

**UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL**

FACULTAD DE CIENCIAS ECONOMICAS Y ADMINISTRATIVAS

CARRERA: ADMINISTRACIÓN DE EMPRESAS

TEMA:

**DISEÑO DE UNA METODOLOGÍA PARA LA IDENTIFICACIÓN Y LA MEDICIÓN DEL
RIESGO OPERATIVO EN SOCIEDADES FINANCIERAS EN LA CIUDAD DE GUAYAQUIL**

AUTOR:

Glenn Andrés Pozo Rodríguez

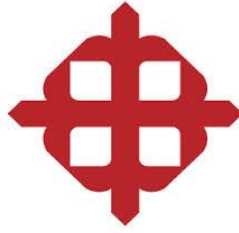
**TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE
INGENIERIA COMERCIAL**

TUTOR:

ING. OMAR MEJIA FLORES Mgs.

Guayaquil, Ecuador

2013



UNIVERSIDAD CATÒLICA

DE SANTIAGO DE GUAYAQUIL

FACULTAD DE CIENCIAS ECONOMICAS Y ADMINISTRATIVAS

CARRERA: Administración de Empresas

CERTIFICACION

Certificamos que el presente trabajo fue realizado en su totalidad por Glenn Andrés Pozo Rodríguez, como requerimiento parcial para la obtención del Título de Ingeniero Comercial

TUTOR

Ing. Omar Gabriel Mejía Flores, Mgs.

REVISORES

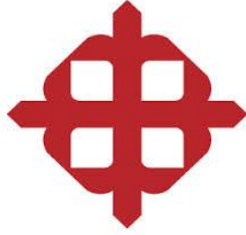
Ing. Wilson Baldeon Barros, Mgs.

Ing. Paola Alexandra Traverso Holguín, Mgs.

DIRECTOR DE LA CARRERA

Ing. Darío Vergara Pereira, Mgs

Guayaquil, a los 24 del mes de Abril del año 2014



UNIVERSIDAD CATÒLICA

DE SANTIAGO DE GUAYAQUIL

FACULTAD DE CIENCIAS ECONOMICAS Y ADMINISTRATIVAS

CARRERA: INGENERIA COMERCIAL

DECLARACIÒN DE RESPONSABILIDAD

Yo, Glenn Pozo

DECLARO QUE:

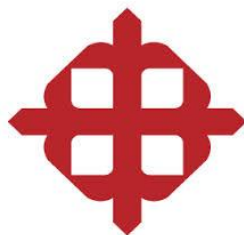
El proyecto de grado denominado TRABAJO DE TITULACIÒN PREVIO A LA OBTENCIÒN DEL TÌTULO DE INGENIERO COMERCIA, .ha sido desarrollado en base a una investigación exhaustiva, respetando derechos intelectuales de tercero conforme las citas que constan al pie de las páginas correspondientes, cuyas fuentes se incorporan en la bibliografía. Consecuente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance científico del proyecto de grado en mención.

Guayaquil, a los 24 del mes de abril del año 2014

EL AUTOR

Glenn Andrés Pozo Rodríguez



UNIVERSIDAD CATÒLICA

DE SANTIAGO DE GUAYAQUIL

FACULTAD DE CIENCIAS ECONOMICAS Y ADMINISTRATIVAS

CARRERA: INGENIERIA COMERCIAL

AUTORIZACIÒN

Yo, Glenn Pozo

Autorizo a la Universidad Católica de Santiago de Guayaquil, la **publicación** en la biblioteca de la institución del proyecto titulado: “TRABAJO DE TITULACIÒN PREVIO A LA OBTENCIÒN DEL TÌTULO DE INGENIERIA COMERCIAL.”, cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y autoría.

Guayaquil, a los 24 del mes de abril del año 2014

EL AUTOR

Glenn Andrés Pozo Rodríguez

Agradecimiento

Primero, quiero agradecer a Dios padre todopoderoso por haberme dado tantas oportunidades en la vida, además por darme la oportunidad de tener vida y sobretodo de tener una madre única en este mundo que desde mi niñez fue padre y madre para mí. Quisiera agradecer por haberme dado fuerza de voluntad de seguir luchando y nunca rendirme a pesar de los obstáculos en mi lucha de la obtención de mi título de Ingeniero Comercial.

También, agradezco a un ser muy especial en mi vida, a mi mejor amiga, a mi madre Alexandra Rodríguez Garcés, por siempre darme su apoyo incondicional y especial ya que sin ella no hubiese conseguido este título de superación personal y profesional en mi vida. Todo se lo debo a ella y nunca podre pagarle todo lo que ella a echo por mi. GRACIAS A TI MAMITA.

Glenn Andrés Pozo Rodríguez

Dedicatoria

En primer lugar debo agradecer sobre todas las cosas a Dios por darme la oportunidad en tener una madre tan comprensiva y única en todos los sentidos. En segundo lugar por darme la valiosa oportunidad de estudiar en una universidad tan prestigiosa como la universidad Católica y sobretodo en poder culminar mis estudios universitarios realizando este proyecto de investigación. Quiero agradecer en especial a mi madre querida la Sra.: Tangge Alexandra Rodríguez Garcés por darme todas las facilidades en poder empezar y culminar mis estudios con tanto esfuerzo y sacrificio, quien como toda madre se sacrifica por el bienestar de sus hijos.

En toda esta etapa universitaria no fue nada fácil el transcurso, aunque mi madre siempre me daba ánimos en seguir adelante y fuerzas para yo nunca rendirme., sin importar cuál sea el obstáculo ya sea de personas o momentos que se presenten hay que superarlos con toda la grandeza y madurez total que se requiera y levantarse cuantas veces sea necesario.

Glenn Andrés Pozo Rodríguez

DECLARACIÓN

“Yo, Glenn Andrés Pozo Rodríguez declaro ser autor del presente trabajo y eximo expresamente a la Universidad Católica de Santiago de Guayaquil y a sus representantes legales de posibles reclamos o acciones legales.”

AUTOR

Glenn Andrés Pozo Rodríguez

AUTORIA

Las ideas expuestas en el trabajo de investigación y que aparecen como propias son en su totalidad de absoluta responsabilidad del autor.

AUTOR

Glenn Andrés Pozo Rodríguez

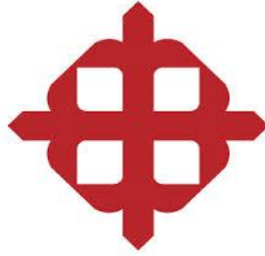
TRIBUNAL DE SUSTENTACIÓN

Ing. Omar Gabriel Mejía Flores

PROFESOR GUIA O TUTOR

Ing. Dario Vergara Pereira, Mgs

PROFESOR DELEGADO



UNIVERSIDAD CATÒLICA

DE SANTIAGO DE GUAYAQUIL

FACULTAD DE CIENCIAS ECONOMICAS Y ADMINISTRATIVAS

CARRERA: INGENERIA COMERCIAL

CALIFICACIÒN

Omar Gabriel Mejía Flores

PROFESOR GUÌA O TUTOR

TABLA DE CONTENIDO

Agradecimiento	V
Dedicatoria	VI
TABLA DE FIGURAS	XIII
TABLA DE GRAFICOS	XIV
Resumen.....	1
Palabras Claves	1
Abstract.....	2
Introducción	3
Justificación y definición del problema	4
Problema	5
Marco Teórico.....	5
Definición de riesgo.....	5
Introducción al Riesgo Operacional.....	7
Acuerdo de requerimiento de capital Basilea II.....	9
Pilar I: el cálculo de los requisitos mínimos de capital	11
Pilar II: el proceso de supervisión de la gestión de los fondos propios	12
Pilar III: la disciplina de mercado	12
Marco legal y metodológico de riesgos operacional definido por la superintendencia de bancos y seguros del ecuador.....	14
Marco Metodológico.....	14
Marco legal de Riesgo Operativo (RO) definido por la Superintendencia de Bancos.....	18
Objetivo	22
Objetivo del estudio	22
Objetivos Generales	22
Objetivos Específicos.....	23
Ámbito del estudio.....	23
Empresas del sector, base del estudio	24
Metodología	24
Metodología para definir el inventario de procesos	24

Proceso de levantamientos de procesos	27
La metodología Coso	30
CAPITULO I.....	31
DISEÑO DE METODOLOGÍAS DE IDENTIFICACIÓN Y MEDICIÓN DE RIESGO OPERACIONAL	31
Definición de líneas de negocio y categorización de fuentes de riesgo	31
Definición de control interno para gestión por procesos identificación de procesos críticos	39
Identificación de puntos de control	40
Definición de Niveles de Seguridad Y Frecuencia para los Eventos de Perdida	42
Pérdida Esperada.....	49
Método del indicador Básico	49
Método Estándar (TSA).....	51
Metodología de Medición Avanzada (AMA)	52
Definición de Frecuencia y Severidad	52
Contenido De La Matriz De Riesgos:	53
Relaciones entre los Eventos de Pérdida y los Indicadores de Riesgo.....	60
Planes de Acción.....	60
Matriz de Monitoreo	61
Reporte de Resultados.....	62
Mapa de Procesos	62
CAPITULO 2	65
ESTRUCTURA ORGANIZACIONAL.....	65
Responsabilidades del directorio en la administración de riesgos	65
Estructura orgánica funcional de la sociedad financiera.....	67
Unidad de riesgos.....	74
CAPITULO 3	79
PRESUPUESTO DE ELABORACIÓN	79
Objetivo del presupuesto del proyecto	79
CONCLUSIONES Y RECOMENDACIONES	91

Análisis de los resultados de la implementación.....	91
Conclusiones	92
Recomendaciones	93
Bibliografía	95
Anexos:	97

TABLA DE FIGURAS

Fig. 1 Gestión de Riesgo Operacional.....	10
Fig. 2 Implementación de Disposiciones SBS	17
Fig. 3 Cadena de Valor de Porter.....	26
Fig. 4 Ejemplo de Proceso Levantado.....	28
Fig. 5 Acuerdo de Capital de Basilea	33
Fig. 6 Ejemplos de Perdidas en Instituciones.....	35
Fig. 7 Metodología de Identificación y Medición de RO.....	38
Fig. 8 Proceso de cuantificación para la recolección de información.....	48
Fig. 9 Formula del Indicador Básico (BIA)	50
Fig. 10 Método Estándar (TSA).....	51
Fig. 11 Ejemplo de Tablas de Frecuencia y Severidad.....	53
Fig. 12 ejemplo de Mapa de Riesgos Operacionales	54
Fig. 9 Estructura Orgánica Funcional	67
Fig. 10 Comité de Administración Integral de Riesgos	69
Fig. 11 Comité de Auditoría.....	71
Fig. 12 Unidad de Riesgos	76

TABLA DE GRAFICOS

Tabla 1 Marco Legal de Riesgo Operacional _____	21
Tabla 2 AUTOEVALUACIÓN DE CONTROLES _____	44
Tabla 3 TABLEROS DE CONTROL _____	44
Tabla 4 Probabilidades en cinco categorías _____	55
Tabla 5 Probabilidades en 3 Categorías _____	56
Tabla 6 Impacto cinco categorías _____	56
Tabla 7 Impacto tres categorías _____	57
Tabla 8 Severidad del Riesgo cinco Categorías _____	58
Tabla 9 Severidad del riesgo tres categorías _____	59
Tabla 10 Exposición al Riesgo _____	62
Tabla 11 Nivel de Exposición al Riesgo _____	63

Resumen

La administración integral de riesgos operacionales y su implementación como modelo de gestión nos permitirán gestionar los diferentes eventos de riesgos y poder mitigarlos de una manera ordenada con sus respectivos derivados y colaterales. Adicional a esto nos permitirá medir el requerimiento de capital mínimo que se podría obtener para sí provisionar este valor en el tiempo para su posterior derivación. Estas metodologías nos permiten conjuntamente con los acuerdos de capital de Basilea II y las metodologías de control interno optimizar los procesos de la empresa tanto en personas como en flujo operativo como en tecnologías de operación. Cabe recalcar que al aplicar “controles”, a los procesos no necesariamente implica una automatización o desarrollo en el scorebusiness de la institución, más bien está ligada a controles de auditoría y gestión de información llevados por formularios y cuestionarios. Basilea II nos guía a seguir mejores prácticas a los procesos internos de la empresa pero no nos asegura su efectividad debido a que toda la organización debe poseer una cultura orientada a riesgos y un gobierno corporativo “saludable” para una buena toma de decisiones. Tomando en cuenta el interés más importante de entidades financieras del país y entidades reguladoras como el Comité de Basilea en el desarrollo del proceso de gestión del riesgo operacional, esta tesis desarrolla un estudio metodológico estructurado para la identificación y cuantificación del riesgo operativo en sociedades financieras, basado en modelos de simulación y se la traslada en la aplicación de una sociedad financiera ecuatoriana llamada GLOBAL FINANCIERA.

Palabras Claves

Liquidez, Solvencia, Suspensión de pago, Rentabilidad, Cash-flow, Riesgo Operacional, Fraude interno, Fraude externo, Comité de Basilea, Blanqueo de capitales, Tasa de descuento.

Abstract

The comprehensive operational risk management and its implementation as a management model will allow us to manage the different events and to mitigate risks in an orderly manner with their respective derivatives and collateral. Additional to this will allow us to measure the minimum capital requirement that could be obtained for this value if provisioned in time for later referral. These methodologies allow us to jointly agreements with Basel II capital and internal control methodologies optimize business processes in both humans and in operating cash flow and operating technologies. It should be noted that applying "controls", processes automation does not necessarily imply scorebusiness or development in the institution, it is rather linked to audit controls and management information carried by forms and questionnaires Basel II leads us to follow best practices to internal business processes, but does not ensure its effectiveness because all the organization must have a risk -oriented and a "healthy" corporate governance for good decision -making culture. Taking into account the important interests of local financial institutions and regulatory bodies such as the Basel Committee in developing the process of operational risk management , this thesis develops a structured methodological study for the identification and quantification of operational risk in financial companies, model-based simulation and the moves in the implementation of an Ecuadorian holding company called GLOBAL FINANCIAL .

Keywords

Liquidity, Solvency, Stop payment, profitability, cash flow, operational risk, internal fraud, external fraud, Basel Committee, Money laundering, discount rate.

Introducción

El sistema financiero ecuatoriano en la actualidad debido a los diversos controles ejercidos por las entidades de regulación se ve en la obligación de mejorar, crear controles y metodologías para que sus modelos de negocios sean eficientes. Uno de estos procesos por decir el más importante de la organización es la administración integral de riesgos.

Definiendo así el “riesgo” que conlleva proponer nueva líneas de negocio proyectos u operaciones para crear valor y rentabilidad del negocio. El estudio del riesgo financiero nos permitirá crear herramientas que nos ayuda a gestionar los diferentes niveles de ejecución de los procesos organizativos de la institución.

La administración del Riesgo Operacional se diferencia del manejo de las otras clases de riesgos, debido a que anula cualquier limitación, segrega cualquier amenaza o problema dentro de los procesos inherentes a las operaciones de las instituciones financieras y a través de la determinación de metodologías para buscar proteger y fortalecer los procesos internos de la institución ante la presencia de pérdidas económicas por la exposición al riesgo.

El desarrollo del concepto del riesgo operacional es innovador por ello se recomienda observar las mejores prácticas establecidas por el Comité de Basilea II para su mejor administración. A partir del 2001, el Comité de Basilea incorpora de manera general, los requerimientos para este tipo de riesgo bajo una definición de las mejores prácticas de entidades líderes en el proceso de cuantificación del Riesgo Operacional, considerando una visión internacional integral del riesgo.

Este desarrollo metodológico será y servirá común un servicio estándar para cualquier tipo de empresa, sea esta en el sector PYMES o en las grandes empresas. También cabe recalcar que la empresa que desee adquirir nuestro servicio podrá comprarlo o a su vez contratándonos como empresa de asesoría para medir y disminuir su riesgo operacional por medio de nuestro análisis en esta tesis. (Ver anexo 3).

Justificación y definición del problema

Las empresas en la actualidad se manejan en un mercado competitivo, por ende siempre están expuestas a diferentes tipos de riesgo, por ende la institución debe gestionar el riesgo operativo, como elemento fundamental de una administración preventiva de diversos eventos y factores para que reduzca al mínimo la posibilidad de pérdidas e mejore internamente sus procesos internos, para lo cual deberá implementar diversos mecanismos, actualizar procesos y contar con personal altamente calificados y que cuente con la suficiente experiencia a fin de mitigar este riesgo alineando sea los parámetros de la resolución por la Junta Bancaria y Superintendencia de Bancos y Seguros: JB-2005-834 de 20 de Octubre del 2005.

Los instrumentos técnicos y metodologías que por ahora están disponibles para ayudar a las organizaciones a medir, controlar y manejar las exposiciones de riesgo están evolucionando exponencialmente, tanto en metodología como en campo de operación, sin embargo, estas herramientas deben de calibrarse y ajustarse con una periodicidad perenne al momento de implementarlas en alguna institución.

Por lo general en el ámbito empresarial una organización siempre está midiendo y controlando sus riesgos debido a que al mitigarlos o en su defecto derivarlos puede obtener una mayor rentabilidad siendo más agresivo con sus operaciones dentro y fuera del ámbito local. Debido a esto, las organizaciones deberán proteger controlar y monitorear sus riesgos a través de técnicas y metodologías de control y sobre todo una cultura orientada al riesgo.

Problema

Según la Resolución JB-2004-834 (SEGUROS, 2004) define que:

Las instituciones del sistema financiero controladas por 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, por ende es de suma importancia que las mismas desarrollen manuales de operatividad y normativos que contemplen las estrategias, políticas, procesos y procedimientos de administración de riesgos que permitan identificar, medir, controlar y monitorear las exposiciones de riesgo que están asumiendo.

Marco Teórico

Definición de riesgo

Entre los procesos varios que toda entidad perteneciente al cualquier tipo de ámbito sea este, financiera, comercial, microempresa etc. Existe la posibilidad de que sus procesos o sus operaciones tengan probabilidades de incurrir en diferentes tipos de riesgos.

Riesgos por definición es el daño o la insuficiencia interna de la organización en los cinco factores incluyentes en la normatividad, ya sean estos por su personal, por la tecnología de información que poseen o como realizan los procesos internos y eventos externos.

Estas “perdidas” como tal representan en realidad lo que la empresa dejaría de percibir económicamente sino se mitigan o se transfieren los mismos, para ello el primer paso que se debería realizar es el de identificar los mismos.

Entre los diferentes tipos de Riesgos que existen se encuentran los siguientes:

1. Riesgos de Mercado, es el riesgo que puede presentarse por fluctuaciones que puedan tener las tasas de interés en diferentes tipos de mercado, ya sean estos el mercado primario o el mercado secundario.
2. Riesgos de Liquidez, es el riesgo que puede presentarse por la deficiencia de valores líquidos a corto plazo, los mismos pueden causar graves inconvenientes en la disposición inmediata de dineros para cubrir los pasivos de la institución.
3. Riesgos de Crédito, es el riesgo que puede presentarse al no destinar o colocar de manera correcta los créditos dependiendo del sector económico y sobre todo al perfil del cliente de la institución.
4. Riesgo Reputacional, es el riesgo que puede presentarse a la pérdida de credibilidad y de imagen del mercado de la institución por diferentes factores, ya sean estos servicios al cliente o calidad del servicio.
5. Riesgo Estratégico, este tipo de riesgo se incurre cuando la estrategia de penetración de mercado de una empresa es errónea y por ende la inversión inicial nunca se recupera, no existe punto de equilibrio
6. Riesgo Legal, este tipo de riesgo puede presentarse por errores, fallas o insuficiencias de documentación legal, o normas que rigen un estado dando lugar al pago de indemnizaciones y pérdidas por vacíos legales.

7. Riesgo Operacional, este riesgo puede presentarse por daño o insuficiencias en personas, procesos o tecnologías de información.

Se eligió el riesgo operacional porque de todos los tipos de riesgo es que usualmente más se incurre en todas las instituciones de todos los tipos de negocio no solo en el sector bancario o financiero. Este estudio define una implementación de una metodología de controles aplicadas a los tres factores más importantes del riesgo operacional como lo son las personas o talento humano, los procesos y la tecnología de información para controlar el riesgo operacional debido a que este tipo de riesgos es el más común y el menos tomado en cuenta en las distintas organizaciones pero el que más conlleva una pérdida económica directa en los activos de la empresa.

Introducción al Riesgo Operacional

El riesgo operacional se ha desarrollado considerablemente a lo largo del tiempo. El término "riesgo operacional" fue mencionado por primera vez después del acontecimiento infame de la bancarrota de Barings Bank, en el cual un comerciante trajo el banco abajo por ocultar futuros y posiciones derivadas en Asia.

Con el nacimiento de la nueva norma llamada Basilea dos en el cual narra que las instituciones tendrán que asignar capital contra este tipo de riesgo, los mismos están siendo presionados por el gobierno corporativo y el ente regulador de control para encontrar y construir metodologías, controles y métricas para modelar, medir y equilibrar el riesgo operacional.

Por tal motivo podemos decir que el riesgo operativo es la falla o insuficiencia en factores como personas, procesos y Tecnología de Información que produzcan pérdidas inesperadas. El riesgo está asociado a todos estos aspectos antes mencionados y cubren dos aspectos claves:

- a. El modelo y la definición de los procesos de negocios.
- b. La habilidad de mantener sin efecto a todos los posibles eventos externos e internos.

Para cumplir y lograr un marco de gestión del Riesgo Operacional se debe de enfocar en lo siguiente:

1. Cultura orientada a Riesgos

Implementación de una cultura orientada al control interno, su importancia y campo de acción.

2. Análisis Cualitativo de Información de Controles

- a. Definición, construcción e implementación de indicadores y auto-evaluaciones.
- b. Creación de una estructura organizativa vertical en base a funciones (Organigrama funcional).
- c. Identificación, medición y mitigación de riesgos, mapa de riesgos y controles.

3. Análisis Cuantitativa de Información de Controles

- a) Cálculo del capital requerido con modelos estadísticos.
- b) Desarrollo del modelo de cuantificación.
- c) Captura de datos en la base de eventos de riesgo

Acuerdo de requerimiento de capital Basilea II

El Riesgo operacional se origina de la necesidad de mitigar las pérdidas económicas de la organización por errores en los procesos operativos, dicho tipo de riesgo se definió como un serio problema de pérdidas de dinero por no tenerlo debidamente controlado.

Por ende en la ciudad europea de Suiza, varios países reunidos incorporaron en un acuerdo los diferentes puntos de conversatorio para realizar un tratamiento a este tipo de Riesgo y poder así llegar al objetivo.

Este Acuerdo de Capital es conocido como Basilea II, aquí varios países como Bélgica, Canadá, Alemania, Japón, EEUU etc. usan sus políticas, procesos y procedimientos para divulgarlas entre los países que poseen este tipo de riesgos para mejorar el manejo financiero para ello emiten “Mejores Prácticas” en todos los tipos de Riesgo que existen.(ver anexo 3)

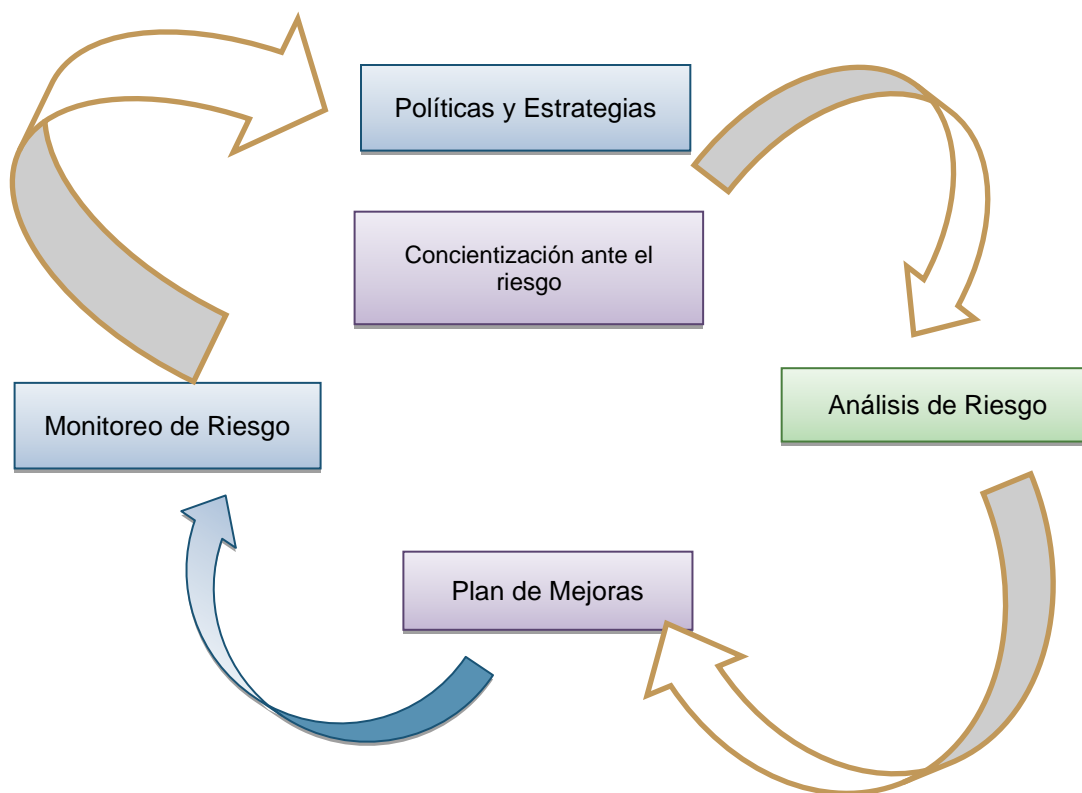


Fig. 1 Gestión de Riesgo Operacional

Fuente: Ilustración tomada de artículo “Acuerdo de Basilea”

Elaborado por: Imagen de Comité de Basilea II

Este “requerimiento de capital “debe cubrir (provisional) todos los diferentes tipos de riesgos como son los de crédito, mercado y demás, cada uno de estos riesgos se mide con lineamientos definidos por la Superintendencia de Bancos y Seguros. El ente regulador fundamenta sus resoluciones en base a las recomendaciones resumidas en “Pilares”, en el año 2005 Basilea II en el cual se divulgó un nuevo conjunto de recomendaciones las cuales las resumimos a continuación:

Pilar I Cálculo De Los Requisitos Mínimos De Capital

Pilar II El Proceso De Supervisión De La Gestión De Los Fondos Propios

Pilar III La Disciplina De Mercado

Pilar I: el cálculo de los requisitos mínimos de capital

Este pilar es por así decirlo el más importante en todo este acuerdo porque define específicamente cuanto se debe de provisionar en términos económicos para asumir el riesgo que conlleva el tratamiento inadecuado de los factores de riesgo en la organización.

“La norma considera: (riesgo de crédito + riesgo de mercado+ riesgo de tipo de cambio + riesgo operacional)”

El riesgo operacional se calcula multiplicando los ingresos por un porcentaje que puede ir desde el 12% hasta el 18% según el tipo de negocio que sea, para entidades financieras se toma el 18% para el cálculo de este valor. Para llegar a definir este valor, la institución deberá realizar modelos estadísticos para definir una metodología de cálculo interna y acorde a su realidad para llegar a medirlo y establecer así según su comportamiento el valor que deberá provisionar y mitigar.

Pilar II: el proceso de supervisión de la gestión de los fondos propios

Los organismos de control en el sistema financiero y comercial, ya sean estos Superintendencia de Compañías, Superintendencia de Bancos, SRI etc., están capacitados para incrementar el nivel de riesgo exigido a las instituciones del sistema financiero bajo su supervisión.

Adicionalmente a ello, se debe de certificar tanto los métodos estadísticos definidos para poder realizar sus diferentes tipos de pronósticos sobre la información requerida por los mismos organismos de control. Para poder validar los métodos estadísticos, los bancos estarán obligados a almacenar datos de información crediticia durante periodos largos, de 5 a 7 años, a garantizar su adecuada auditoría y a superar pruebas de "stress testing" que por su significado en español significa "metodología de verificación de ventanas de tiempo de datos en estadística..

Estas bases de datos deberán ser analizadas por este análisis de stress el cual describe y prueba la calidad de los diferentes modelos de series de tiempo que se construirán en base a la información almacenada y así lograr predecir los diferentes eventos de pérdida las cuales causen deficiencias económicas a la institución

Pilar III: la disciplina de mercado

El tratado de Basilea estableció normas de transparencia en todos los procesos críticos de las instituciones por lo mismo se exigió la publicación periódica del acuerdo y la información de los papeles de trabajo cuyos objetivos son:

1. Establecimiento de buenas prácticas de entidades del sistema financiero para así establecer un marco de ponderación para las diferentes evaluaciones de las instituciones.
2. La transparencia financiera a través de la homogeneización de los informes de riesgo publicados por las instituciones.

Este acuerdo se ha ido implementando en más de 100 países obteniendo excelentes resultados en el tema económico, y de procesos. Las entidades reguladoras en el sistema financiera en el tema de la disciplina del mercado han creado regulaciones y normativas para “normar” el comportamiento tanto crediticio como el de resultados para que el público en general pueda discernir entre que institución poder dejar su dinero, invertir, o tener la factibilidad de obtener una operación crédito.

Para este efecto todas las instituciones del sistema financiero deben de enviar la información financiera para que la superintendencia de bancos registre dicha información y mediante boletines mensuales publique los mismos a través de la página web del ente regulador de control.

Marco legal y metodológico de riesgos operacional definido por la superintendencia de bancos y seguros del ecuador

Marco Metodológico

Por lo general se lo puede definir al Riesgo Operacional como un tipo de riesgo que se encuentra inherente en los diferentes procesos que generan valor a las organizaciones del país. Dichas pérdidas son causadas principalmente por insuficiencias en procesos internos y de negocio que estén dentro de la cadena de valor de producción, así como en las personas que deben de controlar los mismos y la tecnología de información que nos brinda un apoyo directo en este control.

El Riesgo Operacional y su administración se diferencia de los demás riesgos ya sean estos los de mercado o los de crédito, debido a que su consecución como tal se genera directamente del proceso que lo controla mas no de un resultado a corto plazo que se pueda evaluar, así mismo se puede determinar diferentes mecanismos de control para fortalecer la inversión de las instituciones, definir una cultura organizacional orientada a la mitigación de errores y así crear un gobierno corporativo que define políticas para el mejoramiento continuo.

El desarrollo de control del Riesgo operacional nace del acuerdo de Basilea por lo cual se toma como marco de referencia para su implementación, aunque no especifica el cómo, cada institución debe de definir la forma de implementarlo bajo ciertos lineamientos, así como buscar empresas líderes que hayan realizado ya dicho proceso y construir en base a experiencias medir o cuantificar este riesgo considerando el objetivo de Administración de Riesgos financieros.

Bajo esta perspectiva, la Superintendencia de Bancos y Seguros del Ecuador ha desarrollado principios, normativas resoluciones y demás dictámenes para “normalizar” a las entidades a que deben de implementarlo, tal como lo exigen las auditorias in-situ (en el lugar del cliente) y extra-situ (fuera del cliente) en las cuales la exigencia de control de este riesgo es alto. Las actividades que realiza la administración de riesgos operacionales deberán ser consideradas

Desarrollar un trabajo amplio con sinergia entre las diferentes áreas de la organización afirma una eficacia operacional, en donde se nivelan los probables sucesos de riesgos operativos. Por lo cual se constituyen los diferentes tipos de riesgos a los que se ha incidido y se los gestiona con cierta ayuda de un instrumento importante de control, que comúnmente será llamado de aquí en adelante como metodología de control COSO que por sus siglas en inglés (Committe of Sponsoring Organizations). Con esta herramienta se podrá tener un mejor y buen manejo del control interno en los procesos de la cadena del valor de la sociedad financiera.

Por este motivo en este trabajo de investigación se diseñara una metodología de control en base a las normativas de los entes reguladores de control y normas internacionales para mitigar los daños o insuficiencias dadas por este tipo de riesgos.

La Superintendencia de Bancos definió para el sistema financiero una resolución JB-2005-834 de 20 de octubre del 2005 (ver anexo 4), en donde las entidades bancarias deben gestionar el riesgo operativo como el elemento fundamental de una administración preventiva que reduzca al mínimo la posibilidad de pérdidas e incremente su eficiencia, para lo cual deberá implantar mecanismos, procesos y contar con recursos humanos calificados y experimentados a fin de mitigar este riesgo tomando en cuenta lo siguiente:

“Que en el subtítulo VI “De la gestión y administración de riesgos”, del título VII “De los activos y de los límites de crédito”, de la Codificación de Resoluciones de la Superintendencia de Bancos y Seguros y de la Junta Bancaria, consta el capítulo I “De la gestión integral y control de riesgos”;

La Superintendencia de Bancos y Seguros debe propender a que las instituciones del sistema financiero cuenten 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 del público, de acuerdo a lo señalado en el artículo 1 de la Ley General de Instituciones del Sistema Financiero;

Que entre los riesgos frecuentes a las que están expuestas las instituciones del sistema financiero en el desarrollo de sus actividades se encuentra el riesgo operativo;

Que es necesario establecer estándares mínimos prudenciales para que las instituciones del sistema financiero administren el riesgo operativo en un ambiente favorable, previo a la medición del mismo para posteriores requerimientos de capital;”

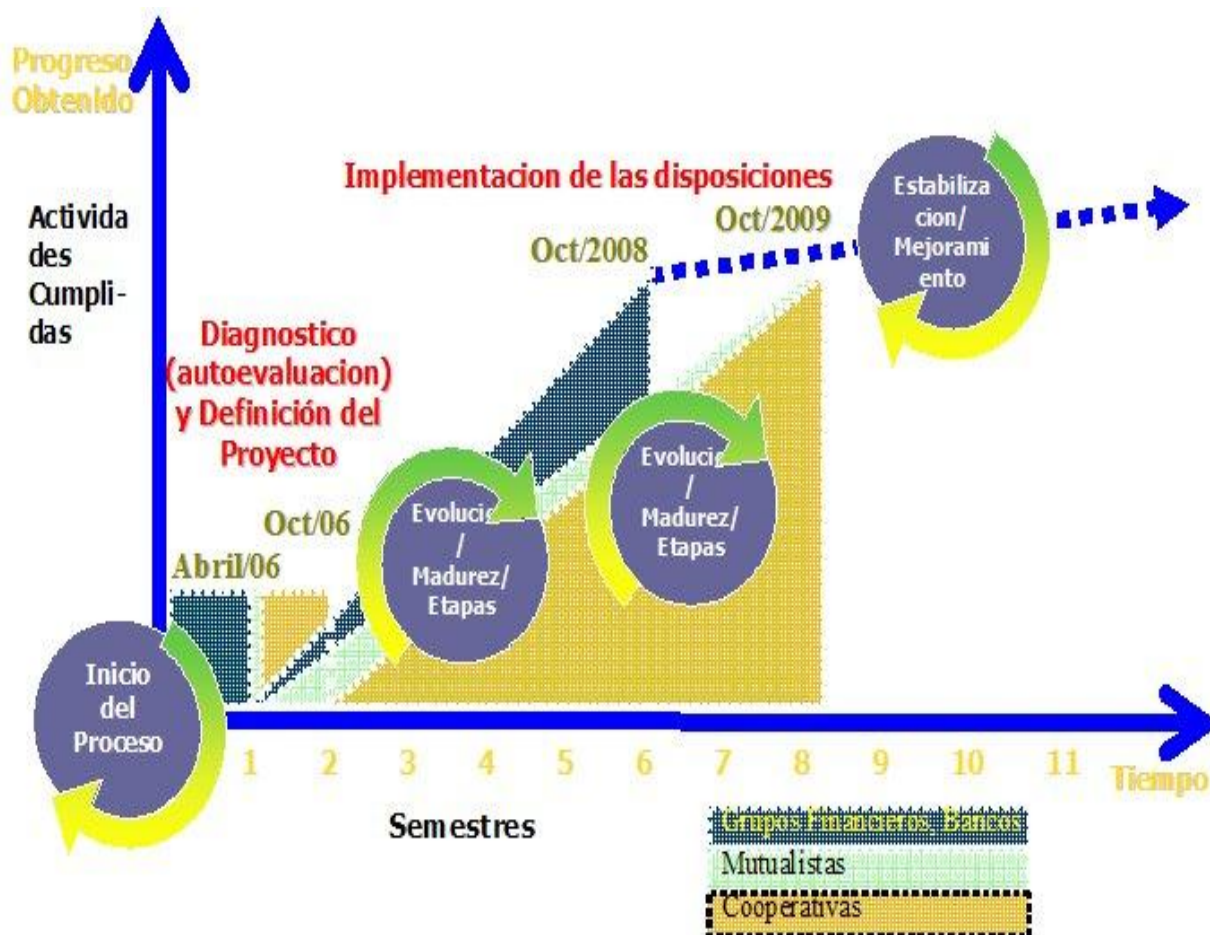


Fig. 2 Implementación de Disposiciones SBS

Fuente: <http://photos1.blogger/2968/3218/1600/figura.0.jpg>

Elaborado por: Superintendencia de Bancos y Seguros (SBS)

De acuerdo con la normativa de la SBS (2005) se define que:

El riesgo operativo incluye el riesgo legal pero excluye los riesgos sistémicos 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.

Marco legal de Riesgo Operativo (RO) definido por la Superintendencia de Bancos.

“El marco legal para la Administración de Riesgos Operacionales está dada por el ente regulador de control, el cual define qué persona o personas son las encargadas de administrar este tipo de riesgos y las políticas procesos y procedimientos de revisión que deben de existir en la institución de la que procede, las mismas se revisarán y actualizará cada año, para garantizar la vigencia y pertinencia de su contenido, la encargada de la revisión y actualización de estas políticas es la Unidad de Administración Integral de Riesgos, la autorización es responsabilidad del Comité Técnico, previa revisión del CAIR; su difusión y reproducción es responsabilidad de la Dirección de Coordinación Técnica y Planeación de la entidad.

El mismo proporciona un marco para la Administración Integral de Riesgos de manera estandarizada para las diferentes Instituciones Financieras independientemente de su forma legal, basada en un sistema de autorregulación dirigido por las propias entidades”.

Los requerimientos definidos por la normativa se reúnen en el cuadro adjunto:

Aspectos de Normativa	Breve Descripción
Administración del Riesgo Operativo (Sección III)	Técnicas o esquemas de administración; códigos de ética y de conducta; supervisión interna; sólida cultura de control interno y adecuados sistemas de control interno; procesos, eventos, fallas e insuficiencias (de procesos, personas, tecnología de información y eventos externos); bases de datos centralizadas para administrar los elementos del riesgo operativo.
Reportes sobre el Riesgo Operativo (Sección III, artículo 9)	Detalle de los eventos de riesgo operativo, el grado de cumplimiento de los procesos, políticas y procedimientos, indicadores de gestión para evaluar la eficiencia y eficacia.
Responsabilidades sobre el Riesgo Operativo (sección V)	Nuevas responsabilidades en la administración de riesgos para el Directorio, Comité de Administración Integral de Riesgos, Unidad de Riesgos. Originales responsabilidades ya fueron establecidas por otra resolución en el 2004.
Procesos (sección II artículo 1.1)	Procesos definidos, clasificados, aprobados, inventariados, difundidos, aplicados, controlados, medidos, evaluados, asignados a un responsable, mejorados continuamente, con la respectiva identificación de cuales son críticos y considerando una adecuada segregación de funciones.
Personas (sección II artículo 1.2)	Identificación apropiada de las fallas o insuficiencias, políticas, procesos y procedimientos técnicos

	<p>definidos para la incorporación, permanencia y desvinculación de las personas, garantizando condiciones laborales idóneas, con información actualizada completa del capital humano.</p>
<p>Eventos Externos (sección II, artículo 1.4)</p>	<p>Oficialmente y estructuradamente se considera la posibilidad de pérdidas derivadas de la ocurrencia de eventos ajenos al control, tales como: - fallas en los servicios públicos, - ocurrencia de desastres naturales, - atentados y - otros actos delictivos.</p>
<p>Tecnología de la Información (sección II, artículo 1.3)</p>	<p>Tecnología de información que garantice la captura, procesamiento, almacenamiento y transmisión de la información de manera oportuna y confiable.</p> <p>Tecnología de información que garantice 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.</p> <p>Políticas, procesos, procedimientos y manuales, definidos y difundidos formalmente, que aseguren una adecuada planificación y administración. Plan Funcional y Plan Operativo. Información con propietario definido, criterios de control interno aplicados para conseguir la eficacia, eficiencia y cumplimiento. Administración controlada de los servicios de terceros. Adecuados controles sobre las aplicaciones. Sistema de Seguridad de la Información implementado, incluyendo adecuada planificación de</p>

	contingencias para la continuidad del negocio, entre otros importantes aspectos asociados a la tecnología de la información.
Continuidad del Negocio (sección IV)	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. Proceso de administración de la continuidad de los negocios.
Servicios Provistos por Terceros (sección VI, disposiciones generales)	Políticas, procesos y procedimientos efectivos que aseguren una adecuada selección y calificación de los proveedores.

Tabla 1 Marco Legal de Riesgo Operacional

Fuente: Normativa de la Superintendencia de Bancos y Seguros

Elaborado por: Superintendencia de Bancos y Seguros

Según lo analizado por (OLAYA T, 2006) menciona que:

Aunque las recomendaciones en la norma son muy claras para los entendidos en el tema, se ha detectado un poco de incertidumbre en algunas instituciones con respecto a cuál será el modelo de referencia específico al implementar los detalles de cada control. Si no se recomienda explícitamente un modelo de referencia, existe el riesgo de que el evaluador externo (Auditores de SBS, Auditores externos, especialistas de Calificadoras de Riesgo, etc.) no coincida con los criterios aplicados internamente, lo cual puede complicar la aceptación de las opiniones y calificaciones, y la percepción sobre el nivel de riesgo.

Un ejemplo de este caso es la referencia a los adecuados sistemas de control interno, Esto sin embargo no resta merito a la SBS sobre los progresos hasta ahora alcanzados en sus normativas, de hecho, la resolución tal como ha sido planteada posiciona al sistema financiero ecuatoriano como el que cuenta con mejores definiciones sobre riesgo operativo en toda Latinoamérica. En todo caso en fechas posteriores la SBS podrá difundir precisiones sobre estos temas y aun estará a tiempo para que las instituciones las contemplen en sus respectivos enfoques.

Objetivo

Objetivo del estudio

Elaboración de una metodología estándar para administración de riesgos operacionales, tanto a nivel de controles como a nivel organizativo y de procesos para aplicarla en una entidad financiera como parte del proyecto de “Gestión de Riesgos Integrales” que por normatividad requiere el organismo de control.

Objetivos Generales

Diseñar de una metodología para la identificación y la medición del riesgo operativo en sociedades financieras.

Objetivos Específicos

1. Identificar y diagnosticar los procesos de control interno
2. Diseñar el mapa de proceso
3. Elaborar la metodología, identificación y medición de riesgo
4. Elaborar el estudio económico financiero del proyecto.

Ámbito del estudio

El alcance o el ámbito del estudio es el manejo de la implementación de la norma JB-2005-834 que indica “de la gestión de Riesgos Operacionales” incluido su alcance en la normativa del año 2011, que indica la creación de bases de datos de eventos de riesgo. (Ver anexo 4)

Sustentabilidad del estudio

El desarrollo de esta implementación sustentara la acción de mitigar medir y controlar los diferentes riesgos operacionales descritos tanto en la norma ecuatoriana definida por el organismo de control y los diferentes acuerdos internacionales que priorizan el control como forma de coexistir por ello llevamos las siguientes premisas a estudiar:

- a) La aplicación de la normatividad vigente, la cual estará definida por la resolución de Riesgo operacional difundida por el ente regulador de control.
- b) La creación de una metodología específica de implementación para la administración de Riesgos operacionales, con sus respectivos sustentos metodológicos, documento que permitirá la correcta gestión de este tipo de riesgo.

- c) Definir las diferentes responsabilidades de cada uno de los funcionarios de la institución para así poder crear un entorno de control acorde a lo implementado y la creación de un gobierno corporativo que alinea a la organización al control.
- d) Definición de políticas, límites, re-ingeniería de procesos y procedimientos para establecer esquemas eficientes y efectivos para la Administración de Riesgos Operacionales.

Empresas del sector, base del estudio

Fuente: Se consideró en el estudio la aplicabilidad de implementar esta metodología de riesgo operacional solamente en Sociedades Financieras del Sistema Financiero Ecuatoriano.

Población: Se analizó la realidad de dos Instituciones Financieras, las cuales se entrevistó a 7 funcionarios tanto del área de procesos como del área de riesgos.

Metodología

Metodología para definir el inventario de procesos

La metodología a usarse para el levantamiento de procesos es la llamada “Gestión por Procesos” la cual (Perez Fernandez, 2009) define como la modelización de los sistemas de un conjunto de procesos interrelacionados mediante vínculos causa-efecto. El propósito final de la Gestión por Procesos es asegurar que todos los procesos de una organización se desarrollan de forma coordinada, mejorando la efectividad y la satisfacción de todas las partes interesadas (clientes, accionistas, personal, proveedores, sociedad en general).

Adicionalmente esto nos lleva a la definición de proceso el cual nos refiere a

“Un conjunto de actividades o eventos (coordinados u organizados) que se realizan o suceden (alternativa o simultáneamente) bajo ciertas circunstancias en un determinado lapso de tiempo. Significados diferentes según la rama de la ciencia o la técnica en que se utilice” (ITESCAM, 2005)

Para definir el inventario de procesos según la metodología “Gestión por Procesos” se debe de realizar lo siguiente:

- 1.- Definir Cadena de Valor del Negocio
- 2.- Realizar los levantamientos de Procesos en base a la metodología de Gestión por Procesos

Definición de cadena de valor

Para una entidad financiera las líneas de negocio son básicamente dos, que son el manejo y administración de créditos y las captaciones que puedan obtener de clientes con los procesos de Depósitos a la vista y depósitos a Plazo.

Según lo analizado por (Porter, 2005) define que “la cadena de valor es un modelo teórico que gráfica y permite describir las actividades de una organización para generar valor al cliente final y a la misma empresa. En base a esta definición se dice que una empresa tiene una ventaja competitiva frente a otra cuando es capaz de aumentar el margen (ya sea bajando los costos o aumentando las ventas).”



Fig. 3 Cadena de Valor de Porter

Fuente: Concepto de la cadena de Valor de Porter 5ta. Edición Administración de Empresas

Elaborado por: Michael Porter

El objetivo de la gestión integral de riesgos operativos es identificar, evaluar, controlar y tratar los riesgos originados por la influencia de factores externos e internos en los procesos críticos de la institución. Según el proceso que se analice, la metodología definida para la gestión del riesgo operacional se enfoca en la totalidad de la institución, una línea de negocio, un proceso operativo o una unidad organizativa.

Proceso de levantamientos de procesos

La metodología de Gestión por procesos realiza la siguiente segmentación para el levantamiento de información a realizarse en la entidad:

Macroproceso; Proceso; Subproceso; Actividad

Macroproceso.- Son un conjunto de procesos que atribuyen metódica y eficazmente a retribuir los requerimientos de una sociedad o entidades con la finalidad de cumplir con los objetivos del estado.

Procesos.- Se define como proceso a la consecución de determinados actos o a su vez al conjunto de actividades relacionadas entre sí, que a su vez se transforman en elementos de entrada en resultados.

Subproceso.-Por definición general un subproceso son aquellos que están dentro de un proceso, es decir tienen como finalidad en formar parte de un proceso grande.

Actividades.- Es un conjunto de acciones que llevan a cabo para cumplir una meta y que están a cargo bajo una administración menor.

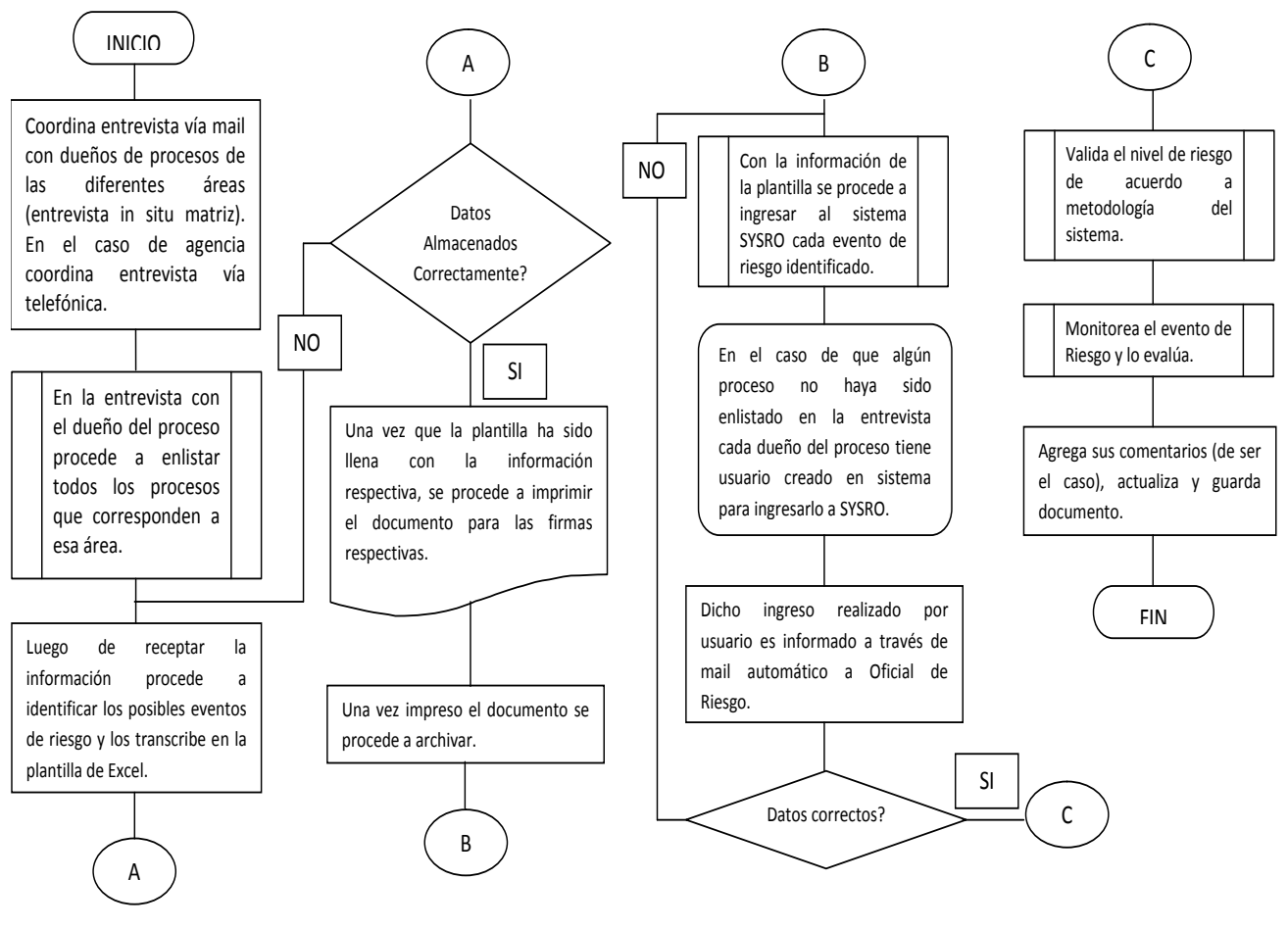


Fig. 4Ejemplo de Proceso Levantado

Fuente: http://blogspot/jhleon/sistema_globalfinanc.com

Elaborado por: AUTOR DE TESIS

Metodología para la identificación de eventos de pérdida

Para definir los diferentes eventos de riesgo debemos de instaurar una metodología de control interno para capturar los eventos por las diferentes líneas de negocio. Esta Metodología debe de mantener un buen gobierno corporativo y poseer diferentes formas de definir controles sobre los procesos adicionalmente deberán cumplirse los siguientes criterios:

- a) La metodología debe ser implementada en toda la empresa en forma consistente.
- b) La empresa debe asignar recursos suficientes para aplicar la metodología en las principales líneas de negocio y en los procesos de control y de apoyo.
- c) La aplicación de la metodología debe estar integrada a los procesos de gestión de riesgos de la empresa.
- d) Deben establecerse incentivos que permitan una mejora continua de la gestión del riesgo operacional.
- e) La aplicación de la metodología de gestión del riesgo operacional debe estar adecuadamente documentada.

La metodología Coso

En esta fase se implementa propiamente la metodología COSO en las áreas de impacto del proceso crítico identificadas en la fase anterior y dentro del ámbito de investigación. Se comienza por realizar entrevistas a los responsables de riesgos de las agencias seleccionadas para identificar eventos de riesgo operativo.

Posteriormente se mide, evalúa y valora el riesgo absoluto en las áreas de impacto. Del mismo modo se determina el nivel de eficiencia de los controles para valorar e identificar el riesgo con control y, como consecuencia, el riesgo residual o riesgo de exposición. La implementación esta metodología COSO consta de seis etapas fundamentales, las cuales serían las siguientes:

- a) Etapa I: Análisis de las áreas de impacto, en esta etapa definimos las áreas críticas donde proceder a verificar el impacto que tienen sobre el negocio.
- b) Etapa II: Identificación de los riesgos absolutos, en esta etapa se definen los riesgos estratégicos y de procesos que de evidencien.
- c) Etapa III: Medición y evaluación, etapa en la cual se desarrollan modelos de medición, para medir el posible requerimiento de capital para proceder a provisionarlo.
- d) Etapa IV: Valoración del riesgo absoluto, en esta etapa se designa el colateral y sobre colateral de la posible pérdida para definir si el mismo se traslada o se lo asume.
- e) Etapa V: Valoración del riesgo con control y del riesgo residual, en esta etapa se definen los diferentes controles para proceder al proceso de mitigación del mismo.
- f) Etapa VI: Monitoreo, etapa por la cual se crean los diferentes reportes e indicadores para poder monitorear todos los procesos y factores de riesgo en personas, procesos y tecnología de información.

CAPITULO I

DISEÑO DE METODOLOGÍAS DE IDENTIFICACIÓN Y MEDICIÓN DE RIESGO OPERACIONAL

Definición de líneas de negocio y categorización de fuentes de riesgo

En este capítulo se establecerán las diferentes anomalías que pueden producir los eventos de riesgo operativo. A lo largo del mismo se desarrollarán definiciones y características propias de cada clase de efecto. El comité de Basilea II según sus mejores prácticas definió una serie de nuevas políticas para las entidades financieras en torno al desarrollo del control de riesgo operacional.

Dichas mejores prácticas se alinean en torno a dos pilares: Control y Monitoreo, los mismos que deben de regir fundamentalmente en las líneas de negocio de la organización. Las líneas de negocio se fundamentan básicamente en la cadena de valor de la organización por ende se debe de analizar que procesos son los que nos generan “valor” para ser tomados en consideración en el estudio de procesos críticos.

“Proceso Crítico: Proceso que afecta de forma directa a la satisfacción del cliente y a la eficiencia económica de la organización. “

Debido a que “afecta” en forma directa los procesos más comunes que existen en una entidad financiera son dos:

- a) Créditos (Ya sea de consumo como comerciales)
- b) Captaciones (Ya sean a la Vista o Depósitos a Plazo)

Por ende las líneas de negocio son Administración del Crédito y Administración de captaciones de Depósitos. Adicionalmente el comité de Basilea II definió una categorización de diferentes fuentes de riesgo, las mismas que estas tipificadas por el factor de riesgo operacional en las que esté definido el evento.

Los diferentes tipos de factores de Riesgo son los siguientes; a) Personas, b) Procesos, c) Tecnología de Información, y d)Eventos Externos.

Según Basilea II para realizar una metodología para identificar y categorizar una posible fuente de riesgos, llámese evento de riesgo por igual, se basa en un esquema de implementación tal como lo indica la figura a continuación:

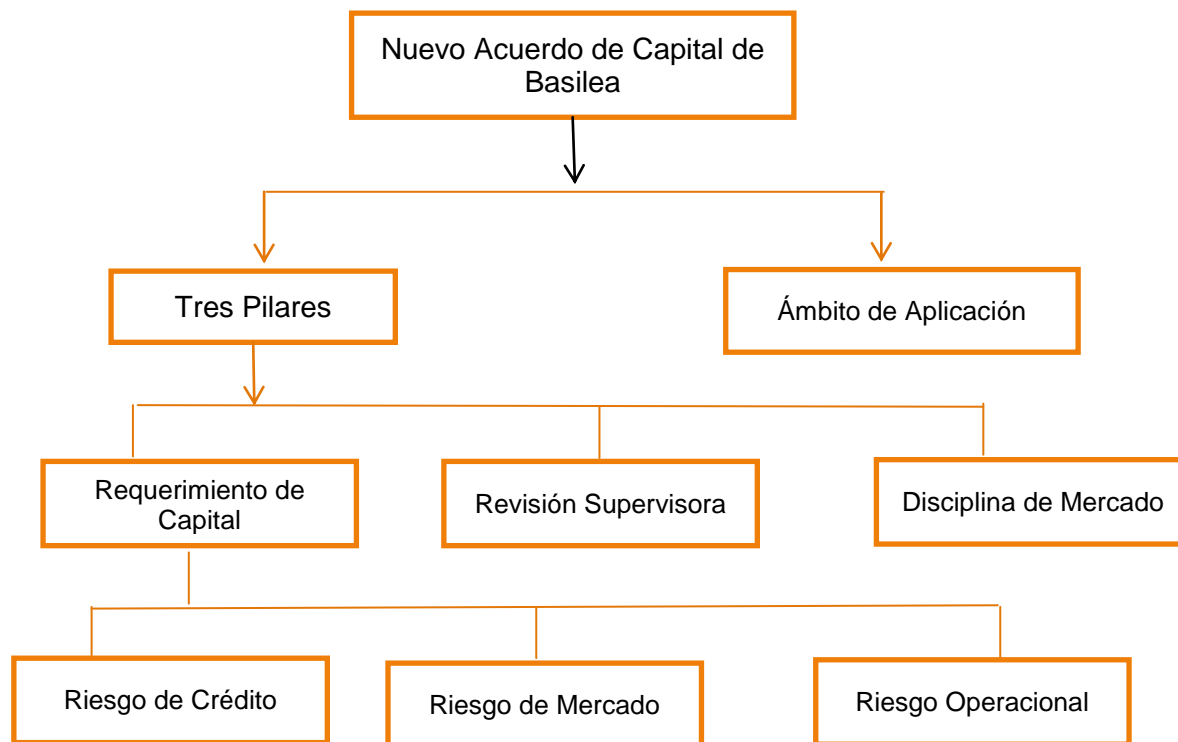


Fig. 5 Acuerdo de Capital de Basilea

Fuente: Acuerdo de Comité de Basilea

Elaborado por: Comité de Basilea

Tal como se lo describió en el capítulo anterior los tres pilares nos ayudaran a implementar paso a paso los requerimientos necesarios para esta identificación de posibles eventos de pérdida, aquí detallamos unos ejemplos de los mismos:

Año	Entidad	Perdidas	Suceso
1995	Barings Bank	1300 M \$	Nick Leeson, trader del Banco Británico Baings, estuvo a lo largo de 2 años acumulando pérdidas no reportadas y negociando contratos de derivados, desde la sucursal del Banco en Singapur. El banco quebró.
1996	Sumitomo Bank	2600 M \$	Un trader de la entidad negocio en el mercado de metales de Londres, contratos de cobre que acumularon perdidas no registradas a lo largo de tres años.
1997	Natwest Bank	127 M \$	KyriacosPapouis, trader del mercado no originado de swaptions, utilizo volatilidades incorrectas para valorar swaps, sobrevalorando los contratos.
2002	AlliedIrish Bank	691 M \$	Un trader del mercado de divisas oculto tres años de pérdidas, en operaciones sobre el tipo de cambio yen / dólar.

2002	Citigroup (Caso Worldcom)	2650 M \$	Bernard Ebbers, presidente de WorldCom, realizó una serie de fraudes contables que llevaron a la quiebra de la compañía. El grupo bancario Citigroup tuvo que llegar a un acuerdo extrajudicial con los accionistas a los que pago 2650 millones de dólares.
2005	Caso Windsor	?	El misterioso incendio del edificio Windsor provoco el lucro cesante de innumerable comercios y sucursales bancarias que se encontraban del perímetro de seguridad.

Fig. 6Ejemplos de Perdidas en Instituciones

Fuente: <http://www.riesgobancario.com>

Elaborado por: <http://www.riesgobancario.com>

Por tal motivo existen tres tipos de efectos que un evento de riesgo operativo puede producir. Las tres categorías, así como las características generales serían las siguientes:

Tipo A: Generan pérdidas y afectan el estado de resultados de la contabilidad.

Tipo B: Generan pérdidas y no afectan el estado de resultados de la contabilidad.

Tipo C: No genera pérdidas y no afecta el estado de resultados de la contabilidad

En un análisis del documento de (FASECOLDA, BANCOMEDIOS, 2010) define que:

Un evento de riesgo operativo puede producir los tres tipos de efectos señalados anteriormente y la combinación de los efectos Tipo A y B. No se puede dar ninguna otra combinación, ya que los efectos Tipo C son excluyentes con las otras dos categorías. Para objeto de este documento las tres categorías se agruparán bajo el nombre de efectos.

La categoría Tipo A también podrá ser llamada pérdidas. Para el caso de los efectos tipo B y C, se utilizará el término incidencias como alternativa para referirse a estas dos categorías.

Por ende tomamos en consideración el extracto específico de la normativa de Riesgo operacional difundida a todo el sistema financiero mediante resolución por la Superintendencia de Bancos y Seguros.

“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.”

Los tipos de eventos son los siguientes:

- a) Fraude interno;
- b) Fraude externo;
- c) Prácticas laborales y seguridad del ambiente de trabajo;
- d) Prácticas relacionadas con los clientes, los productos y el negocio;
- e) Daños a los activos físicos;
- f) Interrupción del negocio por fallas en la tecnología de información; y,

- g) Deficiencias en la ejecución de procesos, en el procesamiento de operaciones y en las relaciones con proveedores y terceros.

Según lo siguiente, estos son los pasos a seguir para realizar esta implementación:

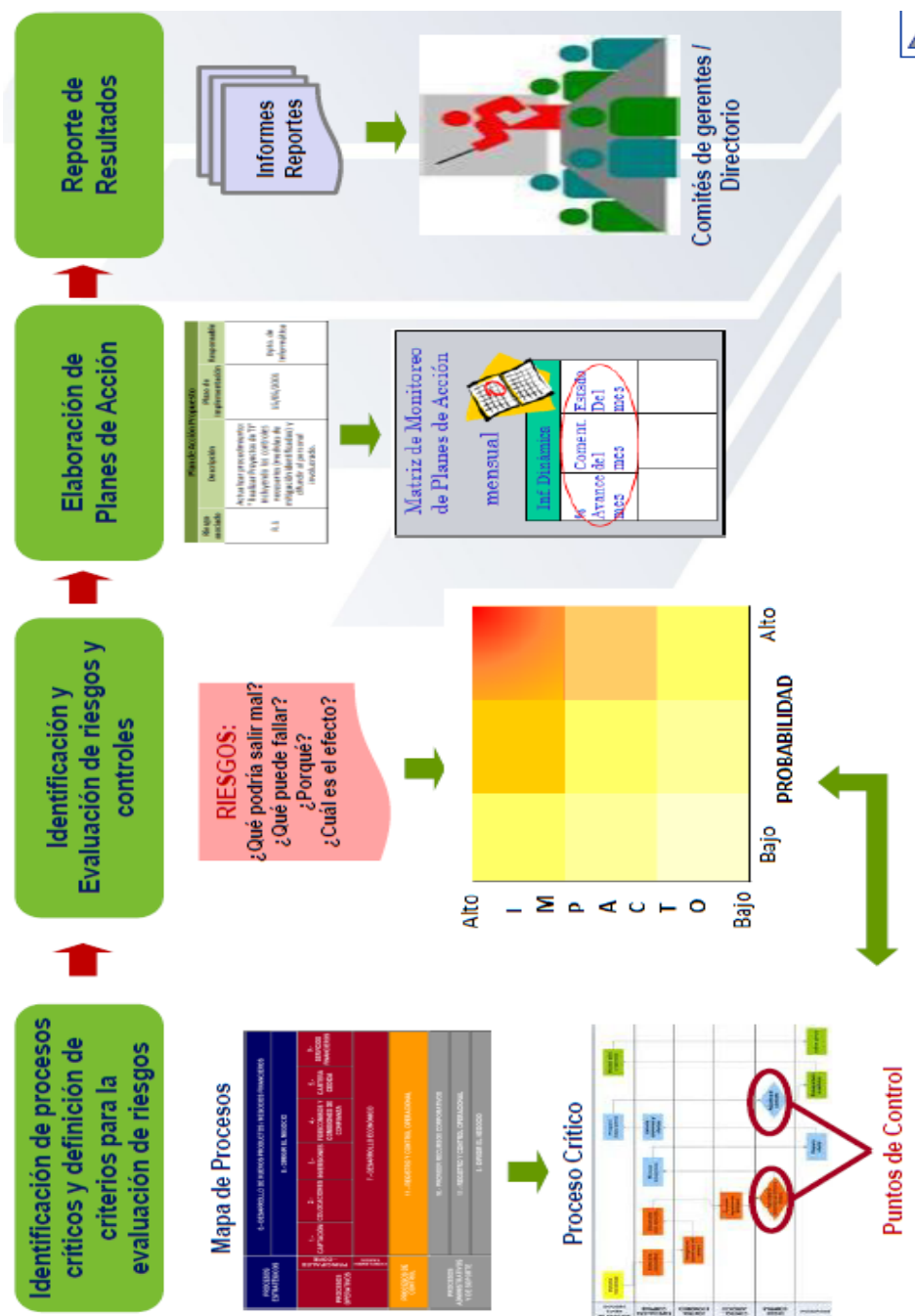


Fig. 7 Metodología de Identificación y Medición de RO

Fuente: Diseño de Consultoría Soluciones Integrales de Procesos.

Elaborador por: Autor de la tesis

Definición de control interno para gestión por procesos identificación de procesos críticos

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 tomando como base la Resolución JB-2008-834 del Riesgo Operacional en los siguientes procesos a mencionar:

- a) Procesos gobernantes o estratégicos:(SEGUROS, Riesgo Operacional, 2008). 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;
- b) 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;
- c) 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.

Identificación de puntos de control

Se la considera una de las actividades más importante y crítica dentro de la gestión y control del riesgo operacional y la de todos los riesgos, por ende si no se define los procedimientos y métodos que se van aplicar a los diferentes procesos no sería posible implementarlos y desarrollarlos. Por tal motivo esta actividad se la puede realizar tomando como origen los subprocesos definidos y los procedimientos asociados a fin de identificar las fallas o problemas que presenten dichos riesgos con el fiel cumplimiento de sus diferentes objetivos.

Causas y Efectos

Es necesario diferenciar entre las causas y los efectos del mismo, aunque no siempre es sencillo delimitar la frontera entre ambas. Las causas nos indican el inicio del riesgo e identifican lo que en esencia llamamos riesgo operacional y sus diferentes tipos (clasificación), a su vez los efectos corresponden a las consecuencias o lo que resulta de dichas causas, las mismas que nos alertan y nos permiten cuantificar y medir este riesgo.

Clasificación del Riesgo

Con la clasificación de los riesgos establecidos por el Comité de Basilea nos ayuda a gestionar el Riesgo Operacional con las Áreas de Apoyo y Soporte. Su finalidad es la de establecer el origen de los mismos, definiendo una causa, esto ayuda y facilita a la correcta clasificación en lo que respecta a la administración del RO.

Es así que es necesario determinar un conjunto de tipos de riesgo con sus respectivos factores como también se lo conoce como pérdidas asociadas, lo que permita su mejor comprensión y a su vez facilite la recolección de los datos. Esta parte es la más crítica e importante para poder lograr un amplio desarrollo posterior de la medición, valoración control y monitoreo del RO.

Para hacer más efectiva y fácil la recolección de eventos de pérdida es aconsejable usar una estructura de las clasificaciones del riesgo operacional, la misma que esté detallada por clases y factores de riesgos excluyentes (acorde a las propias operaciones), funciones y responsabilidades de las instituciones financieras, basada en sus experiencias.

La clasificación del riesgo es de suma importancia al momento de realizar una gestión de riesgos operacionales, debido a que organiza los diferentes tipos de eventos de riesgo por factor, luego por línea de negocio y su posterior evaluación de ser o no considerado como proceso crítico.

La Clasificación del Riesgo puede darse de la siguiente forma:

Evento de Riesgo	Factor de Riesgo	Tipo de Proceso	Frecuencia	Severidad
A	B	C	D	E

Donde el evento la insuficiencia detectada(A), el factor de riesgo es la clasificación normativa de (Personas, Procesos, Tecnología de Información y Eventos Externos)(B), el tipo de procesos si es habilitante, de soporte, estratégico (C) y adicionalmente la frecuencia y severidad del evento en función de nivel de impacto y el número de ocurrencias (D-E).

Definición de Niveles de Seguridad Y Frecuencia para los Eventos de Perdida

Evaluación de Controles

La evaluación de controles consiste básicamente en medir la efectividad del control implementado en el proceso, su uso y aplicabilidad en el proceso evaluado. Para poder realizar esta evaluación en nuestra implementación del modelo de gestión de riesgo operacional vamos a utilizar verificaciones documentales y métodos cualitativos y cuantitativos.

Los Métodos Cualitativos, lo representan los tipos de cuestionarios que realizamos para evaluar a los procesos y que cumplan un determinado orden de ejecución, procesamiento en base a los resultados obtenidos, también se aplican test de operatividad y eficiencia para verificar que la implementación del control sea óptimo.

Los Métodos Cuantitativos, representan numéricamente el grado de cumplimiento y efectividad de un control en un determinado proceso, por ejemplo si estamos midiendo el nivel de efectividad de llamadas entrantes para atención al cliente se coloca un contador que periódicamente se va a ir analizando para evaluar el crecimiento de llamadas, en nuestro caso evaluar cuantitativamente el proceso, así mismo se colocaran en determinados lugares de la cadena de valor del negocio para realizar una posterior evaluación, medir niveles de tendencia y comportamiento y al final poder realizar una proyección del mismo en el futuro.

Si se desea trabajar con el enfoque cualitativo se utiliza como herramienta la autoevaluación que consiste en identificar los riesgos a través del mapa de procesos, evaluación del control existente, determinación de puntos de mejora y de indicadores. El propósito del enfoque cualitativo permite detectar las fortalezas y debilidades del entorno operacional y los riesgos potenciales a los que estarían expuestas las instituciones.

El documento de Basilea II detalla Prácticas Adecuadas para la Gestión y Supervisión del Riesgo Operacional detalla los siguientes elementos para la identificación, medición, seguimiento y control del riesgo operacional:

Mapas y Categorización de riesgo; Sistemas de Auto-evaluación y scorings de riesgo operacional; Indicadores de riesgos; Alertas y controles; Base de datos de pérdidas y modelos de capital.

Clasificación de Controles

a. Oportunidad de la acción del control

Clasificación	Descripción
Preventivo	Controles claves que actúan antes o al inicio de un proceso..
Correctivo	Controles claves que actúan durante el proceso y que permiten corregir las deficiencias.
Detectivo	Controles claves que solo actúan una vez que el proceso ha terminado.

b. Regularidad en la gestión del control:

Clasificación	Descripción
Consistente	Inspecciones claves ejecutados en todo el trabajo, por ende se aplica a cada etapa de la función operativa.
Periódico	Controles claves aplicados en forma constante solo cuando ha transcurrido un periodo específico del tiempo
Ocasional	Controles claves que se aplican solo en forma ocasional en un proceso.

c. Automatización en la aplicación del control:

Clasificación	Descripción
Automatizado	Controles claves incorporados en el proceso, cuya aplicación es completamente informatizada. Están incorporados en los sistemas informáticos..
Semiautomatizado	Controles incorporados en el proceso, cuya aplicación parcialmente es desarrollada mediante sistemas informatizados.
Manual	Controles claves incorporados en el proceso, cuya aplicación no considera uso de sistemas informatizados.

La auto-evaluación de controles implementados en la institución es la herramienta utilizada para documentar los riesgos identificados y su posterior seguimiento.

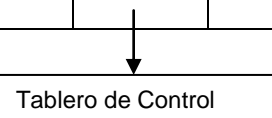
Tabla 2 AUTOEVALUACIÓN DE CONTROLES

Evento de Riesgo	Factor de Riesgo	Severidad	Frecuencia	Efectividad del control	Riesgo Neto	Riesgo Total

Al ser visualizados los riesgos en el que un proceso está referido, se procede a registrarlo en el tablero de control para su ejecución en el plan de acción y mejora (indicadores de gestión de procesos).

Tabla 3 TABLEROS DE CONTROL

Evento de Riesgo	Factor de Riesgo	Severidad	Frecuencia	Efectividad del control	Riesgo Neto	Riesgo Total
E-001	2	3	3	0.25	2	2



Con su finalidad estos tableros o matrices serán claros y precisos los mismos que tendrán distintos directorios.

Enfoque Cuantitativo del Riesgo Operacional

El proceso de cuantificación de riesgo operacional nos permitirá definir cuál será el valor que debemos provisionar por insuficiencias en los procesos de la organización. El cómo hacerlo es básicamente la tarea de cada una de las organizaciones que dependiendo del tamaño de la misma, la data histórica que posean y sobre todo el modelo que usen para calcularlo definirá con un mayor grado de exactitud el requerimiento de capital de la organización para la gestión de riesgos operacionales.

Para lograr aquello vamos a realizar los siguientes pasos secuenciales como se lo indica a continuación:

- a) Identificar las áreas de Riesgo: esto se lo debe de realizar inmediatamente después el inventario de procesos y de la definición de procesos críticos, con esta información tendremos identificadas a las aéreas que debemos “atacar” para mitigar el riesgo inherente al proceso.
- b) Identificar las causas subyacentes de las perdidas, aquí en cambio lo que se realiza ya es la identificación del evento d perdida que es causa de la anomalía del proceso, del control, del plan, etc. De manera que una vez identificado se procede a su tratamiento
- c) Prevenir y/o mitigar su probabilidad de ocurrencia, con esto se analiza el tipo de control a colocar en el proceso, y su evalúa la efectividad del mismo con pruebas de stress para así proceder con su mitigación.

- d) Definir colaterales: (Estrategia de seguros), debido a que si no podemos mitigar el evento de riesgo, lo podemos transferir, para ello existe un sinnúmero de casos reales que podemos analizar para crear colaterales a nuestros procesos

“Se estima o en este caso se provisiona que las pérdidas totales estimadas por riesgos operativos son el 10% de los gastos operativos anuales.”

Adicional a esto también debemos de tomar en consideración lo siguiente:

- a) Implementación de Políticas en los Procesos:

Se tendrá que definir políticas que rijan sobre todo si los procesos que se encuentren en listados en los procesos críticos, que a su vez metodológicamente han sido definidos por la organización, más aun tomando en cuenta que los mismos son el resultado de la cadena de valor de la institución.

- b) Daño o insuficiencia – Evento de Riesgo – Mitigación:

Esta identificación se realiza conjugando las técnicas de levantamiento de información, gestión por procesos y los diferentes controles para su derivación y posterior mitigación con colaterales, este orden se debe de sobrellevar para una identificación efectiva.

Listados de Daños o Insuficiencias

Este es el Listado de los posibles Eventos de riesgos que pueden suscitarse en la institución:

- a) Fallo a la Política o al procedimiento
- b) Controles Inexistentes
- c) Insuficiencia en la dirección y supervisión
- d) Inexistentes políticas de incorporación, permanencia y desvinculación
- e) Inexistente tecnología crediticia
- f) Inconsistencia de Información

Evento de Riesgo:

Estos son los tipos de eventos de riesgos asociados a la insuficiencia en los procesos internos de la organización:

- a) Fraude interno
- b) Fraude externo
- c) Daño en el mobiliario de la organización
- d) Fallas en los aplicativos
- e) Fallas en los procesos y controles
- f) Malas Prácticas laborales (Faltas al código de ética)
- g) Prácticas comerciales y productos inadecuados.

Mitigación:

Estos son las diferentes acciones de mitigación de los diferentes eventos de riesgo que en los procesos conlleva.

- a) Gestión de Seguros
- b) Pólizas de Perdidas
- c) Provisión de valores en cuentas contables
- d) Gestión de controles y tableros BSC (Balance Score Card) Tablero de control de Indicadores

Información de Gestión de la Medición

El proceso de cuantificación se realiza de la siguiente manera:

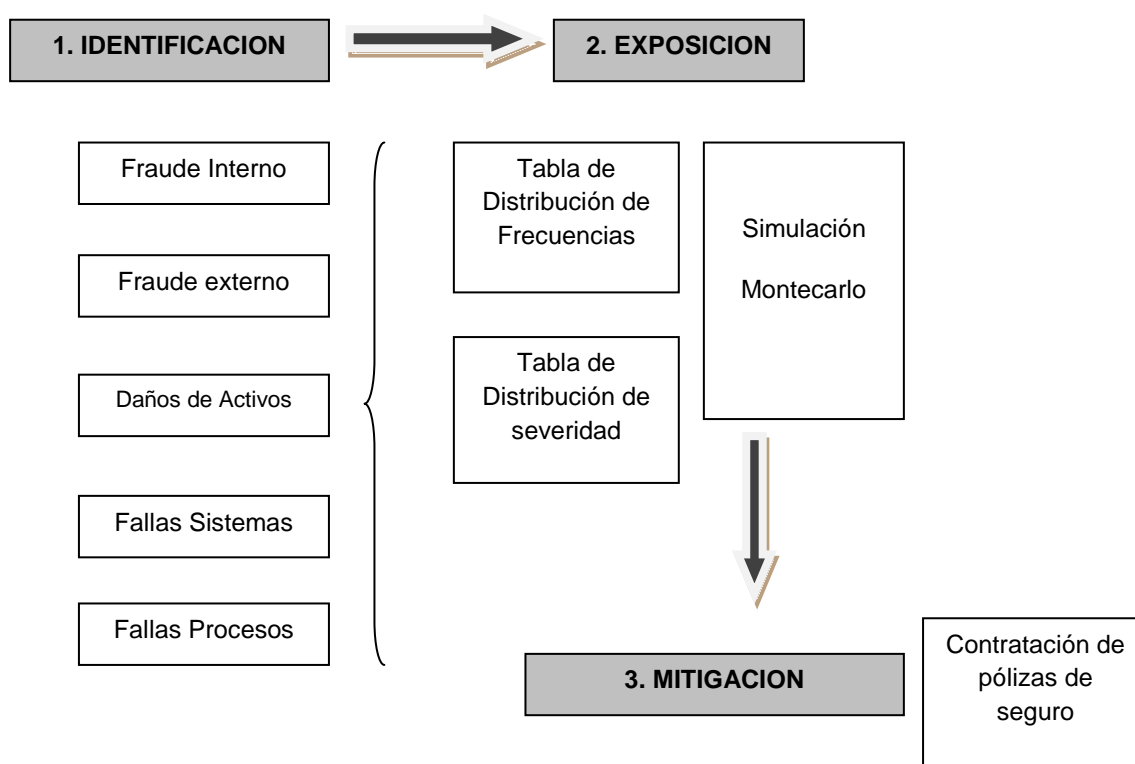


Fig. 8 Proceso de cuantificación para la recolección de información.

Pérdida Esperada

La pérdida esperada radica en el requerimiento e capital esperado de pérdida por afectaciones directas del riesgo, comúnmente este efecto se lo denomina RAROC. Básicamente radica este concepto en la generación de riesgo de crédito, pero es un factor influyente en el riesgo operacional debido a que si manejamos los procesos institucionales con un enfoque a riesgos minimizamos este tipo de pérdida.

Para medir y estimar el proceso de medición de riesgo utilizaremos los siguientes métodos estadísticos:

- 1) Método del Indicador Básico (BIA)
- 2) Método Estándar (TSA)
- 3) Metodologías de Medición Avanzada (AMA)

Método del indicador Básico

Esta metodología es la más sencilla promulgada por el comité de Basilea II, el cual, utiliza los ingresos brutos de la institución para calcular el requerimiento de capital y la exposición de la financiera

Su fórmula es la siguiente:

$$K_{OR-BIA} = \alpha \cdot \frac{\sum_{t=1}^3 \max[IB_t; 0]}{n} \quad (2)$$

Donde,

K_{OR-BIA} : requerimientos de capital por riesgo operacional, según BIA;

α : factor fijo de 15%;

IB_t : ingreso bruto anual del año t anterior;

n: número de años, dentro de los tres últimos, con ingresos brutos anuales positivos.

Fig. 9 Formula del Indicador Básico (BIA)

Fuente: Nota Técnica de Comité de Basilea II

Método Estándar (TSA)

Esta metodología de medición es muy similar al BIA (Indicador Básico) pero usa una variante que es las 8 líneas de negocio promovidas por Basilea II, esta técnica utiliza el promedio simple de los requerimientos de capital por riesgo operacional con una ventana de tiempo de 3 años.

$$K_{OR-TSA} = \frac{\sum_{t=1}^3 \max \left[\sum_{j=1}^8 (IB_{j,t} \cdot \beta_j); 0 \right]}{3} \quad (3)$$

Donde,

K_{OR-TSA} : requerimientos de capital por riesgo operacional, según TSA;

β_j : factor fijo para la línea de negocio j-ésima

$IB_{j,t}$: ingreso bruto anual de la línea de negocio j-ésima en el año t

Fig. 10 Método Estándar (TSA)

Fuente: Nota Técnica de Comité de Basilea II

Metodología de Medición Avanzada (AMA)

Esta metodología es la más evolucionada en el sentido de elaboración, análisis estadístico y paramétrico. El comité de Basilea no ha establecido que técnicas estadísticas usar, debido a que las mismas dependen del tamaño de la institución, la base de datos histórica y el conocimiento y aplicabilidad de los modelos en las diferentes realidades económicas.

Entre las diferentes técnicas encontramos las siguientes:

- a) Redes Bayesianas
- b) Redes Neuronales
- c) Simulación Montecarlo
- d) Modelos Auto regresivos

Definición de Frecuencia y Severidad

El análisis de la frecuencia severidad constituye en un factor fundamental para la obtención del capital requerido para riesgo operacional debido a que cuando cuantificamos estas dos medidas lo que obtenemos de las mismas en el valor probabilístico y el peso en dólares del evento de riesgo que se identificó.

Clasificación	Descripción		Comentarios
20-30	Alta o mayor	Impacto mayor en el paciente; puede llevar a su muerte o provocarle consecuencias de largo plazo.	Se requiere acción urgente
10-19	Moderada	Impacto moderado; puede ocasionar consecuencias de corto plazo para el paciente	Se requiere acción
1-9	Riesgo bajo o menor	Impacto menor; sin consecuencias o con consecuencias menores	Mantener bajo evaluación

Alta severidad	2 - Alta severidad Baja frecuencia (infecciones de torrente sanguíneo causadas por contaminación de solución intravenosa)	1 - Alta severidad Alta frecuencia (infecciones de transmisión sanguínea a partir de la re-utilización de jeringas y agujas)
Baja severidad	4 - Baja severidad Baja frecuencia (infecciones a partir de la ropa hospitalaria)	3 - Baja severidad Alta frecuencia (infecciones de tracto urinario)
	Baja frecuencia	Alta frecuencia

Fig. 11 Ejemplo de Tablas de Frecuencia y Severidad

Fuente: http://www.theific.org/basic_concepts/spanish/IFIC%20Spanish%20Book%202013_ch27_PRESS.pdf

Elaborado por: http://www.theific.org/basic_concepts

Contenido De La Matriz De Riesgos:

La Matriz de Riesgo es el compendio de todos los factores intrínsecos para el cálculo del requerimiento de capital, en este gráfico representativo se evidencia exactamente la posición donde se encuentra la institución al momento de implementar el riesgo operacional.

Dicho gráfico además de visualizar la posición también define el nivel de riesgo en el cual la entidad definió para ver su realidad en requerimientos, controles y procesos.

Probabilidad	Insignificante 1	Menor 2	Moderada 3	Mayor 4	Catastrófica 5
Raro 1	Bajo	Bajo	Moderado	Alto	Alto
Improbable 2	Bajo	Bajo	Moderado	Alto	Extremo
Posible 3	Bajo	Moderado	Alto	Extremo	Extremo
Probable 4	Moderado	Alto	Alto	Extremo	Extremo
Casi Seguro 5	Alto	Alto	Extremo	Extremo	Extremo

Extremo: Los riesgos extremos deben ponerse en conocimiento de los Directores y ser objeto de seguimiento permanente.

Alto: Los riesgos altos requieren la atención del Presidente/ Director Ejecutivo

Moderado: Los riesgos moderados deben ser objeto de seguimiento adecuado por parte de los niveles medios de Dirección.

Bajo: Los riesgos bajos deben ser objeto de seguimiento por parte de los supervisores.

Fig. 12 ejemplo de Mapa de Riesgos Operacionales

Fuente: <http://necksize.wordpress.com/2010/05/11/matriz-de-riesgo-una-herramienta-rapida-y-eficaz/>

Elaborado por: <http://necksize.wordpress.com>

Dicho mapa generalmente posee las siguientes partes:

a. Campo de Probabilidad:

Este campo visualiza la probabilidad de ocurrencia en el que incurriría un evento por ende existe un riesgo inherente a ese proceso.

b. Campo de consecuencias

En este campo se especifican las categorías de consecuencias en las cuales se mide en evento de riesgo, para efectos del ejemplo se miden 5 categorías que van desde el más bajo (Insignificante) hasta el más alto (Catastrófico).

c. Campo calificación de riesgo inherente:

Este campo tipifica la conjugación de los campos consecuencias y probabilidad, el mismo evalúa la posición del mapa en categorías, las cuales para el ejemplo van desde el más bajo (Bajo) hasta el más alto (Extremo).

Tabla Probabilidad Cinco Categorías:

Categoría	Valor	Descripción
Alta	5	Riesgo cuya probabilidad de ocurrencia es muy alta, es decir, se tiene un alto grado de seguridad que éste se presente. (90% a 100%)
Media Alta	4	Riesgo cuya probabilidad de ocurrencia es alta, es decir, se tiene entre 66% a 89% de seguridad que éste se presente.
Media	3	Riesgo cuya probabilidad de ocurrencia es media, es decir, se tiene entre 31% a 65% de seguridad que éste se presente.
Media Baja	2	Riesgo cuya probabilidad de ocurrencia es baja, es decir, se tiene entre 11% a 30% de seguridad que éste se presente.
Baja	1	Riesgo cuya probabilidad de ocurrencia es muy baja, es decir, se tiene entre 1% a 10% de seguridad que éste se presente.

Tabla 4 Probabilidades en cinco categorías

Tabla Probabilidad Tres Categorías:

Categoría	Valor	Descripción
Alta	3	Riesgo cuya probabilidad de ocurrencia es alta, es decir, se tiene entre 65% a 100% de seguridad que este se presente
Media	2	Riesgo cuya probabilidad de ocurrencia es media, es decir, se tiene entre 31% a 64% de seguridad que éste se presente.
Baja	1	Riesgo cuya probabilidad de ocurrencia es baja, es decir, se tiene entre 0% a 30% de seguridad que se presente.

Tabla 5 Probabilidades en 3 Categorías

d. El impacto:

Impacto se refiere al nivel de consecuencia que puede tener un posible evento de riesgo en un proceso, el mismo que deberá estar tipificado en una lista desde el impacto más bajo, hasta el impacto más alto tal como describimos en la tabla adjunta.

Tabla Impacto Cinco Categorías:

Categoría	Valor	Descripción
Alto	5	Riesgo cuya materialización influye gravemente en el desarrollo del proceso y en el cumplimiento de sus objetivos, impidiendo finalmente que éste se desarrolle.
Medio Alto	4	Riesgo cuya materialización dañaría significativamente el desarrollo del proceso y el cumplimiento de sus objetivos, impidiendo que éste se desarrolle en forma normal.
Medio	3	Riesgo cuya materialización causaría un deterioro en el desarrollo del proceso dificultando o retrasando el cumplimiento de sus objetivos, impidiendo que éste se desarrolle en forma adecuada.
Medio Bajo	2	Riesgo que causa un daño menor en el desarrollo del proceso y que no afecta mayormente el cumplimiento de sus objetivos estratégicos.
Bajo	1	Riesgo que puede tener un pequeño o nulo efecto en el desarrollo del proceso y que no afecta el cumplimiento de sus objetivos estratégicos.

Tabla 6 Impacto cinco categorías

Tabla Impacto Tres Categorías:

Categoría	Valor	Descripción
Alto	3	Riesgo cuya materialización dañaría significativamente el desarrollo del proceso y el cumplimiento de sus objetivos, impidiendo que éste se desarrolle en forma normal.
Medio	2	Riesgo cuya materialización causaría un deterioro en el desarrollo del proceso dificultando o retrasando el cumplimiento de sus objetivos, impidiendo que éste se desarrolle en forma adecuada.
Bajo	1	Riesgo que causa un daño menor en el desarrollo del proceso y que no afecta mayormente el cumplimiento de sus objetivos estratégicos.

Tabla 7 Impacto tres categorías

Es el resultado de la combinación entre impacto y probabilidad de ocurrencia, la operación que debe realizarse es una multiplicación entre los valores obtenidos de las dos variables mencionadas, su resultado posee una categorización de severidad del riesgo para la tabla de cinco o tres categorías, tal como consta en los cuadros siguientes, que expresan una exposición sin controles.

Nivel de Severidad del Riesgo Cinco Categorías:

Nivel probabilidad (p)	Nivel impacto (i)	Severidad del riesgo $S=(pxi)$
Alta (5)	Alto (5)	EXTREMO (25)
Alta (5)	Medio Alto(4)	EXTREMO (20)
Alta (5)	Medio(3)	EXTREMO (15)
Alta (5)	Medio Bajo(2)	ALTO(10)
Alta (5)	Bajo(1)	ALTO(5)
Media Alta (4)	Alto (5)	EXTREMO (20)
Media Alta (4)	Medio Alto(4)	EXTREMO (16)

Media Alta (4)	Medio(3)	ALTO(12)
Media Alta (4)	Medio Bajo(2)	ALTO(8)
Media Alta (4)	Bajo(1)	MODERADO(4)
Media (3)	Alto (5)	EXTREMO (15)
Media (3)	Medio Alto(4)	EXTREMO (12)
Media (3)	Medio(3)	ALTO(9)
Media (3)	Medio Bajo(2)	MODERADO(6)
Media (3)	Bajo(1)	BAJO(3)
Media Baja (2)	Alto (5)	EXTREMO (10)
Media Baja (2)	Medio Alto(4)	ALTO(8)
Media Baja (2)	Medio(3)	MODERADO(6)
Media Baja (2)	Medio Bajo(2)	BAJO(4)
Media Baja (2)	Bajo(1)	BAJO(2)
Baja (1)	Alto (5)	ALTO(5)
Baja (1)	Medio Alto(4)	ALTO(4)
Baja (1)	Medio(3)	MODERADO(3)
Baja (1)	Medio Bajo(2)	BAJO(2)
Baja (1)	Bajo(1)	BAJO(1)

Tabla 8 Severidad del Riesgo cinco Categorías

Nivel de Severidad del Riesgo Tres Categorías:

Nivel probabilidad (p)	Nivel impacto (i)	Severidad del riesgo $S = (p \times i)$
Alta (3)	Alto (3)	Alto (9)
Alta (3)	Medio (2)	Alto (6)
Alta (3)	Bajo (1)	Medio (3)
Media (2)	Alto (3)	Alto (6)
Media (2)	Medio (2)	Medio (4)
Media (2)	Bajo (1)	Bajo (2)
Baja (1)	Alto (3)	Medio (3)
Baja (1)	Medio (2)	Bajo (2)
Baja (1)	Bajo (1)	Bajo (1)

Tabla 9 Severidad del riesgo tres categorías

En los esquemas anteriores se muestra el resultado de la combinación entre las categorías del nivel de impacto del riesgo y las categorías del nivel de probabilidad de ocurrencia del riesgo, es decir, el nivel de severidad, para cinco y tres categorías.

De este esquema se puede observar que las categorías de impacto tienen una mayor probabilidad en el nivel de severidad establecido, aunque la probabilidad de ocurrencia sea menor, al tratarse de riesgos con impactos altos, cualquier realización del riesgo tendrá una acción significativa en el fiel cumplimiento de los objetivos del proceso examinado.

Relaciones entre los Eventos de Pérdida y los Indicadores de Riesgo

Planes de Acción

Una vez evaluados los riesgos identificados, es necesario establecer la manera en que se responderá a ellos estableciendo estrategias partiendo de que se puede evitar, reducir, compartir o aceptar el riesgo para su mitigación. La mitigación del riesgo consiste en gestionarlo en etapas tempranas mediante medidas estratégicas definidas de manera inmediata y efectiva, para lo cual será menos costoso.

Un medio de predicción y seguimiento para definir niveles de ocurrencia de un riesgo, es definiendo indicadores internos asociados al proceso crítico bajo las características de fácil medición, rápido acceso y alta correlación con el riesgo. De esta forma se permite también, establecer los niveles de tolerancia bajo los cuales se está dispuesto aceptar el riesgo. A continuación se presentan algunos ejemplos de las medidas que se pueden establecer como respuestas al riesgo identificado.

Categoría	Estrategia
Evitar	Decidir no promover una nueva actividad, producto o servicios que podrían dar lugar a riesgos. Prescindir de un área, producto o servicio
Compartir	Acuerdos contractuales con proveedores, clientes o socios de negocios.
Reducir	Diversificar los productos o servicios, establecer niveles de tolerancia, diseño de Controles
Aceptar	Crear reservas para hacer frente a posibles pérdidas, aceptar el riesgo si se adapta a las tolerancias al riesgo existente

Reporte de Resultados

Una de las más importantes acciones de una buena gestión de riesgos operacionales es la evaluación y su respectivo reporte. Estos reportes evidencian los resultados por proceso, por evento y por línea de negocio de la realidad de la gestión de riesgos en la institución.

Se deberá publicar estos resultados en una intranet institucional para que así cumpla, con el enfoque que nos brinda la metodología COSO de control interno que es la supervisión y difusión de los resultados de implementación de controles.

Mapa de Procesos

Un mapa de procesos es un inventario de valor de los procesos de la institución, evidencia gráficamente como está diagramado el proceso, a veces representa un flujo de información donde los datos viajan a través del flujo originando en sí un diagrama.

Proporciona una visión global de los procesos que se encuentra en la cadena de valor del negocio dándonos una verdadera posición y comunicación de los mismos con otros procesos vinculantes. (Ver anexo 2)

$$\text{Nivel de exposición al riesgo} = \frac{\text{Nivel de Severidad del Riesgo}}{\text{Nivel de Eficiencia del Control}}$$

Nivel de exposición al riesgo para cinco categorías de probabilidad e impacto:

Intervalos (resultados)	Nivel de exposición al riesgo
8.0–25.0	No aceptable
4.0–7.99	Mayor
3.0–3.99	Media
0.0 -2.99	Menor

Tabla 10 Exposición al Riesgo

Nivel de exposición al riesgo para tres categorías de probabilidad e impacto.

Intervalos (resultados)	Nivel de exposición al riesgo
6 - 9.00	Alta
3 - 5.99	Media
0 - 2.99	Baja

Tabla 11 Nivel de Exposición al Riesgo

Una vez tratados los datos a través de esta metodología se obtendrá un listado de eventos de riesgos con su respectiva calificación referente al nivel de exposición. Sobre estos se buscará las opciones más óptimas de tratamiento, siendo los primeros en tratar aquellos que tengan una calificación final de No Aceptable o Alta, luego los de calificación Mayor o Media, y finalmente los de Baja o Menor; se presentarán las diferentes alternativas al Comité de Riesgos para su respectivo análisis y resolución.

El mismo arrojará como resultados de riesgo residual y riesgo inherente una relación semáforo, es decir según el grado de exposición el resultado se reflejará en amarillo, verde o rojo; lo cual permitirá realizar una matriz de relación que no es otra cosa que un gráfico de filas y columnas que permite priorizar el tratamiento de los riesgos y visualizar el nivel de exposición sin controles y con controles.

Su realización será una vez terminada el mapa de procesos. A continuación se dará a conocer la estructura organizacional con sus respectivas funciones en el cual están sujetos a realizar y ejecutar dichas acciones para que las sociedades financieras puedan disminuir más el Riesgo Operacional, dicho esto el presente proyecto tiene como finalidad el cambio de mejoras a la misma.

CAPITULO 2

ESTRUCTURA ORGANIZACIONAL

Dado el dinamismo por el cual las empresas cambian su estructura organizacional, su composición y estrategias de competitividad lo más valioso que posee en activos es el capital humano y administración y como se compone el mismo.

Por ende para cumplir con el objetivo de minimizar y sobre todo mitigar el riesgo operacional toda institución debe de tener una serie de comités y demás organismos que ayuden a realizar la tarea de riesgos.

Responsabilidades del directorio en la administración de riesgos

Según la normatividad y de acuerdo a la Resolución JB-2004-631, las responsabilidades del directorio serán las siguientes (Seguros, Normativas y Resolución, 2004):

1. Conocer y comprender los riesgos inherentes a la estrategia de negocios que asume la institución.
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.

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.
4. Asegurarse que la auditoría interna verifique la existencia y cumplimiento del esquema de la administración integral de riesgos de la institución.
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.
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.
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.
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.
9. Asegurarse de que la institución cuente con recursos humanos, materiales y equipos que permitan la eficiente administración integral de riesgos.

10. Designar a los miembros del comité de administración integral de riesgos, y
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.

Estructura orgánica funcional de la sociedad financiera

La Estructura de la Unidad de Riesgos está conformada de la siguiente forma:

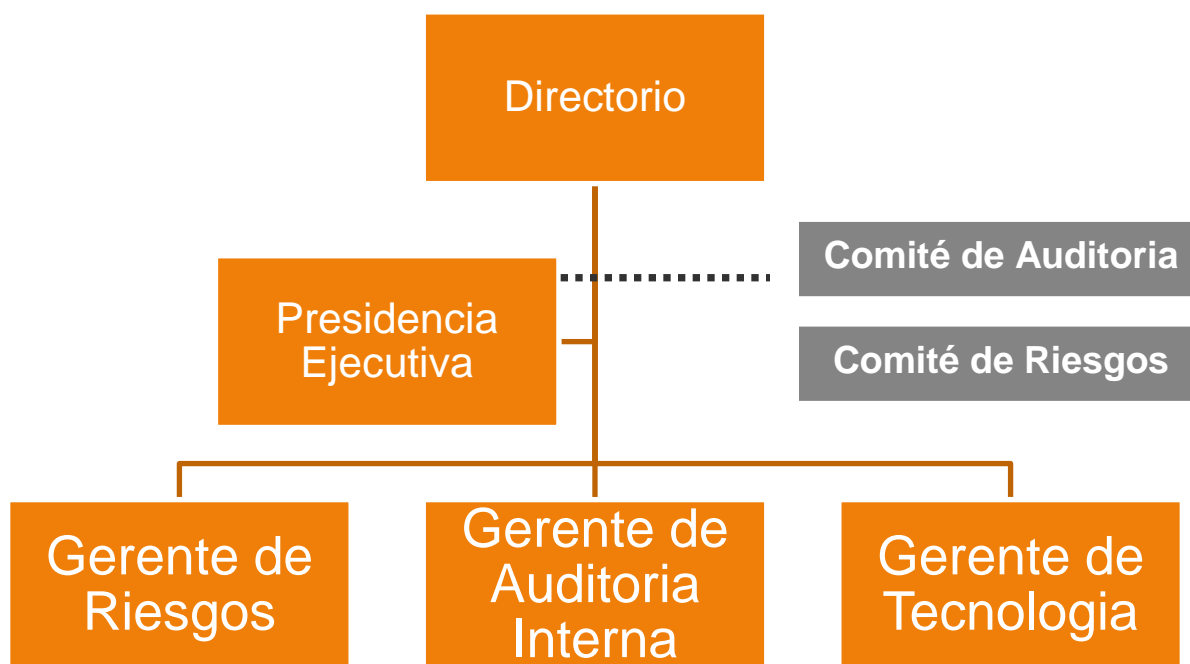


Fig. 13 Estructura Orgánica Funcional

Comité Integral de Administración del Riesgo

Indicado en la normativa vigente el comité de administración integral de riesgos en sus artículos dos y tres de la resolución No. JB-2004-631 del año 2004 del 22 de enero, se conformaran con el objetivo diseñar, medir y controlar el proceso de Administración Integral del Riesgo Integral, es decir, controlar absolutamente todos los riesgos de la institución.(ver anexo 4)

El Comité Integral de Administración del Riesgo está conformado por:

- a) Vocal del Directorio,
- b) Un Representante Legal
- c) Funcionario de la Unidad de Riesgo
- d) Gerente de Riesgo

A continuación se presenta el organigrama del Comité Integral de Administración de Riesgos:

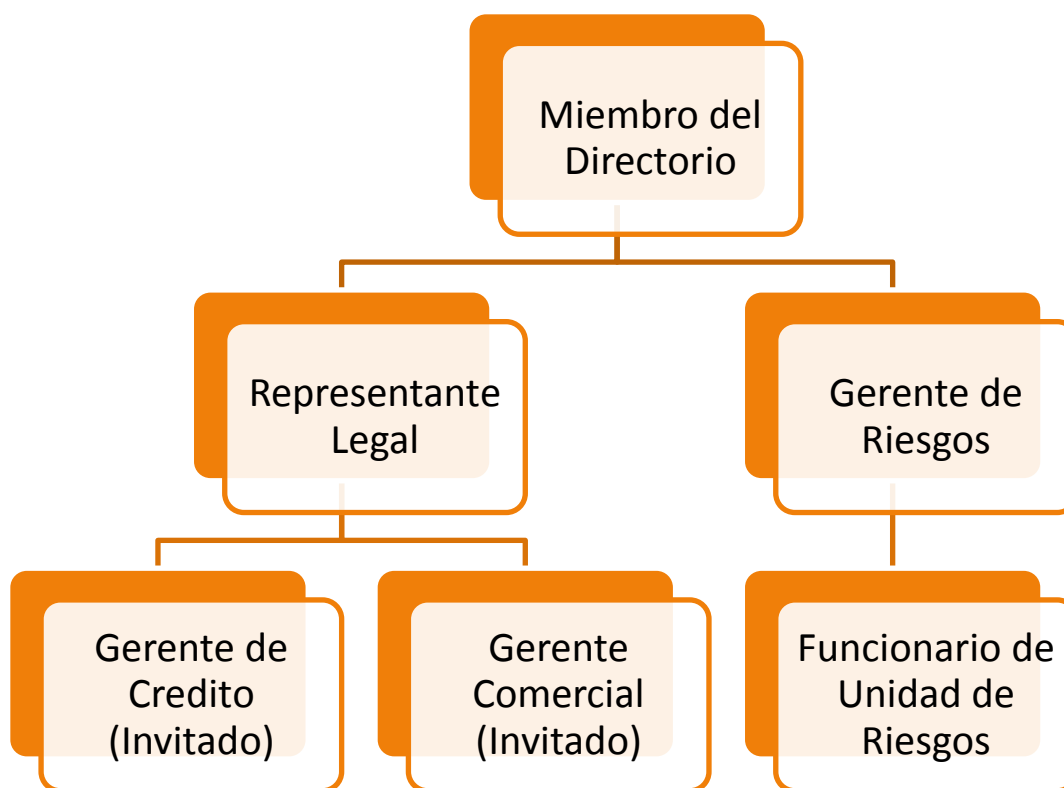


Fig. 14 Comité de Administración Integral de Riesgos

Funciones y responsabilidades

Las funciones de este comité están normalizadas en la Resolución JB-2004-631 del 22 de enero del año 2004 (ver anexo 4) el cual son las siguientes:

- 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.
- 2) Proponer al Directorio o al organismo que haga sus veces los límites específicos apropiados por exposición de cada riesgo.

- 3) 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.
- 4) 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.
- 5) 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.
- 6) 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.
- 7) 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.
- 8) Las demás que determine el Directorio o el organismo que haga sus veces, o que sean dispuestas por la Superintendencia de Bancos y Seguros.

Comité de auditoría

Este comité tiene su naturaleza en la resolución JB-2003-586 del 21 de octubre del 2003 (reformada con Resolución JB-204-664 del 15 de mayo del 2004), en la cual la Superintendencia de Bancos dispone la creación del Comité de Auditoría, el cual su principal labor de la de controlar todos los procesos internos del negocio. (Ver anexo 4).

El Comité estará conformado por:

- 1) Dos Vocales del Directorio
- 2) Un Miembro, elegido por Directorio
- 3) Representante Legal y Auditor Interno (sin voto)
- 4) Opcional: Auditor Externo e invitados (sin voto)

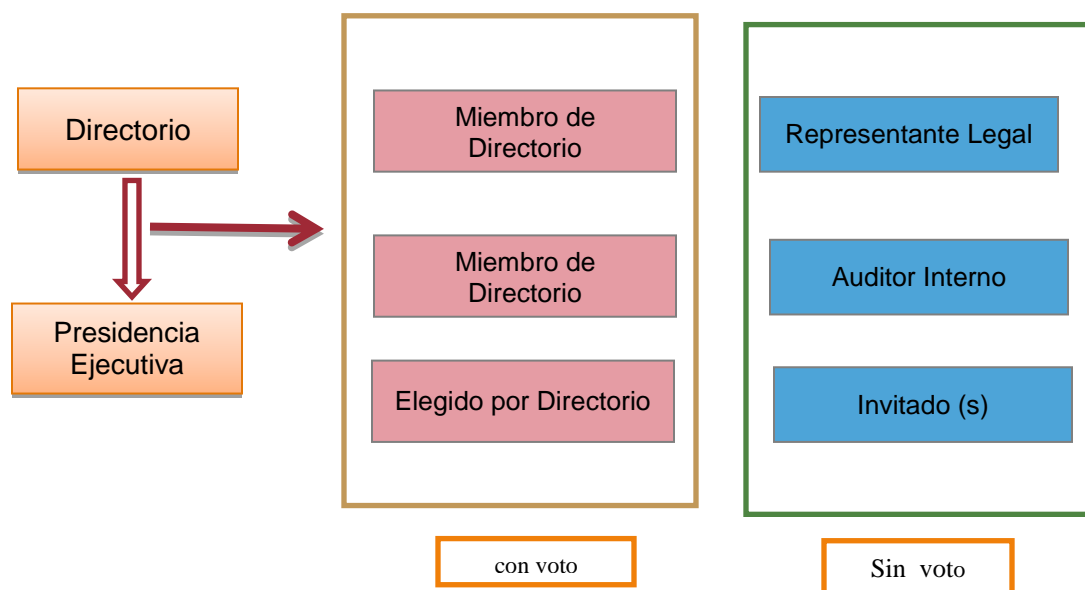


Fig. 15 Comité de Auditoría

Funciones y responsabilidades

Las principales funciones en base (Seguros, 2004) Resolución JB-2004-664 del 18 de mayo del 2004 son las siguientes:

- a) Proponer al Directorio u organismo que haga sus veces la terna de auditores internos y externos para que la junta general de accionistas, asamblea general de socios u organismo correspondiente, nombre al auditor interno o externo.

- b) Proponer al Directorio u organismo que haga sus veces, la nómina para la elección de la calificadora de riesgos.
- c) Informarse sobre el adecuado funcionamiento de los sistemas de control interno, entendiéndose como controles internos, los controles operacionales y financieros establecidos, para dar transparencia a la gestión de la administración y buscar desalentar irregularidades que podrían presentarse en los diferentes niveles de gobierno.
- d) Coordinar las actividades entre los órganos integrantes del sistema de control interno para incrementar la eficiencia, eficacia y economía del control, evitando superposiciones o reiteración de acciones.
- e) Conocer y analizar la información proporcionada por la administración y los auditores internos, que permita verificar que se identifican y evalúan los riesgos de las instituciones financieras y de todas las subsidiarias y afiliadas del grupo financiero; y, que se adoptan medidas para la adecuada administración de esos riesgos.
- f) Conocer y analizar los términos de los contratos de auditoría externa y la suficiencia de los planes y procedimientos pertinentes, en concordancia con las disposiciones generales impartidas por la Superintendencia de Bancos y Seguros; y, analizar los informes de los auditores externos y poner tales análisis en conocimiento del Directorio u organismo que haga sus veces.
- g) Conocer y analizar las observaciones y recomendaciones de los auditores interno y externo y de la Superintendencia de Bancos y Seguros sobre las debilidades de control interno, así como las acciones correctivas implementadas por la Gerencia General, tendientes a superar tales debilidades.

- h) Emitir criterio respecto a los desacuerdos que puedan suscitarse entre la Gerencia General y los auditores interno y externo y que sean puestos en su conocimiento; solicitar las explicaciones necesarias para determinar la razonabilidad de los ajustes propuestos por los auditores; y, poner en conocimiento del Directorio u organismo que haga sus veces su criterio.
- i) Analizar e informar al respecto al Directorio u organismo que haga sus veces los cambios contables relevantes que afecten a la situación financiera de la entidad y demás entidades integrantes del grupo financiero.
- j) Conocer y analizar conflictos de interés que pudieren contrariar principios de control interno e informar al Directorio u organismo que haga sus veces.
- k) Conocer los mecanismos de control interno implantados por la administración para evitar operaciones con personas vinculadas y velar por la cancelación de los saldos pendientes de pago anteriores a la vigencia de la prohibición legal.
- l) Informarse acerca del cumplimiento de las políticas institucionales y de las disposiciones legales y normativas, por parte de las instituciones financieras y las que conforman el grupo financiero.
- m) Requerir a los auditores internos y externos revisiones específicas sobre situaciones que a criterio del comité sean necesarias; o, que exija el Directorio u organismo que haga sus veces; y,
- n) Mantener comunicación periódica con el organismo de control, a fin de conocer sus inquietudes y problemas detectados en la supervisión de las instituciones financieras, así como vigilar el grado de cumplimiento para su solución.

Unidad de riesgos

La superintendencia de bancos dispone en el artículo cuatro en la sección III denominada “Responsabilidad en la Administración de Riesgos” definida en la resolución JB-2004-631 del 22 de enero del 2004, que se deberá de estructurar una unidad denominada “unidad de riesgos”, la misma, tiene como finalidad principal monitorear y asegurar que las líneas de negocio estén alineados correctamente con las políticas, procesos y procedimientos definidos por la administración integral del riesgo. (Ver anexo 4)

Funciones y responsabilidades

La Unidad de Riesgos tendrá como funciones principales:

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 organismos que haga sus veces.
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.
3. Velar por el cumplimiento de los límites de exposición al riesgo y los niveles de autorización dispuestos.
4. Revisar de forma sistemática las exposiciones por tipo de riesgos respecto de los principales clientes, sectores económicos de actividad, área geográfica, entre otros.
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.

6. Preparar estrategias alternativas para administrar los riesgos existentes y proponer al comité los planes de contingencia que consideren distintas situaciones probables, según corresponda.
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.
8. Calcular las posiciones de riesgo y su afectación al patrimonio técnico de la entidad.
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, normativa y estatutaria, en cumplimiento del proceso de administración integral de riesgos.
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,
11. Las demás que determine el comité de administración integral de riesgos de la entidad.

A continuación se define el organigrama de la Unidad:

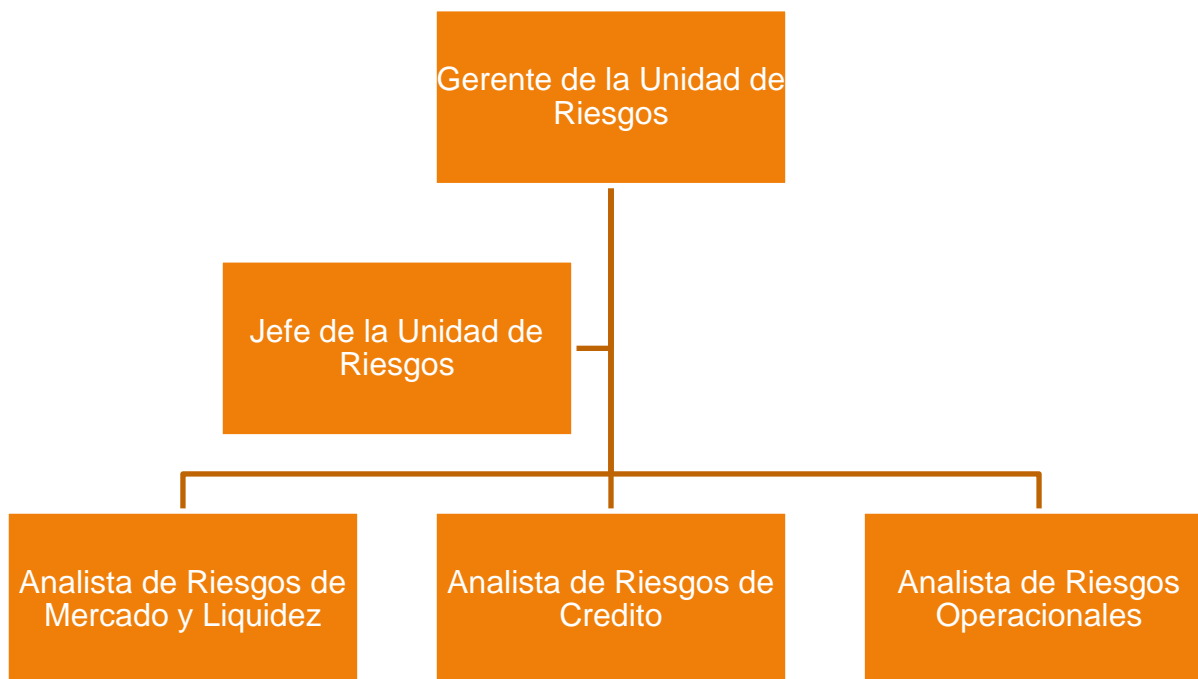


Fig. 16 Unidad de Riesgos

Funciones de la gerencia de riesgos

1. Definir metodología para analizar y cuantificar la exposición de la institución ante los riesgos de liquidez, mercado y tasa de interés.
2. Controlar y valorar el portafolio de inversiones y productos derivados del grupo financiero a precios de mercado y generar indicadores de desempeño y riesgo.
3. Sugerir límites de exposición al Directorio y al Comité Integral de Administración del Riesgo de la Institución.
4. Monitorear y desarrollar sistemas de información gerencial y de control de los límites y políticas establecidos por el Directorio.

5. Elaborar y supervisar la vigencia del plan de contingencia de liquidez.
6. Proponer una metodología de transferencia de precios internos ajustados por riesgos.

Funciones del analista de Riesgo de Crédito

- 1) Identificar y aplicar metodologías de otorgamiento apropiadas para cada uno de los segmentos de clientes en la institución:
 - a) Scoring para el segmento de consumo
 - b) Modelo de Rating para el segmento de banca empresarial,
 - c) Modelos paramétricos para Microcrédito y pymes
- 2) Proponer los límites de exposición al riesgo al Comité Integral de Administración del Riesgo.
- 3) Verificar e informar el cumplimiento de los límites establecidos y monitorear permanentemente el cumplimiento de las políticas de crédito dictadas por el Comité Integral de Administración del Riesgo y el Directorio.

Funciones del analista de Riesgo Operacional

1. Determinar el riesgo en el desarrollo de nuevos productos y servicios.
2. Desarrollo de un modelo de riesgo operacional relación al evento-impacto-probabilidad de los procesos críticos.
3. Desarrollar e implementar metodologías de cuantificación del riesgo operacional y bases de datos.

4. Realizar el Modelo de Cuantificación de Riesgos Operacionales
5. Verificar el buen Gobierno corporativo
6. Verificar que todos los planes de la Institución estén debidamente alineados a la estrategia y cumpliéndose a cabalidad

CAPITULO 3

PRESUPUESTO DE ELABORACIÓN

Objetivo del presupuesto del proyecto

El objetivo es cuantificar el costo que se incurre en la elaboración del proyecto a fin de establecer su precio en el mercado, para lo cual utilizamos el programa Visual Net 2013, herramienta de última tecnología y de uso común, lo que facilita la compatibilidad con otros programas.

La estructura de mi tesis es el de cuantificar el presupuesto y el gasto que incurrirá la entidad financiera en su operatividad para definir si es viable o no la implementación de este trabajo. Se presentan los diferentes estados financieros de una organización para poder analizar sus estados financieros acorde con la implementación en paralelo con el documento. Adicional a esto se tiene los flujos de caja para el año en cuestión y un grupo de indicadores financieros que nos podrán guiar en el análisis económico de la institución.

El presupuesto de costos de implementación lo asume cada entidad debido a que su cuantificación tanto en tiempos por parte del personal operativo como en automatización está contemplado en el presupuesto de la institución presentado a los diferentes organismos de control al inicio de cada año.

Adicionalmente si se tiene que invertir en plataformas tecnológicas para automatizar procesos y controles el área de sistemas posee un presupuesto anual para adquisición de equipos y software que puede utilizar en este proyecto.

La idea de mi tesis se basa en poder enfocar mi modelo de medición de riesgo estándar. Esto quiere decir que cualquier tipo de empresa sea esta sector financiero, bancario y comercial pueda adaptarlo o adquirirlo a su empresa para así poder manejar el riesgo y disminuirlo de manera evidente que permita controlar las fallas sistemáticas y sobretodo el control del dinero que pueda perder la misma.

A continuación se detalla el costo incurrido para el desarrollo del proyecto:

HARDWARE		
Equipo informático		\$ 1.200,00
SOFTWARE		
Visual Studio NET 2013		\$ 646,00
Subtotal		\$ 1.846,00

Recurso Humano	Valor por hora	Total
<i>60 horas de consultoría</i>	25	\$ 1.500,00
<i>80 horas de desarrollo del modelo</i>	25	\$ 2.000,00
Subtotal		\$ 3.500,00

Resumen:	Total
Hardcare	\$ 1.200,00
Software	\$ 646,00
Recurso Humano	\$ 3.500,00
TOTAL	\$ 5.346,00

Como se puede apreciar el costo para el desarrollo del proyecto es de \$ 5.346,00, el mismo que se espera posicionarlo en el mercado a un valor de \$8,500.00 que incluye 80 horas de asesoría para el desarrollo e implementación del proyecto contando con el personal operativo y soporte técnico que brinda la institución contratante.

Importancia del Diseño de la Metodología de Riesgo Operacional

El Comité de Supervisión Bancaria propuso una definición de la gestión del riesgo operativo, la cual radica en la identificación, evaluación, monitoreo, control y mitigación de riesgos.

Por ende al encontrarse intrínsecamente relacionado con todos los procesos de la institución su importancia es vital para el desarrollo y optimización del manejo operativo de los procesos debido a que:

- 1) Identificar y analizar el impacto negativo de las fallas operacionales en la cuenta de resultados.
- 2) Incremento del nivel de eficiencia operativa.
- 3) Mayor nivel de servicio frente a los clientes y agentes externos.
- 4) Mayor nivel de transparencia corporativa.
- 5) Mayor eficiencia en la cobertura del riesgo operacional.

Por ende al elevar la calidad del proceso se verá reflejado directamente en el estado de resultados del ejercicio, debido a que al optimizar los procesos, los errores disminuyen y el costo por error se mitiga, causando una reducción en costos operativos y en reutilización del personal para el monitoreo constante por medio de controles a los procesos críticos de la institución.

Otros índices financieros

Activos productivos / total activos	Mide la calidad de las colocaciones o la proporción de activos que generan rendimientos.. La relación mientras más alta es mejor.
Activos productivos / pasivos con costo	Mide la eficiencia en la colocación de recursos captados. La relación mientras más alta es mejor.
Pasivos con costo / total pasivos	Mide la proporción de pasivos que causan costo. La relación, mientras más baja es mejor.
Cartera vencida / total cartera	Mide la proporción de la caretra que se encuentra en mora. La relación mientras más baja es mejor.
Cartera en riesgo / total cartera y contingentes	Mide la proporción de la cartera y contingentes que se encuentran en mora. La relación mientras más baja es mejor.
Provisiones de cartera / cartera vencida	Mide el nivel de protección que la entidad asume ante el riesgo de cartera morosa. La relación mientras más alta es mejor.
Provisiones de cartera y contingentes / total cartera y contingentes	Mide el nivel de protección que la entidad asume ante el riesgo de cartera y contingentes morosos. La relación mientras más alta es mejor.
Provisiones / activos de riesgo	Mide el nivel de protección que la entidad asume ante el riesgo de pérdida o incobrabilidad de sus activos y contingentes. La relación mientras más alta es mejor.
Cartera en riesgo – provisiones / patrimonio	Mide el efecto sobre el patrimonio de la cartera vencida, sin cobertura de provisiones. La relación mientras más baja es mejor.

Total pasivo / patrimonio	Mide el nivel de endeudamiento asumido por la entidad en relación al patrimonio. La relación mientras más baja es mejor.
Activos improductivos / patrimonio	Mide el nivel de contribución de los recursos patrimoniales para la adquisición de activos improductivos. Una relación mayor al 100 % implica el uso de recursos de terceros. La relación mientras más baja es mejor.
Activos inmovilizados / patrimonio	Mide el nivel de contribución de los recursos patrimoniales destinados a la adquisición de activos fijos y de bienes recibidos en dación. La relación mayor al 100 % implica el uso de recursos de terceros. La relación mientras más baja es mejor.
Total pasivo / total activo	Mide el nivel en que los activos han sido financiados por recursos de terceros. La relación mientras más baja es mejor.

Fondos disponibles / depósitos hasta 90 días	Mide el nivel de disponibilidad que tiene la entidad para atender el pago de pasivos de mayor exigibilidad. La relación mientras más alta es mejor.
<u>Liquidez ampliada:</u> Cálculo dispuesto en el título VII, subtítulo VI, capítulo II de la codificación de resoluciones de la Superintendencia de Bancos y Junta Bancaria.	Mide el nivel de recursos líquidos que tiene la entidad para atender el pago de pasivos exigibles. La relación mientras más alta es mejor.

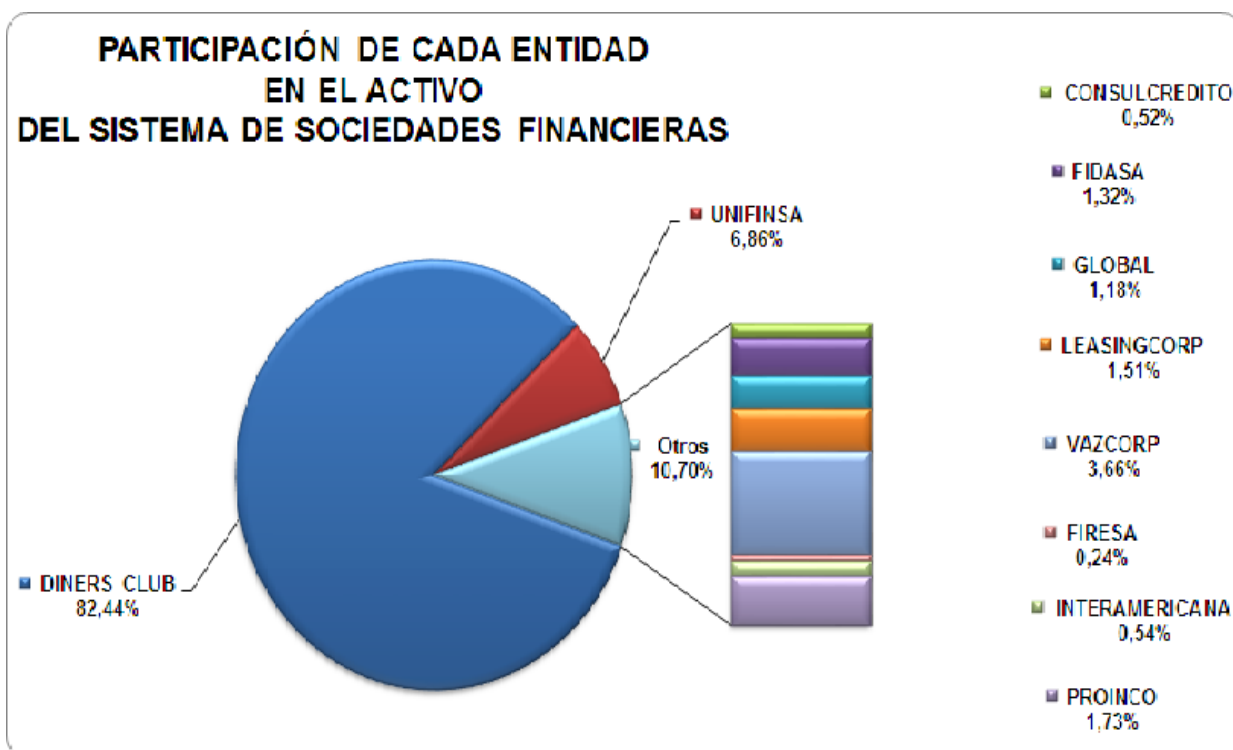
Resultado de ejercicio / patrimonio promedio	Mide el nivel de retorno generado por el patrimonio. La relación entre más alta es mejor.
Resultado operativo del ejercicio / patrimonio promedio	Mide el nivel de utilidad o pérdida que generó la gestión operativa de la entidad en relación al patrimonio. La relación entre más alta es mejor.
Resultado del ejercicio / total activo promedio	Mide el nivel de retorno generado por el activo. La relación entre más alta es mejor.
Resultado operativo del ejercicio / total activo promedio	Mide el nivel de utilidad o pérdida que generó la gestión operativa de la entidad en relación al activo. La relación entre más alta es mejor.
Ingresos extraordinarios netos / resultado operativo	Mide el nivel de utilidad o pérdida generada por actividades que no son propias del giro del negocio. La relación entre más baja es mejor.
Resultados operativos / margen bruto financiero	Mide el nivel de utilidad o pérdida generada por actividades de intermediación. La relación entre más alta es mejor.

Margen bruto financiero / ingresos de la gestión de intermediación	Representa la rentabilidad de la gestión de intermediación en relación a los ingresos generados por dicha actividad. La relación entre más alta es mejor.
Margen bruto financiero + ingresos ordinarios / Activos productivos promedio	Representa la rentabilidad de la gestión operativa en relación con los activos generadores de ingresos. La relación entre más alta es mejor.
Egresos operacionales / margen bruto financiero + ingresos	Establece el nivel de absorción de los egresos operacionales en los ingresos provenientes de la gestión operativa. La relación entre más baja es

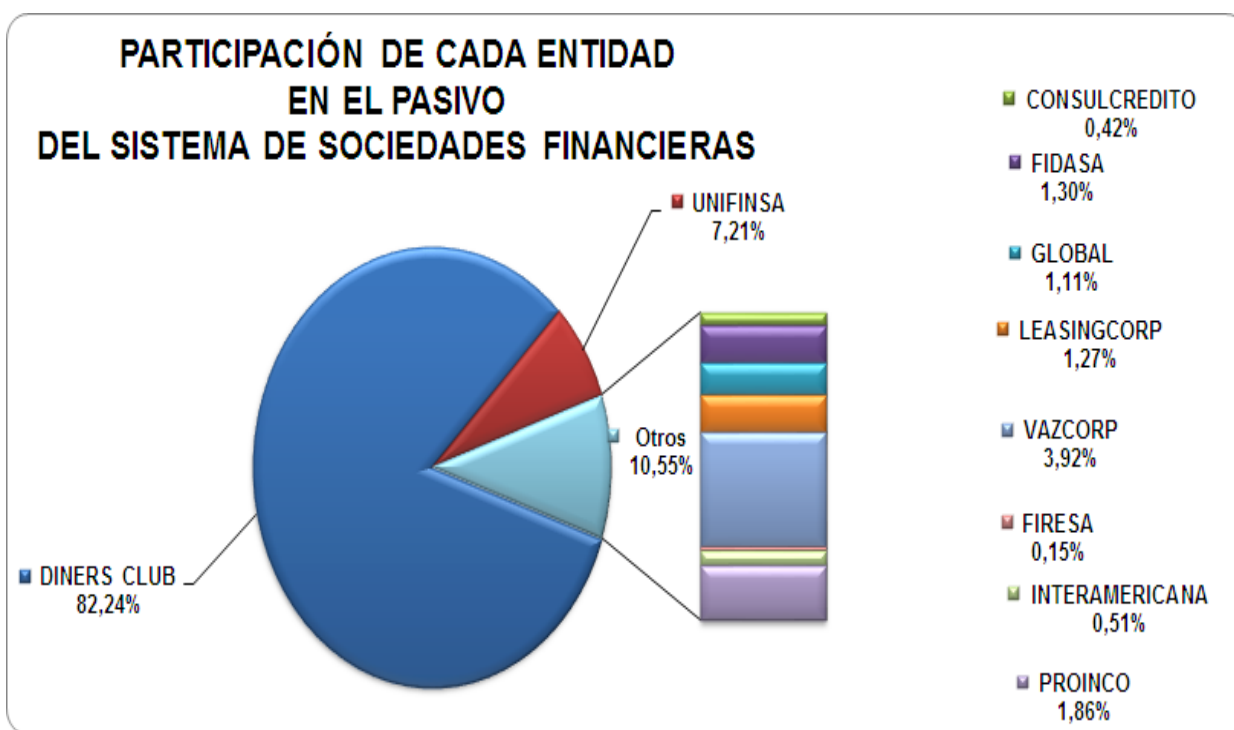
ordinarios	mejor.
Ingresos financieros / activos productivos promedio	Representa la tasa de rendimiento de los activos productivos. La relación entre más alta es mejor.
Egresos financieros / activos productivos promedio	Representa el nivel de costo implícito en el financiamiento de los activos productivos. La relación entre más baja es mejor.
Egresos financieros / pasivos con costo promedio	Representa la tasa de costo de los pasivos generadores de costo. La relación entre más baja es mejor.
<u>Diferencial financiero:</u> Ingresos financieros / activos productivos promedio menos egresos financieros / pasivos con costo promedio	Representa la diferencia entre la tasa activa de colocaciones y la tasa pasiva de captaciones. La relación entre más alta es mejor.
Egresos operacionales / total activo promedio	Representa la carga operacional implícita en el financiamiento de los activos. La relación entre más baja es mejor.
Egresos operacionales / total de recursos captados promedio	Representa la carga operacional implícita de las captaciones. La relación entre más baja es mejor.
Gastos de personal / total activo promedio	Representa el costo de personal implícito en el manejo de activos. La relación entre más baja es mejor.
Gastos de personal / total de recursos captados promedio	Representa el costo de personal implícito en las captaciones

Ingresos y comisiones ganados de cartera y aceptaciones bancarias / total cartera + aceptaciones bancarias en circulación, promedio	Representa el rendimiento de la cartera y aceptaciones bancarias. La relación entre más alta es mejor
Intereses ganados inversiones / total inversiones promedio	Representa el rendimiento de las inversiones en valores mobiliarios. La relación entre más alta es mejor.

Comisiones ganadas contingentes / avales, fianzas, cartas de crédito y anticipos promedio	Representa el rendimiento de las operaciones contingentes. La relación entre más alta es mejor
Intereses y comisiones pagados depósitos / total depósitos + fondos interbancarios comprados promedio	Representa el costo de las captaciones. La relación entre más baja es mejor.
Intereses pagados créditos instituciones financieras / créditos instituciones financieras promedio	Representa el costo de los préstamos recibidos por parte de otras instituciones financieras. La relación entre más baja es mejor.
Intereses pagados valores en circulación / valores en circulación promedio	Representa el costo de los valores en circulación recibidos por parte de otras instituciones financieras. La relación entre más baja es mejor.



Este Cuadro representa la participación en Activos de las entidades relacionadas del sector (Sociedades Financieras) en el sistema financiero en la cual se muestra la partición del activo total en el sistema por cada una de las entidades, siendo el 10.70% de todo el sistema las diferentes sociedades financieras.



Este Cuadro representa la participación en Pasivos de las entidades relacionadas del sector (Sociedades Financieras) en el sistema financiero en la cual se muestra la partición del pasivo total en el sistema por cada una de las entidades, siendo el 10.55% de todo el sistema las diferentes sociedades financieras.

**RANKING EN BASE A LA PARTICIPACION DE LAS PRINCIPALES CUENTAS DEL BALANCE
SISTEMA DE SOCIEDADES FINANCIERAS**

31-dic-13

(en miles de dólares y porcentajes)

ACTIVOS				
ENTIDADES	30/11/2013	30/11/2013	31/12/2013	31/12/2013
	\$	%		%
DINERS CLUB	1.467.009,33	81,84	1.475.754,67	82,44
UNIFINSA	131.511,74	7,34	122.842,02	6,86
VAZCORP	66.085,48	3,69	65.607,74	3,66
PROINCO	32.370,88	1,81	31.057,67	1,73
LEASINGCORP	26.961,84	1,50	27.062,59	1,51
FIDASA	23.890,78	1,33	23.643,09	1,32
GLOBAL	20.945,76	1,17	21.055,15	1,18
INTERAMERICANA	11.901,67	0,66	9.597,06	0,54
CONSULCREDITO	9.588,50	0,53	9.329,43	0,52
FIRESA	2.311,61	0,13	4.220,22	0,24
TOTAL SISTEMA	1.792.577,60	100,00	1.790.169,65	100,00

Como puede observarse en este ranking la financiera supero el 1% de participacion contable dado como esta el mercado entre 5 y 7 puntos se distribuyen en mas de 5 entidades, cumpliendo asi el objetivo en funcion de resultados en libros.

CONCLUSIONES Y RECOMENDACIONES

Análisis de los resultados de la implementación

De acuerdo a los análisis obtenidos de la implementación de la metodología de gestión de riesgo operacional en la institución en las cual trabajamos podemos concluir en lo siguiente:

En términos de costos debido a la obligatoriedad de la implementación de la normativa, las instituciones realizaron una rotación del personal solo incurriendo en el costo de la capacitación del mismo para el cargo a desempeñar, debido a esto se contrató a una empresa externa a realizar el estudio de los procesos, el inventario y paralelamente con los dueños del procesos documentar en los respectivos manuales según formato definido por la consultora.

Debido a que no existen bases de datos de factores de riesgo ni de eventos de riesgo asociadas, estadísticamente es imposible medir la probabilidad real de los eventos que se vayan suscitando, por ende al inicio de la medición las instituciones se basaran en sus cálculos con los porcentajes que el comité de Basilea definen para el tipo de mercado en el cual las instituciones rigen su negocio, esto es banca minorista con un porcentaje del **18%**.

Normativamente las instituciones están cumpliendo con el objetivo del ente regulador de control pero deberán ser evaluadas IN-SITU para verificar que todo el marco metodológico de la norma sea cubierto en su totalidad especialmente en los tres factores de riesgo Personas, Procesos y Tecnología de Información.

Debido a los controles implementados en los procesos de las instituciones, existió resistencia por parte de los usuarios de los mismos, pero esto se contrarrestó por la decisión del gobierno corporativo de incluir en el código interno una política orientada al riesgo en el cual se deberán cumplir todo lo requerido por las metodologías expuestas para el mismo.

Existen implementados bajo esta metodología aproximadamente 145 controles asociados a los procesos tanto críticos como gobernantes y de soporte excluyendo los temas de tecnología de información debido a que se manejó la metodología COBIT para evaluar el proceso de seguridades y de gestión de hardware y software

Conclusiones

Podemos concluir que este trabajo es de suma importancia no solo para las instituciones financieras sino para cualquier tipo de PYME debido a la problemática actual que adolece toda organización que es la gestión correcta de sus procesos. Se debe de concientizar a las personas dentro de la organización que el gestionar cualquier tipo de proceso es vital para el negocio por ende cualquier error implicaría pérdidas monetarias ya seas estas insignificantes como cuantiosas y no debemos de esperar que sucedan sino revisar el procedimiento y hacer el seguimiento respectivo.

Las personas dentro de la organización son las llamadas a identificar todos los posibles eventos de pérdida, adicionalmente también deben de controlar y mitigar los

mismos, concluyendo que las personas son el factor vital para que las alertas del riesgo operacional cumplan su cometido y sean eficaz al momento de ejecutar cualquier tipo de producto o servicio que la institución desee ofertar en el mercado.

Concluimos además, que el diseño de esta metodología nos ayudó a definir los parámetros en los cuales la organización deberá trabajar para redefinir sus procesos que adolecen de insuficiencias, por ende, producen pérdidas monetarias, así mismo, nos permitió reforzar el ámbito de control interno creando diferentes tipos de controles en los procesos críticos de la cadena de valor de la misma, al igual, que documentar todos los procesos para sí llevar a la organización a una mejora continua y de optimización para que todo su negocio genere rentabilidad.

Recomendaciones

Se recomienda que las instituciones realicen y verifiquen sus inventarios de procesos periódicamente debido a cambios por mejora continua o por innovación que los mismos puedan suscitarse. También se recomienda la definición formal de los procesos por medio de manuales para que en todos los casos exista documentado absolutamente toda la operatividad de la institución así como definido una metodología de procesos críticos para tomar ciertas precauciones en el caso de personal nuevo o de apoyo que en su momento gestione los mismos.

Se recomienda que exista una difusión de todas las políticas y procedimientos de la institución a través de medios electrónicos tales como intranets, webs institucionales y demás

para que toda la organización este realmente informada de todos los cambios que existan e tanto en procesos como en rotación de personal en la institución.

Bibliografía

- Antón, Gasol, & Magriña. (2007). *LA INDUSTRIA BANCARIA EN EL MARCO DE BASILEA II* (2da ed.). (Magriña, Ed.) Barcelona, España: Gasol.
- C, Alexander. (2002). *Advanced Risk Management* (2da ed.). Washington, Estados Unidos: IFF.
- Coleman, R. (2000). Using Modeling in Operational Risk Management. *Conference* (pág. 90). Madrid: McGraw Hill.
- Coopers, & Lybrand. (1997). *Los nuevos conceptos de control interno (Informe COSO)* (1era ed., Vol. 1). Madrid, España: Ediciones Díaz de Santos.
- Fernandez Laviada, A. (2008). *LA GESTION DEL RIESGO OPERACIONAL* (1era ed.). España: Ediciones 2010.
- Hernandez Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (2007). *METODOLOGIA DE INVESTIGACION* (5ta ed.). (McGraw-Hill, Ed.) Colombia: Interamericana de Mexico, 2010.
- Hurtado de Barrera, J. (2009). *METODOLOGIA DE LA INVESTIGACION* (4ta ed.). (Quiron, Ed.) Medellin, Colombia: CIEA SYPAL.
- Internacional, B. (2003). Comite de Basilea y la Supervision de la Banca. *The 2002 Lost Data Collection Exercise for Operational Risk*, 110.
- Jimenez Rodríguez, E. (2010). *EL RIESGO OPERACIONAL: METODOLOGIAS PARA SU MEDICION Y CONTROL* (1era ed.). Madrid, España: Delta.
- Jorion, P. (2000). *Value at Risk: The New Benchmark for Managing Financial Risk* (1era ed.). New York, Estados Unidos: McGraw Hill.
- Llorente Olier, J. I. (2010). *ANALISIS DE ESTADOS ECONOMICOS FINANCIEROS* (1era ed.). Mexico: Centro de Estudios Financieros.
- Medina Giopp, A. (2005). *GESTION POR PROCESOS Y CREACION DE VALOR PUBLICO*. (E. Búho, Ed.) Santo Domingo, Republica Dominicana: INTEC.
- Neil, M, & Tranham E. (2002). *Using Baesian Networks to predict op risk* (2da ed.). (D. d. Santos, Ed., & m. Hill, Trad.) Barcelona , España: Ediciones de Santos.

Perdomo Moreno, A. (2004). *FUNDAMENTOS DE CONTROL INTERNO* (9va ed.). Madrid, España: Thompson.

Perez Fernandez, J. (2010). *GESTION POR PROCESOS* (4ta ed.). MADRID, TORREJON DE ARDOZ, ESPAÑA: ESIC.

Privada, B. (2001). *Basel Committee on Banking Supervision*. Milan, Italia: McGraw Hill.

Rhoer, A. (2002). *Modeling Operational Losses* (Vol. vol 5). Sidney, Australia: ALGO RESEARCH QUARTERLY.

Rodríguez Valencia, J. (2002). *CONTROL INTERNO. UN EFECTIVO SISTEMA PARA LA EMPRESA* (1era ed.). (Eduforma, Ed.) Barcelona, España: Trillas.

Smithson, C. W. (1998). *Managing Financial Risk* (3era ed.). Lisboa, Portugal: McGraw-Hill.

Soley Sans, J. (2007). *BASILEA II: UNA NUEVA FORMA DE RELACION BANCA EMPRESA* (2da ed.). (I. D. ESPAÑA, Ed.) Madrid, España: MCGRAW-HILL.

Suarez Suarez, A., & Ramiro Martís, F. (2012). *Gestión por procesos* (1era ed.). (C. Catalán de Ávila, Ed.) Oviedo, España: Universidad de Oviedo.

Torres, A. (2002). *Probabilidad, Variables Aliatorias, Confiabilidad y Procesos Estocasticos* (1era ed.). Mexico: Universidad de los Andes.

Anexos:

Anexo 1: Matriz de Monitoreo

MATRIZ DE MONITOREO PARA SEGUIMIENTO					
Institución Financiera: Institucion S.A.					
Fecha de Corte: 30 DE JUNIO 2013					
No.	OBSERVACIONES POR COMPONENTE/SUBCOMPONENTE GREC	MEDIDA DE ACCIÓN Unidad de Auditoria	COMENTARIO DE LA IFI	DOCUMENTO DE DESCARGO	FECHA DE CUMPLIMIENTO
	RIESGO DE CREDITO				
	IDENTIFICACION				
	PLAN ESTRATEGICO				
1	<p>El plan estratégico-negocio para el año 2013 aprobado por el Directorio en sesión celebrada el 20 de febrero de 2.013, no se sustenta en variables del entorno macro económico del país y en las previsiones financieras de la propia entidad, que le permitan efectuar proyecciones acordes con los objetivos determinados en su planeación.</p> <p>Se han establecidos proyecciones de crecimiento de cartera de crédito para el periodo económico de 2013 en un 15,07% en forma global, teniendo el mayor crecimiento el segmento de cartera de crédito de vivienda en 48,32%, el mismo que no está acorde al producto ofrecido por la entidad financiera que es el financiamiento de vehículos.</p> <p>No se ha podido alcanzar las metas de colocación de cartera de crédito llegando al mes de septiembre de 2.013 al -14,76%. El segmento de cartera que presenta mayor diferencia entre los valores proyectados y los valores reales es la cartera de vivienda con el 58,98%, seguido de la cartera de crédito comercial 42,40%, cartera de consumo con el 10,34%. Por el contrario, el segmento de cartera microcrédito supera las metas de proyección en el 4,68%.</p> <p>La Unidad de Riesgos tiene a cargo el monitoreo de la competencia, el cual consiste en mantener informado a la Gerencia General, de las estrategias, tasas y plazos de otras instituciones financieras, permitiendo a la administración poder replantear las estrategias, políticas, y tasas conforme al mercado del existente, no ha sido realizado hasta la presente fecha.No existe un documento formal en el cual se pueda evidenciar la participación de las unidades de negocio para la actualización de escenarios probables de negocio (colocación y captaciones) que se detallan en el Plan Estratégico- Negocio</p>	<p>El Directorio y la Gerencia General del Institucion S.A., deberán elaborar la planificación estratégica a mediano y largo plazo, como parte de un proceso organizado y continuo.</p> <p>La Planificación Estratégica debe comprender la distribución de los recursos a largo plazo para lograr los objetivos de la institución. El plan operativo debe considerar las medidas a corto plazo que permitan dar cumplimiento a los objetivos estratégicos.</p> <p>El Directorio, deberá aprobar el Plan Estratégico y los cambios efectuados al mismo, considerando, como mínimo, los siguientes aspectos:</p> <ul style="list-style-type: none"> • Establecer la misión y visión de la entidad • Evaluación de las operaciones internas. • Evaluación del entorno operativo, tecnológico y financiero, presente y futuro. <ul style="list-style-type: none"> • Formulación de metas y objetivos. • Estrategias a adoptar para alcanzar las metas. <ul style="list-style-type: none"> • Asignación de recursos adecuados. • Implementación de planes por cada unidad de la financiera. <ul style="list-style-type: none"> • Ejecución y análisis de los resultados. • Plan de contingencias financiero y tecnológico. <ul style="list-style-type: none"> • Revisión del plan. 	<p>Responsables: Directorio y Gerente General Ing. Nury Díaz Calderón</p> <p>Se cumplirá lo observado</p> <p>Se ha contratado los servicios de un Asesor Externo para la elaboración del Plan Estratégico que abarcará todas las recomendación indicadas por el Organismo de Control.</p> <p>Actualmente se está trabajando en el levantamiento de información. Fecha de Cumplimiento: 31 de Marzo del 2014.</p>	<p>Anexo N°01. Acta de Sesión de Directorio celebrada el 17 de Marzo del 2014.</p>	<p>mar-14</p>

Anexo 2: Mapa de Procesos

Proceso	Tipo de Proceso	Sub-Proceso	Riesgo No.	Actividades
APERTURA DE DEPÓSITOS A PLAZO FIJO	PRODUCTIVO	GESTION DE MERCADEO	1	Consigue inversionistas a través de referidos de clientes, amigos, familiares, prensa, flyers
			2	Contacta a los posibles clientes
			3	Envía información del producto
			4	Concreta cita y da información del producto
			5	Negocia los términos para la apertura del Depósito
			6	Cierra negociación con el cliente
			7	Si el contacto decide no invertir, hace seguimiento hasta conseguir que invierta
		RECEPCION DE INFORMACION	1	Entrega de documentación al cliente
			2	Recepción de documentación del cliente

Anexo 3: Principios Básicos de Basilea

25 Principios Básicos de Basilea

Condiciones previas para una efectiva Supervisión Bancaria

1. Proporcionar un sistema de supervisión bancaria efectivo en el cual las responsabilidades y proyectos estén bien definidos para cada una de las instituciones involucradas permitiendo así la supervisión de organizaciones bancarias. Cada institución debe poseer independencia operativa y contar con recursos adecuados. Es necesario contar con leyes apropiadas para la supervisión bancaria, que incluyan provisiones relacionadas con la autorización de organizaciones bancarias y su supervisión; facultades para aplicar las leyes, así como aspectos de seguridad, solvencia y protección legal para los supervisores. También es necesario realizar arreglos para compartir información entre supervisores y proteger la confidencialidad de tal información.

Autorizaciones y Estructura

2. Las actividades que les son permitidas a las instituciones bancarias que son reguladas, deben estar claramente definidas y el uso de la palabra Banco como nombre debe ser controlado lo más posible.

3. La autoridad reguladora debe tener el derecho para plantear criterios y rechazar las solicitudes que no cumplen con los requerimientos. El proceso de autorización debe realizar como mínimo una evaluación de la estructura de la organización bancaria, abarcando a propietarios, directores y la administración superior, el plan operativo, control interno y la situación financiera proyectada, incluyendo su capital base. Deberá obtenerse el

consentimiento previo del supervisor regional cuando el propietario propuesto u organización matriz sea un banco extranjero.

4. Los supervisores bancarios deben de tener la facultad para analizar y la autoridad de rechazar:

a. cualquier propuesta para transferir propiedades significativas o cuantiosas.

b. controlar intereses de bancos existentes en otros grupos empresariales.

5. Los supervisores bancarios deben tener la autoridad para establecer criterios para analizar adquisiciones de gran importancia o inversiones por un banco, asegurándose de que las afiliaciones o estructuras corporativas, no expongan al banco a riesgos excesivos ni entorpezcan la supervisión bancaria.

Regulaciones prudenciales y requerimientos

6. Los supervisores bancarios deben establecer en forma prudente y apropiada los requerimientos mínimos de capital para todos los bancos. Estos requerimientos deben reflejar el riesgo al que los bancos se exponen y deben definir los componentes de este capital, tomando en cuenta su capacidad de absorber pérdidas. Para bancos internacionalmente activos, estos requerimientos no deben ser menores a los establecidos en el Acuerdo de Capitales de Basilea y sus enmiendas.

7. Es esencial para cualquier sistema de supervisión bancaria la evaluación de las políticas, prácticas y procedimientos de un banco, usados para la aprobación de préstamos e inversiones y para la administración de las carteras de préstamos e inversiones.

8. Los supervisores bancarios deben estar cómodos y satisfechos con las políticas, prácticas y procedimientos que establezcan y rijan a los bancos para evaluar la calidad de activos, las provisiones y reservas por pérdidas relacionadas con préstamos.

9. Los supervisores bancarios, deben estar satisfechos con los sistemas de información gerencial de los bancos que les permitan identificar concentraciones dentro de la cartera. Los supervisores deben establecer límites prudenciales y adecuados para restringir la exposición del banco a los préstamos individuales y a los préstamos de grupos empresariales relacionados a los bancos.

10. Para prevenir abusos con los préstamos relacionados, los supervisores bancarios deben tener establecidos y asegurados los requerimientos básicos que los bancos deben cumplir, para que:

a- tal extensiones de crédito sean monitoreadas y supervisadas efectivamente.

b- les sea permitido tomar otras medidas para controlar o disminuir los riesgos.

11. Los supervisores bancarios deben estar satisfechos con las políticas y procedimientos de los bancos para identificar, monitorear y controlar los riesgos del país, los riesgos en sus actividades de préstamos e inversiones internacionales y para mantener reservas apropiadas contra tales riesgos.

12. Los supervisores bancarios deben estar satisfechos con el sistema de los bancos para medir con gran precisión, monitorear y controlar adecuadamente los riesgos del mercado; los supervisores deben tener el poder para imponer límites y/o cargas de capital específicas cuando hay exposición a riesgos en el mercado, que le permitan garantizar el capital activo del banco.

13. Los supervisores de bancos deben estar conformes con el proceso integral para:

- a-** el manejo de los riesgos a nivel administrativo (por medio de una junta o consejo administrativo apropiado y la adecuada supervisión de una administración superior).
- b-** identificar, medir, monitorear y controlar todos los demás objetos de riesgos.
- c-** retener el capital en contra de estos riesgos, cuando sea necesario.

14. Los supervisores bancarios deberán determinar que el control interno de los bancos se encuentran en orden, acorde a la naturaleza y escala de sus negocios. Estos controles internos deberán incluir:

- a-** arreglos para delegar autoridad y responsabilidad a una persona (separándolos de las funciones que puedan comprometer al banco, pagando sus cuentas y llevando registros de sus bienes y compromisos).
- b-** arreglos para la conciliación de estos procesos (salvaguardando de esta forma sus bienes).
- c-** arreglos para una auditoría interna o externa independiente y apropiada (la cual servirá para poner a prueba el seguimiento a estos controles, leyes y regulaciones previamente establecidos).

15. Los supervisores bancarios deben determinar que los bancos tengan políticas, prácticas y procedimientos adecuados, que incluyan la estricta regla de *“CONOCE A TU CLIENTE”*, lo cual promueve altos estándares de ética y profesionalismo en el sector financiero. Estas medidas previenen que los bancos sean utilizados por elementos criminales, en una forma voluntaria o involuntaria.

Métodos de Supervisión Bancaria Progresiva

16. Un sistema de supervisión bancaria efectivo debe de consistir de dos formas de supervisión:

a- una supervisión dentro del lugar de trabajo.

b- una supervisión fuera del lugar de trabajo.

17. Los supervisores bancarios deben mantener un regular contacto con la gerencia de los bancos y un fluido entendimiento en las operaciones de la institución.

18. Los supervisores bancarios deben tener métodos para recolectar, examinar y analizar reportes y datos estadísticos de los bancos en:

a- una base individual.

b- una base consolidada.

19. Los supervisores bancarios deben mantener medios para determinar que la información obtenida en la supervisión sean válidas ya sea por medio de: a- exámenes realizados directamente en el lugar realizando una auditoría externa (con auditores externos).

20. Los supervisores bancarios deben poseer la capacidad para supervisar el grupo bancario en una base consolidada. Siendo esto un elemento esencial en la supervisión de bancos.

Requisitos de Información

21. Los supervisores bancarios deben asegurarse que cada banco mantenga registros adecuados, diseñados de manera que concuerden con políticas contables consistentes, con prácticas que permitan al supervisor obtener una visión verdadera y precisa de la condición financiera del banco y de la rentabilidad de sus negocios y que el banco haga publicaciones regulares del estado financiero, que reflejen realmente su condición.

Poderes formales de los Supervisores

22. Los supervisores bancarios deben tener la facultad de realizar acciones correctivas a tiempo

cuando:

a- los bancos falten al cumplimiento de ciertos requerimientos prudenciales (como los rangos de capital mínimo).

b- existan violaciones a las regulaciones.

c- los depositantes se vean amenazados de alguna manera.

En circunstancias extremas, los supervisores de bancos deben poseer la autoridad, para revocar la licencia del banco o recomendar su revocación.

Bancos Extra-Fronterizos

23. Los supervisores de bancos deben practicar la supervisión global consolidada en organizaciones bancarias internacionalmente activas, aplicando y monitoreando apropiadamente en todos los aspectos las normas prudenciales, a los negocios manejados por estas organizaciones bancarias alrededor del mundo, primordialmente a sus sucursales extranjeras, co-inversiones y subsidiarias.

24. Un componente clave en la supervisión consolidada es establecer el contacto entre los supervisores involucrados y establecer intercambios de información entre todos los demás supervisores involucrados, primordialmente con las autoridades supervisoras del país anfitrión.

25. Con el propósito de llevar a cabo una supervisión consolidada los supervisores bancarios deben:

a- requerir que las operaciones locales de bancos extranjeros, sean conducidas bajo los mismos estándares que son requeridos a las instituciones locales.

b- poseer poderes para compartir la información del supervisor local encargado de estos bancos.

Anexo 4:

CAPÍTULO V.- DE LA GESTIÓN DEL RIESGO OPERATIVO (incluido con Resolución No JB-2005-834 de 20 de octubre del 2005)

SECCIÓN I.- ÁMBITO, DEFINICIONES Y ALCANCE

ARTÍCULO 1.- Las disposiciones de la presente norma son aplicables a las instituciones financieras públicas y privadas, al Banco Central del Ecuador, 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, cuyo control compete a la Superintendencia de Bancos y Seguros, a las cuales, en el texto de este capítulo se las denominará como instituciones controladas. Para efecto de administrar adecuadamente el riesgo operativo, además de las disposiciones contenidas en el capítulo I “De la gestión integral y control de riesgos”, las instituciones controladas observarán las disposiciones del presente capítulo.

ARTÍCULO 2.- Para efectos de la aplicación de las disposiciones del presente capítulo, se considerarán las siguientes definiciones:

2.1 Alta gerencia.- La integran los presidentes y vicepresidentes ejecutivos, gerentes generales, vicepresidentes o gerentes departamentales, entre otros, responsables de ejecutar las disposiciones del directorio u organismo que haga sus veces, quienes toman decisiones de alto nivel, de acuerdo con las funciones asignadas y la estructura organizacional definida en cada institución controlada;

2.2 Evento de riesgo operativo.- Es el hecho que puede derivar en pérdidas financieras para la institución controlada;

2.3 Factor de riesgo operativo.- Es la causa primaria o el origen de un evento de riesgo operativo. Los factores son los procesos, personas, tecnología de información y eventos externos;

2.4 Proceso.- Es el conjunto de actividades que transforman insumos en productos o servicios con valor para el cliente, sea interno o externo;

2.5 Insumo.- Es el conjunto de materiales, datos o información que sirven como entrada a un proceso;

2.6 Proceso crítico.- Es el indispensable para la continuidad del negocio y las operaciones de la institución controlada, y cuya falta de identificación o aplicación deficiente puede generarle un impacto financiero negativo;

2.7 Actividad.- Es el conjunto de tareas;

2.8 Tarea.- Es el conjunto de pasos o procedimientos que conducen a un resultado final visible y medible;

2.9 Procedimiento.- Es el método que especifica los pasos a seguir para cumplir un propósito determinado;

2.10 Línea de negocio.- Es una especialización del negocio que agrupa procesos encaminados a generar productos y servicios especializados para atender un segmento del mercado objetivo definido en la planificación estratégica de la entidad;

2.11 Datos.- Es cualquier forma de registro electrónico, óptico, magnético, impreso o en otros medios, susceptible de ser capturado, almacenado, procesado y distribuido;

2.12 Información.- Es cualquier forma de registro electrónico, óptico, magnético o en otros medios, previamente procesado a partir de datos, que puede ser almacenado, distribuido y sirve para análisis, estudios, toma de decisiones, ejecución de una transacción o entrega de un servicio; (reformado con resolución No. JB-2012-2148 de 26 de abril del 2012)

2.13 Información crítica.- Es la información considerada esencial para la continuidad del negocio y para la adecuada toma de decisiones;

2.14 Administración de la información.- Es el proceso mediante el cual se captura, procesa, almacena y transmite información, independientemente del medio que se utilice; ya sea impreso, escrito en papel, almacenado electrónicamente, transmitido por correo o por medios electrónicos o presentado en imágenes;

2.15 Tecnología de información.- Es el conjunto de herramientas y métodos empleados para llevar a cabo la administración de la información. Incluye el hardware, software, sistemas operativos, sistemas de administración de bases de datos, redes, multimedia, servicios asociados, entre otros;

2.16 Aplicación.- Se refiere a los procedimientos programados a través de alguna herramienta tecnológica, que permiten la administración de la información y la oportuna toma de decisiones;

2.17 Instalaciones.- Es la infraestructura que permite alojar los recursos físicos relacionados con la tecnología de información;

2.18 Responsable de la información.- Es la persona encargada de identificar y definir claramente los diversos recursos y procesos de seguridad lógica relacionados con las aplicaciones;

2.19 Seguridad de la información.- Son los mecanismos implantados que garantizan la confidencialidad, integridad y disponibilidad de la información y los recursos relacionados con ella;

2.20 Seguridades lógicas.- Se refieren a la seguridad en el uso del software, la protección de los datos, procesos y programas, así como la del acceso ordenado y autorizado de los usuarios a la información;

2.21 Confidencialidad.- Es la garantía de que sólo el personal autorizado accede a la información preestablecida;

2.22 Integridad.- Es la garantía de mantener la totalidad y exactitud de la información y de los métodos de procesamiento;

2.23 Disponibilidad.- Es la garantía de que los usuarios autorizados tienen acceso a la información cada vez que lo requieran a través de los medios adecuados que satisfagan sus necesidades;

2.24 Cumplimiento.- Se refiere a la observancia de las leyes, regulaciones y acuerdos contractuales a los que los procesos de las instituciones controladas están sujetos;

2.25 Pista de auditoría.- Es el registro de datos lógicos de las acciones o sucesos ocurridos en los sistemas aplicativos u operativos, con el propósito de mantener información histórica para fines de control, supervisión y auditoría;

2.26 Medios electrónicos.- Son los elementos de la tecnología que tienen características digitales, magnéticas, inalámbricas, ópticas, electromagnéticas u otras similares;

2.27 Transferencia electrónica de información.- Es la forma de enviar, recibir o transferir en forma electrónica datos, información, archivos, mensajes, entre otros;

2.28 Encriptación.- Es el proceso mediante el cual la información o archivos son alterados en forma lógica, con el objetivo de evitar que alguien no autorizado pueda interpretarlos al verlos o copiarlos, por lo que se utiliza una clave en el origen y en el destino;

2.29 Plan de continuidad.- Está orientado a asegurar 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. Un plan de continuidad incluye un plan de contingencia, un plan de reanudación y un plan de recuperación;

2.30 Plan de contingencia.- Es el conjunto de procedimientos alternativos a la operatividad normal de la entidad cuya finalidad es la de permitir su funcionamiento, buscando minimizar el impacto financiero que pueda ocasionar cualquier evento inesperado específico. El plan de contingencia se ejecuta el momento en que se produce dicho evento;

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

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

2.33 Eficacia.- Es la capacidad para contribuir al logro de los objetivos institucionales de conformidad con los parámetros establecidos;

2.34 Eficiencia.- Es la capacidad para aprovechar racionalmente los recursos disponibles en pro del logro de los objetivos institucionales, procurando la optimización de aquellos y evitando dispendios y errores;

2.35 Calidad de la información.- Es el resultado de la aplicación de los mecanismos implantados que garantizan la efectividad, eficiencia y confiabilidad de la información y los recursos relacionados con ella; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

2.36 Efectividad.- Es la garantía de que la información es relevante y pertinente y que su entrega es oportuna, correcta y consistente; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

2.37 Confiabilidad.- Es la garantía de que la información es la apropiada para la administración de la entidad, ejecución de transacciones y para el cumplimiento de sus obligaciones; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

2.38 Banca electrónica.- Son los servicios suministrados por las instituciones del sistema financiero a los clientes a través de internet en el sitio que corresponda a uno o más dominios de la institución, indistintamente del dispositivo tecnológico a través del cual se acceda; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

2.39 Banca móvil.- Son los servicios suministrados por las instituciones del sistema financiero a los clientes a través de equipos celulares mediante los protocolos propios de este tipo de dispositivos; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

2.40 Tarjetas.- Para efectos del presente capítulo, se refiere a las tarjetas de débito, de cajero automático y tarjetas de crédito; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

2.41 Canales electrónicos.- Se refiere a todas las vías o formas a través de las cuales los clientes o usuarios pueden efectuar transacciones con las instituciones del sistema financiero, mediante el uso de elementos o dispositivos electrónicos o tecnológicos, utilizando o no tarjetas. Principalmente son canales electrónicos: los cajeros automáticos (ATM), dispositivos de puntos de venta (POS y PIN Pad), sistemas de audio respuesta (IVR), señal telefónica, celular e internet u otro similares; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

2.42 Tarjeta inteligente.- Tarjeta que posee circuitos integrados (chip) que permiten la ejecución de cierta lógica programada, contiene memoria y microprocesadores y es capaz de proveer seguridad, principalmente en cuanto a la confidencialidad de la información de la memoria; y, (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

2.43 Riesgo legal.- Es la probabilidad de que una institución del sistema financiero sufra pérdidas directas o indirectas; de que sus activos se encuentren expuestos a situaciones de mayor vulnerabilidad; de que sus pasivos y contingentes puedan verse incrementados más allá de los niveles esperados, o de que el desarrollo de sus operaciones enfrente la eventualidad de ser afectado negativamente, debido a error, negligencia, impericia, imprudencia o dolo, que deriven de la inobservancia, incorrecta o inoportuna aplicación de disposiciones legales o normativas, así como de instrucciones de carácter general o particular emanadas de los organismos de control, dentro de sus respectivas competencias; o, en sentencias o resoluciones jurisdiccionales o administrativas adversas; o de la deficiente redacción de los textos, formalización o ejecución de actos, contratos o transacciones, inclusive distintos a los de su giro ordinario de negocio, o porque los derechos de las partes contratantes no han sido claramente estipuladas. (Sustituido con resolución No. JB-2008-1202 de 23 de octubre del 2008 y renumerado con resolución No. JB-2012-2148 de 26 de abril del 2012).

De acuerdo con lo dispuesto en el numeral 2 del artículo 18 del Código Civil, los términos utilizados en la definición de riesgo legal se entenderán en su sentido natural y obvio, según el uso general de las mismas palabras, a menos de que tengan definiciones diferentes expresadas en la ley, reglamentos y demás normativa. (Incluido con resolución No. JB-2008-1202 de 23 de octubre del 2008)

ARTÍCULO 3.- Para efectos del presente capítulo, el riesgo operativo se entenderá como la posibilidad de que se ocasionen pérdidas financieras por eventos derivados de fallas o insuficiencias en los procesos, personas, tecnología de información y por eventos externos.

El riesgo operativo incluye el riesgo legal en los términos establecidos en el numeral 2.43 del artículo 2. El riesgo operativo no trata sobre la posibilidad de pérdidas originadas en cambios inesperados en el entorno político, económico y social.