituciones
SEC	Security Exchange Commission – Comisión de Valores de Estados Unidos
VaR	Valor en riesgo
Volatilidad	Grado de fluctuación que manifiesta el precio del subyacente a través del tiempo

CAPITULO I

INTRODUCCION

1.1 PLANTEAMIENTO DEL PROBLEMA

1.1.1 Descripción del problema

Las instituciones financieras siempre han estado preocupados principalmente por tres tipos de riesgos: el riesgo crediticio, en la que el deudor deja de pagar su deuda; riesgo de liquidez, y el riesgo de mercado, en el cual se basa el análisis respecto a que un colapso anule el valor de determinadas inversiones.

En el transcurso de los últimos años ha surgido un cuarto riesgo que mantiene a las instituciones financieras con mayor preocupación, este riesgo es el operativo, el cual se enfoca en la posibilidad de que una institución pueda paralizarse por culpa de un fallo interno del sistema, como por ejemplo por carecer de protección y controles contra determinadas prácticas comerciales por parte de sus propios empleados, lo cual puede rozar en la ilegalidad, o bien debido a un acontecimiento externo.

Durante los últimos años, se ha empezado a prestar mayor atención a los riesgos operativos, debido a que la presencia de factores tales como falla en procesos, administración de recursos humanos, fallas tecnológicas, son producto de la utilización de tecnología muy automatizada; las fusiones y

adquisiciones a gran escala que por primera vez ponen a prueba la viabilidad de sistemas integrados; la consideración de los bancos como proveedores de gran variedad de servicios y la mayor utilización de técnicas de financiación que reducen los riesgos de crédito y de mercado pero que incrementan el riesgo operativo.

La piedra angular alrededor de la cual gira el riesgo operativo es la inconsistencia al definir dicho riesgo, la escasez de datos y de técnicas de estimación, las limitaciones de acumular capital para hacer frente a este tipo de riesgo, y la importancia de los controles internos y la disciplina del mercado para poder gestionar los riesgos operativos.

El objetivo de la gestión de los riesgos operativos es mejorar la gestión gracias a la identificación anticipada y posterior prevención de malas prácticas empresariales. Se destacan seis principios fundamentales de la gestión de los riesgos operativos, entre los que se incluyen: el compromiso y la cultura en toda la empresa; gobernabilidad en temas de gestión de riesgos operativos; posibles respuestas ante los riesgos operativos; identificación, estimación y respuestas ante los riesgos dinámicos; el papel de la legislación, y los cambios tecnológicos que mejoran la capacidad de la empresa para estimar y gestionar el riesgo operativo.

Así mismo poniendo hincapié en las normas de Basilea para los riesgos operativos, la complejidad de los diferentes riesgos operativos a los que se ha de enfrentar un banco o institución financiera, son aquellos casos en los que el riesgo operativo cobra sentido, clasificando los riesgos entre financieros o no financieros, y a su vez explicando el riesgo operativo como un no-financiero, se divide a su vez en tres principales categorías:[1]

- Riesgo de acontecimientos internos (como los ocurridos en instituciones como Barings, en la que Nick Leeson, agente financiero rogue trader causó enormes pérdidas).
- Riesgo de sucesos externos (donde las pérdidas proceden de un suceso externo imposible de controlar, como por ejemplo un atentado terrorista o una catástrofe natural).
- Riesgo de acontecimientos en el ámbito de los negocios, una categoría que incluye riesgos de todo tipo como aquellos relacionados con las guerras de precios, bajos niveles de actividad o un retroceso en los mercados de valores entre otros.

[1] www.wharton.universia.net/index.cfm

1.1.2 Justificación de la investigación

Por medio del estudio se pretende demostrar la importancia que tiene la gestión del Riesgo Operativo dentro de una institución, sin dejar de lado los otros riesgos existentes, ya que en la actualidad las instituciones deben poner igual énfasis en las pérdidas operacionales como en las inherentes del negocio, debido que a lo largo de los años no se ha tomado en cuenta las pérdidas que sufren las instituciones en el momento de realizar el negocio, lo cual resulta perjudicial para un correcto desenvolvimiento de las actividades de la institución.

El propósito fundamental es el de analizar y observar los resultados que se pueden obtener por medio de una gestión adecuada del riesgo operacional, por medio de la implementación de una metodología acorde con las recomendaciones realizadas por el Comité de Basilea y a su vez a las exigencias de la Superintendencia de Bancos y Seguros.

Dar a conocer cuales son las diferentes actividades críticas generadoras de pérdidas que se derivan de los respectivos macro procesos con sus correspondientes procesos y subprocesos, y la importancia que tiene el saberlos gestionar.

La investigación traerá consigo la formulación de una metodología para poner en consideración de la institución su implementación para de esta forma poder estar en capacidad no solamente de cubrir y minimizar las perdidas generadas por fallas operativas sino también el poder cumplir con el ente de control en el plazo fijado.

FINCA S.A. al ser una institución regulada se encuentra supervisada por la Superintendencia de Bancos y Seguros (SBS) del Ecuador basando su reglamentación en las Leyes, Codificación de Resoluciones, circulares y decretos emitidos por este organismo. Cabe aclarar que la mayoría de reglamentaciones de la SBS son generales para todo el sistema financiero y a la fecha no existe una regulación o normatividad específica para las instituciones de microfinanzas y en particular para las que manejan la metodología crediticia de Bancos Comunales. FINCA S.A. ha tenido que ajustarse a la normatividad vigente para cumplir con las regulaciones de la SBS del Ecuador, lo cual no aplican totalmente a la realidad de la institución y distorsiona en parte sus indicadores.

Frente a lo antes mencionado es importante que FINCA S.A., realice una correcta administración y gestión del riesgo operativo, debido a que por medio de esta se podrá minimizar todos los gastos

inherentes del negocio por las malas prácticas dentro de los diversos procesos, con lo que se ayudara a mejorar los mismos y se podrá entregar productos de calidad a sus clientes, los cuales serán los mayores beneficiarios de los servicios que la entidad presté de una manera mas eficiente.

1.2 Objetivos

1.2.1 Objetivo General

Proponer una metodología para la administración de Riesgo Operativo, el cual servirá como mecanismo para poder identificar, gestionar, medir y mitigar las pérdidas que contrae la institución por errores operativos que se generan por el giro del negocio.

1.2.2 Objetivos Específicos

- Indicar la importancia de la gestión y administración del riesgo operativo dentro de una institución financiera.
- Indicar que factores son los mayores generadores de pérdidas dentro de la institución.
- Establecer el requerimiento de capital que sería necesario para poder cubrir las pérdidas operacionales de acuerdo a los estándares establecidos.

1.3 Preguntas de Investigación

Frente a la problemática presentada anteriormente, el estudio se centrará en base a las siguientes preguntas:

- ¿Cuáles son las actividades generadoras de pérdidas inmersas en los diferentes macro procesos que tiene la institución?.
- ¿Cuáles son las pérdidas económicas generadas en cada uno de los eventos y cual de ellos es la que mayor pérdida representa?.
- ¿Es posible determinar la pérdida de los eventos de riesgo y su requerimiento de capital para cubrir los mismos por medio de un modelo para la administración del riesgo operativo?.

1.4 Delimitación del Problema

1.4.1 **Delimitación Espacial:** El estudio se realizara en FINCA S.A., con información concerniente a los diversos eventos de riesgos, recopiladas por medio de bases de datos recibidas de las diferentes sucursales que posee la Institución a nivel nacional, las cuales están situadas en las siguientes ciudades:

- Quito (Matriz y Sucursal)
- Guayaquil
- Ibarra
- Chone
- Quevedo
- Tulcán
- Libertad
- Santo Domingo
- Portoviejo
- Loja

1.4.2 **Delimitación Temporal:** El horizonte que se plantea para el estudio es a partir del mes de junio del 2005, hasta febrero del 2007, debido a que en junio del 2004, FINCA S.A. pasó de ser Fundación a ser Financiera.

1.5 Hipótesis

Las preguntas 1 y 2 no requieren hipótesis por cuanto pueden ser contestadas con una descripción de acuerdo a la realidad presentada dentro de la institución, en cuanto a la pregunta 3 se plantea la siguiente hipótesis.

La implementación de una metodología para la Administración del Riesgo Operativo en FINCA S.A. ubica a la institución en mejor posición frente a los requerimientos establecidos por la Superintendencia de Bancos y Seguros y le dota de las capacidades para identificar, gestionar, medir y mitigar los diferentes eventos generadores de pérdidas por errores en la parte operativa del negocio, teniendo en cuenta el plan de implementación presentado por la entidad a la Superintendencia de Bancos y Seguros.

CAPITULO II

MARCO TEORICO

2.1 Que es Riesgos

Se entiende por riesgos la posibilidad de sufrir un daño, dentro del ámbito financiero el daño consiste en una pérdida de valor económico.

Para poder caracterizar completamente el riesgo hay que considerar todos los posibles escenarios futuros, asignarles una probabilidad y de esta forma poder determinar los resultados económicos derivados de los mismos, es así que podría conocerse cual es la probabilidad de que las posibles perdidas futuras estuvieran comprendidas en varios niveles monetarios.

La caracterización del riesgo se vuelve complejo ya que se debe establecer todas las combinaciones posibles de las variables que influyen sobre el valor económico de la cartera o del negocio, así mismo su utilidad para la toma de decisiones será limitada sin no existe una adecuada sistematización.

Uno de los problemas dentro de la gestión del riesgo es la medición de los mismos a través de indicadores que sinteticen adecuadamente el nivel de riesgo y sean posibles a los factores del entorno que lo producen.

Frente a estos hechos, se han desarrollado dos grandes grupos de metodologías:

- Análisis de escenarios
- Técnicas de probabilidad

El análisis de escenarios consiste en seleccionar diferentes situaciones consideradas negativas y una vez seleccionadas estimar las pérdidas asociadas a cada una, en general sin tener en cuenta la probabilidad de ocurrencia que estas puedan tener.

Este planteamiento si bien fue uno de los primeros en desarrollarse todavía es útil e incluso insustituible para contemplar situaciones de crisis muy improbables pero que no se descartan que sean posibles de ocurrir, sin embargo es una medida que sirve de complemento a otras caracterizaciones del riesgo, que a su vez presenta algunas deficiencias:

- Los escenarios seleccionados son de manera subjetiva, lo cual impide lograr una homogeneidad necesaria para poder comparar los niveles de riesgo en distintos instantes.

No se llegaría a conocer la probabilidad de ocurrencia de que se pueda sufrir una perdida, ya que para ello sería necesario tener en cuenta la totalidad de los escenarios que podrían ocasionar pérdidas similares.

Las técnicas basadas en probabilidades, han permitido evitar estos problemas, con lo que se ha podido construir tablas en las que se es posible recoger el importe de cada una de las posibles pérdidas junto a su probabilidad de ocurrencia.

Estas metodologías permiten evaluar el riesgo de una forma homogénea a través de medidas comunes.

El concepto de valor en riesgo es importante, debido a que su adecuada utilización conduce al capital del que la institución va a necesitar para poder llevar a cabo el negocio.

Dentro del estudio del riesgo es importante tener en cuenta el concepto de daño, el cual esta fijado en dos principios:

- El daño se ha de medir sobre el valor actual de los negocios, carteras o posiciones que la empresa mantenga.

- El daño se refiere específicamente a las pérdidas inesperadas, mas no a los costos esperados.

De igual forma es necesario precisar el concepto de daño para distinguirlo del de costos, es así que para explicar esta diferencia existente, hay que tener en cuenta que para lograr los ingresos que se persiguen en todo negocio, es necesario incurrir en una serie de costos, los cuales reducen el beneficio final.

El riesgo se refiere exclusivamente a las desviaciones respecto a los beneficios esperados, es decir si una empresa considera que ha sufrido un daño cuando a experimentado una caída de sus beneficios en comparación a los que se preveía recibir, pero no se debe considerar como daño a los costos de producción.

2.1.1 Capital en Riesgo[2]

El capital en riesgo es el nivel de la pérdida de valor del negocio y tiene una clara conexión con el papel del capital regulador o amortiguador de riesgo.

Por lo antes mencionado, para el cálculo del capital en riesgo se requiere decidir primeramente el nivel de solvencia o la calidad crediticia que se desea tener para la institución, es por esto que esta calidad crediticia determinará el grado de seguridad con el que se debe evitar una quiebra.

[2] Soler Ramos, Jose; Gestión de Riesgos Financieros – Un enfoque práctico para los países latinoamericanos, Banco Interamericano de Desarrollo, Grupo Santander, 1999.

Una vez funcionando el negocio, el capital disponible para poder hacer frente a una posible quiebra es el valor propio del negocio, el cual solo cuando sea el valor de mercado del negocio nulo, se empezará a sufrir pérdidas.

Si el capital disponible es superior al capital en riesgo, la solvencia de la empresa es superior a la que se fijo como objetivo, y si esto no es reconocido por los prestamistas ha de considerarse la posibilidad de reducir el capital.

Cabe indicar que la diferencia entre valor en riesgo y capital en riesgo, es que el valor en riesgo es calculado con otros valores numéricos, es calculado con horizontes de tiempo corto, con grados de seguridad relativamente bajos, y omitiendo la rentabilidad esperada y los costos de financiación.

Este marco señalado ha de permitir determinar el capital en riesgo que permitirá sobrevivir a la entidad durante largos períodos de tiempo, con una altísima probabilidad de evitar quiebras, así mismo ayudará a tener en cuenta la totalidad de los riesgos y costos asociados con el negocio.

Dado que el capital en riesgo indica el capital que es necesario mantener dentro de la institución, es relevante relacionarlo con los beneficios que consiguen los accionistas a cambio de arriesgar cierta cantidad de capital.

2.2 Gestión de Riesgos

Aunque el riesgo es inherente a todas las operaciones de negocios y no puede ser eliminado totalmente, si puede ser gestionado, mitigado y, en algunos casos, asegurado.

La Alta Dirección en referencia a la gestión de riesgos en general, debe aprobar un plan estratégico lo suficientemente amplio que garantice la seguridad y solidez de la entidad. El enlace se consigue con la implantación y/o definición de un sistema de gestión integral del riesgo, que básicamente considere los siguientes aspectos:

- Identificación.
- Clasificación.
- Cuantificación.

- Mitigación.
- Seguimiento.

Las herramientas de gestión más utilizadas son aquellas que, dependiendo de su propia naturaleza, combinan los enfoques cuantitativo y cualitativo desde una perspectiva o estrategia, ex-ante o ex-post.

Así por ejemplo, se puede destacar como las técnicas más usuales las siguientes:

Enfoque cualitativo

- Evaluación Cualitativa, basada en la auto-evaluación (self-assessment)- Cuantificación, Mapas de Riesgo.
- VaR cualitativo.

Enfoque cuantitativo

- Base de Datos de Pérdidas- Impacto, análisis estadístico (VaR)

Enfoque mixto: cuantitativo y cualitativo

- Indicadores de Riesgo- Seguimiento, Alertas.

En la fase de diseño de un sistema de Indicadores de Riesgo, uno de los objetivos más difíciles de alcanzar es su enlace con la estrategia de gestión de riesgos de la entidad, y que además sea capaz de proporcionar información no sólo del grado de consecución de los objetivos prefijados, sino también de reflejar cómo se están logrando cada uno de ellos.

Para poder cumplir este objetivo, resulta imprescindible que la entidad tenga la máxima claridad estratégica de los objetivos que pretende alcanzar con la implantación de un programa de gestión y control del riesgo.

La elaboración de un marco de control, aprobado por la Alta Dirección, debe ser el vínculo para concienciar e implicar a toda la organización. Aún teniendo una estrategia de riesgos clara y perfectamente definida, pueden surgir problemas de tipo estructural al diseñar el sistema de indicadores y tratar de relacionarlos con la estrategia de la entidad.

Estos problemas que se mencionan se pueden concretar en los siguientes:

- No reflejar adecuadamente la consecución de objetivos estratégicos por un excesivo énfasis en el corto plazo, no vinculando oportunamente el corto y el largo plazo.

- Carecer de una visión de conjunto de la entidad.

- No considerar las perspectivas y exigencias del negocio.

- Poner especial énfasis en indicadores de tipo financiero.

- Realizar un mal uso de los indicadores al utilizarlos como herramientas de motivación o premio y no como una herramienta de aprendizaje y superación.

- No inducir a la mejora y el perfeccionamiento al ser sistemas concebidos desde una perspectiva más de resultados que de procesos.

2.2.1 Administración de Riesgos[3]

La identificación del riesgo es un proceso continuo y se dirige a reconocer y entender los riesgos inherentes en cada operación efectuada, y así mismo, a aquellos que pueden surgir de iniciativas de negocios nuevos.

Una vez identificados los riesgos deben ser cuantificados o medidos con el objeto de determinar el cumplimiento de las políticas, los límites fijados y el impacto económico en la organización, permitiendo a la administración disponer los controles y/o correctivos necesarios.

[3] Sección II de la Administración de Riesgos, Cáp. 1 De la gestión Integral y Control de Riesgos de la Codificación de Resoluciones de La Superintendencia de Bancos y Seguros y de la Junta Bancaria

Las metodologías y herramientas para medir el riesgo deben reflejar la complejidad de las operaciones y de los niveles de riesgos asumidos por la institución, la que verificará periódicamente su eficiencia para justificar actualizaciones y/o mejoras según demanden sus necesidades.

Todos los niveles de la organización, dentro de sus competencias, harán seguimiento sistemático de las exposiciones de riesgo y de los resultados de las acciones adoptadas, lo cual significa un monitoreo permanente a través de un sistema de información para cada tipo de riesgo, preparado para satisfacer las necesidades particulares de la institución.

Estos sistemas mantendrán información suficiente para apoyar los procesos de toma de decisiones, que permita la generación de informes permanentes, a los menos mensuales, oportunos, objetivos, relevantes, consistentes y dirigidos a los correspondientes niveles de la administración.

Los sistemas de información deben asegurar una revisión periódica y objetiva de posiciones de riesgos, así como de eventuales excepciones.

Todo proceso que se implante dentro de las instituciones financieras, enfocados para la administración integral de riesgos, debe estar permanentemente en revisiones y actualizaciones, de igual forma una adecuada administración integral de riesgos debe incluir, al menos los siguientes puntos, de acuerdo con la complejidad y tamaño de cada institución:

1. Estrategia de negocio de la entidad

2. Políticas para la administración integral de riesgos y definición de límites de exposición para cada tipo de riesgo, así como de excepciones, dictadas por el directorio u organismo que haga sus veces.

3. Procedimientos para identificar, medir, controlar / mitigar y monitorear los distintos tipos de riesgo.

4. Una estructura organizativa que defina claramente los procesos, funciones, responsabilidades y el grado de dependencia e interrelación entre las diferentes áreas de la institución del sistema financiero, que deberá incluir el comité y la unidad de administración integral de riesgos.

5. Sistemas de información que establezcan los mecanismos para elaborar e intercambiar información oportuna, confiable, fidedigna, tanto interna como externa.

2.3 Clasificación de Riesgos

2.3.1 Riesgo de Mercado

El Comité de Basilea define el riesgo de mercado como el riesgo de pérdidas en las posiciones de balance o fuera de él, originadas en movimientos de los precios de mercado, así mismo se ofrece una definición del riesgo de mercado en términos más formales, recurriendo para ello a los conceptos básicos de estadística aplicados a las finanzas; refiriéndose al riesgo en general: El riesgo puede ser definido en términos generales como la incertidumbre sobre los flujos futuros o resultados futuros.

En particular, se define el riesgo de mercado como aquel que se deriva de cambios en los precios de los activos y pasivos financieros (o volatilidades), y se mide a través de los cambios en el valor de las posiciones abiertas.

Esta evaluación se fundamenta principalmente en la medición del valor en riesgo efectuada por el propio banco o en el método estándar del riesgo de mercado.

Asimismo, la entidad deberá prestar una especial atención a la realización de pruebas de tensión a la hora de evaluar que la suficiencia de capital sea suficiente para sustentar sus actividades de negociación.

Las instituciones financieras se encuentran expuestas a pérdidas en posiciones dentro y fuera de la estructura del balance de movimientos en los precios de mercado. Dentro de los riesgos de mercado se pueden detallar los siguientes:

- El tipo de cambio, para las operaciones de monedas.

- Las tasas de interés, para los activos y pasivos financieros (incluyendo los propios de la intermediación financiera).

- El precio de los valores, para la inversión en el mercado de capitales y en el mercado bursátil.

- El precio de los metales preciosos y de los commodities en general, para las actividades propias de inversión y para los casos de activos que estén afectos a esos cambios (prestamos vinculados al sector minero).

Para manejar de una manera prudente la relación riesgo/entorno, así como para controlar y minimizar el riesgo del portafolio, es necesario considerar diversos tipos de factores tales como, la calidad, los tipos de interés, la volatilidad, la diversificación y el vencimiento de los instrumentos que componen la cartera de inversiones. Adicionalmente hay que tener en cuenta aspectos exógenos tales como la profundidad del mercado, la coyuntura económica y situación política del país, los cambios en las regulaciones fiscales, la exposiciones a ataques especulativos de inversionistas extranjeros y fluctuaciones en los mercados internacionales.

2.3.1.1 Riesgo de tipo de cambio

El riesgo de tipo de cambio es el impacto sobre las utilidades y el patrimonio de la institución controlada por variaciones en el tipo de cambio y cuyo impacto dependerá de las posiciones netas que mantenga una institución controlada, en cada una de las monedas con las que opera.

2.3.1.2 Riesgo de tasa de interés

El riego de tasa de interés es la posibilidad de que las instituciones del sistema financiero asuman pérdidas como consecuencia de movimientos adversos en las tasas de interés pactadas, cuyo efecto dependerá de la estructura de activos, pasivos y contingentes.

El riesgo de tasa de interés se descompone en:

- Riesgo de revalorización, que surge por diferencias temporales en los vencimientos (para tasa fija) o en la revalorización (para tasa flotante) de los activos, obligaciones y contingentes de la institución controlada.

- Riesgo de la curva de rendimiento, que surge de cambios en la pendiente y forma de la curva de rendimiento.

- Riesgo de correlación imperfecta que surge de los ajustes de las tasas percibidas y las pagadas en diferentes instrumentos, que por lo demás tienen características de revalorización similares.

- Riesgo de las opciones explícitas o implícitas, incluidas en muchos portafolios de activos, pasivos o contingentes.

El objetivo de los métodos de medición es la estimación del grado de exposición de una institución controlada a las variaciones en las condiciones de sus activos y pasivos por variaciones en las tasas de interés y del tipo de cambio. El uso de estos métodos permitirá a las instituciones controladas y a la Superintendencia de Bancos y Seguros la toma oportuna de las medidas necesarias para mantener y consolidar el patrimonio de la institución.

Uno de los métodos para la medición del riesgo de tasa de interés se utiliza el método de maduración:

- El método de maduración:

  Define la exposición al riesgo de tasas de interés como la brecha o descalce entre los activos y pasivos sensibles a la tasa de interés. La información sobre la medición de riesgo de tasa de interés, se elaborará utilizando el sistema de bandas temporales, estableciendo la brecha entre activos y pasivos sensibles a la tasa de interés. La información se organizará en catorce bandas temporales y los activos y pasivos deberán ser distribuidos en todas esas bandas de acuerdo a su fecha de vencimiento contractual. La brecha o descalce entre los activos y pasivos sensibles a la tasa de interés se calculará dentro de cada banda, y luego se calculará la brecha acumulada existente.

2.3.1.3 El riesgo de los commodities

El riesgo de los commodities es la posibilidad que se presenten pérdidas como consecuencia del deterioro del valor de las posiciones en acciones y participaciones en terceras compañías.

2.3.1.4 El riesgo de los precios de los valores

El riesgo de los precios de los valores es la posibilidad que se presenten pérdidas como consecuencia del deterioro del valor de las posiciones representativas en activos físicos, excepto el oro que es considerado una divisa.

El Capítulo III ñDe la Administración de Riesgo de Mercadoò, Subtítulo VI ñDe la Gestión y Administración de Riesgosò, Título VII ñDe los Activos y de los Límites de Créditoò de la Codificación de Resoluciones de la Superintendencia de Bancos y Seguros y de la Junta Bancaria, en relación con la administración del riesgo de mercado, la Sección II, establece entre otros temas, las responsabilidades y funciones de la Administración, especificando las del Directorio u organismo que haga sus veces, del Comité de Administración Integral de Riesgos, de la Unidad de Administración Integral de Riesgos. (ANEXO 1)

La Sección III, establece el ñMétodo estándar de medición de la exposición al riesgoò que define el método de maduración y la duración como métodos para la medición del riesgo de tasa de interés. Finalmente, la Sección IV define al ñValor patrimonial en riesgoò, a la pérdida de valor patrimonial que una institución controlada pueda incurrir por efectos de la exposición al riesgo que se analiza y a los factores de sensibilidad que, para el efecto, determine la Superintendencia de Bancos y Seguros. (ANEXO 2)

En forma adicional y conforme a lo establecido en las normas antes citadas se emitió la Circular SBS-DNR-DN-2002-2141 del 12 de noviembre de 2002 que expuso a las instituciones controladas la ñNota técnica sobre riesgos de mercado y liquidezò, los requerimientos de información para el control, medición, administración y supervisión de los riesgos de mercado y liquidez, a la vez de desarrollar una explicación metodológica que permita un mayor grado de profundización en el análisis de tales riesgos.

- Formatos de reportes (impresos)
- Estructura de datos

2.3.2 Riesgo de Liquidez

El Capítulo IV ñDe la Administración de Riesgo de Liquidezò, Subtítulo VI ñDe la Gestión y Administración de Riesgosò, Título VII ñDe los Activos y de los Límites de Créditoò, en la sección I, artículo 2, entiende al riesgo de liquidez, cuando la institución enfrenta una escasez de fondos para cumplir sus obligaciones y que por ello, tiene la necesidad de conseguir recursos alternativos o vender activos en condiciones desfavorables, esto es, asumiendo un alto costo financiero o una elevada tasa de descuento , incurriendo en pérdidas de valorización.(ANEXO 3)

La administración de la institución controlada deberá asegurar razonables niveles de liquidez para atender eficientemente y bajo distintos escenarios alternativos, las obligaciones con el público y los otros pasivos de naturaleza financiera que contraiga, dentro del giro de su negocio.

El índice de Liquidez Estructural considera la composición de activos y pasivos líquidos sobre los saldos contables y a una fecha determinada. Este análisis permite comparar niveles de liquidez con las volatilidades de las fuentes de fondeo, de tal manera que queda expuesta la cobertura que se tiene frente a los requerimientos.

Por medio del análisis de Brechas de Liquidez: se clasifica los flujos de capital e intereses de activos y pasivos en bandas de tiempo determinadas de acuerdo a su vencimiento. Para un mejor análisis se han creado tres escenarios: Contractual, Esperado y Dinámico. En cada escenario se da un tratamiento especial a las cuentas con vencimiento cierto y a las cuentas con vencimiento incierto.

2.3.3 Riesgo de Crédito

El riesgo de crédito es la posibilidad de pérdida debido al incumplimiento del prestatario o la contraparte en operaciones directas, indirectas o de derivados que conlleva el no pago, el pago parcial o la falta de oportunidad en el pago de las obligaciones pactadas.

Los informes presentados para analizar la exposición al riesgo de crédito, pretenden su análisis global, por lo que contendrán información a nivel general.

A continuación se muestran algunos de los puntos que se deberían incluir:

- Grado de exposición, dividido por áreas de actividad y por sectores económicos.

- Grado de diversificación de las inversiones, cuantificando el volumen según rating de las contrapartidas o grupos de riesgo.

Las instituciones controladas deben establecer esquemas eficientes de administración y control del riesgo de crédito al que se expone en el giro del negocio, es así que para cada institución controlada existe un perfil propio de riesgo según las características de los mercados en los que opera y de los productos que ofrece, por lo que cada entidad debe desarrollar su propio esquema.

Las instituciones controladas deberán contar con un proceso formalmente establecido de administración del riesgo de crédito que asegure la calidad de sus portafolios y además permita identificar, medir, controlar / mitigar y monitorear las exposiciones de riesgo de contraparte y las pérdidas esperadas, a fin de mantener una adecuada cobertura de provisiones o de patrimonio técnico.

2.3.4 Riesgo Operativo

Se entiende por riesgo operativo a la posibilidad de que se produzcan pérdidas debido a eventos originados en fallas o insuficiencia de procesos, personas, sistemas internos, tecnología, y en la presencia de eventos externos imprevistos. Incluye el riesgo legal pero excluye los riesgos sistémico y de reputación.

El riesgo operativo agrupa una variedad de riesgos relacionados con deficiencias de control interno; sistemas, procesos y procedimientos inadecuados; errores humanos y fraudes; fallas en los sistemas informáticos; ocurrencia de eventos externos o internos adversos, es decir, aquellos que afectan la capacidad de la institución para responder por sus compromisos de manera oportuna, o comprometen sus intereses.

El Art. 1, sección II, del Capítulo V ñDe la Administración del Riesgo Operativoò, Subtítulo VI ñDe la Gestión y Administración de Riesgosò, Título VII ñDe los Activos y de los Límites de Créditoò de la Codificación de Resoluciones de la Superintendencia de Bancos y Seguros y de la Junta Bancaria, en relación con los factores de riesgo operativo, señala que con el propósito de que se minimice la probabilidad de incurrir en pérdidas financieras atribuibles al riesgo operativo, deben ser adecuadamente administrados los siguientes aspectos, los cuales se interrelacionan entre sí:

- Procesos.- Con el objeto de garantizar la optimización de los recursos y la estandarización de las actividades, las instituciones controladas deben contar con procesos definidos de conformidad con la estrategia y las políticas adoptadas, que deberán ser agrupados de la siguiente manera:

    - Procesos gobernantes o estratégicos
    - Procesos productivos, fundamentales u operativos
    - Procesos habilitantes, de soporte o apoyo

- Personas.- Las instituciones controladas deben administrar el capital humano de forma adecuada, e identificar apropiadamente las fallas o insuficiencias asociadas al factor .personas., tales como: falta de personal adecuado, negligencia, error humano, nepotismo de conformidad con las disposiciones legales vigentes, inapropiadas relaciones interpersonales y ambiente laboral desfavorable, falta de especificaciones claras en los términos de contratación del personal, entre otros.

- Tecnología de información.- Las instituciones controladas deben contar con la tecnología de información que garantice la captura, procesamiento, almacenamiento y transmisión de la información de manera oportuna y confiable; evitar interrupciones del negocio y lograr que la información, inclusive aquella bajo la modalidad de servicios provistos por terceros, sea íntegra, confidencial y esté disponible para una apropiada toma de decisiones.

  Para considerar la existencia de un apropiado ambiente de gestión de riesgo operativo, las instituciones controladas deberán definir formalmente políticas, procesos y procedimientos que aseguren una adecuada planificación y administración de la tecnología de información.

Conforme al Nuevo acuerdo de Capital de Basilea, se señala que las metodologías de medición se presentan por medio de tres métodos, por medio de los cuales se puede calcular los requerimientos de capital por riesgo operativo.

En orden de creciente sofisticación y sensibilidad al riesgo, estos métodos son:

- Método del Indicador Básico
- Método Estándar
- Métodos de Medición Avanzada (AMA).

De igual forma se aconseja a los bancos que vayan progresando a lo largo de la gama de métodos disponible a medida que desarrollen sistemas y prácticas de medición del riesgo operativo más sofisticado. (ANEXO 4)

2.3.5 Riesgo Sistemático

El riesgo sistemático es aquel que no puede ser eliminado por la diversificación, el riesgo sistemático de un valor individual es esa porción de su riesgo total que no puede ser eliminado con otros valores en una cartera bien diversificada.

Una manera de cuantificar el riesgo sistemático de un valor y relacionarlo con el riesgo sistemático de una cartera con aquel de sus valores componentes, puede ser establecido dividiendo el rendimiento del valor en dos partes:

1. Perfectamente correlacionada y proporcional al rendimiento del mercado.
2. Independiente (no relacionada con) del mercado.

Como el rendimiento sistemático es proporcional al rendimiento de mercado, puede ser expresado como el símbolo de beta (β) multiplicado por el rendimiento de mercado Rm.

El riesgo sistemático de un valor es igual a β multiplicado por la desviación estándar del rendimiento del mercado:

Riesgo sistemático = βσm

El riesgo sistemático de una cartera es simplemente el promedio ponderado del valor del mercado del riesgo sistemático de los valores individuales.

El riesgo sistemático remanente es igual al β del valor multiplicado por el riesgo de mercado, de igual forma el riesgo sistemático de la cartera es un promedio ponderado de los riesgos sistemáticos de los valores, debido a que el riesgo sistemático del valor es igual al beta del valor multiplicado por σm, el beta es usado como una medida de riesgo relativo. El β da el riesgo sistemático de un valor o cartera relativo al riesgo del índice de mercado.

2.4 Administración de Riesgos

2.4.1 COSO

COSO es el Committee of Sponsoring Organizations of the Treadway Commission, el cual es una iniciativa del sector privado establecida por cinco asociaciones profesionales contables y financieras. Su objetivo es mejorar la calidad de la información financiera concentrándose en el manejo corporativo, las normas éticas y el control interno.

En 1992, COSO publicó ñControl Interno-Sistema Integradoò, el cual es un informe en el que se establece una definición común de control interno y proporciona un estándar por el cual las organizaciones pueden evaluar y mejorar sus sistemas de control, desde el principio, ñControl Interno-Sistema Integradoò, ha sido ampliamente publicado como el estudio más completo que se haya efectuado acerca de control interno.

El sistema presentado por COSO ha sido ampliamente diseminado y reconocido, siendo así el sistema sobre el cual las principales organizaciones realizan sus informes y sus evaluaciones. El Informe COSO, ha logrado, que en el momento en el que se plantee cualquier discusión o problema de control interno, tanto a nivel práctico de las empresas como en el ámbito de auditoria interna o externa, o a los niveles académicos y legislativos, los participantes tengan una referencia conceptual común, lo cual resulta complejo debido a la diversidad de definiciones y conceptos que existen con referencia al tema de control interno.

El impacto del Informe COSO ha sido tal, que tanto las empresas públicas como las privadas han tomado la decisión de implantarlas para un correcto control.

El Informe COSO incluye la siguiente definición del control interno integrado:

> El control interno se define como un proceso, efectuado por el consejo de administración, la dirección y el resto de personal de una entidad, diseñado con el objeto de proporcionar un grado de seguridad razonable en cuanto a la consecución de objetivos dentro de las siguientes categorías:
>
> - Eficacia y eficiencia en las operaciones
> - Fiabilidad de la información financiera
> - Salvaguarda de los recursos de la entidad
> - Cumplimiento de las leyes y normas aplicables

La definición requiere de una adición importante en el segundo objetivo y es la frase **ñ**y operativaò tomada de las Normas para el Ejercicio de la Auditoria Interna (NEPAI) donde se la incluye y se la comparte totalmente. El marco integrado de control interno es toda la organización y no esta circunscrito a la información financiera.

COSO desarrolló una serie de preguntas que ayudan a los gerentes, directores, comités de auditoria y auditores internos a comprender mejor sus sistemas de control interno.

El informe COSO fue considerado como un enfoque voluntario para implementar las mejores prácticas dado que se refieren a un ambiente de control sano, estableciéndose como el parámetro de comparación para determinar el cumplimiento con la ley, dado que otros aspectos de la ley son definidos más claramente o se convierten en aplicables, generando de esta forma que los componentes del Informe COSO tomaron aún más importancia. (ANEXO 5)

Estos componentes cubren no solamente los controles necesarios para adecuarse a las regulaciones para los informes económico-financieros, sino que, además están en la capacidad de identificar los controles operativos, los cuales pueden ser críticos para la evaluación precisa y la exposición de todos los temas sujetos a análisis de acuerdo a las normas, ya sean de naturaleza económico-financieros como operacionales.

Para alcanzar estos objetivos, los siguientes componentes interrelacionados deben estar presentes[4]:

ÅAmbiente/Entorno de control
ÅEvaluación de riesgos
ÅActividades de control
ÅInformación y comunicación
ÅSupervisión/Monitoreo

2.4.1.1 Ambiente / Entorno de Control

Dentro del ambiente de control se establece el enfoque de la organización, en la cual se va a ver influenciado por la conciencia del control de su gente, lo cual sirve como fundamento disciplinario y estructural para todos los otros componentes del control interno.

Los factores claves que se pueden determinar dentro del ambiente de control incluyen:

- la integridad de las personas
- los valores éticos
- la competencia de sus empleados
- la filosofía de la gerencia y su estilo operativo
- la manera en que la gerencia asigna la autoridad y las responsabilidades y organiza y desarrolla a su gente
- la atención y dirección que les brinda el Directorio.

Con lo señalado se puede determinar que el ambiente de control es un punto de partida para determinar si la decisión de la gerencia es la de cumplir con la Ley, lo cual se podrá percibir como un ejercicio de espíritu entre los empleados o simplemente como algo a ser acatado.

[4] Marco Integrado de Control Interno para Latinoamerica (MICIL), Septiembre 2004.

Un enfoque mucho más prudente debe ser el de reconocer que el control interno es responsabilidad del administrador, y debe ser activamente ejercido por todas las personas relacionadas con la institución, lo cual debería ser reflejado en la misión, las políticas de ética, las pautas para la revelación de eventos, y la mesa directiva, los comités de auditoria y los estatutos de auditoria interna.

2.4.1.2 Evaluación de Riesgos

Como es normal cada entidad enfrenta riesgos internos y externos que deben ser cuidadosamente mitigados. Se podría establecer como una condición necesaria para una evaluación de riesgos efectiva, el que se establezcan objetivos que estén relacionados en los diferentes niveles, y que sean internamente consistentes.

La evaluación de riesgos identifica y analiza riesgos que pueden afectar la consecución de dichos objetivos, de igual forma se proveerá de una base de datos para de esta forma poder determinar la forma en la que los riesgos deben ser manejados.

Las instituciones han determinado que el manejo de riesgo es algo exclusivo de los auditores internos y agentes de seguros, los cuales han llegado a tomar un rol determinante dentro de la dirección de las instituciones.

Debido a esta exclusividad generada internamente dentro de las instituciones, muchas corporaciones están tomando conciencia de la importancia estratégica, que el manejo y control del riesgo tienen, a través de la designación de un Ejecutivo de Manejo de Riesgos (CRO ï Chief Risk Officer) para dar a este componente del COSO la atención que merece.

Las condiciones siempre cambiantes del mundo de los negocios hacen de la evaluación de riesgos una actividad dinámica y permanente, la cual requiere de la implementación de un proceso definido para guiar a la organización a través de la definición de áreas claves de riesgo, puntualizando los diferentes riesgos específicos en cada una de ellas, de igual forma se deberá evaluar la probabilidad y severidad de cada riesgo, e identificar los recursos que se requieren para mitigarlos a un nivel aceptable.

2.4.1.3 Actividades de Control

Las actividades de control son las políticas y procedimientos que implantan las diferentes directivas de la gerencia, con lo que se trata de tomar las acciones necesarias para mitigar los riesgos que amenazan el cumplimiento de los objetivos de la organización.

Las actividades de control ocurren en toda la organización, en todos los niveles y en todas las funciones, siendo tan diversos como aprobaciones, autorizaciones, verificaciones, reconciliaciones, revisiones de los resultados operativos, seguridad de activos, y segregación de funciones.

La importancia organizacional de las actividades de control se relaciona con el hecho de que muchos de los esfuerzos que las instituciones han realizado para poder cumplir los objetivos de control han resultado prácticamente como un instrumento para identificar y documentar estos componentes del COSO.

Más aún, muchos de los esfuerzos han estado limitados a los controles financieros, ya que pertenecen a la producción de los estados financieros, de igual forma el esfuerzo requerido para lograr una adecuada documentación en estas áreas adicionales dependerá de la madurez que se haya alcanzado previamente en los controles generales.

2.4.1.4 Información y Comunicación

Dentro de las instituciones la información debe ser identificada, capturada, y comunicada en una forma y dentro de un plazo en el cual sirva para que la gente pueda llevara acabo todas sus responsabilidades de una manera eficiente.

Los sistemas de información que poseen las instituciones son de gran ayuda para la generación de reportes, los cuales se basan primordialmente en temas operacionales, financieros y principalmente los que están relacionados con los diversos procesos de cumplimiento, los cuales ayudan a mantener en marcha y de igual forma establecer un correcto control del negocio.

La información que se genera dentro de las instituciones no son solo datos generados internamente, también son datos extraídos sobre eventos externos, actividades y condiciones necesarias para una toma de decisiones bien informada.

La comunicación efectiva también debe ocurrir en un sentido amplio, debido a que debe fluir hacia abajo, a lo ancho y hacia arriba dentro de la organización. Todo el personal debe recibir un mensaje claro de la alta gerencia en la cual se enfatice y se haga conciencia de que las responsabilidades de control por cada uno de los empleados deben ser tomadas de una manera seria.

Los trabajadores de las instituciones deben tener en cuenta y comprender no solo su propio rol dentro del control interno, sino también como las actividades individuales se relacionan con el trabajo de los otros. Se debe tener un medio de comunicación para poder informar todos los eventos hacia arriba.

Una institución no estará cubierta suficientemente con solo la documentación de las actividades de control que han sido identificadas en cada una de las diversas áreas y de igual forma con las leyes de cumplimiento.

2.4.1.5 Monitoreo

Los sistemas de control interno necesitan ser monitoreados a través de un proceso que asegure la calidad de cada sistema a lo largo del tiempo, estos procesos deben incorporar actividades de monitoreo constantes, evaluaciones independientes, o una combinación de ambas.

El monitoreo constante ocurre en el curso de las operaciones, la cual incluye actividades regulares de supervisión y administración, que debe estar correlacionadas con las diversas acciones que el personal ejecuta mientras desarrolla sus tareas.

El alcance y la frecuencia de las evaluaciones independientes dependerán primordialmente de la evaluación de riesgos y de la efectividad de los procedimientos de monitoreo que han sido implantados dentro de cada una de las áreas, así mismo las deficiencias de control interno deberán ser reportadas inmediatamente, y los problemas que pueden conllevar a mayores pérdidas por eventos de riesgos ser reportadas a la alta gerencia y a su mesa directiva.

Para una organización el factor de éxito más significativo para poder cumplir con los parámetros del marco de control COSO, es la capacidad y habilidad de la medición profunda y consistente del cumplimiento de cada uno de los controles implantados dentro de la institución.

Dentro de una organización se puede testificar por medio de los auditores los tres estados que definen las actividades típicas de una institución, los cuales se indican a continuación:

- La visión del equipo de dirección
- La forma en que esa visión es traducida en políticas y procedimientos
- Qué es lo que hacen realmente en el día a día los trabajadores

Por lo general estos estados deberían reflejar los diversos grados que varían dentro de la institución, con lo que podrían estar atados a componentes pasados por alto y menos utilizados dentro del marco conceptual de COSO.

Es por esto y en oposición al monitoreo estático y esporádico que se hacía en el pasado, es necesario que los sistemas provean a la gerencia la confianza en que el monitoreo en tiempo real está ocurriendo en todos los controles claves de cada proceso, sea este el financiero, operacional y regulatorio.

Evaluando el retorno de la inversión en mejoras tecnológicas, la gerencia debe comparar los costos de esa tecnología contra los costos de mano de obra requerida para llevar a cabo las mediciones manualmente, y los riesgos asociados con los controles inadecuados que no están funcionando en forma continua y que pueden conllevara a grandes pérdidas.

2.4.2 LEY SARVANES-OXLEY

En julio del 2002 después de un profundo debate en la Cámara de Representantes fue aprobada La Ley Sarbanes-Oxley, la cual pretende mejorar la protección a los accionistas a partir de una serie de medidas que afectan a los diferentes agentes que participan en los medios públicos.

Esta Ley contempla una revisión más rigurosa de los datos que una empresa declara en sus estados financiero contables, los cuales son utilizados por los departamentos de control interno, lo cual no solo engloba lo que se refiere a fraudes sino también por inferencias y todos los casos de fraude que tenga impacto dentro de los balances y desvirtúen de manera importante los estados financieros como puede ser la malversación de activos.

El proveer cualquier tipo de información falsa o incorrecta puede traer consigo un sin número de multas las cuales pueden al extremo de encarcelar a los ejecutivos de la empresa y si esta realiza cotizaciones en bolsa, su inmediato retiro.

Dentro de los controles que se tienen en la Ley se exige tener un canal en el cual se vislumbre las irregularidades que son realizadas por parte de los empleados, accionistas, entre otros, para de esta forma poder realizar un correcto control y estar en la capacidad de mitigar dichas pérdidas.

Esta ley fue elaborada por el senador demócrata Paul Sarbanes y el diputado republicano Michael Oxley y esto no solo es un ejercicio para el cumplimiento de nuevos reglamentos sino también una forma alternativa de realizar nuevos negocios.

Los requisitos más importantes que exige esta nueva ley son los siguientes[5]:

- Establecer un nuevo consejo de vigilancia, supervisado por la SEC (Security Exchange Commission - Comisión de Valores de Estados Unidos).
- Definir nuevas funciones y responsabilidades para el comité de auditoria, que debe tener miembros independientes a la administración.
- Nuevas reglas para la conformación de los Consejos de Administración, para que incluyan personas ajenas al grupo de control de la empresa.
- Que los directivos acompañen los reportes con una certificación personal, en general se incrementan las responsabilidades de los directores generales y de los directores de finanzas. Código de ética para los altos funcionarios de la organización.
- Definir un esquema de medición del control interno que se aplique constantemente.
- Que los directivos certifiquen el buen funcionamiento de sus sistemas de control interno.
- Establecer nuevos requerimientos de información, que abarcan cuestiones no financieras y financieras que no aparecen en los estados respectivos.
- El auditor externo tiene que verificar la certificación del control interno y emitir un dictamen al respecto.
- Rotación de los auditores cada cinco años.
- Especificar los servicios que no podrán ser realizados por los auditores externos.

[5] Ley Sarbanes-Oxley Act (SOX, SOA)

- Reforzar penas por fraudes corporativos y de personal administrativo.
- Emitir reglas sobre conflictos de interés.
- Nuevos esquemas de administración de riesgos.
- Aumentar la autoridad y funciones de la SEC.

De igual forma esta Ley tiene un fuerte impacto dentro de los consejos de administración de empresas, bancos de inversión, instituciones financieras, y también dentro de las actividades y regulaciones de los auditores en cada una de éstas.

La Ley Sarbanes-Oxley es un texto cuyos contenidos principales se agrupan en seis grandes áreas, que afectan a todas las empresas que cotizan dentro de los diversos mercados americanos, los cuales se indican a continuación:[6]

1. Mejora en la calidad de la información pública y en los detalles de la misma.
2. Reforzamiento de responsabilidades en el Gobierno Corporativo de las sociedades.
3. Mejora en las conductas y comportamientos éticos exigibles: mayores exigencias de responsabilidad en los temas de gestión indebida de información confidencial.
4. Aumento de la Supervisión a las actuaciones en los mercados cotizados.
5. Incremento del régimen sancionador asociado a incumplimientos.
6. Aumento de exigencia y presión sobre la independencia efectiva de los auditores.

1. Mejora en la calidad de la información pública y en los detalles de la misma

Toda información que las empresas presenten deberá ser certificada por los directivos responsables dentro de la institución, lo que conlleva a que los directivos estarán certificando su responsabilidad y corrección respecto a los siguientes puntos que son considerados importantes:

- Los informes trimestrales y anuales
- La no existencia de omisiones o información confusa en los estados financieros
- Los controles sobre la información que se envía al mercado y la eficiencia del control interno sobre la misma

[6] Ernst & Young, La Ley Sarbanes -Oxley y la Auditoria.

- La comunicación de forma efectiva a los auditores y al Comité de Auditoria de los errores o fraudes que se identifiquen

Adicionalmente a lo señalado se debe tener en consideración que deben existir mejoras en los detalles de la información que se encuentra fuera del balance y de los contenidos en los informes pro-forma.

Debe existir una evaluación del control interno financiero el cual debe ser valorado, documentado y certificado por la Dirección de la institución y auditado por el auditor externo, el mismo que opinará sobre la corrección de lo manifestado por la institución y sobre la eficiencia del control interno financiero a la fecha de cierre de los estados financieros.

Si existiesen cambios en información proporcionada por la Institución y la misma representa un gran impacto dentro de la situación financiera o de las operaciones, motivo por el cual se deberá informar de manera rápida y efectiva dichos sucesos.

2. Reforzamiento de responsabilidades en el Gobierno Corporativo de las Sociedades

Dentro de las responsabilidades que se mantienen dentro de las organizaciones, debe haber especialmente un incremento en lo que se refiere a la comunicación que debe existir entre el Auditor y el Comité de Auditoria en materias relacionadas con políticas contables significativas, tratamientos contables alternativos, entre otros.

Así mismo hay que poner énfasis en regulaciones más completas para los Comités de Auditoria, los cuales son obligatorios dentro de las instituciones, con lo que se debe tomar en cuenta los siguientes puntos:

- Serán responsables directos de designar, retribuir y supervisar al Auditor
- Sus miembros deberán ser consejeros independientes (no ejecutivos)
- Deberán implantar un canal de recogida anónima de denuncias
- Deberán disponer de capacidad de compensación al auditor y a otros asesores si los consideran necesarios en el desarrollo de sus responsabilidades

Dentro de cada institución es obligación de contar con expertos financieros dentro del Comité de Auditoria, así mismo es de suma importancia que se indique o se comuniquen quienes son las personas que tienen dicha experiencia y que formarán parte en el Comité.

3. **Mejora en las conductas y comportamientos exigibles: mayores exigencias de responsabilidad en los temas de gestión indebida de información confidencial**

Debido a que se realiza el manejo de información confidencial, se debe estipular la ilegalidad en el momento de actuar de cualquier consejero o directivo que vaya a influir de forma fraudulenta, coaccionar o confundir de manera intencional al auditor.

Las operaciones que se realizan por parte de los agentes que están en la capacidad de disponer todo tipo de información reservada que no es pública, deberán informar a los agentes del mercado de manera corta y veraz la información a ser utilizada.

Dentro de cada institución debe existir de manera obligatoria un Código de Ética para los Ejecutivos del Área Financiera, así mismo si ocurriese algún tipo de incumplimiento al Código, estos hechos deben ser informados de manera pública.

Debe existir protección especial para los denunciantes anónimos de conductas ilícitas e irregulares de las instituciones, en ningún caso podrán ser perseguidas las denuncias formuladas por este tipo de incumplimientos.

4. **Aumento de la Supervisión a las actuaciones en los mercados cotizados**

- Creación de un organismo público de supervisión: el Public Company Accounting Oversight Board (PCAOB)
- El PCAOB tendrá capacidad de supervisión y establecimiento de estándares de auditoria, controles de calidad, normas de ética e independencia para auditores, etc.
- Cualquier compañía que quiera auditar sociedades cotizadas en mercados americanos deberá estar inscrita adecuadamente en el PCAOB
- El PCAOB desarrollará programas continuos de supervisión del trabajo de las firmas de auditoria para comprobar su cumplimiento efectivo de los estándares profesionales

- La Security Exchange Commission (SEC) podrá reconocer como de general aceptación los principios contables establecidos por organismos reguladores como el FASB.
- La SEC deberá realizar estudios sobre normas contables basadas en principios frente a las basadas en aspectos más formales
- Los emisores de valores en los mercados americanos deberán contribuir mediante las cuotas que se determinen a la financiación de las actividades del PCAOB y del FASB
- La SEC ampliará, de forma importante, las revisiones periódicas sobre los depósitos de las compañías.
- Extensión de las responsabilidades profesionales para los abogados. Estarán obligados a informar cualquier evidencia que dispongan sobre violaciones materiales de leyes sobre actuaciones con títulos cotizados o incumplimientos de obligaciones por el Consejero Delegado o por el Secretario del Consejo (o el responsable legal del mismo). Si se informa a la Dirección y esta no tomara acciones se informaría directamente a la SEC

5. Incremento del régimen sancionador asociado a incumplimientos

En el caso de que se hubiese generado un cobro u obtenido beneficios debido a operaciones financieras realizadas por el Consejero Delegado (CEO) o por el Director Financiero (CFO) en base de información fraudulenta la cual necesite ser re-evaluada, corregida y publicada nuevamente, deberá ser reintegrada a los perjudicados por dichas acciones.

Dentro de las obligaciones que se fijan dentro de las instituciones para el CEO y CFO, está el de certificar, bajo responsabilidad penal, su buena fe en cuanto a que los informes públicos periódicos cumplen con los siguientes puntos:

- Cumplen con todos los requisitos establecidos en la Ley sobre Acciones de 1934 (Securities Exchange Act, 1934).
- Presentan, en todos los aspectos materiales, la situación financiera y los resultados de las operaciones del emisor.
- Responsabilidades penales por manipular, alterar o destruir documentos o impedir, de otra manera, una investigación oficial.
- Extensión de las responsabilidades penales a cualquier persona que altere documentos, incluyendo registros documentales de auditoria, con el fin de obstruir o impedir una investigación.

- Aumento importante de las sanciones a los contables/financieros por no testificar, facilitar documentación o cooperar, en general, con investigaciones oficiales.

6. Aumento de exigencia y presión sobre la independencia efectiva de los auditores

Dentro de las exigencias se determina la prohibición total para que el auditor de cuentas pueda prestar determinados servicios a sus clientes de auditoria, de igual forma el Comité de Auditoria deberá autorizar, de forma previa a su contratación, cualquier servicio permitido que pretenda contratarse con el auditor de cuentas.

De igual forma en la Ley se establecen restricciones importantes para que una entidad contrate personal del equipo de su auditoria sin que esto pueda suponer un posible problema de independencia para la firma auditora, estableciéndose de esta forma un periodo ñde enfriamientoò de un año en el que no se pueden producir estas contrataciones para puestos clave en relación directa con la supervisión financiera de la información del emisor.

2.4.2.1 Efectos de la Ley Sarbanes-Oxley en la auditoria

La Ley Sarbanes-Oxley al ser una forma de controlar las actividades internas en las instituciones, tiene un impacto, mas o menos directo en las actividades de los auditores, empezando por la interlocución más continua con los Comités de Auditoria, y finalizando en la creación de un regulador específico de la Auditoria con lo que se tiene un efecto muy importante dentro de las instituciones.

Los efectos de esta Ley ponen de manifiesto un inventario de servicios no permitidos al auditor de cuentas, de los que se puede destacar los siguientes:

- Elaboración de contabilidades o preparación de los registros de información financiera del cliente.
- Diseño o implementación de sistemas de información financiera.
- Valoraciones, tasaciones u opiniones sobre aportaciones de activos.
- Servicios actuariales.
- Outsourcing integral de servicios de auditoria interna.
- Funciones de dirección/gestión.

- Gestión de recursos humanos/servicios de contratación de personal.
- Asesoramiento de inversiones, actividades de intermediación o servicios de inversión financiera.
- Servicios legales no relacionados con la auditoria.
- Cualesquiera otros que la SEC[7] o el PCAOB[8] puedan establecer en el futuro.

Con estas definiciones establecidas de incompatibilidades tiene un efecto directo en los trabajos que desarrolla el auditor y en la relación profesional que se establece con los clientes, con lo que se complementa y mantiene de forma clara el principio fundamental de independencia real exigible que tiene el auditor en el campo de trabajo.

Una de las finalidades que tiene esta Ley, es la de eliminar cualquier trabajo de la firma auditora que en lo posterior pueda o deba ser auditada por esta misma. Dentro de este marco, las instituciones han optado por separar de una manera mucho más estricta las contrataciones de auditorias con relación a las de contratación por servicios profesionales.

Una de las áreas en la que la Ley tiene un impacto positivo está dada en la obligatoriedad de fortalecer los sistemas de control interno financiero, debido a que está obligada a auditar, a partir de una fecha determinada no solo lo referente a los estados financieros sino también al control interno financiero.

Estas auditorias tienen la finalidad de mejorar la calidad y contabilidad de la información financiera, debido a que se parte del supuesto de adaptación de la metodología del auditor al enfoque de trabajo basado cada vez más en entender los riesgos, los controles, su identificación, valoración y prueba continua.

Se puede considerar que la Ley Sarbanes-Oxley americana, ha influido de manera simultánea a la profunda transformación del marco general del Gobierno Corporativo en otros países, así mismo ha supuesto un importante impacto profesional para la auditoria, en términos generales, se podría clasificar como positivo el efecto que ha generado la Ley, ya que se ha dado un mayor enfoque a los controles de los riesgos y al conocimiento del control interno.

[7] Security Exchange Commission
[8] Public Company Accounting Oversight Board

2.4.3 COSO-ERM

Dentro del marco integrado que proporciona COSO conjuntamente con la gestión de riesgos corporativos (ERM), se proponen técnicas que pueden ser empleadas en diversos niveles dentro de las instituciones.

Las técnicas que se presenta por medio de COSO y ERM son aplicables a organizaciones de menor tamaño y complejidad, mientras que para otras empresas estas técnicas pueden ser relevantes debido a que no se ajustarían de acuerdo al tamaño y la complejidad de las mismas.

Con los cambios continuos que se dan dentro de las entidades, se espera que haya una evolución de directrices adicionales por medio de organizaciones profesionales, grupos industriales, organismos reguladores, para que se pueda desarrollar propuestas y materiales necesarios enfocados apoyar a cada uno de los sectores que se verían beneficiados con nuevas prácticas de evaluación del sistema de control interno de una entidad.

Para poder facilitar el entendimiento de esta práctica de evaluación es necesario tener en cuenta los siguientes elementos claves de cada uno de los componentes de la gestión de riesgos corporativos:

- Ambiente interno
- Establecimiento de objetivos
- Identificación de acontecimientos
- Evaluación de riesgos
- Respuesta a los riesgos
- Actividades de control
- Información y comunicación
- Supervisión

Con estos elementos que forman parte de la gestión de riesgos corporativos, la alta dirección debe ver la forma en como plantear el despliegue de este proceso dentro de la organización y de cómo involucrarla en la entidad, teniendo muy en cuenta el tamaño, complejidad, sector, cultura, estilo de gestión y demás características propias de la institución, para que su implementación sea de la manera más eficaz y eficiente posible. (ANEXO 6)

Para que haya una correcta implementación, se puede señalar las principales etapas que han seguido aquellas direcciones que han podido implementar con éxito la gestión de riesgos corporativos, las mismas que están en la capacidad de dar las directrices fundamentales para que su puesta en marcha sea eficaz y eficiente, teniendo en cuenta de que no es una regla seguirlas previa la implementación de la gestión de riesgos corporativos, dichas etapas son las siguientes:

- Grado de preparación del equipo líder
- Apoyo de la alta dirección
- Desarrollo del plan de implantación
- Diagnóstico de la situación actual
- Visión de la gestión de riesgos corporativos
- Desarrollo de capacidades
- Plan de implantación
- Desarrollo y puesta en marcha de la gestión del cambio
- Seguimiento

2.4.3.1 Ambiente Interno

El ambiente interno se refiere primordialmente al talento de una institución, la cual está en la capacidad de influir en la conciencia de sus empleados en lo que se refiere al tema de riesgos y en formar la base de los otros riesgos componentes de la gestión de riesgos corporativos, dando así disciplina y estructura.

Los factores del ambiente interno incluyen:

- La filosofía de gestión de riesgos de la entidad
- Su riesgo aceptado
- La supervisión ejercida por el consejo de administración
- La integridad
- Valores éticos y competencia de su personal y la forma en que la dirección asigna autoridad y responsabilidad y organiza y desarrolla a sus empleados.

Uno de los principios fundamentales que deben existir dentro de una organización es el de mantener el respeto y la integridad frente a los empleados, clientes y grupos de interés, con lo que el programa de la gestión va asegurar que se mantengan los estándares éticos más elevados siguiendo los valores fundamentales internos.

La gestión de riesgos corporativos facilita a las instituciones a estar en la capacidad de identificar, evaluar y gestionar los riesgos inherentes y por lo tanto brinda la posibilidad de que toda la planta de trabajadores mejore su comprensión en relación a la gestión de riesgos, con lo que se podrá obtener:

- Aceptación responsable del riesgo
- Apoyo a la dirección y al consejo de administración
- Mejoras en los resultados
- Responsabilidad reforzada
- Liderazgo superior

Para poder medir el conocimiento que tienen los empleados con respecto a la filosofía de la gestión de riesgos dentro de la institución, han optado por llevar a acabo encuestas, con lo que se permite medir la presencia y fortaleza de los atributos relacionados con ello, con lo que se estará en la capacidad de proporcionar indicadores de las áreas de fortalezas y debilidades dentro de la cultura organizacional.

2.4.3.2 Establecimiento de Objetivos

Dentro de las instituciones, los objetivos son fijados en base a la escala estratégica, estableciendo de esta forma una base para los objetivos operativos de información y cumplimiento. Todas las instituciones están en constante exposición a los diversos tipos de riegos que existen, tanto internos como externos y de igual forma están condicionadas previamente por los objetivos que persigue para a partir de estos poder identificar, medir y mitigar sus riesgos.

Los objetivos de las instituciones deben estar alineados con los riesgos que estas acepten y orientarlos a su a los niveles de tolerancia al riesgo de las mismas, cabe indicar que los riesgos aceptados son expresados por lo general por medio de mapas de riesgos, con lo que se puede identificar el riesgo mismo aceptado por la empresa, y el riesgo residual, y si este último sobrepasa al aceptado por la

empresa, la dirección debe poner en marcha las acciones pertinentes para poder reducir el impacto y la probabilidad para poderlo situar dentro del nivel aceptado por la misma.

Para poder fijar el nivel aceptado de riesgo por la institución, es recomendable la fijación de un nivel de tolerancia, ya que este es el nivel de aceptación de desviación relativa a la consecución de los objetivos fijados. El operar dentro de los niveles de tolerancia va a proporcionar a la dirección una mayor confianza para que la institución se encuentre dentro de un nivel de aceptación adecuado, brindando una mayor seguridad en que se alcanzarán los objetivos planteados.

2.4.3.3 Identificación de Acontecimientos

Durante el giro del negocio, las instituciones se encuentran en constante exposición frente a diversos riesgos, motivo por el cual la dirección debe identificar los eventos potenciales, que si llegaran a suceder, la entidad se vería afectada, con lo que se debería determinar si estos representan oportunidades o si pueden afectar negativamente a la institución en su fin de implantar estrategias y lograr los objetivos planteados.

Frente a esto se podría determinar que los impactos positivos representan oportunidades para la institución en su afán de implantar las estrategias y la fijación de los objetivos, es por esto que con la identificación de los diversos factores tanto internos como externos pueden dar lugar a eventos de riesgos dentro del ámbito global de la organización.

Las diversas metodologías de identificación de eventos dentro de una institución puede ser la combinación de diversas técnicas y herramientas, las cuales se basan en los eventos que han sucedido en el pasado y que se estiman sucedan en el futuro. Las metodologías de identificación de eventos son utilizadas para poder determinar los posibles acontecimientos que pueden afectar a la consecución de los objetivos, dentro de estos se pueden señalar los siguientes:

- Inventario de eventos
- Talleres de trabajo de identificación de eventos
- Entrevistas
- Cuestionarios y encuestas
- Análisis de flujos de procesos

Bajo determinadas circunstancias, hay diversos eventos que pueden tener impacto sobre la consecución de los objetivos, razón por la cual para tener una mejor visión como comprensión referente a la interrelación que hay entre los eventos y los objetivos, se puede utilizar diagramas de eventos de árbol, debido a que estos proporcionan un medio de identificación y representación de manera gráfica la incertidumbre, teniendo como centro un objetivo.

2.4.3.4 Evaluación de Riesgos

Dentro de las instituciones las evaluaciones de riesgos permiten considerar la amplitud con que los eventos potenciales van a tener un impacto en la consecución de los objetivos planteados, es por esto que se evalúa los acontecimientos desde una doble perspectiva, con lo que se debe utilizar una combinación de métodos cualitativos y cuantitativos.

Los impactos positivos y negativos de los diferentes eventos se deben examinar de manera individual o por categoría dentro de toda la institución con un doble enfoque, como riesgo residual y riesgo inherente.

El riesgo inherente que enfrenta la institución es aquel al que se esta expuesto en ausencia de acciones por parte de la dirección para poder modificar tanto la probabilidad de ocurrencia como el impacto que estos pueden tener a la consecución de los objetivos, siendo aquel que permanezca después de que la dirección desarrolle sus respuestas frente a los riesgos.

El riesgo residual refleja el riesgo permanente una vez que se han realizado las acciones planificadas para la mitigación del riesgo inherente, las cuales pueden incluir estrategias de diversificación relativas a las concentraciones de clientes, productos, políticas y procedimientos por medio de los cuales se han establecido límites, autorizaciones, personal de supervisión y de esta forma poder tener una estandarización de criterios para poder tomar decisiones y de esta forma estar en la capacidad de reducir las probabilidades de ocurrencia de los posibles eventos, su impacto o dependiendo los casos ambos a la vez.

Las metodologías que se pueden utilizar para la evaluación de riesgos dentro de una institución consisten en la combinación de las diferentes técnicas cualitativas y cuantitativas, las cuales son a menudo

aplicadas por las altas direcciones. Las técnicas cuantitativas por lo general brindan una mayor precisión y se usan en actividades más complejas y sofisticadas, las cuales sirven para complementar las técnicas cualitativas.

Algunas evaluaciones cualitativas son establecidas en términos subjetivos y otras objetivos, pero ambas van a depender principalmente del conocimiento y juicio de las personas que se encuentran inmersas, su comprensión frente a los acontecimientos del contexto y la dinámica que los rodea.

Las técnicas cuantitativas pueden ser utilizadas cuando hay información suficiente para estimar la probabilidad de ocurrencia o el impacto que puede tener, por medio de mediciones de intervalo o de razones, esta técnica incluye técnicas probabilísticas, no probabilísticas, y de benchmarking. Uno de los puntos primordiales de las técnicas cuantitativas es la disponibilidad de la información de manera precisa, las mismas que pueden provenir de fuentes internas o externas.

2.4.3.5 Respuesta a los Riesgos

Una vez que se han evaluado y clasificado los riesgos por medio de los métodos cuantitativos y cualitativos, se debe decidir que acciones se tomarán en respuesta a ellos, las mismas que pueden ser de evitar, reducir, compartir y aceptar el riesgo.

Dependiendo de la decisión que se tome, se deberá evaluar el efecto que esto tiene sobre la probabilidad e impacto del riesgo, así como los costes y beneficios que estos conllevan, con la evaluación obtenida se clasifican los riesgos de acuerdo a los rangos de tolerancia de acuerdo a lo establecido. Una vez que se han tomado las acciones frente a los acontecimientos presentados, se va a poseer una visión de los riesgos y respuestas individuales, así como la alineación con las tolerancias asociadas.

Cualquier oportunidad que se presente, se debe asumir una perspectiva del riesgo global para la entidad o bien de la cartera de riesgos, con lo que se podrá determinar si el riesgo residual concuerda con el riesgo aceptado por la institución.

Sea cual fuese la respuesta que se tome frente a los diversos riesgos, siempre existirá algún tipo de coste sea este directo o indirecto que se debe comparar con relación a los beneficios generados en la institución. Frente a esto se debe considerar los costes iniciales de diseño e implementación de una

respuesta frente a los riesgos basadas en procesos, personas y tecnología, de igual forma no hay que descuidar los costes de mantener las acciones de manera continua.

2.4.3.6 Actividades de Control

Posteriormente a las respuestas de los riesgos, hay que tener en cuenta que se debe mantener un control sobre los riesgos presentados, los cuales están definidos como las políticas y procedimientos que ayudan asegurar el que se lleve a cabo las respuestas frente a los riesgos establecidos.

Las actividades de control tienen lugar a través de las instituciones dentro de todos los niveles y todas las funciones, con lo que se incluye una diversidad de actividades, las mismas que pueden ser como aprobaciones, autorizaciones, verificaciones, conciliaciones, revisiones operativas, seguridad en los activos de la institución y la segregación de las funciones.

Una vez que se ha seleccionado las respuestas a cada uno de los riesgos, se debe identificar las actividades necesarias de control para tener una mayor certeza de que las respuestas sean llevadas a cabo de una manera adecuada y oportuna, estas actividades deben ir alineadas con cada una de las respuestas seleccionadas, sea estas las de evitar, mitigar, distribuir y aceptar.

2.4.3.7 Información y Comunicación

Dentro de las instituciones se requiere que exista una tecnología de información, lo cual facilita la identificación y captación de la información que es necesaria para la entidad, para luego comunicarlo de una forma y en un marco de tiempo que permite a las personas llevar a cabo sus responsabilidades.

Los sistemas de información usan datos generados de manera interna y a su vez algunos son provenientes de fuentes externas, con lo que una vez procesados, sus salidas dan las pautas para poder realizar una buena gestión de riesgos, lo cual incluye la toma de decisiones que van a estar alineadas de acuerdo a los objetivos.

La información procedente de fuentes externas o internas debe ser recopilada y analizadas para que estén en condiciones adecuadas para poder establecer las estrategias y los objetivos, identificar los

eventos, analizar los riesgos, determinar las respuestas a ellos y con esto estar en condiciones de llevar a cabo la gestión de riesgos corporativos.

Todo el personal debe percibir el papel que desempeñan dentro de la institución con relación a las actividades que desempeñan como el papel que tienen en la gestión de riesgos a los que se ve expuesta la institución, de igual forma se deben tener los medios suficientes para comunicar hacia arriba la información significativa, al igual que con terceros.

El diseño de una arquitectura de sistemas de información al igual que la adquisición de la tecnología son aspectos importantes dentro de las estrategias que tienen las instituciones al igual que un pilar para la toma de decisiones debido a que por medio de la tecnología se pueden lograr los objetivos institucionales.

A través de la tecnología se mantiene el flujo constante de información de una entidad, información que puede ser muy relevante para la gestión de riesgos corporativos. En algunas instituciones la información es administrada de manera independiente por cada unidad de la institución, mientras que en otras entidades existe un sistema de información integrado.

Por medio de la comunicación se podrá transmitir información específica, las cuales estarán orientadas a las expectativas del comportamiento y responsabilidades del personal, en la cual se incluye una exposición clara de la filosofía y enfoque de la gestión de riesgos corporativos, de igual forma hay que tener en consideración que la comunicación referente a procesos y procedimientos debe estar alineada con la cultura organizacional.

La comunicación es la clave para mantener un entorno adecuado dentro de las instituciones, y de igual forma apoya al resto de componentes de la gestión de riesgos corporativos, en coherencia con la idea de incorporar la gestión de riesgos en la organización. Las soluciones tecnológicas están en la capacidad de proporcionar la información de la gestión al alcance de todos los empleados de una manera simple y constante.

2.4.3.8 Supervisión

Como en toda implementación de y puesta en marcha de tecnologías, es indispensable realizar una supervisión para determinar que el objetivo que se persigue se esté cumpliendo o por lo menos se

encuentre en marcha, así mismo encontrar las fallas en los procesos para rectificarlas y proseguir con las implementaciones.

Dentro de la gestión de riesgos corporativos se revisa la presencia y el funcionamiento de sus componentes a lo largo del tiempo, lo cual se da por medio de una supervisión permanente, el alcance y la frecuencia de las evaluaciones depende principalmente de las evaluaciones de riesgos y de la eficacia de los procedimientos de supervisión permanente.

La supervisión de la eficacia de los componentes de la gestión de riesgos corporativos incluye la revisión diaria de información de las siguientes gestiones que son normales dentro de una institución:

- Revisión de informes de indicadores claves de la actividad del negocio
- Comparación de información generada por el sistema con las obtenidas de las actividades diarias.
- Revisión de rendimientos comparándolos con los límites establecidos.
- Revisión de transacciones comunicadas a través de indicadores de alerta.
- Revisión de indicadores claves de rendimiento.

Para cumplir con los objetivos que tiene la supervisión se dispone de una variedad de metodologías y herramientas, las cuales pueden documentar y evaluar aspectos específicos de la gestión de riesgos corporativos.

Estas metodologías y herramientas deben ser de fácil manejo por parte del personal asignado, su relevancia para el alcance dado y su adecuación a la naturaleza y frecuencia esperada de la evaluación, siendo estas empleadas de forma individual como conjuntamente entre sí, entre las que se destacan las siguientes:

- Diagrama de flujo de procesos
- Matrices de riesgos y de control
- Manuales de referencia de riesgos y de control
- Benchmarking
- Técnicas de auditoria
- Talleres de trabajo de auto evaluación

- Cuestionarios

Hay que tener en cuenta que el nivel de documentación de la gestión de riesgos corporativos de una entidad va a variar según su dimensión, complejidad y factores de riesgo.

2.5 El Nuevo Acuerdo de Basilea y la Gestión de Riesgo Operativo

El desarrollo alcanzado por el sistema financiero internacional en los últimos años llevó al Comité de Basilea a elaborar una propuesta con el fin de establecer un esquema más completo en cuanto al control y administración de los riesgos que asumen las instituciones financieras. La propuesta se orienta a un tratamiento más explícito de otros tipos de riesgos presentes en la actividad financiera, introduciendo el riesgo operativo, con el fin de mejorar las evaluaciones que efectúen las Instituciones sobre los riesgos, de forma tal que los coeficientes de capital sean más representativos del perfil de riesgo de cada entidad.

El Comité de Basilea reconoce que el enfoque para la administración del riesgo de operación dependerá de la institución que lo ponga en práctica, puesto que obedece a una serie de factores como el tamaño, naturaleza y complejidad de las actividades de la misma.

Sin embargo, a pesar de estas diferencias, lo que busca el nuevo acuerdo de Basilea es crear una cultura sólida de control que permita un reporte interno efectivo y una planificación contingente dentro del proceso de administración de riesgo operacional.

Entre los objetivos que persigue el Acuerdo de Basilea II se destacan:

- Perfeccionar el acuerdo anterior (Basilea I).
- Dar la seguridad de los Sistemas Financieros.
- Promover la competencia en igualdad de condiciones.
- Establecer capitales mínimos regulados en base a criterios más sensibles al riesgo.
- Lograr eficiencia en el desarrollo de los procesos.
- Mejorar la supervisión bancaria.
- Transparencia en la información.

El Comité de Basilea indica la importancia de la adopción de estrategias claras para la administración del riesgo operativo, que incluyen responsabilidades, segregación de obligaciones, un sistema interno efectivo de presentación de informes y planes de contingencia.

El Comité reconoce que la administración de riesgos operativos específicos no es una práctica nueva, siempre ha sido importante intentar evitar el fraude, mantener la integridad de los controles internos, reducir los errores en el procesamiento de transacciones, etc., sin embargo, lo que es relativamente nuevo es la perspectiva respecto de la administración del riesgo operativo como una práctica integral comparable a la administración del riesgo de crédito y mercado.

Para dar cumplimiento a estos objetivos, el nuevo enfoque propuesto en Basilea II se basa en los siguientes pilares:

- Requerimiento mínimo de capital.
- Proceso de supervisión bancaria.
- Disciplina de mercado.

Estos tres pilares juntos contribuyen a fortalecer el nivel de seguridad y solidez en el Sistema Financiero. Sin embargo, deben ser las gerencias de cada institución, las responsables de manejar los riesgos y asegurar que el capital mantenido sea el adecuado para su propio perfil de riesgos.

2.5.1 Principios de Basilea para la administración del Riesgo Operativo

El Comité de Basilea establece prácticas sólidas para la identificación, medición, monitoreo y control del riesgo operacional, los cuales están basados en los siguientes principios:

Principio 1: La junta directiva debe estar enterada de los aspectos más importantes de los riesgos operacionales de la institución y debe administrarlos como una categoría de riesgo distinta que debe ser evaluada en forma periódica dentro del marco de administración de riesgos.

La administración del Riesgo Operacional debe incluir políticas que describan el enfoque de la institución para poder identificar, evaluar, monitorear y controlar el riesgo. Se debe establecer una estructura de administración capaz de poder implementar controles internos fuertes, líneas de

responsabilidad claras y reportes administrativos. Además, deben existir responsabilidades segregadas y líneas de reporte entre las funciones de control y el ingreso que generan las líneas de negocio.

Principio 2: La junta directiva debe asegurar que el marco de administración de riesgo está sujeto a una auditoria interna efectiva, competente, apropiadamente calificada y operacionalmente independiente. La función de auditoria interna no debe de ser directamente la responsable de la administración del riesgo operacional.

Las instituciones financieras deben establecer un control adecuado de auditoria interna, que se encargue de verificar que las políticas y procedimientos operativos son efectivamente implementados. La auditoria debe validar continuamente que el marco de administración de riesgo operacional está siendo implementado en forma efectiva, manteniendo la independencia de sus funciones.

Principio 3: La alta gerencia debe tener la responsabilidad de implementar el marco de administración de riesgo operacional, aprobado por la junta directiva, en toda la organización. Adicionalmente, tiene la responsabilidad de desarrollar políticas, procesos y procedimientos para la administración del riesgo operacional en todos los productos, actividades, procesos y sistemas.

Cada nivel de administración es responsable de la propiedad y efectividad de las políticas, procesos, procedimientos y controles, la alta gerencia debe asignar relaciones de autoridad, responsabilidad y reporte para fomentar su responsabilidad. Se debe asegurar que las actividades deben ser realizadas por personal calificado con la experiencia necesaria y capacidades técnicas.

Principio 4: Las instituciones financieras deben identificar y evaluar el riesgo operacional inherente en todos los productos, actividades, procesos y sistemas, y deben asegurar procedimientos adecuados de evaluación.

La identificación efectiva del riesgo considera factores internos y factores externos que podrían afectar en forma adversa el logro de los objetivos de la compañía. Además de identificar la mayoría de los riesgos potencialmente adversos, las instituciones deben evaluar su vulnerabilidad a los mismos. Una evaluación efectiva del riesgo permite comprender mejor el perfil de riesgo y enfocar más efectivamente los recursos de administración del mismo.

Principio 5: Los bancos deben implementar un proceso para monitorear regularmente los perfiles de riesgo operacional y exposición material a las pérdidas. Se debe elaborar un reporte regular de información a la alta gerencia.

Un proceso efectivo de monitoreo es esencial para administrar de manera adecuada el riesgo operacional. Las actividades regulares de monitoreo pueden ofrecer una rápida detección de deficiencias, logrando reducir sustancialmente la frecuencia y severidad potencial de un evento de pérdida.

También deben identificarse indicadores que puedan ser predecibles de riesgos de pérdidas futuras. Estos indicadores son conocidos como claves de riesgo o indicadores de alerta temprana y deben ser previsores para reflejar fuentes potenciales de riesgo operacional, como el crecimiento rápido, introducción de productos nuevos, volumen de ventas del empleado, interrupción de transacciones, tiempo fuera de servicio del sistema, entre otros.

El monitoreo es más efectivo cuando el sistema de control interno está integrado a las operaciones y produce reportes regulares. Los resultados de estas actividades de monitoreo deben incluirse en los reportes a la administración y deben asimismo ser entregados a la alta gerencia de manera periódica.

Principio 6: Las instituciones deben contar con políticas, procesos y procedimientos para controlar o mitigar los riesgos operacionales materiales.

Las actividades de control se diseñan para dirigir los riesgos que se han identificado. Para aquellos riesgos que no pueden ser controlados, las instituciones deben decidir si aceptan este riesgo o reduce o retira la actividad de negocio implicada. Los procesos y procedimientos de control deben estar establecidos y las instituciones deben tener un sistema para asegurar el cumplimiento con un conjunto documentado de políticas internas concernientes al sistema de administración de riesgo.

Los elementos principales de este control deben incluir:

- Revisiones de alto nivel del cumplimiento de los objetivos establecidos.
- Chequeo del cumplimiento con los controles.
- Políticas, procesos y procedimientos.

Un sistema de aprobaciones y autorizaciones documentado para asegurar la responsabilidad en un nivel apropiado de la administración.

Un sistema efectivo de control interno también requiere que exista segregación apropiada de responsabilidades y que al personal no se le asignen responsabilidades que podrían crear un conflicto de interés. La asignación de dichas responsabilidades conflictivas a individuos, pueden ocultar pérdidas, errores o acciones inapropiadas. Por lo tanto, las áreas de conflictos de interés potenciales deben ser identificadas, minimizadas y estar sujetas a un cuidadoso monitoreo y revisiones independientes.

Principio 7: Las instituciones financieras deben tener establecidos planes de continuidad, contingencia y de negocios para asegurar su capacidad de operar frente a eventos imprevistos y minimizar pérdidas que puedan traer la interrupción de las actividades del negocio.

Existen eventos que van más allá del control de la institución y pueden resultar en la inhabilidad para cumplir algunos o todas sus obligaciones de negocios, particularmente donde las estructuras físicas, de telecomunicación, o de tecnología de información han sido dañadas o son inaccesibles. Esto puede, a la vez, resultar en pérdidas financieras significativas, como también interrupciones más amplias en el sistema financiero mediante canales como el sistema de pagos. Las instituciones deben identificar procesos críticos de negocio y plantear mecanismos alternos para reasumir el servicio en caso de un paro.

Adicionalmente, se debe revisar periódicamente los planes de continuidad de negocios y de contingencia para que sean consistentes con las operaciones y estrategias actuales del negocio.

Principio 8: Los supervisores bancarios deben requerir que todas las instituciones financieras, sin considerar el tamaño, tengan un marco efectivo establecido para identificar, evaluar, monitorear y controlar o mitigar los riesgos operacionales como parte de un enfoque global a la administración de riesgos.

Principio 9: Los supervisores deben conducir, directa o indirectamente, la evaluación independiente y regular de las políticas, procedimientos y practicas relacionadas a los riesgos operacionales. Los supervisores deben asegurar que existan mecanismos apropiados de reporte establecidos que les permitan permanecer informados de los desarrollos dentro de las instituciones.

La evaluación independiente del riesgo operacional por parte de los supervisores debe incorporar la revisión de los siguientes puntos:

- El proceso de la institución para evaluar la adecuación de capital global para el riesgo operacional en relación a su perfil de riesgo.

- La efectividad del proceso de administración y el control global con respecto al riesgo operacional.

- Los sistemas para monitorear y reportar su perfil de riesgo operacional, incluyendo datos sobre pérdidas operacionales y otros indicadores de riesgo operacional potencial.

- Los procedimientos adoptados para la resolución oportuna y efectiva de los eventos y vulnerabilidades de riesgo operacional. El proceso de controles, revisiones y auditoria para asegurar la integridad del proceso global de administración de riesgo operacional.

- La calidad y comprensión de los planes de contingencia y continuidad del negocio.

Para que los mecanismos supervisores reciban información actual sobre el riesgo operacional, pueden desear establecer mecanismos de reporte, directamente con bancos y auditores externos. Dado al reconocimiento general de que los procesos de administración de riesgo operacional aún están en desarrollo, los supervisores deben tomar un papel activo en fomentar esfuerzos recurrentes de desarrollo interno para monitorear y evaluar las recientes mejoras y los planes para desarrollos futuros de una institución.

Principio 10: Las instituciones financieras deben hacer divulgación pública para permitir a los participantes del mercado evaluar su enfoque a la administración del riesgo operacional.

El Comité de Basilea cree que la divulgación pública oportuna y frecuente de información relevante por parte de las instituciones financieras puede llevar a una disciplina de mercado mejorada y, por consiguiente, una efectiva administración del riesgo. La cantidad de divulgación debe estar proporcionada con el tamaño y complejidad de las operaciones de la institución.

CAPITULO III

MARCO EMPIRICO

3.1 La Superintendencia de Bancos y Seguros y el Riesgo Operativo

El análisis de Riesgo es un proceso por el cual se identifican, miden, controlan y monitorean los diferentes riesgos a los que se encuentra expuesta una Institución Financiera, con la finalidad de definir el tipo y el nivel máximo de pérdida que se está dispuesto a asumir, así como las medidas de control y los mecanismos de cobertura para proteger los recursos que se encuentran bajo su administración, teniendo de esta forma un permanente control frente a las pérdidas que se pueden generar tanto por factores internos como externos.

El Sistema Bancario Ecuatoriano ha tenido un desarrollo importante dentro de un proceso de consolidación y crecimiento, demostrándose a través de una relativa estabilidad económica, la cual es medida por el crecimiento del PIB.

Con este antecedente se torna fundamental el realizar un correcto control del manejo de las instituciones para de esta forma poder asegurar una administración sana y de igual formar poder mantener un nivel adecuado de capital y reservas para poder hacer frente a los riesgos que son inminentes dentro del giro del negocio.

A partir del año de 1994 en la que la Ley General de Instituciones del Sistema se encuentra en vigencia, ha tenido la función primordial de regular el funcionamiento y las operaciones del sector financiero y de seguros.

El Sistema Financiero Ecuatoriano se ha centrado en el análisis y control de los denominados Riesgos Financieros, sin embargo con el desarrollo de los mercados se ha podido identificar otros tipos de riesgos que las entidades deben medir y cuantificar.

Uno de los riesgos que se pueden identificar a partir del desarrollo de los mercados es el Riesgo Operacional, el cual evidencia las pérdidas resultantes por el inadecuado manejo de los procesos internos, personas, sistemas o a su vez por la falta de previsión de eventuales factores externos que pueden generar pérdidas para la institución.

Las normas de Basilea dentro del proceso de adaptación a las regulaciones de la Superintendencia de Bancos son de manera continuas e implica cambios y reformas legales, de carácter regulatorio y normativo, lo que implica que las entidades financieras reguladas deben realizar los respectivos cambios en sus sistemas administrativos y operacionales para poder cumplir con los requisitos exigidos por el ente de control.

Frente a que debe haber un correcto manejo y control de los diferentes riesgos que amenazan a las instituciones financieras, la Superintendencia de Bancos y Seguros aprobó la resolución JB2005-834, la cual establece que las instituciones del sistema financiero bajo el control de la Superintendencia de Bancos y Seguros deberán establecer esquemas eficientes y efectivos de administración y control de todos los riesgos a los que se encuentran expuestas en el desarrollo del negocio, conforme con su objeto social.

Dentro de la normativa aprobada, las instituciones financieras deben contar con un sistema de administración del riesgo operativo que les permita identificar, medir, controlar-mitigar y monitorear los riesgos de manera que se fortalezca su seguridad y solidez, en orden a proteger los intereses de los clientes.

Conforme a la normativa del Superintendencia de Bancos y Seguros las instituciones del sistema financiero deben gestionar el riesgo operativo, como elemento fundamental de una administración preventiva que reduzca la posibilidad de pérdidas e incremente su eficiencia, para lo cual deberán

implantar mecanismos, procesos y contar con recursos humanos calificados y experimentados a fin de mitigar este riesgo.

Para que las instituciones financieras puedan gestionar el riesgo operativo de la manera más eficiente es necesario establecer estándares mínimos prudenciales para poder operar en un ambiente favorable, previo a la medición del mismo para posteriores requerimientos de capital.

3.1.1 RIESGO OPERATIVO

Conforme al punto 2.9 del Artículo 2, Sección I, Capítulo I, Subtitulo VI, del Titulo VII.- De los Activos y de los Límites de Crédito, el riesgo operativo se define como:

> Es la posibilidad de que se produzcan pérdidas debido a eventos originados en fallas o insuficiencia de procesos, personas, sistemas internos, tecnología, y en la presencia de eventos externos imprevistos. Incluye el riesgo legal pero excluye los riesgos sistémico y de reputación.
>
> Agrupa una variedad de riesgos relacionados con deficiencias de control interno; sistemas, procesos y procedimientos inadecuados; errores humanos y fraudes; fallas en los sistemas informáticos; ocurrencia de eventos externos o internos adversos, es decir, aquellos que afectan la capacidad de la institución para responder por sus compromisos de manera oportuna, o comprometen sus intereses

3.1.2 Factores del Riesgo Operativo[9]

Con la finalidad de minimizar las probabilidades de que se genere pérdidas financieras debido al riesgo operativo, hay que tener en cuenta los siguientes aspectos para su correcta administración:

Procesos.- Con el objeto de garantizar la optimización de los recursos y la estandarización de las actividades, las instituciones controladas deben contar con procesos definidos de conformidad con la estrategia y las políticas adoptadas, que deberán ser agrupados de la siguiente manera:

[9] Resolución No JB-2005-834

Procesos gobernantes o estratégicos.- Se considerarán a aquellos que proporcionan directrices a los demás procesos. Se refieren a la planificación estratégica, los lineamientos de acción básicos, la estructura organizacional, la administración integral de riesgos, entre otros.

Procesos productivos, fundamentales u operativos.- Son los procesos esenciales de la entidad destinados a llevar a cabo las actividades que permitan ejecutar efectivamente las políticas y estrategias relacionadas con la calidad de los productos o servicios que ofrecen a sus clientes.

Procesos habilitantes, de soporte o apoyo.- Son aquellos que apoyan a los procesos gobernantes y productivos, se encargan de proporcionar personal competente, reducir los riesgos del trabajo, preservar la calidad de los materiales, equipos y herramientas, mantener las condiciones de operatividad y funcionamiento, coordinar y controlar la eficacia del desempeño administrativo y la optimización de los recursos.

Una vez identificados los procesos críticos, las instituciones financieras implantarán mecanismos o alternativas que ayuden a evitar la generación de pérdidas o poner en riesgo la continuidad del negocio y sus operaciones.

Para considerar la existencia de un apropiado ambiente de gestión de riesgo operativo, las instituciones controladas deberán definir formalmente políticas para un adecuado diseño, control, actualización y seguimiento de los procesos.

Las políticas deben referirse por lo menos a:

a) Diseño claro de los procesos, los cuales deben ser adaptables y dinámicos.

b) Descripción en secuencia lógica y ordenada de las actividades, tareas, y controles.

c) Determinación de los responsables de los procesos

d) Difusión y comunicación de los procesos buscando garantizar su total aplicación.

e) Actualización y mejora continua a través del seguimiento permanente en su aplicación.

Personas.- Las instituciones controladas deben administrar el capital humano de forma adecuada, e identificar apropiadamente las fallas o insuficiencias asociadas al factor .personas, tales como: falta de personal adecuado, negligencia, error humano, nepotismo de conformidad con las disposiciones legales vigentes, inapropiadas relaciones interpersonales y ambiente laboral desfavorable, falta de especificaciones claras en los términos de contratación del personal, entre otros.

Conforme a lo recomendado por Basilea y normado por la Superintendencia de Bancos y Seguros, es necesario generar un apropiado ambiente de gestión de riesgo operativo, el cual será definido por medio de la formulación de políticas, procesos y procedimientos para de esta forma poder asegurar una apropiada planificación y administración del capital humano, los cuales deberán considerar los procesos de incorporación, permanencia y desvinculación del personal al servicio de la institución.

Dentro de los procesos a ser definidos, se deben tener en cuenta los que corresponden a:

Los procesos de incorporación.- Que comprenden la planificación de necesidades, el reclutamiento, la selección, la contratación e inducción de nuevo personal.

Los procesos de permanencia.- Que cubren la creación de condiciones laborales idóneas; la promoción de actividades de capacitación y formación que permitan al personal aumentar y perfeccionar sus conocimientos, competencias y destrezas; la existencia de un sistema de evaluación del desempeño; desarrollo de carrera; rendición de cuentas; e incentivos que motiven la adhesión a los valores y controles institucionales.

Los procesos de desvinculación.- Que comprenden la planificación de la salida del personal por causas regulares, preparación de aspectos jurídicos para llegar al finiquito y la finalización de la relación laboral.

Tecnología de información.- Las instituciones controladas deben contar con la tecnología de información que garantice la captura, procesamiento, almacenamiento y transmisión de la información de manera oportuna y confiable; evitar interrupciones del negocio y lograr que la información, inclusive aquella bajo la modalidad de servicios provistos por terceros, sea íntegra, confidencial y esté disponible para una apropiada toma de decisiones.

Para generar y mantener la existencia de un apropiado ambiente de gestión de riesgo operativo, las instituciones financieras deberán definir políticas, procesos y procedimientos que aseguren una adecuada planificación y administración de la tecnología de información.

Dichas políticas, procesos y procedimientos se referirán a:

a) Garantizar que la administración de la tecnología de información soporte adecuadamente los requerimientos de operación actuales y futuros de la entidad.

b) Garantizar que las operaciones de tecnología de información satisfagan los requerimientos de la institución.

c) Garantizar que los recursos y servicios provistos por terceros, se administren con base en responsabilidades claramente definidas y estén sometidas a un monitoreo de su eficiencia y efectividad.

d) Garantizar que el sistema de administración de seguridad satisfaga las necesidades de la entidad para salvaguardar la información contra el uso, revelación y modificación no autorizados, así como daños y pérdidas.

e) Garantizar la continuidad de las operaciones.

f) Garantizar que el proceso de adquisición, desarrollo, implementación y mantenimiento de las aplicaciones satisfagan los objetivos del negocio.

g) Garantizar que la infraestructura tecnológica que soporta las operaciones, sea administrada, monitoreada y documentada de forma adecuada.

Eventos externos.- Se debe considerar la posibilidad de pérdidas derivadas de la ocurrencia de eventos ajenos a su control, tales como: fallas en los servicios públicos, ocurrencia de desastres naturales, atentados y otros actos delictivos, los cuales pudieran alterar el desarrollo normal de sus actividades. Para el efecto, deben contar con planes de contingencia y de continuidad del negocio.

3.1.3 Administración del Riesgo Operativo[10]

Las instituciones financieras que se encuentran bajo el control de la Superintendencia de Bancos y Seguros deberán incluir el proceso de administración de riesgo operativo para administrarlo como un riesgo específico, el mismo que si no es administrado adecuadamente puede afectar la estabilidad a largo plazo y la continuidad del negocio.

El proceso de administración de riesgo operativo deberá permitir a las instituciones identificar, medir, controlar-mitigar y monitorear al exposición que se tiene frente a este tipo de riesgos en el desarrollo operaciones y del negocio. Cada institución desarrollará sus propias técnicas o esquemas de administración, considerando su objeto social, tamaño, naturaleza, complejidad y demás características propias.

Para una correcta administración del riesgo operativo las instituciones deberán agrupar los procesos por líneas de negocio, de acuerdo con una metodología establecida de manera formal y por escrito, para lo cual deberán observar los siguientes lineamientos:

a) Los procesos productivos deberán asignarse a las líneas de negocio de acuerdo con los productos y servicios que generan, de forma que a cada uno de los procesos le corresponda una sola línea de negocio y que ningún proceso permanezca sin asignar.

b) Las líneas de negocio también deberán agrupar los procesos gobernantes y los procesos habilitantes que intervienen en las mismas. Si algún proceso gobernante o proceso habilitante interviene en más de una línea de negocio, la entidad deberá utilizar un criterio de asignación objetivo.

Las instituciones controladas deberán identificar, por línea de negocio, los eventos de riesgo operativo, agrupados por tipo de evento, y, las fallas o insuficiencias en los procesos, las personas, la tecnología de información y los eventos externos.

[10] Resolución No JB-2005-834

Los tipos de eventos son los siguientes:

- Fraude interno
- Fraude externo
- Prácticas laborales y seguridad del ambiente de trabajo
- Prácticas relacionadas con los clientes, los productos y el negocio
- Daños a los activos físicos
- Interrupción del negocio por fallas en la tecnología de información
- Deficiencias en la ejecución de procesos, en el procesamiento de operaciones y en las relaciones con proveedores y terceros.

Debido a que la administración del riesgo operativo constituye un proceso continuo y permanente, las instituciones controladas deberán conformar bases de datos centralizadas, suficientes y de calidad, que permitan registrar, ordenar, clasificar y disponer de información sobre los eventos de riesgo operativo; fallas o insuficiencias; y, factores de riesgo operativo clasificados por línea de negocio, determinando la frecuencia con que se repite cada evento y el efecto cuantitativo de pérdida producida y otra información que las instituciones consideren necesaria y oportuna, para que a futuro se pueda estimar las pérdidas esperadas e inesperadas atribuibles a este riesgo.

El esquema de administración del riesgo operativo de las instituciones controladas debe estar sujeto a una auditoria interna efectiva e integral, por parte de personal competente, debidamente capacitado y operativamente independiente.

La función de auditoria interna ayuda al mejoramiento de la efectividad de la administración de riesgos a través de una evaluación periódica, pero no es directamente responsable de la gestión del riesgo operativo.

Frente a todos los requerimientos exigidos por la Superintendencia de Bancos y Seguros, las instituciones financieras deben contar permanentemente con un esquema organizado de reportes que permitan disponer de información suficiente y adecuada para gestionar el riesgo operativo en forma continua y oportuna.

Dichos reportes deberán contener como mínimo los siguientes puntos:

a) Detalle de los eventos de riesgo operativo, agrupados por tipo de evento; las fallas o insuficiencias que los originaron relacionados con los factores de riesgo operativo y clasificado por líneas de negocio.

b) Informes de evaluación del grado de cumplimiento de las políticas relacionadas con los factores de riesgo operativo y los procesos y procedimientos establecidos por la institución.

c) Indicadores de gestión que permitan evaluar la eficiencia y eficacia de las políticas, procesos y procedimientos aplicados.

Estos informes deben ser dirigidos a los niveles correspondientes de la institución de manera que puedan ser analizados con una perspectiva de mejora constante del desempeño en la administración del riesgo operativo; así como para establecer o modificar políticas, procesos, procedimientos, de la institución.

3.1.4 Responsabilidades en la Administración del Riesgo Operativo[11]

Las responsabilidades del directorio u organismo que haga sus veces, en cuanto a la administración del riesgo operativo, se regirán por lo dispuesto en la sección III Responsabilidad en la administración de riesgos, del capítulo I .De la gestión integral y control de riesgos. (ANEXO 7)

El comité de administración integral de riesgos tendrá las siguientes responsabilidades en relación con la administración del riesgo operativo:

- Evaluar y proponer al directorio u organismo que haga sus veces las políticas y el proceso de administración del riesgo operativo y asegurarse que sean implementados en toda la institución y que todos los niveles del personal entiendan sus responsabilidades con relación al riesgo operativo.

[11] Resolución No JB-2005-834

- Evaluar las políticas y procedimientos de procesos, personas y tecnología de información y someterlas a aprobación del directorio u organismo que haga sus veces.

- Definir los mecanismos para monitorear y evaluar los cambios significativos y la exposición a riesgos.

- Evaluar y someter a aprobación del directorio u organismo que haga sus veces los planes de contingencia y de continuidad del negocio, asegurar la aplicabilidad; y, cumplimiento de los mismos.

- Analizar y aprobar la designación de líderes encargados de llevar a cabo las actividades previstas en el plan de contingencia y de continuidad del negocio.

La unidad de riesgos tendrán las siguientes responsabilidades en relación con la administración del riesgo operativo:

- Diseñar las políticas y el proceso de administración del riesgo operativo.

- Monitorear y evaluar los cambios significativos y la exposición a riesgos provenientes de los procesos, las personas, la tecnología de información y los eventos externos.

- Analizar las políticas y procedimientos de tecnología de información, propuestas por el área respectiva, especialmente aquellas relacionadas con la seguridad de la información.

- Liderar el desarrollo, la aplicabilidad y cumplimiento de los planes de contingencia y de continuidad del negocio, así como proponer los líderes de las áreas que deban cubrir el plan de contingencias y de continuidad del negocio.

3.2 Matriz y Mapas de Riesgo

Una matriz de riesgo constituye una herramienta de control y de gestión normalmente utilizada para identificar las actividades (procesos y productos) más importantes de una empresa, el tipo y nivel de riesgos inherentes a estas actividades y los factores exógenos y endógenos relacionados con estos riesgos

(factores de riesgo). Igualmente, una matriz de riesgo permite evaluar la efectividad de una adecuada gestión y administración de los riesgos financieros que pudieran impactar los resultados y por ende al logro de los objetivos de una organización.[12]

El principal insumo que permite analizar y adaptar la información a los criterios exigidos, por normas técnicas, son los registros y/o mapas de riesgos que son elaborados por cada institución de acuerdo al tamaño de cada una.

Los mapas de riesgos son mecanismos de control que facilitan la identificación de áreas con debilidades, por medio de la categorización de los tipos de riesgo que afectan a los diferentes procesos, departamentos o unidades del negocio, de manera que se pueda tomar medidas donde sea necesario actuar en forma prioritaria, para poder evitar pérdidas.

La clasificación de los riesgos se realiza por medio de una matriz en función del impacto del riesgo, es decir, de su importancia medida en términos monetarios y por la probabilidad de ocurrencia o frecuencia del mismo.

La matriz es un elemento fundamental para la toma de decisiones, ya que implica todos los niveles y ayuda a generar procedimientos para la mitigación y monitoreo de los riesgos.

La Matriz de Riesgos se la puede elaborar mediante técnicas de entrevistas con el personal clave de cada una de las áreas que forman parte de la Organización, para posteriormente agrupar los riesgos percibidos, tabularlos y mostrarlos.

Para la elaboración de la matriz, la primera actividad que se debe llevar a cabo es la elaboración de un cuestionario, en el cual se deben incluir los siguientes temas:

Identificación: Entorno interno y externo, modelo de negocios, creación de valor, tiempo de servicio, calidad en el servicio, satisfacción del cliente, tipos de riesgos (deseables y no deseables).

Determinación: Factores internos y externos que son causantes fundamentales de posibles riesgos.

[12] Keneth V.McKee, Metodología de Riesgos, Federal Reserve Banks of Dallas USA, 2004.

Cálculo: Pérdidas, repercusiones sobre el capital, indicadores claves de desempeño y reputación, probabilidades de ocurrencia de futuros eventos de riesgo.

3.2.1 Elaboración del Mapa de Riesgos

La elaboración del Mapa de Riesgos, empieza una vez que se llevan a cabo las entrevistas, con lo que se procede a tabularlas y realizar el feedback de la información, es decir, utilizar la información obtenida para identificar los riesgos y calificarlos respecto a su impacto y a su probabilidad, generando la matriz de riesgos.

La valoración de la importancia y frecuencia que se asigna corresponde a un análisis cualitativo, pues si bien se puede contar con registros de casos de fraude, éstos no constituyen una base de datos integra que recopile la materialización de todos los riesgos a los que históricamente ha estado expuesta una Institución.

Luego de la implementación de un programa de administración de riesgos, hay que identificar y valorar los riesgos asociados a las diversas actividades, funciones o procesos que ejecutan y señalan las acciones de su manejo.

El proceso que se puede utilizar para la elaboración del mapa de riesgos es el siguiente[13]:

- Adaptación de la información a la estructura y característica del modelo de administración de riesgo, para lo cual se debe identificar las fuentes genéricas del riesgo o los factores y componentes que pueden iniciarlo y que están bajo el control de la Institución.

- Una vez realizado el análisis anterior , se debe identificar los riesgos por medio del siguiente método:

[13] Procuraduría General de la Nación, Mapa de Riesgos Institucional, Bogota, Julio 2005.

Cuadro 1.

Identificación de Riesgos

Area de Impacto ¿Qué podría ocurrir?	Consecuencias y efectos	¿Por qué? ¿Cómo?	Eventos causas
Entidad - Proceso disciplinario	Pérdida de imagen	Ineficacia de la acción disiciplinaria	Mora en la actuación
Gastos de funcionamiento	Costos operativos	Reprocesos	Errores en trámites
Comunicación institucional	Reputación	Inadecuado manejo de la información	Filtración de noticias
Cumplimiento	Sanciones	Presentación extemporánea de informes	Desconociemiento de la norma

Fuente: procuraduría General de la Nación ï Bogota ï Colombia
Elaboración: Autor

- A continuación se debe clasificar bajo este esquema los datos obtenidos en el sistema de información.

- Realizar el ajuste de la información para la valoración y/o calificación de los riesgos utilizando una escala de medida cualitativa definida a través de tres categorías en los mapas de riesgos:

    - Alta
    - Media
    - Baja

Con la finalidad de hacerlas equivalentes estas categorías con los cálculos y escalas utilizadas se propone una escala de cinco posibles valores para asignar peso a las variables consecuencia y probabilidad, por medio de una metodología de priorización como se indica en los siguientes cuadros:

Cuadro 2.

Valoración de los Riesgos
Consecuencias o Impactos que general el Riesgo

Nivel	*Rangos*	*Descripción*
5	Catastrófico	Pérdidas de reputación e imagen enormes, pérdidas económicas enormes
4	Mayor	Pérdidas de reputación e imagen mayores, pérdidas económicas mayores
3	Moderado	Pérdidas de reputación e imagen medias, pérdidas económicas medias
2	Menor	Pérdidas de reputación e imagen bajas, pérdidas económicas bajas
1	Insignificante	Pérdidas de reputación e imagen mínimas, pérdidas económicasmínimas

Fuente:Procuraduria General de la Nación - Bogota - Colombia
Elaboración: Autor

Cuadro 3.

Probabilidad de Ocurrencia de Riesgos

Nivel	*Rangos*	*Descripción*
5	Casi cierta	La expectativa de ocurrencia se da en todas las circunstancias
4	Muy probable	Probabilidad de ocurrencia en la mayoría de las circunstancias
3	Moderada	Puede ocurrir
2	Improbable	Podría ocurrir algunas veces
1	Rara	Puede ocurrir solo bajo cinrcunstancias escepcionales

Fuente:Procuraduria General de la Nación - Bogota - Colombia
Elaboración: Autor

Una vez que se ha identificado y valorado los riesgos absolutos, se debe proceder a identificar y calificar los controles de tipo preventivo aplicados en las diferentes dependencias, los definidos dentro de la institución y los de origen externo.

Con la calificación de los controles, se valora nuevamente el riesgo utilizando los parámetros de las escalas antes señaladas, con la finalidad de determinar el impacto que estos controles ejercen sobre el riesgo, dando como resultado el nivel de exposición y una nueva calificación dando el riesgo residual.

La severidad del riesgo es el resultado de cruzar la consecuencia con la probabilidad, siendo así como el riesgo se ubica en cualquiera de los cuatro rangos establecidos: extremo, alto, moderado y bajo.

Cuadro 4.

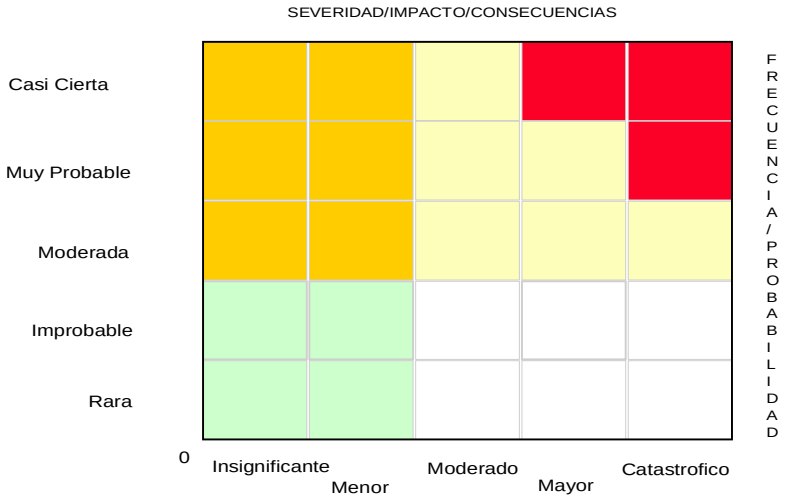
Nivel de Exposición o Severidad del Riesgo

Riesgo	*Descripción*
Extremo	Riesgo extremo, se requiere acción inmediata. Planes de tratamiento requeridos, implementados y reportados a la alta dirección
Alto	Riesgo alto, requiere atención de la alta dirección. Planes de tratamiento requeridos, implementados y reportados a Jefes, Oficinas, etc
Moderado	Riesgo moderado, aceptable, debe ser administrado con procedimientos normales de control.
Bajo	Menores efectos que pueden ser facilmente remediados. Riesgo bajo, se administra con procedimientos rutinarios, riesgo insignificante. No se requiere ninguna acción.

Fuente:Procuraduria General de la Nación - Bogota - Colombia
Elaboración: Autor

Los colores para su identificación se presentan en la siguiente matriz:

Cuadro 5.



Fuente: Seminario Internacional "Riesgo Operativo y Control de Calidad Institucional en la Banca"
Elaboracion: Autor

El nivel de severidad de los riesgos, según los cuadrantes de combinación de consecuencia y probabilidad es el siguiente:

Cuadro 6. **Nivel de Severidad**

x	y	Rotulo	Color
1	1	Bajo	
2	1	Bajo	
3	1	Moderado	
5	1	Alto	
2	2	Bajo	
3	2	Moderado	
4	2	Alto	
5	2	Extremo	
1	3	Bajo	
2	3	Moderado	
3	3	Alto	
5	3	Extremo	
1	4	Moderado	
3	4	Alto	
5	4	Extremo	
2	5	Alto	
5	5	Extremo	

Fuente:Procuraduria General de la Nación - Bogota - Colombia

Elaboración: Autor

Es conveniente tener en cuanta que la severidad es el resultado de la probabilidad de que ocurra el riesgo por la consecuencia que es generado por este, con lo que se presentan dos calificaciones, una del riesgo absoluto y otra dependiendo de la existencia y eficacia de los controles, se convierte en riesgo residual.

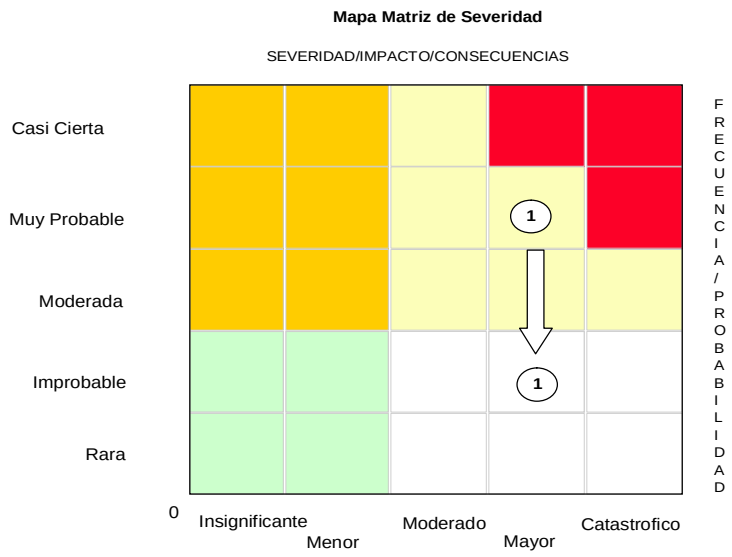
A partir del análisis y determinación del riesgo residual los administradores pueden tomar decisiones como la de continuar o abandonar la actividad dependiendo del nivel de riesgos; fortalecer controles o implantar nuevos controles; o finalmente, podrían tomar posiciones de cobertura, contratando por ejemplo pólizas de seguro. Esta decisión está delimitada a un análisis de costo beneficio y riesgo.

3.2.2 Mapa Gráfico de la Matriz de Severidad[14]

En resumen con todo lo que se ha mencionado, se puede visualizar el riesgo en tres momentos: riesgo absoluto, riesgo en controles y riesgo residual.

En el riesgo residual como se indicó, se puede ver en la gráfica una flecha con la cual se demuestra el desplazamiento de la severidad en razón de la eficacia de los controles, esto se lo puede visualizar a continuación:

Cuadro 7.



Fuente: Seminario Internacional "Riesgo Operativo y Control de Calidad Institucional en la Banca"
Elaboracion: Autor

[14] Procuraduría General de la Nación, Mapa de Riesgos Institucional, Bogota, Julio 2005.

Una vez valorados los controles y vista la posición que ocupa el riesgo dentro de la matriz de severidad, se procede a definir el tratamiento que se le debe a este de acuerdo con los criterios o lineamientos que se indican a continuación:

Cuadro 8.

Lineamientos para el tratamiento del Riesgo

Severidad	Consideración	Medidas de respuesta
Extrema	El riesgo es inaceptable	Es aconsejable, si es posible, eliminar la actividad que genera el riesgo, de lo contrario se deben implementar nuevos controles de prevensión, para reducir la probabilidad; de protección para disminuir las consecuencias o compartir el riesgo, si es posible, por medio de pólizas u otras opciones disponibles.
Alta	El riesgo es importante	Se deben tomar medidas para bajar la severidad del riesgo; si es posible, fortalecer y mejorar controles existentes.
Moderada	El riesgo es tolerable	Se pueden tomar medidas para bajar la severidad; si es posible, se deben conservar y mejorar controles.
Baja	El riesho es aceptable	La entidad puede asumir el riesgo sin necesidad de tomar otras medidas de control diferentes a las que posee.

Fuente:Procuraduria General de la Nación - Bogota - Colombia
Elaboración: Autor

3.3 Base de Datos de Riesgo Operativo

Una base de datos es el lugar donde se almacenan los datos en reposo y al cual acceden las diferentes aplicaciones (sistemas o programas) de una organización dada.[15]

3.3.1 Ventajas de la utilización de las Bases de Datos

Dentro de las principales ventajas de la utilización de las bases de datos se pueden señalar entre las más importantes las siguientes:

- Normalizar los datos de las bases de datos.

[15] Ezequiel, Bases de Datos y su Aplicación con SQL, Manuales USERS. MP Ediciones, Buenos Aires 2004.

- Evitar la redundancia de datos.
- Evitar la inconsistencia de datos.
- Garantizar la integridad de los datos.
- Garantizar la seguridad de los datos.
- Compartir los datos.
- Facilidad de modificar los datos.

Normalizar los datos: Permite minimizar entre otras cosas las redundancia de datos y agilizar y garantizar la actualización de los mismos.

Evitar redundancia de datos: Estos se tratan de guardar en un único lugar y cuando existe la necesidad de acceder a ellos, se hace por medio de relaciones entre los mismos.

Evitar inconsistencia de datos: Dado que las bases de datos utilizan transacciones se puede garantizar prácticamente la inexistencia de inconsistencia de datos.

Garantizar la integridad de los datos: El concepto básico de integridad es que la información obtenida de la base de datos es la correcta en todo momento.

Garantizar la seguridad de los datos: Dado que los accesos a la base de datos tanto para usuarios como para aplicaciones están dados por medio de permisos, si estos últimos están bien definidos nadie podrá ingresar a ningún lugar que no le esté permitido ni acceder a un conjunto de datos que no le este permitido.

Compartir los datos: Dado que los datos se encuentran en un mismo lugar lógico, estos se pueden compartir sin problema entre distintos usuarios y aplicaciones.

Facilidad de modificar datos: Debido a que se evita la redundancia y son a su vez almacenados en un mismo lugar lógico, es más fácil poder realizar modificaciones sobre ellos.

3.3.2 Arquitectura de una Base de Datos

La arquitectura de una base de datos se refiere a las presentaciones físicas y lógicas de las bases dentro de una organización. Anteriormente las bases de datos de las organizaciones se ubicaban principalmente en macro computadoras, a las cuales se tenía acceso desde lugares remotos en toda la empresa mediante terminales no inteligentes.

Dentro de la arquitectura de la base de datos se han realizado cambios importantes, debido a que tanto las bases como los programas que las ejecutaban cambiaron de macro computadoras a PCS, pasando de un modelo centralizado a uno distribuido.

3.3.3 Base de datos distribuidas

Muchas instituciones operan a través de sitios geográficos remotos, sin embargo mucho de los datos que se usan en un sitio con frecuencia se usan en otros. Por supuesto, la organización puede usar una base de datos central permitiendo que otros sitios la usen a través de líneas de comunicación, a este tipo de estructuras se la llama base de datos distribuida, la cual puede a su ves ser duplicada o fragmentada.

El administrador de las bases de datos duplica la base de manera que haya copias en varios lugares o la fragmenta, para que haya distintas partes en la base de datos en diferentes máquinas.

Duplicar una base de datos significa que se almacena una copia integra de ella en todos los sitios que necesitan accesarla, este método es costoso y no garantiza la integridad de los datos, porque debe realizarse todas las actualizaciones en cada uno de los sitios donde se encuentren, y es alta la posibilidad que se presenten errores debido a las actualizaciones tardías y a los errores de copiado.

Muchas corporaciones han optado por fragmentar la base de datos, ya que las diferentes partes de la base de datos se almacenan en lugares cuyo acceso sea más frecuente, pero continúan estando

disponibles para otros usuarios a través de telecomunicaciones, con lo que en conjunto todas las partes componen la base de datos.

El uso de aplicaciones de fragmentos remotos de la base de datos resulta fácil para los usuarios, quienes no necesitan preocuparse por cual parte de la base de datos reside localmente en un sitio y cual se procesa de manera remota.

Una ventaja de las bases de datos fragmentadas es el bajo costo de comunicaciones, así mismo otra de las ventajas es que en una sola copia se tiene mejor integridad de los datos.

3.3.4 Bases de Datos y Riesgo Operativo

Con la construcción de la Base de Datos de eventos operacionales y el registro de las pérdidas operacionales, lo cual conjuntamente con la información cualitativa, se puede realizar una gestión proactiva del riesgo operacional lo cual puede anticipar las posibles causas de riesgo y reducir su impacto económico, con la consiguiente adaptación de las necesidades de recursos propios.

La Base de Datos de eventos operacionales tiene como premisa fundamental disponer de una base de datos de eventos de pérdida íntegra y de un volumen suficiente de datos para que los cálculos de riesgo sean óptimos.

El objetivo de crear una base de datos que contenga las pérdidas operacionales, es conformar una plataforma de información poblada con datos de por lo menos 3 años de anterioridad, con el fin de poder efectuar inferencias en los mismos.

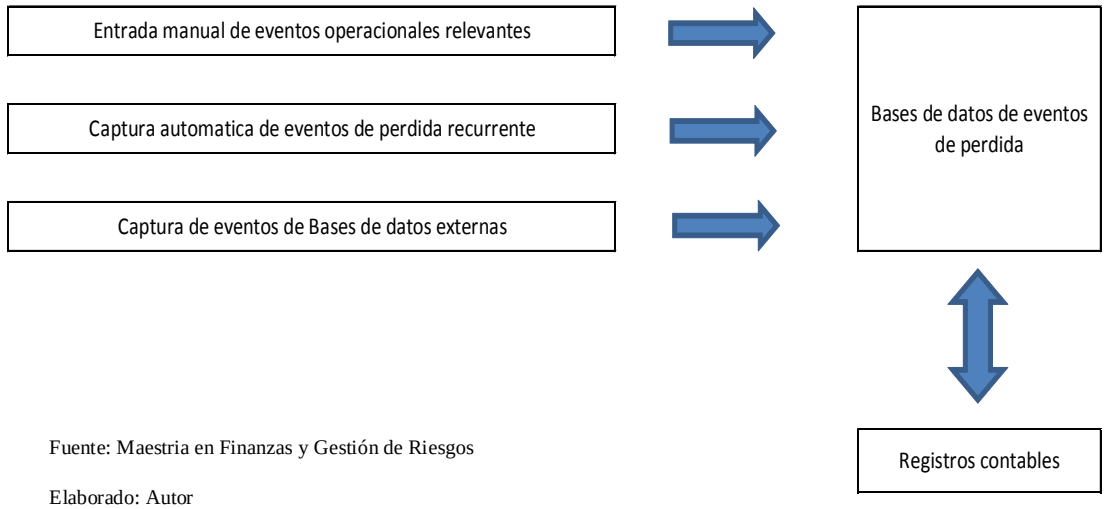
Uno de los elementos más importantes para la gestión y la cuantificación del Riesgo Operacional es la disponibilidad de datos, principalmente de pérdidas operativas, tanto internas como externas. El Comité de Basilea, manifiesta la necesidad de las Instituciones Financieras de empezar a capturar los datos internos de estas pérdidas; por tanto, se ha propuesto a las entidades a compartir este tipo de información a través de iniciativas sectoriales.

Adicionalmente, el Comité de Basilea pone énfasis en la utilización de datos externos como complemento a los datos internos. Sin embargo, los datos internos de pérdidas son estrictamente

necesarios ya que son la mejor representación de la estructura de negocio, de los sistemas de control y de la cultura de cada organización. Los datos externos son importantes como información de soporte, ya que no se puede predecir a futuro únicamente por medio de datos pasados.

Cuadro 9.

PROCESO DE CAPTURA DE EVENTOS



Fuente: Maestria en Finanzas y Gestión de Riesgos

Elaborado: Autor

Así mismo se tiene que establecer como proyecto fundamental, el diseño de la base de datos que permita registrar la información relacionada con los eventos de riesgo que se presenten en la Institución, a partir de la cual se desarrollarán modelos, los mismos que servirán para determinar el requerimiento de capital para poder cubrir este tipo de riesgos.

Es por eso que a cada evento de riesgo se les asignará un factor, tal como se sugiere en el acuerdo de Basilea II y en la normativa planteada por la Superintendencia de Bancos y Seguros, sin embargo, se requiere un detalle más amplio por cada evento, por lo que se ha considerado que cada registro de la base de datos debe contener los siguientes campos: período, categoría de evento de riesgo, descripción del evento, entre los mas importantes.

Con la elaboración de la base de datos para pérdidas operacionales, esta se convertirá en el insumo para que una vez aplicado un sistema, se puedan establecer medidas preventivas y correctivas tendientes a mitigar los riesgos y cuantificar el requerimiento de capital.

Las actividades iniciales que se deben llevar a cabo, una vez que se ha diseñado el detalle de la base de datos, son:

- Programación del sistema (pantallas de ingreso, consultas, reportes, actualizaciones, controles, etc.).
- Elaboración de la documentación de soporte (manual técnico y manual del usuario).
- Capacitación a los usuarios del sistema.
- Prueba e implementación definitiva del sistema.

3.4 Metodologías de Medición del Riesgo Operativo

La medición es, sin duda, el aspecto más complejo y a la vez el más trascendental en el tratamiento del riesgo operacional.

Una correcta cuantificación del riesgo operacional permitirá una reducción de capital regulatorio para los enfoques más avanzados, de igual forma desde un punto de vista práctico, la medición del riesgo operacional permite su inclusión en el cálculo de la rentabilidad ajustada al riesgo y, por tanto, acercar más a la realidad el modelo de creación de valor de la compañía.

El Comité de Basilea propone tres enfoques para calcular los requerimientos de capital por riesgo operacional que, ordenados de menor a mayor grado de sofisticación y sensibilidad al riesgo son:

- Método del Indicador Básico (Basic Indicator Approach, BIA)
- Método Estándar (Standardized Approach, SA)
- Metodologías de Medición Avanzada (Advanced Measurement Approach, AMA).

Además de seguir las directrices del Comité de Basilea, los bancos que deseen utilizar el Método Estándar o las metodologías AMA tendrán que cumplir una serie requisitos mínimos en la gestión y control de este riesgo.

3.4.1 Metodologías Top-Down

Dentro de estas metodologías se engloban el Método del Indicador Básico y el Modelo Estándar, ambos cubren el riesgo operacional con un capital equivalente a un porcentaje fijo de los ingresos brutos.

La principal diferencia entre uno y otro es que en el Método Estándar, el total de capital requerido se calcula como la suma de las necesidades de capital regulatorio de cada una de las líneas de negocio descritas por Basilea.

Por otro lado, Basilea II se basa en la simplicidad de su concepto para convertir la variable ingresos brutos en una aproximación al tamaño o nivel de la exposición al riesgo operacional. Pero frente a eso hay que tener una mayor precaución debido a que el volumen de ingresos depende del marco normativo de cada país, dando lugar a posibles arbitrajes regulatorios.

Además, este hecho puede derivar en situaciones paradójicas, así una entidad con unos elevados ingresos brutos pero con mejores prácticas podría tener menores riesgos operacionales.

3.4.1.1 Método del Indicador Básico (Basic Indicator Approach, BIA)[16]

Los bancos que utilicen el Método del Indicador Básico deberán cubrir el riesgo operativo con un capital equivalente al promedio de los tres últimos años de un porcentaje fijo (denotado como alfa) de sus ingresos brutos anuales positivos. Al calcular este promedio, se excluirán tanto del numerador como del denominador los datos de cualquier año en el que el ingreso bruto anual haya sido negativo o igual a cero.

[16] Comité de Supervisión Bancaria de Basilea, Convergencia Internacional de medidas y normas de capital, Banco de Pagos Internacionales, junio 2004.

La exigencia de capital puede expresarse del siguiente modo:

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

Donde:

K_{BIA} = la exigencia de capital en el Método del Indicador Básico.

GI = ingresos brutos anuales medios, cuando sean positivos, de los tres últimos años.

n = número de años (entre los tres últimos) en los que los ingresos brutos fueron positivos.

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

Los ingresos brutos se definen como los ingresos netos en concepto de intereses más otros ingresos netos ajenos a intereses. Se pretende que esta medida:

1. Sea bruta de cualquier provisión dotada (por ejemplo, por impago de intereses).

2. Sea bruta de gastos de explotación, incluidas cuotas abonadas a proveedores de servicios de subcontratación.

3. Excluya los beneficios / pérdidas realizados de la venta de valores de la cartera de inversión.

4. Excluya partidas extraordinarias o excepcionales, así como los ingresos derivados de las actividades de seguro.

3.4.1.2 Método Estándar (Standardized Approach, SA)

En el Método Estándar, las actividades de los bancos se dividen en ocho líneas de negocio, los cuales son:

- Finanzas corporativas

- Negociación y ventas
- Banca minorista
- Banca comercial
- Pagos y liquidación
- Servicios de agencia
- Administración de activos
- Intermediación minorista.

El ingreso bruto de cada línea de negocio es un indicador amplio que permite aproximar el volumen de operaciones del banco y, con ello, el nivel del riesgo operativo que es probable que asuma la institución en estas líneas de negocio.

El requerimiento de capital de cada línea de negocio se calcula multiplicando el ingreso bruto por un factor (denominado beta) que se asigna a cada una de las líneas. Beta se utiliza como una aproximación a la relación que existe en el conjunto del sector bancario entre el historial de pérdidas debido al riesgo operativo de cada línea de negocio y el nivel agregado de ingresos brutos generados por esa misma línea de negocio.

La exigencia total de capital se calcula como la media de tres años de la suma simple de las exigencias de capital regulador en cada una de las líneas de negocio cada año.

Para un año dado, los requerimientos de capital negativos (resultantes de ingresos brutos negativos) en cualquiera de las líneas de negocio podrán compensar los requerimientos positivos en otras líneas de negocio sin límite alguno. No obstante, cuando el requerimiento de capital agregado para todas las líneas de negocio dentro de un año en concreto sea negativo, el argumento del numerador para ese año será cero.

El requerimiento total de capital puede expresarse como:

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

Donde:

K_{TSA} = la exigencia de capital en el Método Estándar

GI_{1-8} = los ingresos brutos anuales de un año dado, como se define en el Método del Indicador Básico, para cada una de las ocho líneas de negocio

β_{1-8} = un porcentaje fijo, establecido por el Comité, que relaciona la cantidad de capital requerido con el ingreso bruto de cada una de las ocho líneas de negocio

Los valores de los factores beta se enumeran a continuación.

Líneas de negocio	Factores Beta
Finanzas Corporativas (ϐ1)	18%
Negociación y ventas (ϐ2)	18%
Banca minorista (ϐ3)	12%
Banca comercial (ϐ4)	15%
Pagos y liquidación (ϐ5)	18%
Servicios de agencia (ϐ6)	15%
Administración de activos (ϐ7)	12%
Intermediación minorista (ϐ8)	12%

3.4.2 Metodologías Bottom-Up.

Para estas metodologías el requerimiento de capital será igual a la medida generada por el sistema interno de medición de riesgo operacional de la institución. Las metodologías AMA, son más sensibles al riesgo pero a la vez más costosas y complejas, se encuentran con un gran obstáculo para su aplicación, que es la ausencia de una base de datos interna de pérdidas, con las cuales aproxima las variables a utilizar. Si bien, la mayoría de las instituciones financieras se inclinan por este enfoque, el grado de implantación irá íntimamente ligado a la disponibilidad de los datos de pérdidas de la entidad.

Dentro de las metodologías AMA, el Comité propone tres enfoques:

- Modelo de Medición Interna (Internal Measurement Approach, IMA)
- Cuadros de Mando (Scorecards)
- Modelo de Distribución de Pérdidas (Loss Distribution Approach, LDA).

Si bien el Comité de Basilea parecía tender al IMA, como metodología más acorde para el cálculo de capital regulatorio por riesgo operacional, terminó dando un mayor enfoque al Modelo de Distribución de Pérdidas (LDA), dejándolo de esta forma en mejor posicionamiento frente al resto de las metodologías AMA.

El enfoque LDA se fundamenta en la información de pérdidas históricas recopiladas internamente y complementadas con datos externos. Las pérdidas registradas se clasifican en base a una matriz, como la que se indica a continuación (Cuadro 10), en la que se relaciona las ocho líneas de negocio con los siete tipos de pérdidas operacionales estandarizados por el Comité.

Cuadro 10.

Matriz Línea de Negocio

Tipo de Riesgo / Linea de Negocio	Fraude Interno	Fraude Externo	Practicas de empleo y seguridad laboral	Clientes, productos y practicas comerciales	Daños a activos fisicos	Interrupcion deoperaciones y fallos de sistemas	Ejecucion, entrega y gestión de procesos
Banca Corporativa							
Negociacion y Ventas							
Banca Minorista							
Banca de Empresas							
Pagos y Liquidaciones							
Servicios a Sucursales							
Gestión de Activos							
Intermediación Minorista							

Fuente: Maestria en Finanzas y Gestión de Riesgos - Normatividad

Elaborado: Autor

La matriz contiene un total de 56 casillas en las que hay que estimar, para cada celda, la distribución de la frecuencia, por un lado, y la distribución de la severidad, por el otro.

Una vez acotadas éstas, el objetivo es obtener la distribución de pérdidas agregada por riesgo operacional asociada a cada casilla. Para el cálculo del capital regulatorio vinculado a éstas se introduce el concepto de Valor en Riesgo (VaR) aplicado en este caso al riesgo operacional y tomando la nomenclatura, ya aceptada, de OpVaR o CaR (Capital-at-Risk).

Es decir, OpVaR y CaR son términos sinónimos; algo que no ocurre con los conceptos de pérdida esperada e inesperada. En sentido estricto, el capital económico debería cubrir la pérdida inesperada (unexpected loss, UL) ya que la pérdida esperada (expected loss, EL) se provisiona.

No obstante, en sentido amplio y, a petición del Comité, el capital regulatorio debe contemplar ambas pérdidas para su cómputo; de ahí que se de la identidad entre éste y el concepto de OpVaR y se representa de acuerdo a la siguiente fórmula:

$$OpVaR \equiv CaR(i, j;\alpha) = EL(i, j) + UL(i, j;\alpha)$$

Donde:

EL (Expected Loss): Pérdida Esperada.
UL (Unexpected Loss): Pérdida Inesperada.

Finalmente, el capital regulatorio de la entidad por riesgo operacional será el cómputo del capital de las 56 casillas, de donde se desprende la siguiente expresión:

$$K_{LDA} = CaR(\alpha) = \sum\sum CaRij(\alpha)$$

3.4.3 Modelo de Distribución de Pérdidas Agregadas (LDA)

Como se ha mencionado anteriormente, el Valor en Riesgo Operacional requiere, para su correcta interpretación, la definición de la metodología utilizada en su cálculo, debido a que tiene, importantes

consecuencias prácticas. Y es que, en función de la metodología empleada y los parámetros seleccionados, se podrá obtener una cifra OpVaR, distinta según el caso.

Dicho de otro modo, dependiendo de lo realistas, restrictivas o simplificadoras que sean las hipótesis subyacentes, las estimaciones del OpVaR obtenidas, aplicando una determinada metodología, serán más o menos fiables y precisas.

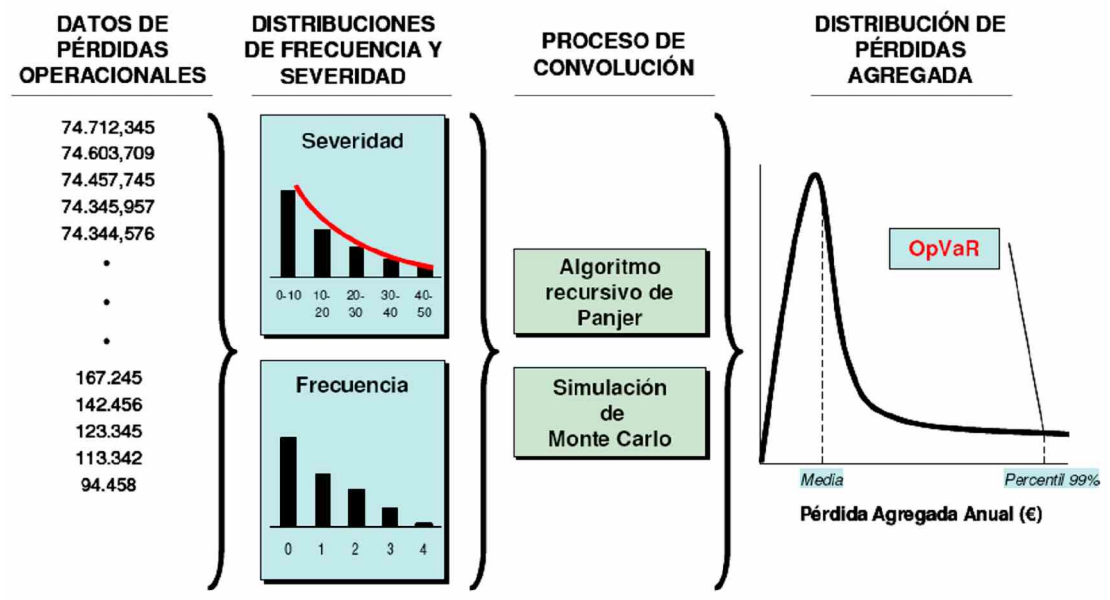
El enfoque LDA parece erigirse como un estándar a la hora de estimar el OpVaR, debido a que se trata de una técnica estadística, proveniente del ámbito actuarial que tiene como objetivo la obtención de la función de distribución agregada de pérdidas operacionales.

Con lo que bajo este enfoque, las instituciones están en capacidad de estimar, para cada combinación línea de negocio y tipo de riesgo, la función de distribución de la severidad y de la frecuencia para el próximo año, utilizando sus datos internos, y computando la distribución de las pérdidas operacionales acumulada.

Para efectos prácticos, la distribución de pérdida agregada a partir de la cual inferir el OpVaR, se obtiene a través de la siguiente secuencia de pasos, que se ilustra a continuación:

Cuadro 11.

Distribución de Pérdidas Agregadas



Fuente: Maestria en Finanzas y Gestión de Riesgos

Elaborado: Autor

3.5 Planes de Contingencia y Continuidad

El enfoque de la contingencia, en teoría administrativa, destaca que no se alcanza la eficacia organizacional siguiendo un único y exclusivo modelo organizacional, con lo que se fundamenta en que no existe un modelo organizacional único y exclusivo para organizar. Existe dependencia del ambiente externo, la variación en el medio ambiente y la tecnología influyen en la variación de la estructura organizacional.

El enfoque de la contingencia requiere la identificación de las variables que producen mayor impacto en la organización, como el ambiente y la tecnología, para predecir las diferencias en la estructura y el funcionamiento de las organizaciones debidas a las diferencias en estas variables, las que pueden conducir a variaciones en la estructura organizacional.

3.5.1 Importancia del Plan de Contingencia

Dentro del funcionamiento de las instituciones no siempre ocurre el escenario deseado o más probable, debido a los diferentes eventos a los cuales toda actividad que se realiza se encuentra expuesta, es por eso que si ocurre algo inesperado y especialmente si sus consecuencias son negativas, es conveniente que se tenga preparado planes para poder reaccionar oportuna y convenientemente y de esta forma poder evitar que las acontecimientos conlleven a grandes pérdidas para la institución.

Un ñplan de contingenciaò es un plan, de grado variable de elaboración y detalle, que debe ser preparado para tener prevista la reacción en el caso de que ocurra un evento que pueda afectar a la continuidad del negocio.

Dado que los planes de contingencia requieren de un esfuerzo de preparación que amerita tiempo y recursos, es necesario que dentro de su preparación se tenga en cuenta los siguientes criterios:

- Probabilidad de ocurrencia de la contingencia;
- Impacto de la contingencia sobre la entidad;
- Necesidad de estar preparados ante la contingencia.

Si la contingencia es probable, se puede considerar que va a tener un impacto importante, razón por la cual es necesario que la institución esté preparada para enfrentarlo, de igual forma la decisión debe ser clara, esto implica que un plan de contingencia debe estar preparado con todos los detalles que sean necesarios para poderlos ejecutar de la forma más efectiva posible.

Un buen plan de continuidad debe contemplar diversos aspectos tales como procesos, servicios, infraestructura y personal, entre los más importantes, con lo que las diversas áreas de la entidad deben trabajar en conjunto para poder desarrollar de la manera más efectiva un correcto y eficiente plan.

3.5.2 Elaboración del Plan de Contingencia y Continuidad[17]

La continuidad del negocio y recuperación de desastres no significan lo mismo, pero la recuperación de pérdidas es parte de mantener la continuidad del negocio. En cada entidad los requerimientos son diferentes; sin embargo, existen lineamientos generales que pueden ayudar a cualquier entidad a diseñar un plan de contingencia y continuidad acorde a sus necesidades.

Las instituciones deben implementar planes de contingencia y de continuidad, a fin de garantizar su capacidad para operar en forma continua y minimizar las pérdidas en caso de una interrupción severa del negocio.

Para el efecto, deberán efectuar adecuados estudios de riesgos y balancear el costo de la implementación de un plan de continuidad con el riesgo de no tenerlo, esto dependerá de la criticidad de cada proceso de la entidad; para aquellos de muy alta criticidad se deberá implementar un plan de continuidad, para otros, bastará con un plan de contingencia.

Las instituciones financieras deberán establecer un proceso de administración de la continuidad de los negocios, que comprenda los siguientes aspectos claves:

1) Definición de una estrategia de continuidad de los negocios en línea con los objetivos institucionales.

[17] Codificación de Resoluciones de la Superintendencia de Bancos y Seguros y de la Junta Bancaria, Titulo VII De los Activos y de los límites de Crédito, Sección IV.

2) Identificación de los procesos críticos del negocio, aún en los provistos por terceros.

3) Identificación de los riesgos por fallas en la tecnología de información.

4) Análisis que identifique los principales escenarios de contingencia tomando en cuenta el impacto y la probabilidad de que sucedan.

5) Evaluación de los riesgos para determinar el impacto en términos de magnitud de daños, el período de recuperación y tiempos máximos de interrupción que puedan ocasionar los siniestros.

6) Elaboración del plan de continuidad del negocio para someterlo a la aprobación del directorio u organismo que haga sus veces.

7) Realización de pruebas periódicas del plan y los procesos implantados que permitan comprobar su aplicabilidad y realizar los ajustes necesarios.

8) Incorporación del proceso de administración del plan de continuidad del negocio al proceso de administración integral de riesgos.

Los planes de contingencia y de continuidad de los negocios deben comprender las previsiones para la reanudación y recuperación de las operaciones.

Los planes de contingencia y de continuidad deberán incluir, al menos, los siguientes puntos:

1) Las personas responsables de ejecutar cada actividad y la información (direcciones, teléfonos, correos electrónicos, entre otros) necesaria para contactarlos oportunamente.

2) Acciones a ejecutar antes, durante y una vez ocurrido el incidente que ponga en peligro la operatividad de la institución.

3) Acciones a realizar para trasladar las actividades de la institución a ubicaciones transitorias alternativas y para el restablecimiento de los negocios de manera urgente.

4) Cronograma y procedimientos de prueba y mantenimiento del plan.

5) Procedimientos de difusión, comunicación y concienciación del plan y su cumplimiento.

3.5.3 Responsabilidad Organizacional

Dentro de cada institución no existe ningún precedente de gestión de situaciones de contingencia; debido a que cada contingencia es única, sin embargo, por medio de la experiencia que tiene cada institución demuestra que las contingencias tienden a seguir ciertos modelos reconocibles y documentados, con lo que una buena gestión de una situación contingente depende mayormente del conocimiento que se ha ido adquiriendo con el pasar del tiempo y de las medidas que se han sabido adoptar para que sus tratamientos sean efectivos.

Si bien las instituciones han logrado correctas gestiones frente a eventos inesperados, la gestión de contingencia comparte muchas de las características de una buena gestión en general, debido a que existe un número de singularidades que la distinguen:

- El bienestar de la entidad está en juego.

- El tiempo de reacción es breve.

- Los factores de riesgo son altos y las consecuencias de los errores o los retrasos pueden ser desastrosos.

- Hay mucha incertidumbre.

- La inversión de una planificación de contingencia y en otras actividades preparatorias es fundamental.

- El personal y los gestores pueden estar sometidos a un grado de estrés.

- No existen respuestas correctas evidentes.

La gestión de contingencia dentro de las instituciones puede definirse como la organización de las capacidades y de los recursos para hacer frente a las amenazas que pueden tener las mismas, teniendo en cuenta que la capacidad se la puede entender como aptitud organizativa interna en la que se incluye la planificación, dotación de personal, estructura, sistemas, procedimientos, directrices, flujo de información, comunicación, toma de decisiones y apoyo administrativo.

De igual forma si el nivel de capacidad es bajo, lo más probable es que su acción de respuesta frente a las emergencias sea baja, incluso si se dispone de los recursos adecuados, así mismo una buena capacidad de respuesta puede mitigar la escasez de recursos, haciendo su utilización más eficaz.

La capacidad de acción es un aspecto de la gestión de contingencia a la que, a veces, no se da la importancia que se merece, debido a que se suele dar mayor prioridad a los recursos durante la fase de planificación y operativa por ser un elemento más tangible, pero, no se tiene en cuenta que la capacidad de acción es la que determina la calidad de la respuesta a la emergencia.

Una organización bien capacitada tiene más posibilidades de poner en marcha una gestión creíble y efectiva y de atraer los recursos necesarios, para poder tener una mejor respuesta frente a las amenazas a las que se encuentra expuesta la institución.

3.6 Caso FINCA S.A.: Gestión de Riesgo Operativo

3.6.1 Metodología Interna para la medición del Riesgo Operativo

Cumpliendo con lo establecido por la Superintendencia de Bancos y Seguros para la gestión de riesgos, FINCA S.A. cuenta con un sistema para identificar, evaluar, controlar, y monitorear los diferentes

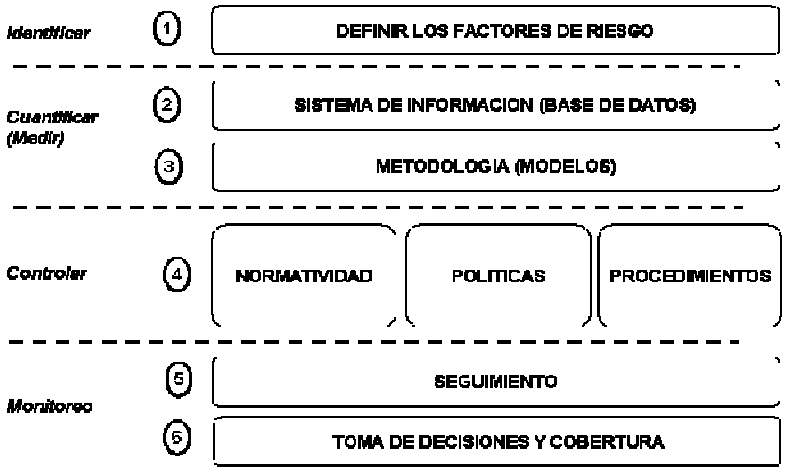
riesgos inherentes del negocio, a través de un conjunto de herramientas que permiten reducir las posibles pérdidas e incrementar la eficiencia de la institución.

El objetivo de diseñar e implementar un Sistema de Gestión Integral de Riesgo es buscar un costo de oportunidad que permita equilibrar la relación existente entre riesgo y rentabilidad, de manera que se puedan identificar los elementos que disminuyen el valor de la Organización, con el fin de colocar a la Gestión de Riesgos del negocio como una fuente de ventaja competitiva y generadora de valor.

Para poder medir las posibles pérdidas ocasionadas por los diferentes eventos a los que la institución se ve expuesta, se ve necesario desarrollar un sistema de administración de riesgos integrales la cual debe abarcar los principios de las mejores prácticas financieras tanto a nivel nacional como internacional.

Cuadro 12.

Procesos de Administración de Riesgo Operacional



Fuente: Curso de Normatividad de Gestión de Riesgos
Elaboración: Autor

Dentro de este sistema de gestión, la administración del Riesgo de Operacional, además de ser parte de la normativa de la Superintendencia de Bancos y Seguros, es un requerimiento importante y fundamental. Es por esto que se le ha dado el mismo trato que a los demás riesgos, estableciéndose las siguientes herramientas para la identificación de las posibles pérdidas operacionales, su medición y control, las cuales se detallan a continuación:

- Mapas de Riesgos

- Auto evaluación
- Modelos de Gastos
- Base de Datos

3.6.1.1 Mapas de Riesgos

Los mapas de riesgos son mecanismos de control que facilitan la identificación de áreas con debilidades, por medio de la categorización de los tipos de riesgo que afectan a los procesos, departamentos o unidades del negocio, de manera que puedan tomarse medidas donde sea necesario actuar en forma prioritaria.

El objetivo de los mapas de riesgos es el determinar las relaciones entre los procesos con sus respectivos eventos y de esta forma estar en la capacidad de cuantificar la severidad y frecuencia de los eventos de riesgos a lo largo de diferentes líneas de negocios o procesos sustantivos.

La clasificación de los riesgos se realiza por medio de una matriz en función del impacto del riesgo, es decir, de su importancia medida en términos monetarios y por la probabilidad de ocurrencia o frecuencia del mismo. Esta matriz es un elemento fundamental para la toma de decisiones, ya que implica todos los niveles y ayuda a generar procedimientos para la mitigación y monitoreo de los riesgos.

FINCA S.A. determinará los procesos sustantivos que se desarrollan par la consecución de los objetivos empresariales, se identificaran los eventos de riesgos a los que está expuesta tales procesos.

Los procesos y eventos de riesgo seleccionados se dividen en distintos niveles de apertura, con lo que se elaborará una matriz de datos que permitirá acumular datos periódicamente relacionados a la frecuencia y severidad de los diferentes eventos de riesgos.

La Matriz de Riesgos fue elaborada mediante técnicas de entrevistas con el personal clave de cada una de las áreas que forman parte de la Institución, para posteriormente agrupar los riesgos

percibidos, tabularlos y mostrarlos. La primera actividad que se llevó a cabo fue la elaboración del cuestionario, en el cual se incluyeron los siguientes temas:

Identificación: Entorno interno y externo, modelo de negocios, creación de valor, tiempo de servicio, calidad en el servicio, satisfacción del cliente, tipos de riesgos.

Determinación: Factores internos y externos que son causantes fundamentales de posibles riesgos.

Cálculo: Pérdidas, repercusiones sobre el capital, indicadores claves de desempeño y reputación, probabilidades de ocurrencia de futuros eventos de riesgo.

Para la calificación de cada uno de los riesgos presentados se deben considerar dos factores: magnitud del impacto y probabilidad de ocurrencia o frecuencia del evento de riesgo. Posteriormente, se debe obtener los promedios con la siguiente gradación y asignación de valores:

Cuadro 13.

Ponderaciones Matriz de Riesgos

Nivel	Rango	Descripción
4	Casi cierta	La expectativa de ocurrencia se da en todas las circunstancias
3	Muy probable	Probabilidad de ocurrencia en la mayoría de las circunstancias
2	Moderada	Puede ocurrir
1	Improbable	Podria ocurrir algunas veces

Nivel	Rango	Descripción
4	Catastrófico	Pérdidas financieras muy grandes que compromete la continuidad de las operaciones
3	Mayor	Pérdidas financieras mayor, que compromete algunas operaciones
2	Moderado	Pérdidas financieras altas
1	Menor	Pérdidas financieras minimas

Fuente: Finca S.A.
Elaboración: Autor

La fusión de estos dos factores da como resultado la siguiente ponderación:

Cuadro 14.

Factores Matriz de Riesgos

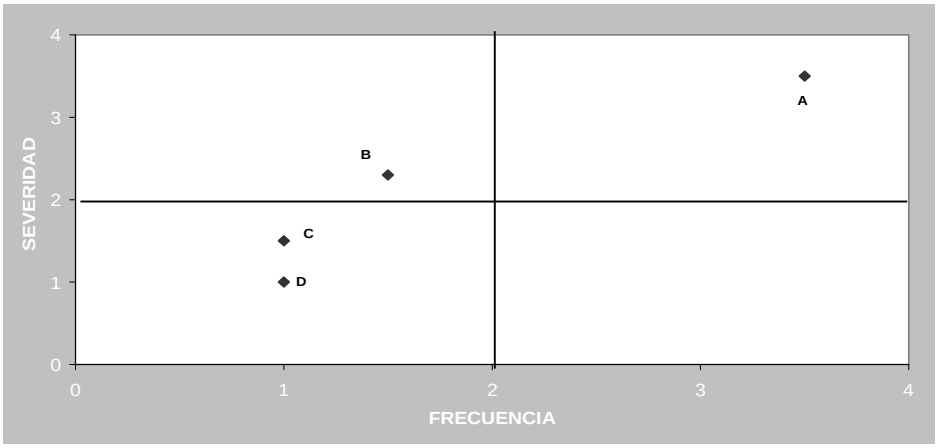
IMPACTO	PROBABILIDAD	PONDERACION	COLOR
Menor	Improbable	Bajo	Verde
Moderado	Improbable	Bajo	Verde
Mayor	Improbable	Bajo	Verde
Catastrófico	Improbable	Moderado	Amarillo
Menor	Muy probable	Bajo	Verde
Moderado	Muy probable	Bajo	Verde
Mayor	Muy probable	Moderado	Amarillo
Catastrófico	Muy probable	Alto	Anaranjado
Menor	Moderada	Bajo	Verde
Moderado	Moderada	Moderado	Amarillo
Mayor	Moderada	Alto	Anaranjado
Catastrófico	Moderada	Alto	Anaranjado
Menor	Casi Certeza	Moderado	Amarillo
Moderado	Casi Certeza	Alto	Anaranjado
Mayor	Casi Certeza	Alto	Anaranjado
Catastrófico	Casi Certeza	Extremo	Rojo

Fuente: Finca S.A.
Elaboración: Autor

La Matriz de Riesgos resultante resume la cultura sobre la administración de riesgos de la Institución y la prioridad e importancia que se otorga a cada uno de ellos. Con el propósito de contribuir a la cultura organizacional, la matriz fue distribuida dentro de la Institución y ha servido como elemento de capacitación en el proceso de administración integral de riesgos.

Cuadro 15.

MATRIZ DE RIESGOS



Fuente: Finca S.A.
Elaboración: Autor

3.6.1.1 Flujos de Procesos

Una vez elaborada la matriz en la cual se identifican los riesgos existentes en la Institución, el paso siguiente es verificar que cada una de las actividades y funciones que realiza el personal sea documentada en procesos, subprocesos, controles, políticas, etc.

Toda organización tiene procesos18, sin embargo, muchos de ellos han sido tradicionalmente fragmentados, no medidos e incluso ignorados o invisibles. Orientarse y desarrollar las actividades en torno a procesos hace que el trabajo sea proyectado y replicable.

Por lo general, los procesos son bastante complejos y pueden abarcar demasiadas actividades dentro de uno solo, lo que complicaría su entendimiento y por tanto, su ejecución. Para simplificarlos, estos deben ser agrupados o divididos en macroprocesos, procesos y subprocesos.

Es así que los macroprocesos son todos aquellos con los cuales debe operar el negocio, al más alto nivel de generalización, es decir con el menor nivel de detalle. Los procesos son la descomposición de los macroprocesos en el siguiente nivel de detalle y los subprocesos una división adicional de estos últimos.

Con la finalidad de mantener un trabajo efectivo, FINCA S.A. elaboró un inventario de procesos, en el cual, cada área de la Institución establece los procesos con los que cuenta, los clasifica de acuerdo al grupo que pertenecen y especifica el objetivo del proceso, la persona encargada de ejecutarlo, la persona encargada de supervisarlo, el tiempo estimado, los insumos utilizados, el producto entregado, etc.

Para lograr este objetivo, se deberá contar con una persona en cada una de las áreas, que será la encargada de revisar periódicamente la actualización, creación o eliminación de procesos, de acuerdo a lo que se lleva día a día.

Con todo lo mencionado anteriormente FINCA S.A. ha adoptado la agrupación de Procesos Sustantivos Genéricos, en la cual estructura para el NIVEL 1 de macroprocesos de la siguiente forma19:

---

[18] Un proceso es un grupo de actividades, tareas o incluso procedimientos de menor nivel relacionadas de manera lógica entre sí y en evolución continua, que en conjunto, crean valor para el cliente.

[19] Sociedad Financiera FINCA S.A.

MACROPROCESO: Proceso estratégico global, con objetivos propios y específicos que da contexto a procesos menores. A los efectos de la medición de riesgo operacional la institución identificará tres macroprocesos:

Front Office.- Siendo el conjunto de actividades para establecer relaciones de la institución con contrapartes externas con la finalidad de iniciar la generación de negocios.

Middle Office.- Es el conjunto de actividades en donde se genera la toma de decisiones, generación de políticas, su ejecución y control de las mismas, generalmente por parte de la dirección y alta gerencia con el objetivo de hacer que los negocios lleguen a buen fin.

Back Office.- Está determinado como el conjunto de actividades de orden operativo que tienen por objeto la documentación, registro, contabilidad, entrega, control de ejecución del desarrollo de los negocios de la institución y otras actividades auxiliares administrativas, además el área de sistemas.

La institución adoptará en un NIVEL 2 la agrupación de los Procesos dentro de cada macroproceso.

De la misma forma dentro de cada proceso en un NIVEL 3 se distinguen Subprocesos, los cuales están definidos como el conjunto de actividades dentro de un proceso específico. (ANEXO 8)

3.6.1.2 Auto evaluación[20]

La auto-evaluación es un proceso por el cual las unidades de negocio, de forma subjetiva, identifican los riesgos inherentes a sus actividades, evalúan el nivel de control existente internamente y determinan los puntos que pueden ser mejorados.

Por medio de una auto evaluación se desagrega la información de elementos básicos para su respectivo seguimiento, por lo general están conformados a través de un listado de puntos en cuestión y son completados internamente en cada organización por funcionarios responsables.

[20] IBID

El objetivo que tiene una auto evaluación es el de medir el ambiente de control de áreas o funciones expuestas al riesgo operacional mediante la determinación de porcentajes o puntajes de cumplimiento de estándares, lo que permite evaluar el desempeño de una organización ante su exposición a riesgos de operación.

Las respuestas de la auto evaluación está valorada según ponderaciones de la intensidad o peso del respectivo ítem en el control del ambiente de riesgos. Los cuestionarios de auto evaluación son respondidos periódicamente de manera trimestral por funcionarios de áreas específicas.

3.6.1.3 Modelo de Gastos

El objetivo de este modelo es el de medir el riesgo de pérdidas por exposición al riesgo operacional mediante la determinación de la evolución de los gastos operacionales. Con este modelo se asume que las fluctuaciones del valor de dichos gastos dentro de la institución es causada por fraudes, negligencia de recursos humanos, errores en procesos, caída de sistemas informáticos, reclamos judiciales, o daño a activos físicos u otros eventos externos producidos, todos estos factores típicos relativos a la exposición de riesgo operacional.

La finalidad específica de la utilización de este modelo es el de generar un resultado único que cuantifique de una forma objetiva y de rápido proceso la exposición global de una institución con respecto al riesgo operacional.

3.6.1.4 Base de Datos

Como parte de la Administración Integral de Riesgo, se ha establecido el diseño de una base de datos que permita registrar la información relacionada con los eventos de riesgo que se presenten en la Institución, a partir de la cual se desarrollarán modelos para medir, controlar y mitigar los riesgos operativos a los que está expuesta la misma, la cual servirá también, para determinar el requerimiento de capital para cubrir este tipo de riesgos.

FINCA S.A. cuenta con un modelo AMA, el cual servirá para la identificación, medición, control y monitoreo del Riesgo Operacional, siendo este un sistema para el registro, consulta, actualización y

reporte de los distintos eventos de riesgos presentados dentro de la Institución a lo largo del tiempo, así mismo aportará al fortalecimiento de la estructura de control, riesgo y medidas preventivas en las operaciones del negocio.

A cada evento de riesgo se les asignará un factor, tal como se sugiere en el acuerdo de Basilea II y en la normativa planteada por la Superintendencia de Bancos y Seguros. El diseño de las bases antes detalladas debe considerar la flexibilidad de registrar nuevos campos que se podría requerir por futuras necesidades.

Para poder proceder con la recolección de la información, se ha llevado a cabo la elaboración de un documento en el cual se registrará la ocurrencia de todos los eventos de riesgo, siendo este la primera línea de captura de datos. Los diferentes sucesos asociados a eventos de riesgo operacional que suceden en determinada oficina, departamento o sección de la institución serán registrados en dicho documento. (ANEXO 9)

Con la finalidad de estandarizar el contenido de los campos y facilitar la consolidación de la información para la presentación de ésta a través de reportes, es necesario definir las tablas que contengan los códigos de las alternativas de repuesta entre los cuales el usuario debe seleccionar la que necesite.

Las tablas deben tener las siguientes características:

Tipo de evento de riesgo: se registrará la categorización de los eventos de Riesgo Operacional que contendrá el código como un campo numérico de dos posiciones y la descripción escrita como un campo alfanumérico.

Cuadro 16.

Tipos de Eventos de Riesgo Operacional

Categorias	Descripción
01	RRHH
02	PROCESOS
03	FRAUDE INTERNO
04	FRAUDE EXTERNO
05	RECLAMOS LABORALES
06	DAÑOS ACTIVOS FIJOS
07	FALLAS INFORMATICAS

Fuente: Finca S.A.
Elaboración: Autor

Actividades de Riesgo Operacional: se registrará los eventos posibles que se pueden presentar y que tienen relación con los tipos de evento de riesgo operacional.

Cuadro 17. **Actividades de Riesgo Operacional**

Codigo Act. Riesgo	Descripción
01	Ingreso de información errónea del cliente
02	Retraso en entrega de documentación
03	Entrega incompleta de documentación
04	Inadecuada planificación
05	Manipulación de identidad
06	Manipulación de documentos
07	Faltas de control en el sistema
08	Pérdidas, errores, o problemas con base de datos

Fuente: Finca S.A.
Elaboración: Autor

Otras tablas codificadas: Se requiere disponer de tablas con códigos y descripciones para las diferentes áreas de la Institución, Cargos de funcionarios de la organización, etc.

La base de datos que se elabore para alimentar el programa, se convertirá en el insumo para que, a través del mismo, se puedan establecer medidas preventivas y correctivas tendientes a mitigar los riesgos y cuantificar el requerimiento de capital de la Organización por Riesgo Operacional.

3.6.2 Transferencia y Mitigación del Riesgo[21]

Después de identificar cada uno de los diferentes riesgos es de suma importancia si se tiene un mitigante que cubra una posible ocurrencia o pérdida, los cuales en la mayoría de los casos pueden ser mitigados por medio de seguros contra eventos puntuales.

Dependiendo del caso se debe analizar debidamente y definir el mitigante que FINCA S.A. puede tener o aplicar frente a los eventos de pérdida que se pueden presentar.

[21] Sociedad Financiera FINCA S.A.

Dentro de estos mitigantes FINCA S.A. a podido determinar los siguientes:

Planes de contingencia

Planes de continuidad del negocio

Back up de información

Correcto entrenamiento al personal

Transferencia de riesgo

Políticas establecidas y difundidas al personal

En el caso de los eventos puntuales que pueden ser mitigados por medio de los seguros, hay que tener en cuenta que algunas empresas aseguradoras que operan en mercados internacionales están estructurando pólizas para cubrir eventos tales como pérdidas por ñbaja frecuencia / alta intensidadò como en el caso de errores y omisiones, pérdidas físicas de valores y fraude.

La mitigación de los riesgos, que son derivados de transferencias de los mismos a terceros, debe ser reflejada en el cargo de capital de cobertura; en consecuencia la institución debe restar el monto de la intensidad de pérdida en cada uno de los eventos, y los resarcimientos generados por la transferencia de riesgos a terceros.

CAPITULO IV

RESULTADOS, CONCLUSIONES Y RECOMENDACIONES

4.1 Resultados

Una vez que se ha realizado la investigación de cómo va el proceso de gestión de riesgo operativo dentro de FINCA S.A., se ha podido llegar a los siguientes resultados, los cuales responden a las dos primeras preguntas planteadas, las cuales no requieren de hipótesis y a la hipótesis de la tercera pregunta.

Pregunta 1.

Las actividades que pueden generar pérdidas a la institución y que se encuentran inmersos en los diferentes procesos, son los relacionados a todo tipo de fraudes, sean estos internos como externos; prácticas relacionadas con clientes y proveedores, daños a los activos físicos, problemas con lo relacionado a tecnología de información, fallas en ejecución de procesos y fallas en lo relacionado en prácticas del recurso humano de la institución.

Se puede determinar que uno de los mayores problemas que se presentan está en la parte de recursos humanos, ya que en las actividades que se realizan diariamente se corre un mayor riesgo al ser estas elaboradas de manera manual, ya que no se tiene una mayor atención a los procedimientos, de igual forma al ser actividades que se realizan constantemente se transforman en actividades mecánicas, con lo

que se pierde el control en la elaboración de las mismas, debido a que se las hacen sin tener mayores precauciones.

En virtud de lo antes mencionado y mediante el levantamiento de la información proveniente de diversas áreas, se puede determinar cuales son las actividades que generan pérdidas dentro de la institución, las cuales se detallan en el Anexo 10.

Pregunta 2.

Como se mencionó anteriormente en la respuesta a la pregunta uno, existen varias actividades que son generadoras de perdidas operacionales, así podemos destacar entre las mas importantes y que tienen un mayor impacto las relacionadas al recurso humano y los procesos.

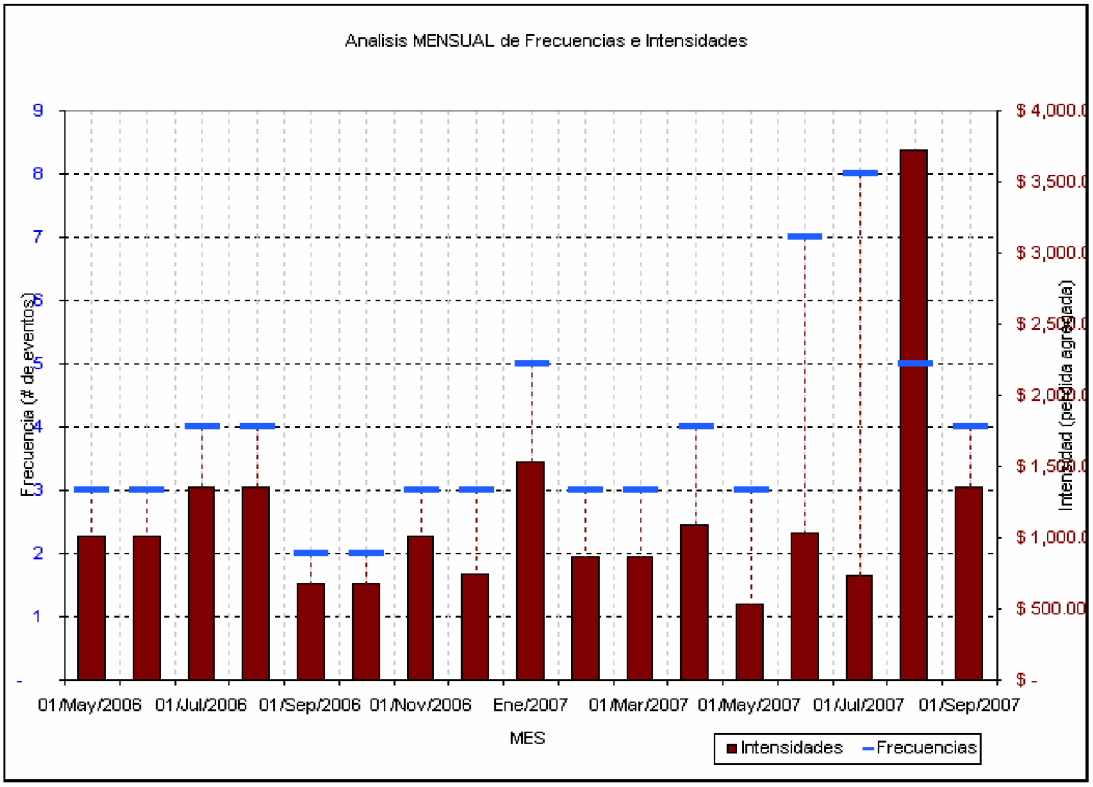
Dentro de la normatividad presentada por la Superintendencia de Bancos y Seguros no se ha determinado las metodologías de medición de pérdidas, actualmente se encuentra en el nivel de levantamiento de información relacionada a los macro procesos, procesos, subprocesos, actividades críticas, para que una vez levantada la información se elabore la base de datos pertinente para que partiendo de esto se pueda proceder a la medición de las pérdidas operacionales.

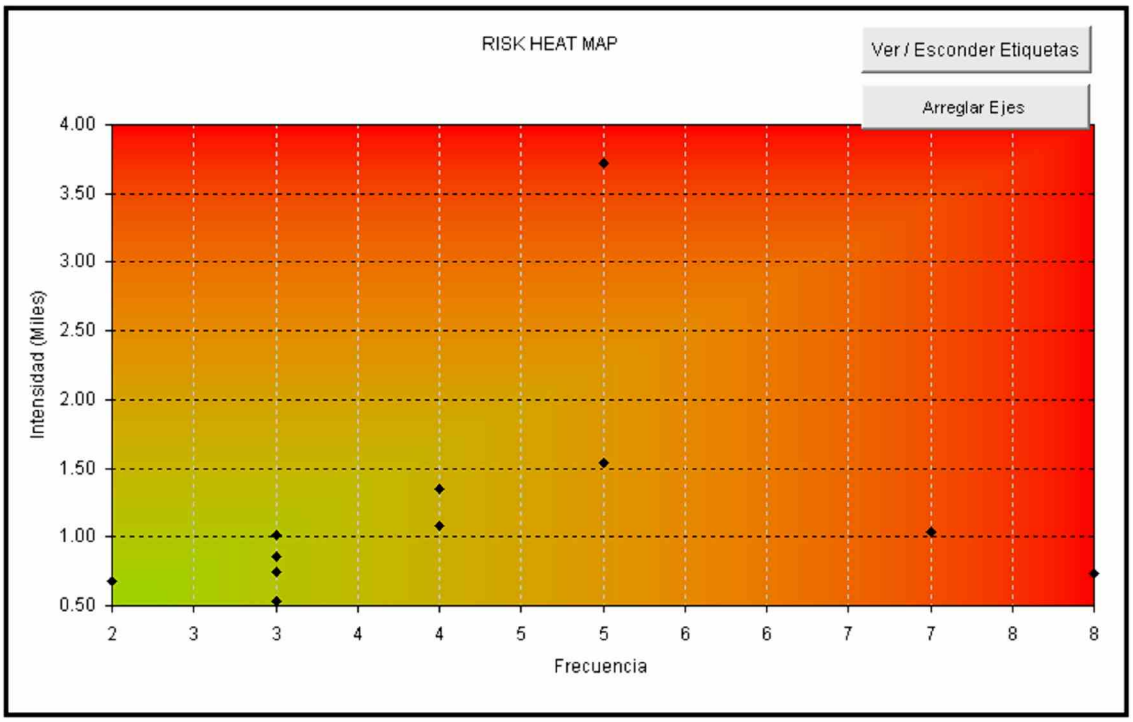
Con la aplicación adecuada de una metodología para la gestión de riesgos, se permite establecer con claridad la línea de negocio y partiendo de esta la determinación de los macro procesos, procesos y subprocesos, para finalizar con las actividades críticas generadoras de pérdidas, con lo que se podría armar una base de datos que puede facilitar la identificación posterior de las actividades generadoras de pérdidas.

Una vez establecidas las actividades y armada una base de datos, con información histórica, se procede a revisar los impactos y frecuencias de cada uno de estos para determinar el impacto que tendrían dentro de la institución, para posteriormente proceder a la implementación de un modelo para el cálculo del requerimiento de capital necesario para cubrir las pérdidas esperadas.

Teniendo establecidas las actividades y armada la base de datos de las actividades generadoras de pérdidas, se ha podido determinar cuales son las actividades generadoras de pérdidas que tienen mayor relevancia tomando en cuenta su frecuencia y el impacto que estas tienen dentro de la institución, las mismas que se pueden ver detalladas a continuación:

ACTIVIDADES CRITICAS	Frecuencia	Pérdida USD
Migración de SIEM a COBIS	1	67.44
Entrega erronea de información a los clientes	3	552.00
Entrega a destiempo de documentacion	1	3.95
Socios fugados	2	743.05
Ingreso de información errónea de la operación	3	296.00
Errores en contabilizaciones	1	6.81
Entrega a destiempo de valores y error en valores a declarar	1	237.75
Pago de cheques	5	40.57
Devolución de cheques a destiempo por no tener en cuenta el proceso	3	33.55
Omisión de información en contratos	1	2,629.98
Negligencia	44	14,900.45
Errores en pagos a terceros	1	70.81
Total	**66**	**19,582.36**





Pregunta 3.

Para poder obtener una respuesta clara a la tercera pregunta se ha formulado una hipótesis, la cual durante el desarrollo de la investigación se he podido comprobar de manera adecuada.

Previa la determinación de la pérdida de los eventos de riesgo y su requerimiento de capital es necesaria la implementación de una metodología para la gestión de riesgo operativo, es decir la aplicación correcta y adecuada de la norma que presenta la Superintendencia de Bancos al igual que las recomendaciones de Basilea.

Por medio de la implementación de una metodología para la gestión de riesgo operativo si se puede determinar las pérdidas a las que se encontraría inmersa la institución, debido a que por medio de esta se puede realizar un correcto control de cada uno de los factores de riesgo.

El Comité de Basilea propone tres enfoques para calcular los requerimientos de capital por riesgo operacional que, ordenados de menor a mayor grado de sofisticación y sensibilidad al riesgo son:

- Método del Indicador Básico
- Método Estándar
- Metodologías de Medición Avanzada

Además de seguir las recomendaciones del Comité de Basilea, la institución previa la utilización del Método Estándar o las metodologías AMA tendrán que cumplir una serie requisitos mínimos en la gestión y control de este riesgo.

Una de los requisitos que se necesita previa la utilización de cualquiera de las metodologías presentadas es que la institución debe definir con claridad la línea de negocio en el cual se encuentra, de acuerdo a cada una de las definiciones que presenta Basilea, debido a que si se utiliza el Método Estándar hay que tener en consideración el factor beta que se utiliza dependiendo de la línea de negocio en el que se encuentra inmersa la institución.

De acuerdo a lo antes mencionado y con la información recopilada de las diferentes actividades generadoras de pérdidas se puede realizar el cálculo del requerimiento de capital que la Institución necesitaría para poder cubrir con las pérdidas operativas.

El modelo a tomar podría ser el básico o a su vez el estándar, debido a que FINCA S.A. solo cuenta con una línea de negocio, aunque hay que considerar que los factores α y β respectivamente difiere entre sí, con lo que el requerimiento de capital va a variar de un método a otro, como se puede ver a continuación:

CUANTIFICACIÓN CON METODO DEL INDICADOR BÁSICO (BIA)

α= 15%

AÑO	INGRESOS BRUTOS	n	INGRESOS BRUTOS >0
1	590,486.46	1	590,486.46
2	1,634,219.00	1	1,634,219.00
3	1,678,977.03	1	1,678,977.03
Total:	**3,903,682.49**	**3**	**3,903,682.49**
	REQUERIMIENTO DE CAPITAL		**195,184.12**

El requerimiento de capital se determina como un porcentaje del promedio de sus "ingresos brutos" anuales positivos.
Se excluyen los datos de cualquier año en el que se presenten ingresos brutos negativos o cero.

CUANTIFICACIÓN CON METODO ESTÁNDAR (SA)

INGRESOS BRUTOS POR LINEA DE NEGOCIO									
Linea Negocio	1	2	3	4	5	6	7	8	Total
AÑO	Finanzas corporativas	Negociación y ventas	Banca minorista	Banca comercial	Pago y liquidación	Servicios de agencia	Administración de activos	Intermediación minorista	Ingreso bruto anual
1			590,486.46						590,487.46
2			1,634,219.00						1,634,221.00
3			1,678,977.03						1,678,980.03
BETAS	β 1	β 2	β 3	β 4	β 5	β 6	β 7	β 8	Total
	18%	18%	12%	15%	18%	15%	12%	12%	
1			70,858.38						70,858.38
2			196,106.28						196,106.28
3			201,477.24						201,477.24
								REQUERIMIENTO DE CAPITAL	156,147.30

Las actividades de la Institución se clasifican en las ocho líneas de negocio definidas.
ÂEl requerimiento de capital se determina para cada línea de negocio:
ï El requerimiento es un porcentaje fijo del promedio de sus ñingresos brutosòanuales positivos.
ï Consideración de Ingreso Bruto por línea de negocio para no netear entre áreas con diferentes cargos por riesgo.

4.2 Conclusiones

La implantación del Riesgo Operativo dentro de FINCA S.A., permite la creación de una cultura de riesgos dentro de la institución, favoreciendo que se cumpla con los procesos, normas y políticas internas.

Por medio de una cultura de riesgos es posible concienciar a las personas de las medidas y actitudes que deben mostrar frente a sus responsabilidades, ya que esto trae consigo beneficios para la institución, con lo que se podrá dar un mejor cumplimiento y mejor funcionamiento de las políticas y los procesos para un correcto funcionamiento del negocio.

Por medio de una metodología adecuada dentro de la institución se podrá determinar con mayor claridad cuales son los eventos de riesgo a los que se encuentra expuesta, y frente a esto poder contar con la técnica apropiada para realizar el control, bases de datos lo suficientemente elaboradas, modelos de cálculo de pérdidas y requerimientos de capital para cubrir cualquier eventualidad que se presente, al igual que los respectivos planes de contingencia y continuidad del negocio frente a los eventos generadores de riesgo.

Dentro de las tres metodologías de cálculo de requerimiento de capital se puede señalar que las dos primeras (Básico y el Estándar) son diseñadas con un enfoque general para las instituciones ya que se

basa primordialmente en un factor beta el cual es determinado por la línea de negocio en la que se encuentra la institución, con lo que no se puede dar una estimación mas o menos exacta del requerimiento que se necesite frente a posibles eventos de pérdidas, de igual forma dichos porcentajes presentados por el Comité de Basilea no reflejan la realidad nacional en la que se encuentra el sistema financiero, ya que estos valores son en base a la experiencia y la información de los grande bancos del exterior.

Con respecto al método avanzado, podría ser el que mejor se ajuste a las necesidades de la institución debido a que este se basa en datos internos y externos, los mismos que de acuerdo a la normatividad vigente de la Superintendencia de Bancos, debe ser información histórica de aproximadamente tres años, lo que es necesario para poder realizar estimaciones estadísticas. Así mismo hay que tener en cuenta que FINCA S.A. tiene un período de aproximadamente dos años como institución financiera, lo que dificulta tener una base da datos de acuerdo a los requerimientos estipulados por el ente de control.

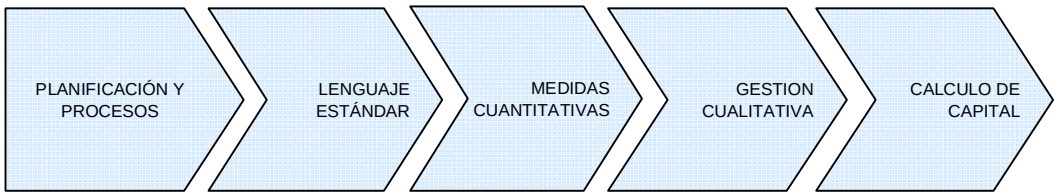
Una vez implementada la cultura de riesgo operacional dentro de la institución, se podrá estimar las pérdidas máximas que esta tiene en función de la información histórica y con esto se estará en la capacidad de estimar las posibles pérdidas futuras que puede tener y así establecer los parámetros necesarios para determinar cual es el requerimiento de capital necesario para poder cubrir dichas pérdidas.

Si bien FINCA S.A. es una financiera que tiene poco tiempo en el mercado se ha podido ver que en el tema de riesgo operacional se encuentra adelantando en algunos puntos primordiales dentro de lo que es la gestión de riesgos, es así que ya se cuenta con una base de datos histórica de casi dos años de los eventos que han sucedido en ese período, de acuerdo a cada uno de los distintos subprocesos, con lo que se estaría en la capacidad de empezar a armar la matriz de riesgos, para poder ver el impacto que estos eventos pueden tener de acuerdo a su frecuencia e impacto y de que medidas se deberían adoptar para su mitigación y control.

4.3 Recomendaciones

Para iniciar un adecuado manejo de riesgo operacional, se pueden considerar los siguientes pasos:

Cuadro 18.



Fuente: Seminario de Riesgo Operativo – Junio 2007
Elaboración: Autor

El primer paso para una correcta gestión de riesgos operativos es la de planificación y procesos, en el cual debe constar la planificación estratégica de la institución, por medio de la cual se establecerán la misión y visión de la institución, los contextos internos y externos que influyen en el accionar de las actividades, los objetivos estratégicos y el mapa estratégico. Igualmente dentro de este paso se debe tener el levantamiento de los diferentes procesos de la entidad, para de esta forma poder determinar los eventos de riesgo a los que se puede ver envuelta la institución, los manuales internos que facilitan al funcionamiento de las actividades y la estructura organizacional, para poder tener clara cual es su distribución departamental.

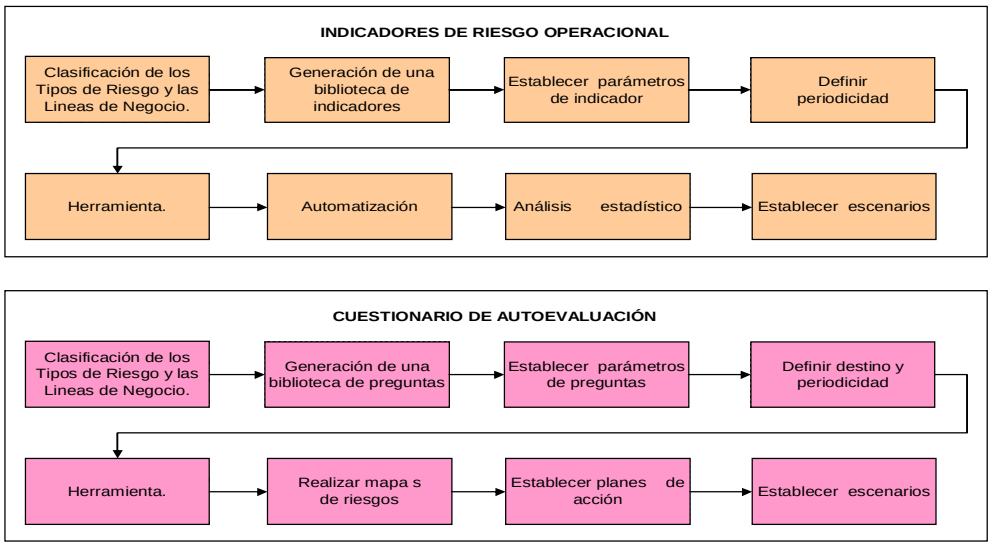
Con respecto al segundo paso, se debe identificar los diferentes tipos de riesgo a los que FINCA S.A. se encuentra expuesta, como fraude interno; fraude externo; relaciones laborales y seguridad en el puesto de trabajo; clientes, productos y prácticas empresariales; daño a los activos físicos; interrupción del negocio y fallas en los sistemas y deficiencias en la ejecución, la entrega y el proceso. De igual forma se debe asignar la línea de negocio en la cual se encuentra la institución, las líneas de negocio han sido clasificadas por el Comité de Basilea en un total de ocho, de las cuales dependiendo de las actividades que realice la institución podrá tener mas de una de las líneas dentro del negocio.

En el tercer paso es la identificación de los eventos internos y externos, los cuales son identificados por cada línea de negocio, por medio de auto-evaluaciones, mapas de riesgos, indicadores, tablas de control (scorecards), base de datos, entre otros.

Dentro del cuarto paso está la gestión cualitativa, en la cual se desarrollan los indicadores, y las auto-evaluaciones, para posteriormente proceder con la mitigación. Dentro de lo que se refiere a la gestión cualitativa del riesgo operacional, se establecen las alertas de acuerdo a los eventos de riesgo que se presenten, los distintos escenarios para el cálculo de capital, y por último un análisis de correlación entre pérdidas y niveles de riesgo de los indicadores.

Con respecto al desarrollo de los indicadores y las auto-evaluaciones se recomiendan las siguientes metodologías:

Cuadro 19.

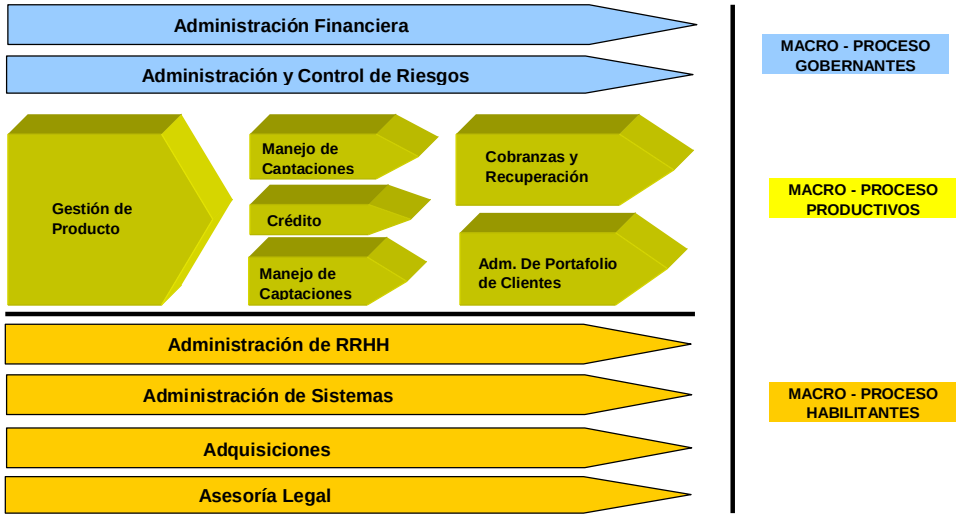


Fuente / Elaboración: Autor

Y por último el quinto paso es el correspondiente al cálculo de capital, en el cual se encuentran inmersos las diversas metodologías y escenarios para poder estimar que requerimientos son los necesarios para cubrir las pérdidas y las posibles pérdidas generadas por los diversos eventos de riesgo operacional.

Frente a los pasos recomendados para la gestión de riesgo operacional, se recomendaría que la agrupación de los procesos se realice conforme su característica, es decir en procesos gobernantes, productivos y habilitantes, como se indica a continuación:

Cuadro 20.



Fuente / Elaboración: Autor

Por medio de esta clasificación permitirá tener un mayor enfoque de los diversos procesos y subprocesos para poder identificar las actividades críticas, debido a que es indispensable para la continuidad del negocio y las operaciones de la institución, debido que la falta de identificación o aplicación deficiente puede generar un impacto negativo.

De acuerdo al paso uno es indispensable de igual forma la elaboración de planes de acción de cada proceso en el cual se indiquen los objetivos que se pretenden alcanzar, conjuntamente con las acciones a ejecutarse, fechas de finalización y los responsables de su ejecución, adicionalmente la elaboración de códigos de ética y conducta, fortalecimiento de una cultura de control interno y planes de contingencia y continuidad del negocio.

Los planes de continuidad y contingencia del negocio deberá estar compuesto por:

> Plan de continuidad: Es aquel que asegura la continuidad del negocio, la satisfacción del cliente y la productividad a pesar de eventos inesperados. Se ejecuta permanentemente como parte de la administración de riesgos tanto en la información como en la operación.

Plan de contingencia: Es el conjunto de procedimientos alternativos a las operatividad normal de la entidad cuya finalidad es la de permitir su funcionamiento, buscando minimizar el impacto financiero.

Plan de reanudación: Especifica los procesos y recursos para mantener la continuidad de las operaciones en la misma ubicación del problema.

Plan de recuperación: Especifica los procesos y recursos para recuperar las funciones del negocio en una ubicación alterna dentro o fuera de la institución.

La administración del riesgo operativo es un proceso continuo, para el cual se debe conformar bases de datos centralizadas, suficientes y de calidad para estimar las pérdidas esperadas e inesperadas atribuibles a cada tipo de riesgo, de igual forma se debe contar con sistemas de control interno adecuado, formalmente establecido y valido periódicamente.

ANEXO 1

CODIFICACION DE RESOLUCIONES DE LA SUPERINTENDENCIA DE BANCOS Y SEGUROS Y DE LA JUNTA BANCARIA

TITULO VII.-DE LOS ACTIVOS Y DE LOS LIMITES DE CREDITO

SUBTITULO VI.-DE LA GESTION Y ADMINISTRACION DE RIESGOS

(sustituido con resolución No JB-2003-601 de 9 de diciembre del 2003)

CAPITULO III.- DE LA ADMINISTRACION DEL RIESGO DE MERCADO

(incluido resolución No JB-2002-429 de 22 de enero del 2002, reenumerado con resolución No JB-2003-601 de 9 de diciembre del 2003 y reformado con resolución No JB-2003-615 de 23 de diciembre del 2003)

SECCIÓN II.- RESPONSABILIDADES DE LA ADMINISTRACION

ARTICULO 1.- Para el cumplimiento cabal de la responsabilidad de administrar sus riesgos, las instituciones del sistema financiero deben contar con procesos formales de administración integral de riesgos que permitan identificar, medir, controlar / mitigar y monitorear las exposiciones de riesgo que están asumiendo.

Cada institución del sistema financiero tiene su propio perfil de riesgo, según sus actividades y circunstancias específicas; por tanto, al no existir un esquema único de administración integral de riesgos, cada entidad desarrollará el suyo propio. (sustituido con resolución No JB-2003-615 de 23 de diciembre del 2003)

ARTICULO 2.- El Directorio o el organismo que haga sus veces deberá, en ejercicio de lo previsto en la letra a) del artículo 30 de la Ley General de Instituciones del Sistema Financiero, cuando menos, cumplir con lo siguiente:

2.1 Aprobar las políticas, estrategias y procedimientos, que permitan un adecuado manejo de los riesgos de mercado, las mismas que deberán ser actualizadas permanentemente de acuerdo a las situaciones que se prevea pueden presentarse. Estas políticas, estrategias y procedimientos deberán ser compatibles con el volumen y complejidad de las operaciones que realiza la institución controlada, y contener al menos lo siguiente:

2.1.1. La composición de los activos, pasivos y contingentes; el nivel de sensibilidad de éstos respecto de las variaciones de mercado y de las tasas de interés por tipo de instrumento y plazo; y, el grado de confianza con relación al nivel de liquidez y solvencia de los mecanismos e instrumentos que utilice para administrar la cobertura de las posiciones;

2.1.2. Las medidas para que la administración de la institución controlada pueda efectivamente identificar, hacer el seguimiento y controlar los riesgos de mercado que asume;

2.1.3. Las pautas de las estrategias de cobertura; y,

2.1.4. Las opciones que puede tener la institución controlada para solucionar los problemas que se presenten en el corto, mediano y largo plazos.

2.2 Informarse periódicamente y al menos mensualmente, acerca de la implementación y el cumplimiento de las políticas, estrategias y procedimientos por ellos aprobadas;

2.3 Establecer las acciones correctivas en caso de que las políticas, estrategias y procedimientos no se cumplan o se cumplan parcialmente, o incorrectamente;

2.4 Informarse regularmente y al menos quincenalmente, sobre la evolución de los riesgos de mercado, así como sobre los cambios sustanciales de tal situación y de su evolución en el tiempo;

2.5 Establecer límites generales prudenciales para la administración de los riesgos de mercado, compatibles con las actividades, estrategias y objetivos de la institución controlada, que permitan una adecuada reacción frente a situaciones adversas;

2.6 Determinar las clases de operaciones de derivados que la institución controlada puede realizar y los límites, procedimientos y controles a seguir respecto de ellas; y,

2.7 Las demás señaladas en el artículo 1, de la sección III "Responsabilidad en la administración de riesgos", del capítulo I "De la gestión y administración de riesgos"; del subtítulo VI "De la gestión y administración de riesgos", del título VII "De los activos y de los límites de crédito" de esta Codificación. (sustituido con resolución No JB-2003-615 de 23 de diciembre del 2003)

Las decisiones del directorio o del organismo que haga sus veces, sobre las disposiciones de este artículo, deben constar en actas.

ARTICULO 3.- El comité de administración integral de riesgos, además de las funciones señaladas en el artículo 3, de la sección III "Responsabilidad en la administración de riesgos", del capítulo I "De la gestión y administración de riesgos"; del subtítulo VI "De la gestión y administración de riesgos", del título VII "De los activos y de los límites de crédito" de esta Codificación, respecto de los riesgos de mercado, tendrá las siguientes funciones: (sustituido con resolución No JB-2003-615 de 23 de diciembre del 2003)

3.1 Elaborar y proponer al directorio u organismo que haga sus veces la expedición de los manuales de funciones y procedimientos para la administración de los riesgos de mercado;

3.2 Establecer los sistemas de información gerencial y la metodología de medición de los riesgos de mercado, si es que la Superintendencia de Bancos y Seguros no fija una metodología obligatoria;

3.3 Establecer los límites específicos internos apropiados por exposición a los riesgos de mercado y, en toda clase de inversiones financieras, incluyendo aquellas en instrumentos financieros derivados. Dichos límites se establecerán por tipo de instrumento financiero y por tipo de riesgos de mercado;

3.4 Medir, evaluar y efectuar un seguimiento continuo, sistemático y oportuno de los riesgos de mercado para lo cual también establecerá sistemas de alerta temprana en los que sean consideradas las variables relevantes que afecten los riesgos asumidos en el portafolio ante cambios en el mercado;

3.5 Implementar programas de difusión, capacitación y evaluación continua sobre el cumplimiento de las políticas, estrategias y procedimientos que permitan un adecuado manejo de los riesgos de mercado, a los cuales deberá tener acceso todo el personal involucrado;

3.6 Establecer e implementar planes de contingencia frente a los riesgos de mercado que consideren distintos escenarios y evaluar su efectividad y rapidez de respuesta;

3.7 Informar oportunamente al directorio u organismo que haga sus veces respecto de la efectividad, aplicabilidad, conocimiento por parte del personal y funcionarios, su cumplimiento y cualquier otro aspecto relacionado a las políticas, estrategias y procedimientos fijadas por tal órgano;

3.8 Recomendar al directorio u organismo que haga sus veces la elaboración, promulgación, reforma o eliminación de políticas, estrategias y procedimientos

relacionadas con los riesgos de mercado;

3.9 Identificar, medir y controlar los riesgos de mercado, y en especial el riesgo de tasa de interés, por la introducción de nuevos productos y operaciones; los que deberán realizarse de acuerdo a las políticas y procedimientos establecidos para tal fin; (numeral renumerado con resolución No JB-2003-615 de 23 de diciembre del 2003)

3.10 Establecer mecanismos de evaluación de su exposición al riesgo que se deriva de la variación de la tasa de cambio, debiendo para ello realizar un análisis de sus activos y pasivos a fin de determinar su posición en cada una de las monedas en las que opera la institución controlada; (numeral renumerado con resolución No JB-2003-615 de 23 de diciembre del 2003)

3.11 Establecer mecanismos de evaluación de su exposición al riesgo de tasa de interés, debiendo para ello realizar un análisis de sensibilidad de sus activos, pasivos y contingentes a la tasa de interés; (numeral renumerado con resolución No JB-2003-615 de 23 de diciembre del 2003)

3.12 Coordinar su gestión en consistencia con la administración del riesgo de liquidez; y, (numeral renumerado con resolución No JB-2003-615 de 23 de diciembre del 2003)

3.13 Las demás que le fije el directorio o el organismo que haga sus veces o que sean impartidas por la Superintendencia de Bancos y Seguros. (artículo y numeral renumerado con resolución No JB-2003-615 de 23 de diciembre del 2003)

ARTICULO 4.- El comité de administración integral de riesgos, respecto de los riesgos de mercado tendrá a su cargo el establecimiento y aprobación de las políticas, objetivos, límites y procedimientos, específicos, para la administración de los riesgos inherentes a las operaciones con derivados y fijará los criterios bajo los cuales deberá implementarse, los mismos que serán aprobados por el directorio u organismo que haga sus veces. (Reformado con resolución No JB-2003-615 de 23 de diciembre del 2003)

Deberá, adicionalmente, establecer programas de seguimiento, procedimientos de operación y control; y, los niveles de tolerancia, para lo cual:

4.1 Valorizará diariamente el portafolio con la consideración del valor de las posiciones a precios de mercado;

4.2 Evaluará el comportamiento del portafolio frente a situaciones extremas de cambio en el mercado respecto de los supuestos establecidos o pruebas de límites de variación; y,

4.3 Establecerá sistemas de alerta temprana en los que sean consideradas las variables relevantes que afecten el riesgo asumido en el portafolio ante cambios en el mercado. (artículo renumerado con resolución No JB-2003-615 de 23 de diciembre del 2003)

ARTICULO 5.-Si fuere del caso, dado el volumen y complejidad de las operaciones, el comité de administración integral de riesgos conformará en la unidad de riesgo, una área especializada para el manejo de los riesgos originados en las operaciones con derivados, la que deberá constituirse de manera independiente de la de negocios que contrata los derivados con los clientes. (Sustituido con resolución No JB-2003-615 de 23 de diciembre del 2003)

Esta área de riesgo tendrá como función principal la asesoría y seguimiento continuo de la administración de los riesgos inherentes a las operaciones con derivados, esto es de: (reformado con resolución No JB-2003-615 de 23 de diciembre del 2003)

5.1 Los riesgos que surgen por el comportamiento del subyacente;

5.2 Los riesgos que surgen por el incumplimiento de las obligaciones contractuales por parte de los clientes;

5.3 El riesgo operacional que surja por deficiencias en algún aspecto relacionado a la ejecución de un programa de derivados, como fallas en los controles gerenciales, en los sistemas de información, en las liquidaciones, incompetencia, negligencia, error humano, entre otras; y,

5.4 Los riesgos jurídicos que surgen, entre otras, de fallas en la elaboración de los contratos o desconocimiento de las autoridades y juzgadores de tales figuras jurídico – financieras. (artículo renumerado con resolución No JB-2003-615 de 23 de diciembre del 2003)

ARTICULO 6.-La unidad de administración integral de riesgos, además de las funciones señaladas en el artículo 4, de la sección III "Responsabilidad en la administración de riesgos", del capítulo I "De la gestión y administración de riesgos"; del subtítulo VI "De la gestión y administración de riesgos", del título VII "De los activos y de los límites de crédito" de esta Codificación, respecto de los riesgos de mercado, tendrá las siguientes funciones: (sustituido con resolución No JB-2003-615 de 23 de diciembre del 2003)

6.1 Proponer al comité de administración integral de riesgos las políticas de administración y control de riesgo, las metodologías de análisis y valoración de las posiciones, así como las estrategias de cobertura adecuadas para tales posiciones; (reformado con resolución No JB-2003-615 de 23 de diciembre del 2003)

6.2 Implementar y verificar el cumplimiento de las políticas y procedimientos referentes a la administración y control de riesgos de mercado definidas por el directorio o el organismo que haga sus veces y por el comité de administración integral de riesgos; (reformado con resolución No JB-2003-615 de 23 de diciembre del 2003)

6.3 Calcular y valorar las posiciones sensibles al riesgo de mercado y tasa de interés e informar al comité de administración integral de riesgos; (reformado con resolución No JB-2003-615 de 23 de diciembre del 2003)

6.4 Analizar las pérdidas potenciales que podría sufrir la institución controlada bajo diversas situaciones utilizando los respectivos análisis de sensibilidad; y,

6.5 Preparar las actas de las sesiones llevada a cabo por el comité de administración integral de riesgos para su conocimiento y aprobación. (reformado con resolución No JB-2003-615 de 23 de diciembre del 2003)

La unidad de administración integral de riesgos deberá ser independiente de las áreas de negocios. Así mismo, deberá existir separación funcional entre las áreas y personas encargadas de evaluar y tomar los riesgos, de aquellas áreas y personas que deben hacer un seguimiento y control de los riesgos y de aquellas áreas y personas operativas. El personal que integre esta unidad deberá ser idóneo y calificado. (artículo renumerado y reformado con resolución No JB-2003-615 de 23 de diciembre del 2003)

ARTICULO 7.-El comité de administración integral de riesgos, elaborará los manuales de políticas y procedimientos relacionados a los riesgos de mercado, sobre la base de las políticas, estrategias y procedimientos aprobadas por el directorio u organismo que haga sus veces. En dichos manuales deberán establecerse también el esquema de organización, las funciones y las responsabilidades de las áreas y posiciones involucradas. (reformado con resolución No JB-2003-615 de 23 de diciembre del 2003)

Estos manuales deberán ser actualizados periódicamente de tal manera que siempre estén adecuados a la realidad del mercado y de la institución y a sus posibles escenarios futuros.

El esquema de organización de la administración de los riesgos de mercado debe tomar en cuenta la necesaria separación funcional entre las áreas y personas encargadas de evaluar y tomar los riesgos, de aquellas áreas y personas que deben hacer un seguimiento y control de los riesgos y de aquellas áreas y personas operativas. (artículo renumerado con resolución No JB-2003-615 de 23 de diciembre del 2003)

ARTICULO 8.-Las instituciones controladas deben disponer de un sistema informático capaz de proveer a la administración y a las áreas involucradas, toda la información necesaria para evaluar, controlar y otorgar el soporte para la toma de decisiones oportunas y adecuadas, para el manejo de los riesgos de mercado y de tasa de interés.

Estos sistemas deben incorporar los procesos definidos para la elaboración de los informes necesarios, que involucren todas las variables relacionadas con la medición de los riesgos y la vulnerabilidad institucional, bajo diversas condiciones del entorno.

Esta información debe ser suministrada a la Superintendencia de Bancos y Seguros en la realización de las visitas de inspección que ésta realice así como estar disponible para su envío a la Superintendencia de Bancos y Seguros en caso ella fuera solicitada por ésta. (artículo renumerado con resolución No JB-2003-615 de 23 de diciembre del 2003)

ARTICULO 9.-La unidad de administración integral de riesgos deberá utilizar métodos apropiados para medir y valorar las posiciones sensibles a los riesgos de mercado que la institución controlada enfrenta. Deberá incluir, en las mediciones de riesgos, los respectivos análisis retrospectivos y de peor escenario futuro, para evaluar el ajuste y los pronósticos de los métodos internos. Una vez conocidos los resultados de los análisis retrospectivos y de peor escenario futuro, la unidad deberá hacerlos conocer al comité de administración integral de riesgos, con las recomendaciones del caso. (reformado con resolución No JB-2003-615 de 23 de diciembre del 2003)

El análisis retrospectivo consiste en comparar, para un período determinado, las pérdidas estimadas por riesgos de mercado, con los resultados efectivamente generados.

La unidad de administración integral de riesgos, en sus respectivos análisis de sensibilidad, simulará diferentes escenarios y realizará pruebas de estrés relevantes para la administración de los riesgos de mercado y, en especial, del riesgo de tasas de interés, incluyendo el análisis del peor escenario, que consiste en escoger el movimiento de precios más adverso en un día dentro del período seleccionado y aplicar ese conjunto de precios a las posiciones actuales. (reformado con resolución No JB-2003-615 de 23 de diciembre del 2003)

Los resultados obtenidos se deberán considerar para establecer y revisar políticas, procedimientos y limites de exposición a los riesgos.

Los análisis que se hagan deberán tener especial consideración en las condiciones del entorno económico y del grado de afectación ante la vulnerabilidad de la institución controlada. (artículo renumerado con resolución No JB-2003-615 de 23 de diciembre del 2003)

ANEXO 2

CODIFICACION DE RESOLUCIONES DE LA SUPERINTENDENCIA DE BANCOS Y SEGUROS Y DE LA JUNTA BANCARIA

TITULO VII.-DE LOS ACTIVOS Y DE LOS LIMITES DE CREDITO

SUBTITULO VI.-DE LA GESTION Y ADMINISTRACION DE RIESGOS

(sustituido con resolución No JB-2003-601 de 9 de diciembre del 2003)

CAPITULO III.- DE LA ADMINISTRACION DEL RIESGO DE MERCADO

(incluido resolución No JB-2002-429 de 22 de enero del 2002, reenumerado con resolución No JB-2003-601 de 9 de diciembre del 2003 y reformado con resolución No JB-2003-615 de 23 de diciembre del 2003)

SECCIÓN III.- METODO ESTANDAR DE MEDICIÓN DE LA EXPOSICION AL RIESGO

ARTICULO 1.-El objetivo de los métodos de medición es la estimación del grado de exposición de una institución controlada a las variaciones en las condiciones de sus activos y pasivos por variaciones en las tasas de interés y del tipo de cambio.

El uso de estos métodos permitirá a las instituciones controladas y a la Superintendencia de Bancos y Seguros la toma oportuna de las medidas necesarias para mantener y consolidar el patrimonio de la institución.

ARTICULO 2.-Para efectos de la aplicación de las normas contenidas en esta sección se entiende por:

2.1 Activos (pasivos) sensibles a la tasa de interés, a aquellos cuyo valor es afectado por la tasa de interés de modo que un cambio de ésta pueda generar cambios en su valor de mercado, o variaciones en el flujo de ingresos (egresos) que de ellos se derivan;

2.2 Brecha de activos y pasivos sensibles a la tasa de interés, a la diferencia entre los activos y pasivos sensibles a la tasa de interés, expresada en dólares de los Estados Unidos de América;

2.3 Duración, a la que señala el tiempo o el período en el cual se recupera el monto invertido, en términos de valor presente, en un instrumento de acuerdo a los flujos de caja allí implícitos. Por ello, mide la sensibilidad a la tasa de interés de los flujos de caja asociados al instrumento financiero el cual puede ser de renta fija, de renta variable, un préstamo o un portafolio de instrumentos financieros;

2.4 Fecha de reprecio, al momento en el cual se revisa la tasa de interés, según lo pactado contractualmente, para ajustarla a las condiciones vigentes en el mercado; y,

2.5 Instrumentos de cupón cero, a los instrumentos que no pagan cupones, por lo que su valor nominal es pagado íntegramente a su vencimiento. En su colocación en el mercado, estos instrumentos son emitidos bajo la par.

ARTICULO 3.- Son métodos para la medición del riesgo de tasa de interés:

3.1 El método de maduración:

El modelo estándar para medir los riesgos de tasas de interés es el de maduración, que define la exposición al riesgo de tasas de interés como la brecha o descalce entre los activos y pasivos sensibles a la tasa de interés.

La información sobre la medición de riesgo de tasa de interés, se elaborará utilizando el sistema de bandas temporales, estableciendo la brecha entre activos y pasivos sensibles a la tasa de interés. Esta información se pondrá en conocimiento de la Superintendencia con la periodicidad y formato que se establezca para el efecto.

La información se organizará en catorce bandas temporales y los activos y pasivos deberán ser distribuidos en todas esas bandas de acuerdo a su fecha de vencimiento contractual. La brecha o descalce entre los activos y pasivos sensibles a la tasa de interés se calculará dentro de cada banda, y luego se calculará la brecha acumulada existente:

- Brecha marginal$_n$ = [(ACT$_n$ – PAS$_n$) + DO$_n$] para la banda temporal n.
- Brecha acumulada$_n$ = Brecha marginal$_n$ + Brecha acumulada$_{n-1}$ Donde:

ACT$_n$ = Activos en la banda n

PAS$_n$ = Pasivos en la banda n

DO$_n$ = Monto delta neto de opciones en la banda n

n n – ésima banda de tiempo, donde n = 1, 2, 3, …, q, siendo q el número de bandas.

- Cuando la institución controlada mantenga un portafolio de opciones, ésta deberá incluir en el cálculo del riesgo de la tasa de interés el monto delta neto de las opciones, que se calculará para cada banda temporal como la diferencia entre los montos delta positivo y negativo. El monto delta se obtiene de:

$$DO = \delta * X * D^{M}$$

Donde:

D se refiere al monto delta de la opción;

δ, es el delta determinado para la opción i-ésima y de acuerdo al modelo black – scholes (para las opciones europeas), binomial (opciones americanas) o de acuerdo a otro modelo de valuación previo conocimiento de la Superintendencia;

X, valor de mercado del monto contractual del activo subyacente de la opción; y,

D^{M}, la duración modificada del activo subyacente a la tasa de interés, toma el valor de uno cuando el subyacente es una tasa de interés.

El horizonte de análisis de las brechas es la vida útil de la institución controlada. Por ello, se debe incluir todas las operaciones activas y pasivas ya que, a largo plazo, todas las operaciones son líquidas y están afectas al riesgo de tasas de interés.

En los activos y pasivos sensibles a la tasa de interés se deben incluir todas las operaciones contingentes que sean sensibles a la tasa de interés. La distribución de las diversas cuentas a lo largo de las bandas deberá realizarse de acuerdo al plazo de vencimiento contractual.

En los casos de las cuentas con vencimiento incierto, se deberá realizar un análisis de tendencia y de estacionalidad a través del uso de métodos estadísticos apropiados, tal como

el uso de modelos de regresión múltiple, en donde se incorpore como variable explicativa al Producto Interno Bruto y todas aquellas que las instituciones controladas consideren pertinentes, de acuerdo al mercado al cual atienden. Se debe tener especial cuidado en la elección del número de variables explicativas de modo que la regresión contenga los suficientes grados de libertad que permitan obtener resultados a un nivel de confianza de al menos 99%.

Considerando que la distribución de las cuentas de vencimiento incierto se realizará a lo largo de la vida útil de la institución controlada, se deberá efectuar el análisis pertinente que asegure que las series de tiempo asociadas a cada una de ellas es estacionaria.

El primer formulario que se entregue deberá incluir un informe sobre los supuestos empleados para el cálculo de los datos numéricos constantes en él y los modelos estadísticos utilizados. Las posteriores modificaciones a dichos supuestos o modelos deberán ser comunicadas a la Superintendencia de Bancos y Seguros con los argumentos justificativos de tales modificaciones, dentro de los ocho días posteriores a su aprobación por el directorio o el organismo que haga sus veces. El jefe o encargado de la unidad de administración y control de riesgo de mercado será el responsable de la elaboración y presentación de dicho formulario.

Al momento de presentar la información sobre la medición del riesgo de tasa de interés, se señalarán las notas metodológicas correspondientes para que dicho formulario sea adecuadamente completado.

3.2 La Duración en la medición del riesgo de tasas de interés:

La información de las duraciones implícitas en los activos y pasivos sensibles a la tasa de interés, para cada una de las bandas temporales analizadas, se reportará con la periodicidad y en el formato que la Superintendencia determine y que se pondrá en conocimiento mediante circular.

El objetivo es capturar la exposición al riesgo de tasas de interés al cual está expuesta la institución controlada. El resultado de la brecha entre los activos y pasivos sensibles a la tasa de interés señalará el descalce existente de plazos. La información que proporcione la duración será una medida que permita profundizar el análisis de la sensibilidad a la tasa de interés, al cual está afecto cada una de las instituciones controladas.

La duración es la relación de la suma ponderada por los plazos de los flujos de caja descontados respecto al valor descontado de dicho flujo. Esto es:

$$D = \frac{\sum_{s=1}^{n} s \; FC_s (1+r)^{-s}}{P_0}$$

en donde:

D es la duración

S es el momento en que tiene lugar un flujo de caja

FC es el flujo de caja del activo o pasivo analizado

r es la tasa de descuento del activo o pasivo

P_0 es el valor presente del activo o pasivo en el momento del cálculo de la duración

El concepto de duración tiene las siguientes características:

- La duración está expresada en unidades de tiempo (días, meses, años);

- La duración es siempre menor que el plazo contractual o la maduración original del instrumento, excepto los casos de los instrumentos de cupón cero, ya que éstos tienen un sólo flujo.

- Si el activo o el pasivo analizado tiene un único flujo de efectivo que ocurre al vencimiento, éste debe ser tratado como un instrumento de cupón cero, en donde la duración será igual al plazo de vencimiento.

- Si la tasa de interés aumentara, el valor de la tasa de descuento deberá incrementarse por lo que el valor de la duración será menor, recogiendo el efecto negativo sobre el valor del instrumento que se deriva del aumento de la tasa de interés.

Se calculará la duración por cada activo, pasivo y contingente sensible a la tasa de interés. La tasa de descuento que se utilizará, será aquella señalada por la Superintendencia de Bancos y Seguros para cada tipo de instrumento.

Asimismo, deberá considerarse:

- Instrumento pactado a fecha cierta o fija de vencimiento. La duración de un instrumento así pactado se calculará de acuerdo a la fórmula arriba definida. Los flujos se proyectarán según lo pactado contractualmente.

- Instrumento pactado a tasa variable. La duración de un instrumento así pactado es equivalente al número de períodos restantes hasta la siguiente fecha de reprecio del instrumento. Así se tiene que un instrumento pactado a tasa variable con fecha de reprecio de un mes, la duración será equivalente a un mes.

- Instrumento pactado a tasa fija con una porción variable. El cálculo de la duración de un instrumento así pactado debe realizarse por separado en cada una de sus partes y de acuerdo a lo señalado para cada uno de los casos respectivos. Luego, la duración del instrumento será el resultado de la suma ponderada de cada una de sus partes, siendo el factor de ponderación para la parte fijada a tasa fija como el ratio (valor presente de la parte a tasa fija / valor total del instrumento) y el correspondiente para la tasa variable como el ratio (valor presente de la parte a tasa variable / valor total del instrumento).

  El valor total del instrumento equivale a la suma de los valores presentes de cada una de las partes conformantes del instrumento. Los valores presentes de cada una de las partes deberá calcularse empleando las mismas tasas de descuento.

- Cuentas de vencimiento incierto. La duración para todas las cuentas sin fecha contractual de vencimiento deberá considerar que estas cuentas mantienen relativa independencia a la tasa de interés.

  Para determinar la exposición al riesgo de tasas de interés, las instituciones controladas deberán estimar estadísticamente la porción volátil y la que tienen carácter de permanente. La porción volátil se considerará en la primera banda temporal (esto es, de 1 a 7 días) por lo que se asumirá una duración de siete días. La parte estable deberá distribuirse en las restantes bandas y de acuerdo al análisis estadístico que para el efecto se realice.

ARTICULO 4.-La medición del riesgo de tipo de cambio deberá efectuarse a través de la medición de la posición neta que en cada divisa posea una institución controlada, de acuerdo a la siguiente fórmula:

$$PN_j = \sum_{j=1}^{mm} (PA_j) - \sum_{j=1} (PP_j)$$

en donde:

PN_j	Posición neta en la divisa j, donde (j = 1, …, m)
PA_j	Posición activa, incluyendo contingencias deudoras, en la divisa j
PP_j	Posición pasiva, incluyendo contingencias acreedoras, en la divisa j

La posición neta en cada divisa se entiende como la diferencia entre la suma de las posiciones activas y la suma de las posiciones pasivas en dicha divisa. Los derechos originados en contingencias deudoras se considerarán como posiciones activas mientras que las obligaciones generadas en contingencias acreedoras como posiciones pasivas.

Para obtener la posición neta total en cada divisa, se deberá añadir a la posición neta de divisas ya calculada, las compras a futuro, forward y swap y se debe restar las ventas a futuro, forward y swap, en cada divisa.

Las posiciones sensibles al riesgo de tipo de cambio, por moneda, que maneje la institución controlada, serán reportadas a la Superintendencia de Bancos y Seguros con la periodicidad y en el formato que este organismo de control determine. El jefe o encargado de la unidad de administración y control de riesgos de mercado y tasas de interés será el responsable de la elaboración y presentación de dicho formulario. Como anexo a dicha información, se señalarán las notas metodológicas correspondientes para que dicho formulario sea adecuadamente completado.

ARTICULO 5.- Las instituciones controladas deberán remitir a la Superintendencia de Bancos y Seguros la información sobre riesgos de tasa de interés y tipo de cambio con la periodicidad que ésta determine y al menos mensualmente.

SECCION IV.- DEL VALOR PATRIMONIAL EN RIESGO

ARTICULO 1.- Se entiende por “Valor patrimonial en riesgo”, a la pérdida de valor patrimonial que una institución controlada pueda incurrir por efectos de la exposición al riesgo que se analiza y los factores de sensibilidad que, para el efecto, determine la Superintendencia de Bancos y Seguros. Para cada banda temporal, se multiplicará el factor de sensibilidad señalado anteriormente, por la brecha correspondiente. Luego, el “valor patrimonial en riesgo” será la suma de los valores calculados para cada banda temporal.

El valor patrimonial en riesgo reflejará los efectos que los cambios en las condiciones del mercado puedan tener sobre el valor del patrimonio. Esta medida también mostrará los efectos potenciales en las condiciones de mercado sobre el valor de los flujos de caja de las posiciones activas y pasivas de una institución controlada y en la posición neta en divisas de dicha institución.

La Superintendencia de Bancos y Seguros determinará, mediante resolución, los requerimientos de capital frente al valor patrimonial en riesgo.

ANEXO 3

CODIFICACION DE RESOLUCIONES DE LA SUPERINTENDENCIA DE BANCOS Y SEGUROS Y DE LA JUNTA BANCARIA

TITULO VII.- DE LOS ACTIVOS Y DE LOS LIMITES DE CREDITO

SUBTITULO VI.- DE LA GESTION Y ADMINISTRACION DE RIESGOS

(sustituido con resolución No JB-2003-601 de 9 de diciembre del 2003)

CAPITULO IV.-DE LA ADMINISTRACION DEL RIESGO DE LIQUIDEZ

(incluido con resolución No JB-2002-431 de 22 de enero del 2002, reenumerado con resolución No JB-2003-601 de 9 de diciembre del 2003 y reformado con resolución No JB-2003-615 de 23 de diciembre del 2003)

SECCIÓN I.- ALCANCE Y DEFINICIONES (reformada con resolución No JB-2003-615 de 23 de diciembre del 2003)

ARTICULO 1.- Las disposiciones de la presente norma son aplicables al Banco Central del Ecuador, a las instituciones financieras públicas y privadas, a las compañías de arrendamiento mercantil, a las compañías emisoras y administradoras de tarjetas de crédito y a las corporaciones de desarrollo de mercado secundario de hipotecas. (incluido con resolución No JB-2003-615 de 23 de diciembre del 2003)

ARTICULO 2.-Se entiende por riesgo de liquidez, cuando la institución enfrenta una escasez de fondos para cumplir sus obligaciones y que por ello, tiene la necesidad de conseguir recursos alternativos o vender activos en condiciones desfavorables, esto es, asumiendo un alto costo financiero o una elevada tasa de descuento, incurriendo en pérdidas de valorización.

ANEXO 4

CODIFICACION DE RESOLUCIONES DE LA SUPERINTENDENCIA DE BANCOS Y SEGUROS Y DE LA JUNTA BANCARIA

TITULO VII.- DE LOS ACTIVOS Y DE LOS LIMITES DE CREDITO

SUBTITULO VI.- DE LA GESTION Y ADMINISTRACION DE RIESGOS

(sustituido con resolución No JB-2003-601 de 9 de diciembre del 2003)

CAPÍTULO V.- DE LA GESTIÓN DEL RIESGO OPERATIVO (capítulo incluido con resolución No JB-2005-834 de 20 de octubre del 2005)

SECCIÓN II.- FACTORES DEL RIESGO OPERATIVO

ARTÍCULO 1.- Con el propósito de que se minimice la probabilidad de incurrir en pérdidas financieras atribuibles al riesgo operativo, deben ser adecuadamente administrados los siguientes aspectos, los cuales se interrelacionan entre sí,:

1.1 Procesos.- Con el objeto de garantizar la optimización de los recursos y la estandarización de las actividades, las instituciones controladas deben contar con procesos definidos de conformidad con la estrategia y las políticas adoptadas, que deberán ser agrupados de la siguiente manera:

1.1.1 Procesos gobernantes o estratégicos.- Se considerarán a aquellos que proporcionan directrices a los demás procesos y son realizados por el directorio u organismo que haga sus veces y por la alta gerencia para poder cumplir con los objetivos y políticas institucionales. Se refieren a la planificación estratégica, los lineamientos de acción básicos, la estructura organizacional, la administración integral de riesgos, entre otros;

1.1.2 Procesos productivos, fundamentales u operativos.- Son los procesos esenciales de la entidad destinados a llevar a cabo las actividades que permitan ejecutar efectivamente las políticas y estrategias relacionadas con la calidad de los productos o servicios que ofrecen a sus clientes; y,

1.1.3 Procesos habilitantes, de soporte o apoyo.- Son aquellos que apoyan a los procesos gobernantes y productivos, se encargan de proporcionar personal competente, reducir los riesgos del trabajo, preservar la calidad de los materiales, equipos y herramientas, mantener las condiciones de operatividad y funcionamiento, coordinar y controlar la eficacia del desempeño administrativo y la optimización de los recursos.

Identificados los procesos críticos, se implantarán mecanismos o alternativas que ayuden a la entidad a evitar incurrir en pérdidas o poner en riesgo la continuidad del negocio y sus operaciones.

Para considerar la existencia de un apropiado ambiente de gestión de riesgo operativo, las instituciones controladas deberán definir formalmente políticas para un adecuado diseño, control, actualización y seguimiento de los procesos.

Las políticas deben referirse por lo menos a: (i) diseño claro de los procesos, los cuales deben ser adaptables y dinámicos; (ii) descripción en secuencia lógica y ordenada de las actividades, tareas, y controles; (iii) determinación de los responsables de los procesos, que serán aquellas personas encargadas de su correcto funcionamiento, a través de establecer medidas y fijar objetivos para

gestionarlos y mejorarlos, garantizar que las metas globales se cumplan, definir los límites y alcance, mantener contacto con los clientes internos y externos del proceso para garantizar que se satisfagan y se conozcan sus expectativas, entre otros; (iv) difusión y comunicación de los procesos buscando garantizar su total aplicación; y, (v) actualización y mejora continua a través del seguimiento permanente en su aplicación.

Deberá existir una adecuada separación de funciones que evite concentraciones de carácter incompatible, entendidas éstas como aquellas tareas cuya combinación en las competencias de una sola persona, eventualmente, podría permitir la realización o el ocultamiento de fraudes, errores, omisiones u otros eventos de riesgo operativo.

Las instituciones controladas deberán mantener inventarios actualizados de los procesos existentes, que cuenten, como mínimo con la siguiente información: tipo de proceso (gobernante, productivo y de apoyo), nombre del proceso, responsable, productos y servicios que genera el proceso, clientes internos y externos, fecha de aprobación, fecha de actualización, además de señalar si se trata de un proceso crítico.

1.2 Personas.- Las instituciones controladas deben administrar el capital humano de forma adecuada, e identificar apropiadamente las fallas o insuficiencias asociadas al factor .personas., tales como: falta de personal adecuado, negligencia, error humano, nepotismo de conformidad con las disposiciones legales vigentes, inapropiadas relaciones interpersonales y ambiente laboral desfavorable, falta de especificaciones claras en los términos de contratación del personal, entre otros.

Para considerar la existencia de un apropiado ambiente de gestión de riesgo operativo, las instituciones controladas deberán definir formalmente políticas, procesos y procedimientos que aseguren una apropiada planificación y administración del capital humano, los cuales considerarán los procesos de incorporación, permanencia y desvinculación del personal al servicio de la institución.

Dichos procesos corresponden a:

> **1.2.1 Los procesos de incorporación.-** Que comprenden la planificación de necesidades, el reclutamiento, la selección, la contratación e inducción de nuevo personal;
>
> **1.2.2 Los procesos de permanencia.-** Que cubren la creación de condiciones laborales idóneas; la promoción de actividades de capacitación y formación que permitan al personal aumentar y perfeccionar sus conocimientos, competencias y destrezas; la existencia de un sistema de evaluación del desempeño; desarrollo de carrera; rendición de cuentas; e incentivos que motiven la adhesión a los valores y controles institucionales; y,
>
> **1.2.3 Los procesos de desvinculación.-** Que comprenden la planificación de la salida del personal por causas regulares, preparación de aspectos jurídicos para llegar al finiquito y la finalización de la relación laboral.

Los procesos de incorporación, permanencia y desvinculación antes indicados deberán ser soportados técnicamente, ajustados a las disposiciones legales y transparentes para garantizar condiciones laborales idóneas.

Las instituciones controladas deberán analizar su organización con el objeto de evaluar si han definido el personal necesario y las competencias idóneas para el desempeño de cada puesto, considerando no sólo experiencia profesional, formación académica, sino también los valores, actitudes y habilidades personales que puedan servir como criterio para garantizar la excelencia institucional.

Las instituciones controladas mantendrán información actualizada del capital humano, que permita una adecuada toma de decisiones por parte de los niveles directivos y la realización de análisis cualitativos y cuantitativos de acuerdo con sus necesidades. Dicha información deberá referirse al personal existente en la institución; a la formación académica y experiencia; a la forma y fechas de selección, reclutamiento y contratación; información histórica sobre los eventos de capacitación en los que han participado; cargos que han desempeñado en la institución; resultados de evaluaciones realizadas; fechas y causas de separación del personal que se ha desvinculado de la institución; y, otra información que la institución controlada considere pertinente.

1.3 Tecnología de información.- Las instituciones controladas deben contar con la tecnología de información que garantice la captura, procesamiento, almacenamiento y transmisión de la información de manera oportuna y confiable; evitar interrupciones del negocio y lograr que la información, inclusive aquella bajo la modalidad de servicios provistos por terceros, sea íntegra, confidencial y esté disponible para una apropiada toma de decisiones.

Para considerar la existencia de un apropiado ambiente de gestión de riesgo operativo, las instituciones controladas deberán definir formalmente políticas, procesos y procedimientos que aseguren una adecuada planificación y administración de la tecnología de información.

Dichas políticas, procesos y procedimientos se referirán a:

1.3.1 Con el objeto de garantizar que la administración de la tecnología de información soporte adecuadamente los requerimientos de operación actuales y futuros de la entidad, las instituciones controladas deben contar al menos con lo siguiente:

1.3.1.1 El apoyo y compromiso formal del directorio u organismo que haga sus veces y la alta gerencia;

1.3.1.2 Un plan funcional de tecnología de información alineado con el plan estratégico institucional; y, un plan operativo que establezca las actividades a ejecutar en el corto plazo (un año), de manera que se asegure el logro de los objetivos institucionales propuestos;

1.3.1.3 Tecnología de información acorde a las operaciones del negocio y al volumen de transacciones, monitoreada y proyectada según las necesidades y crecimiento de la institución;

1.3.1.4 Un responsable de la información que se encargue principalmente de definir y autorizar de manera formal los accesos y cambios funcionales a las aplicaciones y monitorear el cumplimiento de los controles establecidos;

1.3.1.5 Políticas, procesos y procedimientos de tecnología de información definidos bajo estándares de general aceptación que garanticen la ejecución de los criterios de control interno de eficacia, eficiencia y cumplimiento, debidamente aprobados por el directorio u organismo que haga sus veces, alineados a los objetivos y actividades de la institución;

1.3.1.6 Difusión y comunicación a todo el personal involucrado de las mencionadas políticas, procesos y procedimientos, de tal forma que se asegure su implementación; y,

1.3.1.7 Capacitación y entrenamiento técnico al personal del área de tecnología de información y de los usuarios de la misma.

1.3.2 Con el objeto de garantizar que las operaciones de tecnología de información satisfagan los requerimientos de la entidad, las instituciones controladas deben contar al menos con lo siguiente:

1.3.2.1 Manuales o reglamentos internos, debidamente aprobados por el directorio u organismo que haga sus veces, que establezcan como mínimo las responsabilidades y procedimientos para la operación, el uso de las instalaciones de procesamiento de información y respuestas a incidentes de tecnología de información;

1.3.2.2 Un procedimiento de clasificación y control de activos de tecnología de información, que considere por lo menos, su registro e identificación, así como los responsables de su uso y mantenimiento, especialmente de los más importantes;

1.3.3 Con el objeto de garantizar que los recursos y servicios provistos por terceros, se administren con base en responsabilidades claramente definidas y estén sometidas a un monitoreo de su eficiencia y efectividad, las instituciones controladas deben contar al menos con lo siguiente:

1.3.3.1 Requerimientos contractuales convenidos que definan la propiedad de la información y de las aplicaciones; y, la responsabilidad de la empresa proveedora de la tecnología en caso de ser vulnerables sus sistemas, a fin de mantener la integridad, disponibilidad y confidencialidad de la información; y,

1.3.3.2 Requerimientos contractuales convenidos que establezcan que las aplicaciones sean parametrizables, que exista una transferencia del conocimiento y que se entregue documentación técnica y de usuario, a fin de reducir la dependencia de las instituciones controladas con proveedores externos y los eventos de riesgo operativo que esto origina.

1.3.4 Con el objeto de garantizar que el sistema de administración de seguridad satisfaga las necesidades de la entidad para salvaguardar la información contra el uso, revelación y modificación no autorizados, así como daños y pérdidas, las instituciones controladas deben contar al menos con lo siguiente:

1.3.4.1 Políticas y procedimientos de seguridad de la información que establezcan sus objetivos, importancia, normas, principios, requisitos de cumplimiento, responsabilidades y comunicación de los incidentes relativos a la seguridad; considerando los aspectos legales, así como las consecuencias de violación de estas políticas;

1.3.4.2 La identificación de los requerimientos de seguridad relacionados con la tecnología de información, considerando principalmente: la evaluación de los riesgos que enfrenta la institución; los requisitos legales, normativos, reglamentarios y contractuales; y, el conjunto específico de principios, objetivos y condiciones para el procesamiento de la información que respalda sus operaciones;

1.3.4.3 Los controles necesarios para asegurar la integridad, disponibilidad y confidencialidad de la información administrada;

1.3.4.4 Un sistema de administración de las seguridades de acceso a la información, que defina las facultades y atributos de los usuarios, desde el registro, eliminación y modificación, pistas de auditoría; además de los controles necesarios que permitan verificar su cumplimiento en todos los ambientes de procesamiento;

1.3.4.5 Niveles de autorización de accesos y ejecución de las funciones de procesamiento de las aplicaciones, formalmente establecidos, que garanticen una adecuada segregación de funciones y reduzcan el riesgo de error o fraude;

1.3.4.6 Adecuados sistemas de control y autenticación para evitar accesos no autorizados, inclusive de terceros; y, ataques externos especialmente a la información crítica y a las instalaciones de procesamiento;

1.3.4.7 Controles adecuados para detectar y evitar la instalación de software no autorizado o sin la respectiva licencia, así como instalar y actualizar periódicamente aplicaciones de detección y desinfección de virus informáticos y demás software maliciosos;

1.3.4.8 Controles formales para proteger la información contenida en documentos; medios de almacenamiento u otros dispositivos externos; el uso e intercambio electrónico de datos contra daño, robo, accesos, utilización o divulgación no autorizada de información para fines contrarios a los intereses de la entidad, por parte de todo su personal y de sus proveedores;

1.3.4.9 Instalaciones de procesamiento de información crítica en áreas protegidas con los suficientes controles que eviten el acceso de personal no autorizado y daños a los equipos de computación y a la información en ellos procesada, almacenada o distribuida;

1.3.4.10 Las condiciones físicas y ambientales necesarias para garantizar el correcto funcionamiento del entorno de la infraestructura de tecnología de información;

1.3.4.11 Un plan para evaluar el desempeño del sistema de administración de la seguridad de la información, que permita tomar acciones orientadas a mejorarlo; y,

1.3.4.12 Las instituciones controladas que ofrezcan los servicios de transferencias y transacciones electrónicas deberán contar con políticas y procedimientos de seguridad de la información que garanticen que las operaciones sólo pueden ser realizadas por personas debidamente autorizadas; que el canal de comunicaciones utilizado sea seguro, mediante técnicas de encriptación de información; que existan mecanismos alternos que garanticen la continuidad del servicio ofrecido; y, que aseguren la existencia de pistas de auditoría.

1.3.5 Con el objeto de garantizar la continuidad de las operaciones, las instituciones controladas deben contar al menos con lo siguiente:

1.3.5.1 Controles para minimizar riesgos potenciales de sus equipos de computación ante eventos imprevistos, tales como: fallas, daños o insuficiencia de los recursos de tecnología de información; robo; incendio; humo; inundaciones; polvo; interrupciones en el fluido eléctrico, desastres naturales; entre otros;

1.3.5.2 Políticas y procedimientos de respaldo de información periódicos, que aseguren al menos que la información crítica pueda ser recuperada en caso de falla de la tecnología de información o con posterioridad a un evento inesperado;

1.3.5.3 Mantener los sistemas de comunicación y redundancia de los mismos que permitan garantizar la continuidad de sus servicios; y,

1.3.5.4 Información de respaldo y procedimientos de restauración en una ubicación remota, a una distancia adecuada que garantice su disponibilidad ante eventos de desastre en el centro principal de procesamiento.

1.3.6 Con el objeto de garantizar que el proceso de adquisición, desarrollo, implementación y mantenimiento de las aplicaciones satisfagan los objetivos del negocio, las instituciones controladas deben contar al menos con lo siguiente:

1.3.6.1 Una metodología que permita la adecuada administración y control del proceso de compra de software y del ciclo de vida de desarrollo y mantenimiento de aplicaciones, con la aceptación de los usuarios involucrados;

1.3.6.2 Documentación técnica y de usuario permanentemente actualizada de las aplicaciones de la institución;

1.3.6.3 Controles que permitan asegurar la adecuada administración de versiones de las aplicaciones puestas en producción; y,

1.3.6.4 Controles que permitan asegurar que la calidad de la información sometida a migración, cumple con las características de integridad, disponibilidad y confidencialidad.

1.3.7 Con el objeto de garantizar que la infraestructura tecnológica que soporta las operaciones, sea administrada, monitoreada y documentada de forma adecuada, las instituciones controladas deberán contar con políticas y procedimientos que permitan la adecuada administración, monitoreo y documentación de las bases de datos, redes de datos, software de base y hardware.

1.4 Eventos externos.- En la administración del riesgo operativo, las instituciones controladas deben considerar la posibilidad de pérdidas derivadas de la ocurrencia de eventos ajenos a su control, tales como: fallas en los servicios públicos, ocurrencia de desastres naturales, atentados y otros actos delictivos, los cuales pudieran alterar el desarrollo normal de sus actividades. Para el efecto, deben contar con planes de contingencia y de continuidad del negocio.

ANEXO 5

COSO

Monitoreo

- Evaluación de la efectividad del sistema de control a largo plazo.
- Combinación de una evaluación continua e independiente.
- Actividades gerenciales y de supervisión.
- Actividades de auditoría interna.

Actividades de Control

- Políticas/procedimientos que aseguran que se siguen las directrices de la gerencia.
- Rango de actividades tales como aprobaciones, autorizaciones, verificaciones, recomendaciones, revisiones de rendimiento, seguridad de activos y segregación de funciones.

Información y Comunicación

- Información adecuada identificada, ingresada y comunicada de manera oportuna.
- Acceso a información generada interna y externamente.
- Un flujo de información que permite actividades de control exitosos – desde asignaciones de responsabilidades hasta resumen de hallazgos para acciones de la gerencia.

Ambiente de Control

- Define el rumbo para medidas de concientizar los empleados en términos de controles.
- Factores que incluyen integridad, valores éticos, competencia, autoridad, responsabilidad.
- Base para todos los demás componentes de control.

Evaluación de Riesgo

- Evaluación de riesgo es la identificación y análisis de riesgos relevantes para lograr los objetivos de la entidad – formando la base para definir las actividades de control.

Fuente: COSO Internal Control By Commitee of Sponsoring Organizations of the Treadway Commision (COSO)

ANEXO 6

COSO - ERM

Ambiente Interno:
- Establece la cultura de riesgo de la entidad.
- Considera cómo las acciones de la entidad pueden afectar su cultura de riesgo.

Establecimiento de Objetivos:
- La administración considera los riesgos estratégicos en el establecimiento de objetivos.
- Define el apetito/ tolerancia al riesgo de la entidad.

Identificación de Eventos:
- Se identifican los eventos internos y externos que afectan la estrategia y el logro de los objetivos.
- Diferencia entre riesgos y oportunidades.

Evaluación de Riesgos:
- Comprensión del grado (probabilidad e Impacto) en que eventos potenciales pueden impactar el logro de los objetivos.
- Requiere una combinación de métodos cualitativos y cuantitativos

Respuesta al Riesgo:
- Identifica y evalúa posibles respuestas al riesgo considerando el apetito al riesgo de la entidad, los costos y beneficios de las potenciales respuestas al riesgo y el grado en el cual una respuesta reducirá el impacto probabilidad del riesgo.

Actividades de Control:
- Políticas y procedimientos que ayudan a asegurar que las respuestas al riesgo son ejecutadas.
- Incluye controles de tecnología.

Información y Comunicación:
- Se identifica, captura y comunica información relevante en forma oportuna para permitir al personal ejecutar sus responsabilidades.

Monitoreo:
- Actividades de seguimiento contínuo
- Evaluaciones separadas
- Una combinación de ambos

Fuente: COSO ERM by Committee of Sponsoring Organizations of the Treadway Commission (COSO)

ANEXO 7

CODIFICACION DE RESOLUCIONES DE LA SUPERINTENDENCIA DE BANCOS Y SEGUROS Y DE LA JUNTA BANCARIA

TITULO VII.-DE LOS ACTIVOS Y DE LOS LIMITES DE CREDITO

SUBTITULO VI.-DE LA GESTION Y ADMINISTRACION DE RIESGOS (sustituido con resolución No JB-2003-601 de 9 de diciembre del 2003)

CAPITULO I.- DE LA GESTION INTEGRAL Y CONTROL DE RIESGOS (incluido con resolución No JB-2003-601 de 9 de diciembre del 2003 y sustituido con resolución No JB-2004-631 de 22 de enero del 2004)

SECCION III.- RESPONSABILIDAD EN LA ADMINISTRACION DE RIESGOS

ARTÍCULO 1.-El directorio o el organismo que haga sus veces, deberá en ejercicio de lo previsto en la letra a) del artículo 30 de la Ley General de Instituciones del Sistema Financiero, cuando menos, cumplir con lo siguiente:

1.1 Conocer y comprender los riesgos inherentes a la estrategia de negocio que asume la institución;

1.2 Determinar y actualizar permanentemente las estrategias, políticas, procesos y procedimientos, que permitan una eficiente administración integral de riesgos; además de su adecuado seguimiento, así como el modo de divulgación y concienciación de la política organizativa, que enfatice la importancia del control del riesgo en todos los niveles de la institución;

1.3 Informarse por lo menos en forma trimestral, sobre los riesgos asumidos, la evolución y el perfil de los mismos y su efecto en los niveles patrimoniales y las necesidades de cobertura, así como sobre la implantación y cumplimiento de estrategias, políticas, procesos y procedimientos por ellos aprobados;

1.4 Asegurarse que la auditoría interna verifique la existencia y cumplimiento del esquema de la administración integral de riesgos de la institución;

1.5 Aprobar la incursión de la institución en nuevos negocios, operaciones y actividades de acuerdo con la estrategia del negocio, a las normas legales y estatutarias y en cumplimiento a las políticas internas de administración integral de riesgos;

1.6 Establecer límites generales prudenciales para la administración de los riesgos, compatibles con las actividades, estrategias y objetivos institucionales y que permitan una eficaz reacción frente a situaciones adversas;

1.7 Implantar medidas correctivas en caso de que las estrategias, políticas, procesos y procedimientos para la administración integral de riesgos no se cumplan, o se cumplan parcialmente o en forma incorrecta;

1.8 Asegurarse de que los niveles de la administración de riesgo establezcan un sistema de medición para valorar los riesgos, vincular el riesgo al de patrimonio técnico de la institución y aplicar un esquema para vigilar la observancia de las políticas internas;

1.9 Asegurarse de que la institución cuente con recursos humanos, materiales y equipos

que permitan la eficiente administración integral de riesgos;

1.10 Designar a los miembros del comité de administración integral de riesgos; y,

1.11 Las demás que determine la junta general de accionistas u organismo que haga sus veces, o que sean dispuestas por la Superintendencia de Bancos y Seguros.

El directorio o el organismo que haga sus veces debe contar con documentos probatorios respecto del cumplimiento de las disposiciones de este artículo.

ARTICULO 2.-El comité de administración integral de riesgos es un organismo colegiado, que estará conformado por los siguientes miembros como mínimo:

2.1 Un vocal del directorio o del organismo que haga sus veces, que no sea miembro del comité de auditoría, que lo presidirá;

2.2 El máximo o primer representante legal de la institución de que se trate; y,

2.3 El funcionario responsable de la unidad de riesgos.

El comité deberá contar con la participación de especialistas de cada uno de los riesgos, si los hubiere; los funcionarios responsables de las áreas de negocios; y, otros que se consideren funcionarios vinculados con los temas a tratarse. Ninguno de estos funcionarios tendrán derecho a voto.

Las designaciones y las sustituciones en la nómina de los miembros del comité deberán ser conocidas y aprobadas por el directorio o el organismo que haga sus veces de la institución del sistema financiero, lo cual debe quedar consignado en las respectivas actas y ser puestas en conocimiento de la Superintendencia de Bancos y Seguros, dentro de los siguientes ocho días contados desde la fecha de la pertinente sesión.

El comité de administración integral de riesgos sesionará con la mitad más uno de sus integrantes, sus decisiones serán tomadas por mayoría absoluta de votos. El presidente del comité tendrá voto dirimente.

ARTICULO 3.- Las funciones principales que debe asumir el comité de riesgos integrales, son las siguientes:

3.1 Diseñar y proponer estrategias, políticas, procesos y procedimientos de administración integral de riesgos o reformas, y, someterlos a la aprobación del directorio u organismo que haga sus veces;

3.2 Asegurarse de la correcta ejecución tanto de la estrategia, como de la implantación de políticas, metodologías, procesos y procedimientos de la administración integral de riesgos;

3.3 Proponer al directorio o al organismo que haga sus veces los límites específicos apropiados por exposición de cada riesgo;

3.4 Informar oportunamente al directorio u organismo que haga sus veces respecto de la efectividad, aplicabilidad y conocimiento por parte del personal de la institución, de las estrategias, políticas, procesos y procedimientos fijados;

3.5 Conocer en detalle las exposiciones de los riesgos asumidos en términos de afectación al patrimonio técnico y con relación a los límites establecidos para cada riesgo;

3.6 Aprobar, cuando sea pertinente, los excesos temporales de los límites, tomar acción inmediata para controlar dichos excesos e informar inmediatamente tales asuntos al

directorio u organismo que haga sus veces;

3.7 Proponer al directorio u organismo que haga sus veces la expedición de metodologías, procesos, manuales de funciones y procedimientos para la administración integral de riesgos;

3.8 Aprobar los sistemas de información gerencial, conocer los reportes de posiciones para cada riesgo y el cumplimiento de límites fijados, y adoptar las acciones correctivas según corresponda;

3.9 Analizar y aprobar los planes de contingencia; y,

3.10 Las demás que determine el directorio o el organismo que haga sus veces, o que sean dispuestas por la Superintendencia de Bancos y Seguros.

ARTICULO 4.- El Banco Central del Ecuador, las instituciones financieras públicas y privadas, las compañías emisoras y administradoras de tarjetas de crédito y las compañías de arrendamiento mercantil, deben contar con una unidad de riesgos, la cual estará bajo la supervisión y dirección del comité de administración integral de riesgos y tendrá la responsabilidad de vigilar y asegurar que las áreas de negocios estén ejecutando correctamente la estrategia, políticas, procesos y procedimientos de administración integral de riesgos.

Las principales funciones de la unidad de riesgos, son:

4.1 Proponer al comité de administración integral de riesgos de la entidad las políticas, de riesgos para la institución, de acuerdo con los lineamientos que fije el directorio u organismo que haga sus veces;

4.2 Elaborar y someter a consideración y aprobación del comité de administración integral de riesgos la metodología para identificar, medir, controlar / mitigar y monitorear los diversos riesgos asumidos por la institución en sus operaciones;

4.3 Velar por el cumplimiento de los límites de exposición al riesgo y los niveles de autorización dispuestos;

4.4 Revisar de forma sistemática las exposiciones por tipo de riesgos respecto de los principales clientes, sectores económicos de actividad, área geográfica, entre otros;

4.5 Diseñar un sistema de información basado en reportes objetivos y oportunos, que permitan analizar las posiciones para cada riesgo y el cumplimiento de los límites fijados; e, informar periódicamente al comité de administración integral de riesgos;

4.6 Preparar estrategias alternativas para administrar los riesgos existentes y proponer al comité los planes de contingencia que consideren distintas situaciones probables, según corresponda;

4.7 Implantar de manera sistemática en toda la organización y en todos los niveles de personal las estrategias de comunicación, a fin de entender sus responsabilidades con respecto a la administración integral de riesgos;

4.8 Calcular las posiciones de riesgo y su afectación al patrimonio técnico de la entidad;

4.9 Analizar la incursión de la institución del sistema financiero en nuevos negocios, operaciones y actividades acorde con la estrategia del negocio, con sujeción a las disposiciones legales, normativas y estatutarias, en cumplimiento del proceso de administración integral de riesgos;

4.10 Analizar el entorno económico y de la industria y sus efectos en la posición de riesgos de la institución, así como las pérdidas potenciales que podría sufrir ante una situación adversa en los mercados en los que opera; y,

4.11 Las demás que determine el comité de administración integral de riesgos de la entidad.

ARTICULO 5.-El número de miembros o vocales del comité y de la unidad de que trata el presente capítulo, deberá guardar proporción con la naturaleza, complejidad y volumen de los negocios, operaciones y actividades desarrollados por la institución. Estos organismos estarán dotados de manera permanente de los recursos administrativos y tecnológicos necesarios para el cumplimiento de sus funciones, y, estarán conformados por personas idóneas que deben acreditar un alto conocimiento y experiencia, en materia de gestión y control de riesgos y capacidad de comprender las metodologías y procedimientos utilizados en la institución para medir y controlar los riesgos asumidos y por asumir, de manera tal que garanticen el adecuado cumplimiento de sus funciones.

Las instituciones del sistema financiero podrán crear subunidades de riesgo especializadas cuyo funcionamiento se regirá por las disposiciones de este capítulo, atendiendo la naturaleza de su función.

ARTICULO 6.- Los miembros del comité y unidad responsables de la administración integral de riesgos, serán independientes de las áreas de gestión comercial y operativa de la institución, con excepción del funcionario a que se refiere el numeral 2.2 del artículo 2, de la sección III de este capítulo, que forma parte del comité de administración integral de riesgos.

ANEXO 8

MACROPROCESO

FRONT OFFICE

	PROCESO	SUBPROCESO	EVENTOS	ACTIVIDADES CRITICAS
1	PROMOCION	Contacto y difusión producto	RRHH	Destrucción o perdida intencional de documentos
2	FORMACION BANCO COMUNAL O GRUPO DESARROLLO	Formación de grupo	RRHH	Ingreso de información errónea del cliente
		Entrega documentación	RRHH	Entrega errónea de documentación
		Verificación información y referencias	RRHH	Errores en la revisión de información de los clientes
			FRAUDE INTERNO	Manipulación de la información
			FRAUDE EXTERNO	Información falsa
3	CREDITO INDIVIDUAL	Entrega documentación	FRAUDE INTERNO	Manipulación de la información Destrucción o perdida intencional de documentos
			FRAUDE EXTERNO	Información falsa
		Verificación información y referencias	RRHH	Reportar actividades inexistentes sin previa visita
			FRAUDE EXTERNO	Información falsa
		Verificación de garantías	RRHH	Fallas en chequeo de información
			FRAUDE INTERNO	Manipulación de la información
			FRAUDE EXTERNO	Información falsa
4	PREPARACION DOCUMENTACION	Legalización, verificación documentación	FRAUDE INTERNO	Manipulación de la información
			FRAUDE EXTERNO	Información falsa
		Recepción garantías	FRAUDE INTERNO	Manipulación de la información
		Requisiciones	RRHH	Entrega de información errónea
5	APROBACION OPERACIÓN	Aprobación de Comité	RRHH	Entrega de información errónea
		Entrega de crédito	RRHH	Demora en entrega de crédito - anulación de cheque Emision de cheques equivocados - anulaciones
6	RECUPERACION	Visitas para cobro pagos	FRAUDE EXTERNO	Manipulación de documentos
		Cuadre de pagos con hoja fiscal	RRHH	Ingreso erroneo de valores
			FRAUDE INTERNO	Manipulación de la información
			FRAUDE EXTERNO	Manipulación de valores
			FALLAS INFORMATICAS	Pérdidas, errores, o problemas con base de datos
		Recuperaciones	RRHH	Fallas en proceso de cobros y recuperaciones
			FRAUDE INTERNO	Manipulación de la información
			FRAUDE EXTERNO	Manipulación de documentos
		Ejecución garantías	RRHH	Fallas en elaboración de actas de remates de prendas
		Cierre ciclo	RRHH	No verificación de documentos
			FRAUDE EXTERNO	Robos ficticios Socios fugados Falsificación de información
7	OTROS FRONT OFFICE	Entrega de información a otras áreas	RRHH	Entrega de información errónea
				Retraso en entrega de información
		Inicio de DPF's	RRHH	Inadecuada tramitación de operación en el sistema No hacer caso a las advertencias que da el sistema respecto al cliente
		Cancelación de DPF's	FRAUDE EXTERNO	Información falsa

MACROPROCESO

MIDDLE OFFICE

	PROCESO	SUBPROCESO	EVENTOS	ACTIVIDADES CRITICAS
1	AUDITORIA	Revisión de procesos y procedimientos	RRHH	Entrega errónea de documentación Ingreso de información errónea del cliente Inadecuada planificación
		Emisión de reportes	RRHH	Entrga de informes incompletos e inoportunos
		Seguimiento de justificación y/o cumplimiento	RRHH	Omisión de seguimientos No dar adecuada importancia a eventos sucitados
2	RIESGOS	Reportes a entidades de control	RRHH	Entrega de información errónea Retraso en entrega de información
			FALLAS INFORMATICAS	Fallas en generación de informacion para reportes
		Evaluación de Riesgos	RRHH	Digitación errónea de información
			FALLAS INFORMATICAS	Fallas en generación de reportes
		Medición y control de riesgos	RRHH	Digitación errónea de información
			FALLAS INFORMATICAS	Fallas en generación de informacion para reportes
		Multas	RRHH	Entrega tardía de documentos

MACROPROCESO

BACK OFFICE

	PROCESO	SUBPROCESO	EVENTOS	ACTIVIDADES CRITICAS
1	OPERACIONES	Recepción de documentación de operaciones	RRHH	Ingreso de información incorrecta
			FRAUDE INTERNO	Manipulación de la información
		Revisión de documentación	RRHH	Fallas en chequeo de información
		Ingreso al sistema operación nueva	RRHH	Ingreso de información errónea de la operación
			FRAUDE INTERNO	Manipulación de la información
		Impresión documentos	RRHH	Impresión de documentos equivocados
			FALLAS INFORMATICAS	Problemas de impresión por problemas informáticos
		Entrega carpetas a Comité	RRHH	Entrega errónea de documentación
		Aprobación de Trámites	RRHH	Fallas en revisión de la información
			FALLAS INFORMATICAS	Fallas en el sistema
		Desembolsos	RRHH	Falla en ingresos de códigos
2	CONTABILIDAD	Contabilización operaciones	RRHH	Ingreso de información incorrecta
		Contabilización pagos recibidos	RRHH	Fallas en chequeo de información Ingreso de información errónea
		Otras contabilizaciones	RRHH	Fallas en chequeo de información Ingreso de información errónea
		Conciliación contable	RRHH	Documentación incorrecta Fallas en chequeo de información Ingreso de información errónea del cliente
			FRAUDE INTERNO	Manipulación de la información Manipulación de valores Manipulación de documentos Perdida intencional de documentos
			FRAUDE EXTERNO	Pérdida intencional de documentos Información falsa Manipulación de valores Manipulación de documentos Cobros por manejo administrativo de los bancos
		Emisión cheques	RRHH	Retraso en entrega de documentación Entrega incompleta de documentación Entrega errónea de documentación Ingreso de información errónea del cliente
			PROCESOS	Devolución de cheques a destiempo por no tener en cuenta el proceso
		Declaración Impuestos	RRHH	Entrega a destiempo de información y error en los valores a declarar
3	ADMINISTRACION	Administración nómina y políticas RRHH	FRAUDE EXTERNO	Información falsa
			RECLAMOS LABORALES	Conflictos por accidentes laborales Conflictos por compensaciones, beneficios, despidos, etc
		Contratación personal nuevo	RRHH	Retraso en la búsqueda y selección de nuevo personal
			FRAUDE EXTERNO	Información falsa
		Carpetas individuales personal	RRHH	Recepción de documentación erronea
		Entrenamiento, evaluaciones	RRHH	Falta de capaciatción a los empleados
		Contrataciones con terceros	RRHH	Contrataciones sin sustentos necesarios Omisión de información en contratos
			RECLAMOS LABORALES	Conflictos por accidentes laborales Conflictos por compensaciones, beneficios, despidos, etc
4	ACTIVOS Y PROVEEDURIA	Manejo de activos fijos	RRHH	Fallas en chequeo de información Errores en pagos a terceros Fallas en chequeo de inventarios
			DAÑOS ACTIVOS FIJOS	Mala utilización de los equipos
		Manejo y control proveeduría	RRHH	Fallas en chequeo de inventarios
			DAÑOS ACTIVOS FIJOS	Mala utilización de los equipos
5	OTROS BACK OFFICE	Manejo de caja chica	RRHH	Inadecuado control de los respaldos de fondos entregados Inadecuado manejo de dinero
			FRAUDE INTERNO	Manipulación de la información
		Manejo y control archivos	RRHH	Inadecuado manejo del archivo-pérdida de documentos
6	SISTEMAS	Administración de la red y sistemas	FALLAS INFORMATICAS	Interrupción sistemas eléctricos Interrupción por falla en hardware / software
		Soporte técnico a usuarios	RRHH	Asistencia inoportuna en resolución de problemas
		Comunicaciones	FALLAS INFORMATICAS	Problemas con conección de red

ANEXO 9

RIESGO OPERACIONAL
BITACORA DE CAPTURA DE DATOS PARA ELABORACION DE MAPA DE RIESGO

SUCURSAL		INGRESE SUCURSAL
RESPONSABLE		
MES DE REPORTE		INGRESE MES DE REPORTE

DESCRIPCION DEL EVENTO	*CAUSAS APARENTES DEL EVENTO*	*MACROPROCESO*	*PROCESO*	*SUBPROCESO*	*ESTIMACION MONETARIA DE PERDIDA (U$S)*

FINCA S.A | EVENTOS | PROCESOS

ANEXO 10

ACTIVIDADES GENERADORAS DE PÉRDIDAS	
1	Asistencia inoportuna en resolución de problemas
2	Cobros por manejo administrativo de los bancos
3	Conflictos por accidentes laborales
4	Conflictos por compensaciones, beneficios, despidos, etc
5	Contrataciones sin sustentos necesarios
6	Demora en entrega de crédito - anulación de cheque
7	Destrucción o perdida intencional de documentos
8	Devolución de cheques a destiempo por no tener en cuenta el proceso
9	Digitación errónea de información
10	Documentación incorrecta
11	Emision de cheques equivocados - anulaciones
12	Entrega a destiempo de información y error en los valores a declarar
13	Entrega de información errónea
14	Entrega errónea de documentación
15	Entrega incompleta de documentación
16	Entrega tardía de documentos
17	Entrga de informes incompletos e inoportunos
18	Errores en la revisión de información de los clientes
19	Errores en pagos a terceros
20	Falla en ingresos de códigos
21	Fallas en chequeo de información
22	Fallas en chequeo de inventarios
23	Fallas en el sistema
24	Fallas en elaboración de actas de remates de prendas
25	Fallas en generación de informacion para reportes
26	Fallas en generación de reportes
27	Fallas en proceso de cobros y recuperaciones
28	Fallas en revisión de la información
29	Falsificación de información
30	Falta de capaciatción a los empleados
31	Impresión de documentos equivocados
32	Inadecuada planificación
33	Inadecuada tramitación de operación en el sistema
34	Inadecuado control de los respaldos de fondos entregados
35	Inadecuado manejo de dinero
36	Inadecuado manejo del archivo-pérdida de documentos
37	Información falsa
38	Ingreso de información errónea
39	Ingreso de información errónea de la operación
40	Ingreso de información errónea del cliente
41	Ingreso de información incorrecta
42	Ingreso erroneo de valores
43	Interrupción por falla en hardware / software
44	Interrupción sistemas eléctricos
45	Mala utilización de los equipos
46	Manipulación de documentos
47	Manipulación de la información

48	Manipulación de valores
49	No dar adecuada importancia a eventos sucitados
50	No hacer caso a las advertencias que da el sistema respecto al cliente
51	No verificación de documentos
52	Omisión de información en contratos
53	Omisión de seguimientos
54	Perdida intencional de documentos
55	Pérdidas, errores, o problemas con base de datos
56	Problemas con conección de red
57	Problemas de impresión por problemas informáticos
58	Recepción de documentación erronea
59	Reportar actividades inexistentes sin previa visita
60	Retraso en entrega de documentación
61	Retraso en entrega de información
62	Retraso en la búsqueda y selección de nuevo personal
63	Robos ficticios
64	Socios fugados

BIBLIOGRAFIA

- Soler Ramos, Jose, *Gestión de Riesgos Financieros ï Un enfoque práctico para los países latinoamericanos*, Banco Interamericano de Desarrollo, Grupo Santander, 1999.

- V.McKee, Keneth, *Metodología de Riesgos*, Federal Reserve Banks of Dallas USA, 2004.

- Ezequiel, *Bases de Datos y su Aplicación con SQL, Manuales USERS*. MP Ediciones, Buenos Aires 2004.

- Jorion P, *Valor en Riesgo*, Ed. Limusa, 1999.

- Comité de Supervisión Bancaria de Basilea, *Convergencia Internacional de medidas y normas de capital*, Banco de Pagos Internacionales, 2004.

- Comité de Supervisión Bancaria de Basilea, *Aplicación de Basilea II: aspectos prácticos*, Banco de pagos internacionales, 2004.

- Comité de Supervisión Bancaria de Basilea, *Documento de Consulta ï El nuevo Acuerdo de Capital de Basilea*, Banco de pagos internacionales, 2003.

- Price Waterhouse Coopers, ñBIS II, Alcance del Nuevo Acuerdoò, 2004.

- Asociación de Instituciones Financieras del Ecuador; *Seminario Taller ñPapel de la Auditoria interna en la administración del Riesgo Operacionalò*, 2007.

- Asociación de Instituciones Financieras del Ecuador; *Seminario Integral de Riesgo Operacional*, Quito, 2007.

- Procuraduría General de la Nación, *Mapa de Riesgos Institucional*, Bogota, 2005.

- Marco Integrado de Control Interno para Latinoamerica (MICIL), 2004

- Ley Sarbanes-Oxley Act (SOX, SOA)

- Ernst & Young, La Ley Sarbanes -Oxley y la Auditoria, 2004.

- Codificación de Resoluciones de la Superintendencia de Bancos y Seguros y de la Junta Bancaria.

- www.wharton.universia.net/index.cfm

- Sociedad Financiera FINCA S.A

- Apuntes de la cátedra de Normativas Sobre la Gestión de Riesgos Financieros, Maestría en Finanzas y Gestión de Riesgos, Universidad Andina Simón Bolivar, 2007.

- Apuntes de la cátedra de Gestión de Riesgo Operativo, Maestría en Finanzas y Gestión de Riesgos, Universidad Andina Simón Bolivar, 2007.