

ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE CIENCIAS

METODOLOGÍA PARA LA ADMINISTRACIÓN INTEGRAL DEL RIESGO OPERATIVO EN INSTITUCIONES FINANCIERAS BASADAS EN LAS MEJORES PRÁCTICAS DE LA INDUSTRIA

**PROYECTO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE
INGENIERO EN LA CARRERA DE CIENCIAS ECONÓMICAS Y FINANCIERAS**

DIANA FERNANDA BARRIONUEVO BALLADARES
ve_dfbb@hotmail.com

Director: Ing. Carlos Fernando Cevallos Jácome
fcevallosj@gmail.com

Quito, octubre 2011

DECLARACIÓN

Yo, Diana Fernanda Barrionuevo Balladares, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

La Escuela Politécnica Nacional puede hacer uso de los derechos correspondientes a este trabajo, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

DIANA FERNANDA BARRIONUEVO BALLADARES

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por la Srta. Diana Fernanda Barrionuevo Balladares, bajo mi supervisión.

Ing. Fernando Cevallos.

DIRECTOR

ÍNDICE DE CONTENIDO

	Lista de Figuras.....	I
	Lista de Tablas.....	II
	Lista De Anexos.....	III
	Resumen.....	IV
	Abstract.....	V
1	INTRODUCCIÓN.....	1
1.1	Antecedentes.....	1
1.2	Planteamiento del Problema.....	3
1.3	Formulación y sistematización del problema.....	3
1.4	Objetivos.....	4
1.5	Justificación.....	4
1.6	Hipótesis.....	5
1.7	Variables e Indicadores.....	5
2	MARCO TEÓRICO.....	7
2.1	Sistema Financiero.....	7
2.1.1	Sistema Financiero Ecuatoriano.....	7
2.1.1.1	Integrantes.....	7
2.1.1.2	Funciones.....	8
2.2	Indicadores Financieros.....	8

2.2.1	Calidad Activos.....	8
2.2.2	Calidad de la Cartera.....	9
2.2.3	Liquidez.....	9
2.2.4	Rentabilidad.....	9
2.3	Regulación del Comité de Basilea.....	9
2.3.1	Necesidad de Regulación.....	9
2.3.2	Comité de Basilea.....	10
2.3.3	Acuerdos de Capitales de Basilea (Basilea I).....	11
2.3.3.1	Normas Generales.....	11
2.3.3.2	Riesgo de la Actividad Bancaria.....	12
2.3.3.3	Riesgo Operacional.....	13
2.4	Acuerdo de Basilea II.....	14
2.4.1	Introducción.....	14
2.4.2	Ámbito de Aplicación.....	15
2.4.3	Los Tres Pilares.....	16
2.4.3.1	Pilar I: Requerimientos Mínimos de Capital.....	16
2.4.3.2	Pilar II: Proceso del Examen Supervisor.....	16
2.4.3.3	Pilar III: Disciplina del Mercado.....	17
2.4.4	Tipos de Evento de Riesgo Operativo.....	18
2.4.5	Gobierno Corporativo.....	20
2.4.6	Principios de Basilea para una administración sólida del Riesgo de Operación.....	21

3	NORMATIVA NACIONAL Y METODOLOGÍAS APLICADAS AL RIESGO OPERATIVO.....	24
3.1	Antecedentes.....	24
3.2	Resolución JB2005-834: De la Gestión del Riesgo Operativo.....	24
3.2.1	Procesos.....	27
3.2.2	Personas.....	27
3.2.3	Tecnología de la Información.....	28
3.2.4	Eventos Externos.....	28
3.3	Administración del Riesgo Operativo en el Sistema Financiero Ecuatoriano.....	28
3.3.1	Ciclo del Riesgo Operativo.....	29
3.3.2	Responsabilidades en la Administración del Riesgo Operativo....	31
3.4	Identificación Top Dow-Bottom up.....	32
3.4.1	Fases de la Metodología de Gestión del Riesgo Operacional a nivel corporativo.....	33
3.5	CORRE (Control de los Recursos y los Riesgos Ecuador).....	40
4	METODOLOGIA COSO Y SIMULACION MONTE CARLO...	50
4.1	Introducción.....	50
4.2	Implementación del Riesgo de Operación.....	51
4.2.1	Metodología COSO.....	53
4.2.1.1	COSO-ERM.....	54
4.2.1.1.1	Ambiente de Control.....	58

4.2.1.1.2	Establecimiento de Objetivos.....	60
4.2.1.1.3	Identificación de Eventos.....	61
4.2.1.1.4	Evaluación de Riesgo.....	62
4.2.1.1.5	Respuesta al Riesgo.....	64
4.2.1.1.6	Actividades de Control.....	65
4.2.1.1.7	Información y Comunicación.....	68
4.2.1.1.8	Monitoreo.....	69
4.3	Propuesta Metodológica para el Riesgo Operativo.....	70
4.3.1	Planteamiento de la Propuesta.....	71
4.4	Desarrollo de Metodologías aproximadas para la cuantificación del Riesgo Operativo.....	93
4.4.1	Modelaje de Pérdidas Esperadas en Riesgo Operativo.....	93
4.4.2	Medición Cuantitativa del Riesgo Operativo.....	102
4.4.3	Metodología de Medición de Riesgo Operativo según Basilea.....	108
4.4.3.1	Proceso.....	108
4.4.3.1.1	Modelo Montecarlo.....	111
4.4.3.1.2	Resultados del Modelo.....	114
5	CONCLUSIONES Y RECOMENDACIONES.....	119
	BIBLIOGRAFÍA.....	122
	ANEXOS.....	124

LISTA DE FIGURAS

Figura 1	Pilares de Basilea II.....	18
Figura 2	Ciclo del Riesgo Operativo.....	29
Figura 3	Ciclo del Riesgo Operativo Ampliado.....	32
Figura 4	Integración Top dow-Bottom up.....	33
Figura 5	COSO I (Control Interno-Marco Conceptual Integrado) y COSO II-ERM: Marco de Gestión Integral de Riesgo.....	55
Figura 6	Componentes del COSO-ERM.....	56
Figura 7	Criterio de Impacto.....	82
Figura 8	Enfoque de Análisis de Riesgo.....	83
Figura 9	Evaluación del Riesgo de un Proceso.....	84
Figura 10	Estrategias de mitigación de riesgo.....	85
Figura 11	Riesgo Residual.....	85
Figura 12	Matriz de Riesgo por Proceso.....	87
Figura 13	Distribución de pérdidas.....	94
Figura 14	Distribución de pérdidas sesgadas.....	94
Figura 15	Proceso Markoviano.....	96

Figura 16	Flujo de pérdidas.....	98
Figura 17	Evolución Ps en función de n.....	99
Figura 18	Histograma de Frecuencias.....	105
Figura 19	Modelo de Riesgo Operacional.....	106
Figura 20	Resultados de Modelo Montecarlo.....	116

LISTA DE TABLAS

Tabla 1	Variables del Riesgo Operacional.....	6
Tabla 2	Tipos de Actividades de Control.....	67
Tabla 3	Asignación de las Líneas de Negocio.....	74
Tabla 4	Clasificación Detallada de Tipos de Eventos de Pérdida por Niveles.....	77
Tabla 5	Guía de Uso: Para la Elaboración de una Matriz por Proceso.....	89
Tabla 6	Guía de Uso: Matriz de Riesgo.....	91

LISTA DE ANEXOS

- ANEXO 1 Reglamento Ley Financiera.
- ANEXO 2 Eventos de Riesgo.
- ANEXO 3 Segmentos de las Instituciones Financieras.
- ANEXO 4 Base de Datos.
- ANEXO 5 Diagnóstico de la empresa
- ANEXO 6 Formulario de recolección de datos de pérdida
- ANEXO 7 Resultados de la Simulación Montecarlo

RESUMEN EJECUTIVO

El Sistema Financiero del Ecuador ha centrado su análisis y control de riesgos en aquellos llamados financieros, como son los riesgos de liquidez, tasas de interés, crédito y tipo de cambio. Sin embargo, el desarrollo de los mercados financieros ha identificado otro tipo de riesgo que las Instituciones Financieras deben administrar y monitorear, éste es el Riesgo Operativo, considerado por la Superintendencia de Bancos y Seguros (SBS) como las pérdidas resultantes de un manejo no adecuado de los procesos internos, personas o sistemas, o por la falta de previsión de eventuales efectos externos que amenacen con ocasionar eventuales pérdidas.

Con el fin de introducir el concepto de riesgo y establecer un ambiente de estabilidad al interior del Sistema Financiero ecuatoriano, la Superintendencia de Bancos y Seguros, en base a lo dispuesto por el acuerdo de capital de Basilea aprobó la resolución JB2005-834, para el manejo y control del Riesgo Operacional, con el fin de que las Instituciones Financieras del Ecuador cuenten con las normas para una adecuada administración del Riesgo de Operación.

El Riesgo Operativo es fundamental dentro de la administración preventiva e integral del riesgo, por tanto, de acuerdo a los requerimientos que plantea la norma vigente, las Instituciones Financieras requieren contar con recursos humanos calificados, mecanismos, políticas y procesos que reduzcan las posibles pérdidas operacionales. Adicionalmente, se deben establecer estándares mínimos prudenciales de administración del Riesgo Operación y garantizar un capital mínimo necesario para cubrir este tipo de riesgos.

Sin embargo, no existen reglas estrictas para la correcta administración del Riesgo de Operación. Este documento busca dar pautas mediante una metodología para un correcto monitoreo y control del mismo, basado en los principios propuestos por el Acuerdo del Capital Basilea II y por las recomendaciones planteadas por la Superintendencia de Bancos y Seguros en su resolución JB2005-834. Adicionalmente busca complementar estas propuestas con algunas prácticas nacionales e internacionales con el fin de servir como guía a las Instituciones Financieras para el mejor manejo del Riesgo de Operación, como parte de su Gestión Integral de Riesgos.

En los primeros capítulos de este documento se dará una visión global a las mejores prácticas para la administración y monitoreo del Riesgo Operacional, tomando en cuenta las pautas sugeridas por la Superintendencia de Bancos y Seguros y las recomendaciones planteadas por Basilea que han sido aplicadas en otros países. En el siguiente capítulo se planteará una metodología para el cálculo de las pérdidas operativas dentro de las Instituciones Financieras, de forma que se cuente con una herramienta para el control de las pérdidas derivadas del Riesgo de Operación.

El objetivo de este análisis es lograr que las instituciones privadas del Sistema Financiero del Ecuador identifiquen los factores de Riesgo Operativo que alteran el normal funcionamiento del negocio, con el fin de que se tomen las medidas necesarias para la mitigación y control del Riesgo Operacional, y de esta manera, se dé cumplimiento a lo establecido por la Superintendencia de Bancos y Seguros para minimizar las pérdidas ocasionadas por este tipo de riesgo.

ABSTRACT

The Financial System of Ecuador has focused its analysis and control of financial risks in those calls, such as liquidity risk, interest rates, credit and exchange rate. However, the development of financial markets has identified another type of risk that financial institutions should manage and monitor, this is the Operational Risk, considered by the Superintendency of Banks and Insurance (SBS) and the losses resulting from inappropriate handling internal processes, people or systems, or lack of foresight of any external effects that threaten to cause leaks.

To introduce the concept of risk and establish a stable environment inside the Ecuadorian financial system, the Superintendency of Banks and Insurance, based on the provisions of the Basel Capital Accord adopted resolution JB2005-834, for Risk management and operational control, in order that Ecuador's financial institutions have adequate standards for Operational Risk Management.

Operational Risk is essential in the prevention and integral management of risk, therefore, according to the requirements posed by the current rule, financial institutions are required to have skilled human resources, mechanisms, policies and processes that reduce operational losses . Additionally, it should establish minimum standards of prudential risk management operation and ensure a minimum capital required to cover such risks.

However, there are no strict rules for the proper management of operational risks. This paper seeks to provide guidance through a proper methodology for monitoring and control thereof, based on the principles proposed by the Basel II Capital Accord and the recommendations made by the Superintendency of Banks and Insurance JB2005-834 resolution. Additionally seeks to complement these proposals with some national and international practices to serve as a guide to Financial Institutions for the best risk management operation, as part of its Integrated Risk Management.

In the early chapters of this document will give an overview of best practices for managing and monitoring operational risk, taking into account the guidelines suggested by the Superintendency of Banks and Insurance and the recommendations made by Basel have been applied in other countries. In the next

chapter will consider a methodology for calculating operating losses in financial institutions, so that has a tool to control the losses from operational risks.

The objective of this analysis is to ensure that private institutions of Ecuador's financial system to identify operational risk factors that alter the normal operation of the business, so that necessary measures are taken to mitigate and control operational risk and thus giving effect to the provisions of the Banking and Insurance to minimize losses caused by this type of risk.

CAPITULO I

1. INTRODUCCION

1.1 Antecedentes

El Análisis del riesgo es un proceso por el cual se identifican, miden, controlan y monitorean los diferentes riesgos a los que se encuentra expuesta una Institución Financiera, con el fin de definir el tipo y el nivel máximo de pérdida que está dispuesta a asumir dicha institución en el desarrollo del negocio, así como las medidas de control y los mecanismos de cobertura para proteger los recursos que se encuentran bajo su administración. Esto implica un permanente control frente a los riesgos, tanto internos como externos.

El sistema bancario ecuatoriano ha tenido un desarrollo importante dentro de un proceso de consolidación y crecimiento. La relativa estabilidad económica de los últimos años ha permitido la reactivación del sector, así como también la entrada de nuevos participantes. Es por ello que la supervisión de las instituciones financieras es fundamental dentro de un entorno económico sólido, con el fin de asegurar que los bancos operen de manera sana y que mantengan el capital y reservas suficientes para dar soporte a los riesgos que surgen en su negocio.

La ley general de Instituciones Financieras (LGISF) está en vigencia desde el año 1994, y su última modificación fue en el año 2001; su función es regular el funcionamiento y las operaciones de este sector. Esta ley ha sido modificada en varias ocasiones, con el objeto de cubrir las deficiencias y establecer bases legales y sólidas para evitar crisis como la del año 1999.¹

La Superintendencia de Bancos y Seguros tiene a su cargo el control y vigilancia del Sistema Financiero así como también las Compañías de Seguros. (Ver Anexo 1)

¹ Crisis Bancaria Financiera causada principalmente por la liberación de la ley bancaria, excesiva deuda pública, devaluación de la moneda, inestabilidad política y especulación. Terminó con el congelamiento de los depósitos bancarios, el cierre definitivo de varias instituciones del Sistema Financiero y por último, adoptando a la dolarización como medida de estabilización.

El Sector Financiero Ecuatoriano, en base a las normas planteadas por la Junta Bancaria, se han centrado en el análisis y control de los llamados riesgos financieros: tasas de interés, de crédito y liquidez. Sin embargo, el desarrollo de los mercados financieros ha identificado otro tipo de riesgo que las instituciones deben medir, cuantificar y mitigar, el llamado Riesgo Operativo, evidenciando como el riesgo de pérdidas resultantes de un inadecuado manejo de los procesos internos, personas o sistemas, o por la falta de previsión de eventuales efectos externos que amenacen con ocasionar eventuales pérdidas.

El Acuerdo de Basilea señala una gestión integral de riesgo que incluya el reconocimiento, monitoreo constante y aplicación de políticas para la mitigación del Riesgo Operacional. Para su aplicación, exige que las Instituciones Financieras enfrenten desafíos importantes, como la implementación dentro de su estructura organizacional un Comité de Administración Integral de Riesgos, la evaluación en las metodologías internas para el manejo de los riesgos de crédito y operacional; la recopilación y organización de gran cantidad de información, documentos y procedimientos de administración, etc.; con el fin de lograr un equilibrio entre riesgo y rentabilidad; además de establecer un ambiente de solidez y estabilidad en el Sistema Financiero Ecuatoriano. La Junta Bancaria, sobre la base de los dispuesto por el Acuerdo de Basilea II, aprobó la resolución JB2005-834², para el manejo y control del Riesgo Operacional, con el fin de establecer las normas para una adecuada administración de este tipo de riesgos, los cuales deben ponerse en práctica permanente en las instituciones que están bajo su control, de acuerdo a lo que está determinado en dicha resolución.

² Sobre la Gestión Integral y control de Riesgos. Noviembre 2005 (Ver Anexo 2)

1.2 Planteamiento del Problema

El Riesgo Operacional ha sido el último de los riesgos objeto de tratamiento por el sector financiero, después del riesgo de mercado y el riesgo de crédito. Este ha recibido fundamentalmente un tratamiento cualitativo; sin embargo, la importancia de su implementación se debe al aumento de las pérdidas ocasionadas por el desconocimiento del mismo, las fallas en los procesos entre otros.

La ausencia de medidas que permitan controlar, monitorear y mitigar el Riesgo de Operación dentro de las Instituciones Financieras y la falta de conocimiento sobre el mismo, llevo a la Superintendencia de Bancos y Seguros (SBS) ha emitir la resolución JB 2005-834 el 05 de Octubre del 2005, y fue publicada por la misma el 09 de Noviembre del 2005. Sin embargo, el proceso de adaptación incluye reformas legales y normativas y cambios en las políticas, procesos y procedimientos, lo cual implica tiempo en la aplicación e incluye resistencia en la implementación.

El objetivo de este análisis es valorar las metodologías que puedan contribuir a las Instituciones del Sistema Financiero para mitigar y disminuir el riesgo causado por los errores operativos, los cuales alteran el normal funcionamiento del negocio, con el fin de que se tomen las medidas necesarias para el control del Riesgo Operacional, de manera que se dé cumplimiento a los establecido por la Superintendencia de Bancos y Seguros y se minimice las pérdidas ocasionadas por el mismo.

1.3 Formulación y Sistematización del Problema

Las siguientes son las preguntas básicas que serán respondidas por medio de la investigación:

Preguntas de Diagnóstico

- ¿Cuáles son las políticas más adecuadas adoptadas por las instituciones financieras de acuerdo a lo que plantea Basilea para manejar el Riesgo Operativo?
- ¿Cuáles han sido los efectos causados en las Instituciones Financieras sobre la resolución de la Superintendencia de Bancos y Seguros para la aplicación del Riesgo Operativo en el Ecuador en la actualidad?

Preguntas de Propuesta

- ¿Cuáles serían las medidas de mitigación que deben tomarse en cuenta en las Instituciones del Sector Financiero Ecuatoriano para reducir el nivel de pérdidas ocasionadas al incurrir en riesgos operacionales?

1.4 Objetivos

a). Objetivo General

Establecer el efecto del Riesgo Operacional en las instituciones financieras controladas por la Superintendencia de Bancos y Seguros.

b). Objetivos Específicos

- i. Analizar los acuerdos de Basilea I y II para establecer las políticas más adecuadas para el manejo del Riesgo Operativo.
- ii. Identificar y establecer una base conceptual del Riesgo Operativo que vaya acorde con la resolución establecida por la Superintendencia de Bancos y Seguros.
- iii. Proponer alternativas a las instituciones del Sistema Financiero para mitigar los Riesgos Operacionales.

1.5 Justificación

La identificación del riesgo es un proceso continuo el cual se dirige a reconocer y entender los riesgos existentes en cada operación efectuada dentro de las instituciones.

Para la implementación de una metodología de administración del riesgo operativo las instituciones deben cumplir con códigos de ética y conducta formalmente establecidas con la supervisión del directorio de la organización, el cual va hacer las veces de la alta gerencia, con una sólida cultura de control interno.

Al identificar los eventos y factores de riesgo se puede medir el impacto, el mismo que debe ser cuantificado o medido, con el objeto de determinar el cumplimiento de las políticas, los límites fijados y el impacto económico en la organización; para así permitir a la administración disponer los controles y correctivos necesarios.

En el proceso del desarrollo de esta administración hay que reflejar la complejidad de las operaciones y el nivel de riesgo que las instituciones asumieron. Como parte del sistema de control interno la administración de las instituciones del sistema financiero deben establecer controles administrativos, financieros, contables, tecnológicos, en procesos y personas necesarios para asegurar que la administración del riesgo operativo sea adecuada, todo este proceso debe ser respaldado por la política de cada institución.

1.6 Hipótesis

- ✓ Los Acuerdos de Basilea I y II han servido a las Instituciones Financieras controladas por la Superintendencia de Bancos y Seguros para regular sus operaciones.
- ✓ La resolución JB2005-834 emitida por la Superintendencia de Bancos y Seguros establece los parámetros adecuados para manejar el Riesgo Operativo.
- ✓ Las instituciones financieras que manejan el Riesgo Operativo pueden mitigar, minimizar, transferir y eliminar los errores cometidos en sus operaciones

1.7 Variables e Indicadores

Las variables del riesgo operativo serán utilizadas para el estudio y análisis, las mismas que complementos de las hipótesis y requieren observar cada una; las variables internas de las instituciones financieras sirven para identificar los factores principales del riesgo operativo y observa de qué forma se ven afectadas las mismas, todo esto con el fin de establecer parámetros de medición. A continuación se muestra el cuadro de las variables:

TABLA. 1

Variables del Riesgo Operacional	Indicadores
1. Fraude Interno	Casos de fraudes internos, frecuencia, tipo, magnitud.
2. Fraude Externo	Número de transacción fraudulenta, tipo, magnitud.
3. Prácticas relacionadas con clientes, productos y el negocio	Cuantificación de la pérdida, frecuencia de la pérdida.
4. Daños y activos físicos	Número de activos dañados, frecuencia del daño.
5. Interrupción del negocio	Posibles pérdidas por interrumpir el funcionamiento en un tiempo determinado, frecuencia de la interrupción.
6. Fallas en la ejecución de procesos	Frecuencia de ocurrencia eventos de riesgo, magnitud de las pérdidas por fallas en la ejecución de procesos. Pruebas en los procesos y controles operativos.
7. Política Laboral	Incumplimiento de procedimientos y políticas. Posibles pérdidas por contratar capacitación, etc.
8. Eventos de pérdidas	Bases de Datos con clasificación de eventos de riesgo.

CAPITULO II

2. MARCO TEORICO

2.1 Sistema Financiero

El sistema financiero se define como el conjunto de instituciones cuyo objetivo es canalizar el excedente que generan las unidades de gasto con superávit para encauzarlos hacia las unidades que tienen déficit.

La transformación de los activos financieros emitidos por las unidades inversoras en activos financieros indirectos, más acordes con las demandas de los ahorradores, es en lo que consiste la canalización. Esto se realiza principalmente por la no coincidencia entre unidades con déficit y unidades con superávit, es decir, ahorradores e inversores. Del mismo modo que los deseos de los inversores y ahorradores son distintos, los intermediarios han de transformar estos activos para que sean más aptos a los últimos.

La eficiencia de esta transformación será mayor cuanto mayor sea el flujo de recursos de ahorro dirigidos hacia la inversión.

El que las distintas unidades económicas se posicionen como excedentarias o deficitarias podrá ser debido a razones como: la riqueza, la renta actual y la esperada, la posición social, si son unidades familiares o no lo son, la situación económica general del país y los tipos de interés (las variaciones de estos puede dar lugar a cambios en los comportamientos en las unidades de gasto).

2.1.1 Sistema Financiero Ecuatoriano

2.1.1.1 Integrantes

Se puede entender al Sistema Financiero Nacional, como el conjunto de instituciones financieras (bancos, sociedades financieras, asociaciones mutualistas de ahorro y crédito para la vivienda y las cooperativas de ahorro y crédito) que realizan intermediación financiera con el público³.

- ***Estructura del Sistema Financiero Nacional***

Autoridades Monetarias: Banco Central del Ecuador, Superintendencia de Bancos, Junta Bancaria.

³ Sistema Financiero Nacional (Ecuador), Ma. Fernanda Bonilla, 2009

Instituciones Financieras Públicas: Corporación Financiera Nacional, Banco Ecuatoriano de la Vivienda, Banco Nacional de Fomento, Banco del Estado, Instituto Ecuatoriano de Crédito Educativo y Becas.

Instituciones Financieras Privadas: Bancos Privados, Sociedades Financieras, Asociaciones Mutualistas de Ahorro y Crédito para la vivienda, Cooperativas de Ahorro y Crédito que realizan intermediación Financiera con el público.

Instituciones de Servicios Financieros: Almacenes Generales de Depósitos, Compañías de Arrendamiento Mercantil, Compañías emisoras o administradoras de tarjetas de crédito, Casas de cambio, Corporaciones de Garantía y Retro garantía, Compañías de Titularización.

Instituciones de Servicios Auxiliares del Sistema Financiero: Transporte de especies monetarias y valores, Servicios de Cobranza, Cajeros, entre otros.

2.1.1.2 Funciones

Los bancos y las sociedades financieras o corporaciones de inversión y desarrollo se caracterizan principalmente por ser intermediarios en el mercado financiero, en el cual actúan de manera habitual, captando recursos del público para obtener fondos a través de depósitos o cualquier otra forma de captación, con el objeto de utilizar los recursos así obtenidos, total o parcialmente, en operaciones de crédito e inversión⁴.

2.2 Indicadores Financieros

2.2.1. Calidad Activos

El activo es el conjunto de todas las posesiones de la entidad, sean en efectivo, papeles convertibles, bienes o acreencias. Para el diagnóstico del activo se suelen utilizar el siguiente indicador:

⁴ Art. 2 Ley de Instituciones del Sistema Financiero

Activos productivos / activo total.- Mide la calidad y eficiencia de las colocaciones o la porción de activos que generan rendimientos. La relación, mientras más alta mejor.

2.2.2. Calidad de la Cartera

La cartera de créditos es una parte importante en las instituciones financieras de la cual depende en gran parte el éxito de las operaciones. Para analizar el estado de la cartera crediticia se utilizan entre otros, los siguientes índices:

Cartera vencida / cartera total.- Conocido como el índice de morosidad, mide la porción de la cartera que se encuentra en mora. La relación mientras más baja mejor.

Provisiones / cartera vencida.- Mide el nivel de cobertura que guarda la institución frente a la cartera morosa. Una cobertura por el orden del 100% o mayor, de acuerdo a la cobrabilidad de la cartera, es considerada saludable.

2.2.3. Liquidez

La liquidez de una institución financiera permite que esta pueda operar normalmente, atendiendo las necesidades de efectivo de los clientes. Un índice que se utiliza para analizar los niveles de liquidez es:

(Fondos disponibles + inversiones) / (Depósitos a la vista + depósitos a plazo).- Mide el nivel de disponibilidad que tiene la entidad para atender el pago de sus pasivos. La relación mientras más alta mejor.

2.2.4. Rentabilidad

- **Resultados / patrimonio promedio:** Mide el nivel de generado por el patrimonio. La relación mientras más alta es mejor.
- **Resultados / activo promedio:** Mide el nivel de retorno generado por el activo. La relación mientras más alta es mejor.

2.3 Regulación del Comité de Basilea

2.3.1 Necesidad de Regulación

Las instituciones financieras, al ser un importante sector de la economía, la cual provee servicios de pago, moviliza ahorro y asigna créditos, siempre

han estado bajo la mira de los gobiernos locales para crear regulaciones que garanticen un funcionamiento seguro y rentable de estas entidades. Debido a que estas instituciones manejan una gran cantidad de dinero del público, existe la necesidad de un marco regulatorio que garanticen el correcto accionar de sus actividades financieras y provea cierto grado de seguridad a los usuarios del sector financiero.

A nivel mundial, la regulación bancaria siempre ha tomado muy en cuenta los lineamientos que propone el Comité de Basilea, el cual está conformado por los gobernadores de los bancos centrales de los países del Grupo de los Diez⁵.

Las sugerencias del Comité tienen un alto grado de complejidad en materia financiera ya que se mantienen en constante investigación en cuanto a riesgos bancarios y temas relacionados con el mismo.

Nuestro país al igual que otros en América sigue las directrices del Comité de Basilea; las autoridades regulatorias se encargan de buscar la mejor manera de implementar los principios adoptados en Basilea y difundirlos o normarles. Las leyes que norman la actividad financiera se encuentran difundidas en:

- Constitución de la República
- Codificación de la Ley de Instituciones del Sistema Financiero.
- Ley de Régimen Monetario y Banco del Estado.
- Codificaciones de las Resoluciones de la Superintendencia de Bancos y Junta Bancaria.
- Codificación de las Resoluciones del Directorio del Banco Central del Ecuador.

2.3.2 Comité de Basilea

El Comité tiene por objetivo formular estándares de supervisión para entidades financieras y recomendar las mejores prácticas para que las autoridades locales correspondientes evalúen y coordinen la mejor manera de implementarlas en casa uno de los países.

⁵ Llerena Endara Valeria, Introducción del Riesgo Operacional dentro del Sistema Financiero Ecuatoriano, Quito, 2006

Los miembros del Comité se reúnen regularmente cuatro veces al año en el Banco de Pagos Internacionales en la ciudad de Basilea-Suiza, para discutir acerca de la supervisión a entidades financieras y son asistidos por alrededor de treinta grupos técnicos.

Cada país está representado por un Banco Central, pero también por la autoridad con responsabilidad formal de la supervisión al negocio bancario, que no forman parte del Banco Central.

El Comité no pese ninguna autoridad para supervisión supranacional de carácter formal y por lo tanto es política del Comité no poseer injerencia legal directa sobre ninguna nación en el mundo⁶.

El Comité posee 22 publicaciones oficiales desde marzo de 1982 hasta febrero del 2006; en ellos se puede encontrar varias recomendaciones y documentos técnicos sobre supervisión y manejo prudente de la actividad financiera. Los acuerdos de capitales mejor conocidos como Basilea I y II también constan dentro de estas publicaciones.

2.3.3 Acuerdo de Capitales de Basilea (Basilea I)

2.3.3.1 Normas Generales

En julio de 1988 el Comité de Basilea con su publicación número cuatro “International Convergente of Capital Measurement and Capital Standars”, propuso las normas mínimas que deberían cumplir las entidades financieras para mantener un manejo prudente de sus actividades. El convenio, ahora conocido como Basilea I, se rige bajo cinco principios básicos⁷: **i)**. hacer que los requerimientos de capital guarden relación con diferentes perfiles de riesgo entre bancos; **ii)**. Hacer que las cuentas contingentes sean tomadas en cuenta al calcular la suficiencia de capital; **iii)**. Minimizar los incentivos a tener activos líquidos y de bajo riesgo; **iv)**. Favorecer la cooperación entre las autoridades supervisoras de los principales países industrializados; **v)**. Reducir las desigualdades

⁶ <http://www.wikipedia.org>

⁷ Almeida José Luis, Chimboya Luis Alberto, “Metodología Off Side de Análisis y Supervisión Financiera”, Quito-Ecuador, Renacer 2002, pág. 4

competitivas concedidas por diferencias en las políticas de capital bancario entre países.

Para el tiempo en que este acuerdo salió a la luz pública representó una importante referencia para las instituciones financieras a nivel mundial debido a que abordó la necesidad de regulaciones de capital desde la óptica de la determinación de los riesgos a las que la actividad financiera tenía exposición. Esto fue el principal acierto de Basilea I, a tal punto que el acuerdo llegó a convertirse en un estándar a nivel mundial en materia de regulación como lo explican Wambeke y Herrera (1994) en su estudio sobre suficiencia de capital.

En un análisis de bancos norteamericanos en los años 1982 a 1989, Avery y Berger encuentran que aquellos bancos que no hubieran cumplido con los estándares de Basilea, hubieran tenido una probabilidad mayor de quiebra que aquellos que hubieran cumplido dichos estándares de haber estado vigentes; esto se constituye en puntos a favor del Acuerdo de Basilea I, pero no quiere decir que los requerimientos que planteó son infalibles. Varias críticas se vertieron sobre la metodología aplicada en este acuerdo y muchos de ellos se cristalizaron cuando la crisis financiera mundial acabó paulatinamente con bancos en Asia, Rusia, México. Por ejemplo, Badley, Wambeke y Whidbee (1991) y Cordell, Gordon y Wambeke (1994), concluyeron en sus estudios realizados a instituciones financieras de Estados Unidos que el requerimiento de capital que propone el acuerdo no es suficiente. No obstante, la mayor obvia debilidad de este acuerdo es que, cuando fue difundida en 1998, se centró solamente en un tipo de riesgo, el crediticio; y posteriormente se realizó una enmienda (1996) donde se incorporó el riesgo de mercado.

2.3.3.2 Riesgo de la Actividad Bancaria

El riesgo⁸ es la probabilidad de un evento adverso y sus consecuencias; el *riesgo financiero* se refiere a la probabilidad de ocurrencia de un evento que tenga consecuencias financieras negativas para una organización.

⁸ <http://www.wikipedia.org>

El concepto debe entenderse en sentido amplio, incluyendo la posibilidad de que los resultados financieros sean mayores o menores de los esperados. De hecho, habida la posibilidad de que los inversores realicen apuestas financieras en contra del mercado, movimientos de éstos en una u otra dirección pueden generar tanto ganancias o pérdidas en función de la estrategia de inversión.

La legislación ecuatoriana por su parte, en relación con la normativa planteada a instituciones financieras, define el riesgo como “la posibilidad de que se produzca un hecho generador de pérdidas que afecten el valor económico de las instituciones”⁹ y establece claras directrices de cómo las instituciones financieras deben cubrirse de los riesgos. En el artículo primero de la codificación dónde se encuentra la definición de riesgo, la Superintendencia de Bancos y Seguros insta a las entidades financieras bajo su supervisión a realizar prácticas prudentes sobre el control de riesgos.

Art. 1.- 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, conforme su objeto social, sin perjuicio de cumplimiento de las obligaciones que sobre la materia establezcan otras normas especiales y/o particulares.

La administración integral de riesgos es parte de la estrategia institucional y del proceso de toma de decisiones.

2.3.3.3 Riesgo Operacional

El Riesgo Operacional se entiende como la posibilidad de que se ocasionen pérdidas potenciales¹⁰ resultantes de sistemas inadecuados,

⁹ Codificación de Resoluciones de la Superintendencia de Bancos y Seguros-Título VII-Subtítulo VI- Cap. I- Sección I-Art 2-Inciso 1.

¹⁰ Zorrilla Salgado Juan Pablo, La administración de riesgos, 2004.

fallas administrativas, controles defectuosos, fraude, o error humano. La definición incluye el riesgo legal¹¹ y excluye el riesgo reputacional¹².

El Riesgo de operación ha recibido un tratamiento cualitativo en las instituciones financieras, a través de la Área de Riesgos y Control Interno. Su análisis cuantitativo parte de los pilares establecidos en el acuerdo de Basilea II, sin embargo, su cuantificación no ha alcanzado el mismo grado de desarrollo que en el caso del riesgo crediticio y de mercado. Al plantear una exigencia de capital mínimo, Basilea II buscó crear incentivos para que las instituciones financieras desarrollen técnicas que permitan cuantificarle de manera más ajustada a sus actividades y a los riesgos subyacentes.

2.4 Acuerdo de Basilea II

2.4.1 Introducción

El primer Acuerdo del Comité de Basilea fue un esfuerzo muy loable por regularizar y supervisar la actividad bancaria; además tuvo mucha aceptación ya que varios países que no eran parte del Comité, incluido el Ecuador, pudieron implementar leyes y controles nacionales en concordancia con lo planteado en el acuerdo. No obstante, la metodología de Basilea I fue criticada en muchas ocasiones, debido principalmente a su inflexibilidad frente al rápido avance y evolución de la actividad financiera en el mundo¹³.

En 1997 ocurrió la crisis financiera a nivel mundial, la cual asestó un duro golpe a la credibilidad de las actividades regulatorias, que de una u otra manera, en mayor o menor grado se guiaban en lineamientos similares a los propuestos en Basilea I.

Dentro del nuevo contexto caracterizado por el desarrollo de las actividades financieras y una creciente necesidad de implementar nuevos

¹¹ El Riesgo Legal es la probabilidad de que se presenten pérdidas o contingencias negativas como consecuencia de falla, error, dolo, negligencia o imprudencia en la ejecución de contratos y transacciones que pueden afectar al funcionamiento o condición de una determinada institución.

¹² Las pérdidas operacionales pueden ser directas (pérdidas financieras), indirectas (pérdida de reputación) y de costo de oportunidad (falta de capacidad para acometer negocios). Sin embargo, estas dos últimas debido a su grado de incertidumbre y la dificultad de estimación, se excluye de la definición de Riesgo Operacional.

¹³ Llerena Endara Valeria, Introducción del Riesgo Operacional dentro del Sistema Financiero Ecuatoriano, Quito, 2006

parámetros para el control de capitales nace el Nuevo Acuerdo de Capitales de Basilea más conocido como Basilea II, propuesta que fue presentada en junio de 1994 por el Grupo de los Diez.

El desarrollo de Basilea II respecto a su antecesor es notable ya que abarcan una serie de implementaciones en cuanto al manejo de riesgos, supervisiones externas, manejo de incentivos, incluso se incluyeron rondas constituidas para lograr consensos y depurar ciertos puntos de interés. Basilea II fue concebido, a diferencia de Basilea I, con el conocimiento de que las directrices que tome este acuerdo van a ser seguidas por varias naciones y varios tipos de entidades financieras a pesar de no ser obligatorias.

Se debe destacar que una de las consideraciones nuevas que aparece en Basilea II, y que representa un gran acierto con respecto al acuerdo original, tiene que ver con el tratamiento más depurado y menos intuitivo del riesgo operativo en las entidades financieras. Las cooperativas de ahorro y crédito no están obligadas a calcular el capital mínimo requerido conforme el nuevo acuerdo de Basilea, pero como toda entidad financiera, estas se encuentran expuestas a similares riesgos que la banca pero con distintas magnitudes. Por lo tanto es importante mirar que opciones nos ofrece para la metodología de Basilea II y además resulta interesante poder determinar el impacto de la introducción del riesgo de mercado en estas entidades.

2.4.2 Ámbito de aplicación

El Nuevo Acuerdo de Capitales es aplicable en estricto sentido a bancos con actividad internacional¹⁴, como era el caso de Basilea I; pero en esta ocasión se busca ampliar el marco de acción de la actividad supervisora revisando el accionar consolidado de las entidades, incluyendo (si aplica) el Holding al cual pertenecen. Al ampliar el marco de aplicación de Basilea, se intenta cubrir la exposición a un mayor número de riesgos.

¹⁴ BANCO DE PAGOS INTERNACIONALES – Comité de Supervisión Bancaria de Basilea, “International Convergence Capital Measurement and Capital Standards, A Revised Framework”. Junio 2004, pág.19

2.4.3 Los Tres Pilares

Basilea II se sustenta en tres pilares: 1) Requisitos mínimos de capital, 2) Alcance de la revisión del supervisor y 3) Disciplina del mercado.

2.4.3.1 Pilar I: Requerimientos Mínimos de Capital

En lo que respecta a riesgo de mercado, tiene el mismo tratamiento que el dado en Basilea I. El riesgo de crédito incorpora tres métodos de cálculo: básico, estándar y avanzado, e incentiva el uso de métodos sofisticados que incluyen controles y requisitos cuantitativos y cualitativos. Basilea II incorpora el riesgo de operación y sugiere tres métodos de cálculo sujetos al cumplimiento de criterios de calificación, tales como:

a) Método del Indicador Básico. El requerimiento de capital es igual al promedio de los ingresos brutos del banco en los últimos tres años multiplicado por un factor de 0.15.

b) Método Estándar. Para el método estandarizado se definieron ocho líneas de negocio: finanzas corporativas, negociación y ventas, banca minorista, banca comercial, pagos y liquidación, servicios de agencia, administración de activos e intermediación minorista.

Entonces para el requerimiento de capital se calcula a nivel de cada línea de negocio. Se multiplican los ingresos brutos de cada línea de negocio por unos factores establecidos por el Comité.

Luego se suman todos los resultados para cada línea de negocio.

c) Método Avanzado. Los bancos pueden usar sus propias metodologías, previamente aprobadas por los supervisores de la institución financiera.

2.4.3.2 Pilar II: Proceso del examen supervisor

Su finalidad es asegurar que cada banco cuente con procesos internos confiables para evaluar la suficiencia de su capital, a partir de una apreciación meticulosa de sus riesgos.

Este pilar tiende a fortalecer la labor del supervisor bancario, con el fin de que éste conozca efectivamente el grado de riesgo de las instituciones que

supervisa y a su vez, que las mismas cuenten con el capital suficiente de acuerdo a su perfil de riesgo.

En ese tenor, los supervisores deben evaluar las actividades de riesgo de los bancos y las cuantificaciones que estos realicen de sus requerimientos de capital, debiendo estar en capacidad de determinar cuándo una institución necesita un capital más elevado y las medidas correctivas que deben aplicarse, inclusive requerir a las instituciones que lo necesiten, un capital superior al mínimo normativo así como estar en capacidad de llevar a cabo una intervención temprana de aquellos bancos que lo requieran. La intención del Comité al proponer este pilar es promover un diálogo más activo entre los bancos y sus supervisores para poder actuar con rapidez y decisión; y reducir el riesgo o restaurar el capital cuando se identifiquen deficiencias.

El proceso de supervisión bancaria, además, apunta a cubrir los factores externos, tales como la influencia de comportamientos cíclicos, así como, las áreas del riesgo que no han sido tomadas en cuenta total o parcialmente en el cómputo de los requerimientos de capital. Por ejemplo, riesgos de tipo de interés en la libreta de ahorros e incertidumbres en la medición los riesgos operacionales.

2.4.3.3 Pilar III: Disciplina de Mercado

Su principal objetivo es fomentar la disciplina de mercado sobre las entidades bancarias mediante la divulgación de información financiera veraz y completa.

Eso quiere decir que si los mercados están bien informados, premiarán a aquellas entidades con un perfil de riesgo inferior, contribuyendo, con el apoyo de los dos pilares anteriores, a la estabilidad del sistema bancario.

Con esta mayor transparencia informativa en cuanto a las actividades de un banco, sus controles internos, el manejo de sus exposiciones al riesgo y el papel que el Gobierno Corporativo realiza, el público estará en mejores condiciones para decidir con qué institución bancaria llevará a cabo sus operaciones, premiando a las que manejen sus riesgos prudentemente y penalizando a aquellas que no lo hagan.

En definitiva, este pilar busca que los depositantes estén mejor informados sobre las características y particularidades de los bancos y puedan tomar sus decisiones en función de sus propias valoraciones de riesgo. A su vez, los bancos podrán fijar sus tasas de remuneración en la medida en que demuestren su eficiencia. En resumen se refiere a la motivación para promover seguridad y solidez de las instituciones financieras precisando revelaciones esenciales y suplementarias de información, tanto financiera como no financiera. A continuación se muestra en la Figura 1 el resumen de las características de cada uno de los pilares:

FIG. 1 PILARES DE BASILEA II

PILARES BASILEA II		
PILAR I REQUISITOS MINIMOS DE CAPITAL	PILAR II ALCANCE DE LA REVISION SUPERV.	PILAR III DISCIPLINA DEL MERCADO
RIESGO DE MERCADO	RIESGO DE MERCADO	Motiva esfuerzos para promover seguridad y solidez de las Ifis Precisa revelaciones esenciales de información básica sobre situación del sistema Necesita revelaciones de información suplementaria que hagan efectiva la disciplina del mercado Se requiere revelar información financiera y no financiera
Igual que Basilea I	Bancos tendrán proceso para evaluar suficiencia de capital y estrategias para mantener niveles mínimos	
RIESGO DE CREDITO	RIESGO DE CREDITO	
Cambio significativo de Basilea I Tres métodos para calcular Incentivos para utilizar métodos sofisticados Métodos exigen controles y requisitos cuantitativos y cualitativos Adecuar administración de riesgo de crédito	Evaluar calificaciones internas y suficiencia de capital Se exige que entidades operen por encima de los indicadores de capital mínimo	
RIESGO OPERACIONAL	RIESGO OPERACIONAL	
No cubierto en Basilea I Tres métodos para calcular Adopción del método sujeto a cumplimiento de criterios de calificación definidos	Supervisores intervienen en una etapa temprana para evitar que capital caiga por debajo de niveles mínimos	

Fuente: Basilea II

Elaboración: La autora

2.4.4 Tipos de evento de Riesgo Operativo

De acuerdo con lo establecido en Basilea II, las instituciones del sistema financiero son las que deben escoger sus propias definiciones de riesgo operacional y por tanto los factores para su administración y control. Los tipos de evento de riesgo operacional que el Comité de Basilea ha identificado y

que tiene potencial de resultar en pérdidas sustanciales incluyen los siguientes:

- **Fraude interno:** Se considera fraude interno a los actos que impliquen malversación de fondos o evasión de regulaciones, la ley o políticas de la institución, excepto los eventos de diversidad o discriminación. Ej. Mala información intencional, apropiación indebida de activos, falsificación, etc.
- **Fraude externo:** Los eventos de fraude externo abarcan los actos por una tercera persona que involucren la malversación de fondos o evasión de la ley. Los ejemplos incluyen robo, alteración de cheques, daños causados por hackers¹⁵, etc.
- **Prácticas de empleo y seguridad de lugar de trabajo:** Son actos inconsistentes con las leyes o contratos de empleo, salud o seguridad, o que resultan en pago de reclamos de perjuicio personal, o reclamos relacionados a temas de diversidad o discriminación. Los ejemplos incluyen reclamos de compensación de trabajadores, violación de la salud del empleado y a reglas de seguridad, actividades de labor organizada, reclamos de discriminación y responsabilidad general. Por ejemplo atentar contra la salud del empleado o contra las reglas de seguridad, demandas por discriminación y responsabilidad general, etc.
- **Prácticas relacionadas con clientes, los productos y el negocio:** Son fallas no intencionadas o negligentes al cumplir una obligación profesional a clientes específicos o de la naturaleza o diseño de un producto. Los ejemplos incluyen infracciones fiduciarias, abuso de información confidencial de clientes, actividades impropias de negociación, lavado de dinero, etc.
- **Daños a activos físicos:** Se considera como daño la pérdida de los activos físicos por desastre natural u otros eventos. Los ejemplos incluyen terrorismo, vandalismo, terremoto, incendios e inundaciones.

¹⁵ Daños provocados por pirateo computacional.

- **Interrupción de negocios:** Incluye los eventos que afectan al normal funcionamiento del negocio o provocan fallas de los sistemas. Ejemplo fallas de hardware y software, problemas de telecomunicación, cortes en los servicios públicos, etc.
- **Deficiencias en la ejecución de procesos, en el procesamiento de operaciones y en las relaciones con proveedores y otros externos:** Son fallas de procesamiento de transacción o proceso, y relaciones con contrapartes comerciales y vendedores. Los ejemplos incluyen errores de entrada de datos, fallas de administración colateral, documentación legal incompleta, acceso no autorizado dado a cuentas de clientes, mal desempeño de contraparte no-cliente y disputas de vendedor.
- **Información no alineada:** Esta categoría incluye eventos que por sus características no pueden ser incluidos en ninguno de los grupos detallados, sin embargo, tienen el potencial de resultar en pérdidas sustanciales para la organización.

2.4.5 Gobierno Corporativo

El manejo del concepto de gobierno corporativo, nace en los países desarrollados del oeste de Europa, Canadá, Estados Unidos y Australia, ante la necesidad de información de los accionistas minoritarios, sobre sus inversiones, lo cual inició un proceso de apertura de la información, de profesionalismo y transparencia, que se cristalizó en el concepto de gobierno corporativo.

En 1999 la Organización para la Cooperación y el Desarrollo Económico, OECD, emitió los principios de gobierno corporativo y el siguiente concepto:

“Gobierno corporativo, es el conjunto de principios y normas que regulan el diseño, integración y funcionamiento de los órganos del gobierno de la empresa, como son los tres poderes dentro de una sociedad: los accionistas, directorio y Alta Administración, provee los incentivos para proteger los

intereses de la compañía y los accionistas, monitorea la creación de valor y uso eficiente de los recursos”¹⁶.

Principios del Gobierno Corporativo:

- ✓ Proteger los derechos de accionistas.
- ✓ Asegurar el tratamiento equitativo para todos los accionistas.
- ✓ Todos los accionistas deben tener la oportunidad de obtener una efectiva reparación de los daños por la violación de sus derechos.
- ✓ Reconocer los derechos de terceras partes interesadas y promover una cooperación activa entre ellas y las sociedades en la creación de riqueza, generación de empleos y logro de empresas financieras sustentables.
- ✓ Asegurar que haya una revelación adecuada y a tiempo de todos los asuntos relevantes de la empresa, incluyendo la situación financiera, su desempeño, la tenencia accionaria y su administración.
- ✓ Asegurar que haya una revelación adecuada y a tiempo de todos los asuntos relevantes de la empresa, incluyendo la situación financiera, su desempeño, la tenencia accionaria y su administración.

La OECD¹⁷ es una organización de cooperación internacional, compuesta por 30 estados, cuyo objetivo es coordinar sus políticas económicas y sociales. Es un foro mundial donde se analiza y establece orientaciones sobre temas de relevancia internacional como economía, educación y medioambiente. Fue fundada en 1961 y su sede se encuentra en Francia.

En la actualidad el manejo del gobierno corporativo es tan importante como el desempeño financiero eficiente, en virtud de que brinda mayor seguridad a la inversión y garantiza la sostenibilidad y crecimiento de las empresas.

2.4.6 Principios de Basilea para una administración sólida del Riesgo de Operación

El comité de Basilea establece prácticas sólidas para la identificación, medición, monitoreo y control del riesgo operacional, en base a los siguientes principios:

¹⁶ <http://www.wikipedia.com>

¹⁷ Organización para la Cooperación y el Desarrollo Económico

Principio 1: La junta directiva¹⁸ debe estar enterada de los aspectos más importantes de los riesgos operacionales de la institución y debe administrarlos como una categoría de riesgo distinta que debe ser evaluada en forma periódica dentro del marco de administración de riesgo.

La junta directiva debe revisar el marco de administración en forma regular para asegurar que la institución esté administrando los riesgos operacionales que surgen de cambios externos en el mercado y otros factores, actividades o sistemas.

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

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

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

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

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

Las actividades de control se diseñan para dirigir los riesgos que se han identificado. Para aquellos riesgos que no pueden ser controlados, las

¹⁸ La junta directiva se refiere a una estructura de administración compuesta de un consejo de directores y la alta gerencia.

instituciones deben decidir si aceptan este riesgo o reduce o retira la actividad de negocio implicada.

Principio 7: Los bancos deben tener establecidos planes de continuidad de contingencia y de negocios para asegurar su capacidad de operar en medio de eventos imprevistos y minimizar pérdidas que puedan traer la interrupción de las actividades del negocio.

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

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

Principio 9: Los supervisores deben conducir, directa o indirectamente, la evaluación independiente y regular de las políticas, procedimientos y prácticas relacionadas a los riesgos operacionales. Los supervisores deben asegurar que existen mecanismos apropiados de reporte establecidos que les permitan mantenerse informados de los desarrollos en los bancos.

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

La cantidad de divulgación debe estar proporcionada con el tamaño y complejidad de las operaciones de la institución.

CAPITULO III

3 **NORMATIVA NACIONAL Y METODOLOGIAS APLICADAS AL RIESGO OPERATIVO**

3.1 **Antecedentes**

Con el fin de establecer un ambiente de solidez y estabilidad en el Sistema Financiero, la Junta Bancaria de la Superintendencia de Bancos y Seguros (SBS), emitió la resolución **JB2005-834**, “Sobre la Gestión Integral y Control de Riesgos”, las metodologías y procedimientos que deben llevar a cabo las instituciones controladas para una adecuada administración del Riesgo de Operación.

El objetivo de esta resolución es lograr que las Instituciones del Sistema Financiero Nacional gestionen el Riesgo de Operación como un instrumento fundamental dentro de la administración preventiva de riesgos, con el fin de reducir la posibilidad de ocurrencia de pérdidas operacionales que interrumpa el normal funcionamiento del negocio.

La Superintendencia de Bancos y Seguros propone medidas de mitigación y control que incluyen recursos humanos, sistemas, mecanismos, procesos y otras herramientas, que permitirán mitigar el Riesgo de Operación. Sin embargo, son las instituciones controladas las encargadas de desarrollar sus propias técnicas de administración, tomando en cuenta su objeto social, naturaleza, complejidad y demás características propias a sus actividades. El objetivo es lograr una administración adecuada del Riesgo Operacional, que no afecte la estabilidad y la continuidad del negocio a largo plazo¹⁹

3.2 **Resolución JB2005-834: De la Gestión del Riesgo Operativo**

En el proceso de elaboración, discusión y emisión de la norma de riesgo operativo y en cumplimiento a las recomendaciones internacionales respecto a

¹⁹ Llerena Endara Valeria, Introducción del Riesgo Operacional dentro del Sistema Financiero Ecuatoriano, Quito, 2006

que los organismos de control supervisores consulten públicamente a sus controlados, fue puesta a consideración de los organismos representantes de las entidades financieras ecuatorianas, quienes ratificaron que el enfoque de la norma de riesgo operativo era aplicable a la realidad ecuatoriana, ya que no exige el desarrollo de sofisticadas metodologías de dotación de capital, promueve y guía a las entidades en el desarrollo de un apropiado ambiente de gestión del riesgo operativo, contribuyendo a la solidez y seguridad del sistema financiero y guardando coherencia con los lineamientos establecidos por el Comité de Basilea.

La SBS en el segundo trimestre del 2004, llevó a cabo una encuesta sobre el estado de situación y expectativas del mercado sobre diferentes aspectos de los riesgos operacionales a que están expuestas las instituciones, llegando a determinar que éstas se hallan en una primera fase, que consiste en el diagnóstico interno de su situación de riesgo y en el diseño de proyectos y cronogramas de implementación de los procesos.

La segunda fase que implica usar un enfoque más avanzado denominado Advance Model Approach AMA, sugerido por Basilea II, el cual propone “medir objetivamente las fallas en los procesos, cuantificando frecuencias y su impacto monetario de una manera sistemática, ordenada y periódica, con el objeto de obtenerse series temporales históricas de dichas frecuencias e impactos con las que finalmente se pueden obtener promedios y desviaciones para calcular valores de cobertura de pérdidas esperadas y no esperadas”²⁰.

No obstante, existen limitaciones en las instituciones, como la inexistencia de bases de datos o series temporales históricas debidamente estructuradas, es decir escasez de información procesable tanto en contenido como en formato, además el personal de riesgos operativos requiere tener habilidades más relacionadas a las técnicas de auditoría que a las técnicas financieras, los sistemas informáticos requieren especificidad y algunas instituciones aún no

²⁰ Boletín Económico Financiero-AIFE- Asociación de Instituciones Financieras del Ecuador, Estado de situación de la gestión de riesgo operativo, No.10, Junio 2006

están convencidas de adicionar aportes patrimoniales para cubrir este riesgo, más aún si ello representa reducción de sus beneficios líquidos.

La norma fue elaborada en función de los resultados de la encuesta a las entidades controladas, los principios recomendados por el Comité de Basilea a través del documento “Prácticas adecuadas para la gestión y supervisión de los riesgos de operación”, los aspectos relevantes sobre “Administración de procesos y de la administración del recurso humano”, y para el caso de la tecnología de información se ha observado las especificaciones del “Código de práctica para la administración de la seguridad de la información”, contenidas en la norma ISO 17799 y adicionalmente, las mejores prácticas establecidas en el Modelo COBIT²¹.

La norma ecuatoriana busca promover y guiar a las entidades controladas en el desarrollo de un apropiado ambiente de gestión del riesgo operativo, conforme con los principios establecidos por el Comité de Supervisión Bancaria de Basilea y a establecer la supervisión preventiva enfocada a riesgos, bajo la responsabilidad del organismo de control. “Entendiéndose como adecuado ambiente de gestión a la existencia de:

- Compromiso institucional, donde es imprescindible el involucramiento del directorio y la alta gerencia.
- Metodología de trabajo definida.
- Participación de todas las áreas sin excepción.
- Seguimiento continuo y cumplimiento de las responsabilidades asumidas.
- Comunicación y difusión apropiada, fundamental en todo el proceso.”²²

²¹ www.superban.gov.ec.ec/downloads/Memorias_2005

²² Ramírez, Ricardo, *Taller para levantamiento de eventos de riesgo para el BNF*. Credit Solutions, 2008.

La resolución establece cuatro factores, con el fin de minimizar la probabilidad de incurrir en pérdidas financieras provenientes del Riesgo de Operación, los cuales son los siguientes:

- Procesos
- Personas
- Tecnología de la Información
- Eventos Externos

3.2.1 Procesos

Estos deben ajustarse a las exigencias del mercado y del entorno. La adecuada administración de procesos asegura el funcionamiento armónico de la organización y maximiza su efectividad, no obstante, exige el establecimiento de procesos estructurados y organizados, en función de la misión, visión y objetivos estratégicos. La norma propone agrupar los procesos en tres categorías:

- a) Gobernantes o estratégicos;
- b) Fundamentales, productivos, de negocio u operativos; y,
- c) Habilitantes, de soporte o de apoyo.

Además las entidades vigilarán por su cumplimiento y mejora continua, mediante el desarrollo de políticas para identificar, diseñar, medir, analizar, actualizar y controlar los procesos.

3.2.2 Personas

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

entidades definirán políticas y procesos para la administración del capital humano, conforme con su filosofía y sus propias necesidades, contando fundamentalmente con políticas y procesos para la incorporación, permanencia y desvinculación del personal.

3.2.3 Tecnología de Información

Que soporte adecuadamente sus operaciones y procesos, planificando ordenadamente sus requerimientos de tecnología, actuales y futuros; estableciendo requisitos, condiciones de seguridad y continuidad del negocio.

3.2.4 Eventos Externos

Las entidades deberán identificar eventos externos (no derivados del entorno político, económico y social) frente a los que tiene vulnerabilidad, como: fallas en los servicios públicos, ocurrencia de desastres naturales, atentados y otros actos delictivos, con el fin de establecer planes de contingencia que ayuden a mitigar su impacto en la operatividad del ente.

3.3 Administración del Riesgo Operativo en el Sistema Financiero Ecuatoriano

Las instituciones deberán incluir la administración del riesgo operativo, como un proceso específico; estableciendo sistemas de gestión para identificarlo medirlo, controlarlo y monitorearlo. Cada institución desarrollará sus propios esquemas de acuerdo con su objeto social, tamaño, naturaleza y características particulares. En la figura 2 se puede apreciar el ciclo del riesgo operativo.

FIG. 2 CICLO DEL RIESGO OPERATIVO



Fuente: ROP UASB. Velastegui Iván

Elaboración: La autora

3.3.1 CICLO DEL RIESGO OPERATIVO

Identificación.- se considerará el entorno interno y externo de la entidad para determinar los aspectos que podrían afectar al logro de los objetivos y generar pérdidas. Las instituciones identificarán, por línea de negocio, los eventos de riesgo de operativo, agrupados por tipo de evento, fallas en procesos, personas, tecnología de información y eventos externos.

Estos eventos son los definidos por el Comité de Basilea en los documentos "Prácticas Adecuadas para la Gestión y Supervisión de los Riesgos de Operación" y el "Nuevo Acuerdo de Capital de Basilea" y son los siguientes: fraude interno; fraude externo; prácticas laborales y seguridad del ambiente de trabajo; prácticas relacionadas con los clientes; los productos y el negocio; daños a los activos físicos; interrupción del negocio por fallas en la tecnología

de información y deficiencias en la ejecución de procesos, en el procesamiento de operaciones y en las relaciones con proveedores.

Medición.- se deberán conformar bases de datos con información suficiente y oportuna que a futuro permita estimar las pérdidas esperadas e inesperadas de riesgo operativo, esas bases deberán contener la siguiente información clasificada por línea de negocio: eventos de riesgo de operativo, fallas o insuficiencias por factores de riesgo de operativo, frecuencia con que se repite cada evento, y efecto cuantitativo de pérdida.

Control.- se deberá establecer un sistema de control interno integrado a las actividades cotidianas de la entidad, que cuente con políticas, procesos y procedimientos formalmente establecidos que propicien una sólida cultura de control. Dicho sistema deberá estar sujeto a revisiones periódicas por parte de auditoría interna sin que exista responsabilidad sobre el riesgo operativo.

Monitoreo.- se deberá disponer de un esquema organizado de reportes que permita contar con información suficiente y adecuada para gestionar el riesgo operativo en forma continua y oportuna. La frecuencia de monitoreo depende de las características de cada entidad y los reportes deberán contener al menos la siguiente información:

- Detalle de los eventos de riesgo operativo, agrupados por tipo de evento, las fallas o insuficiencias que los originaron, relacionados con los factores de riesgo operativo y clasificados por líneas de negocio;
- Informes de evaluación del grado de cumplimiento de las políticas relacionadas con los factores de riesgo operativo y los procesos y procedimientos establecidos por la institución;
- Indicadores de gestión que permitan evaluar la eficiencia y eficacia de las políticas, procesos y procedimientos aplicados.

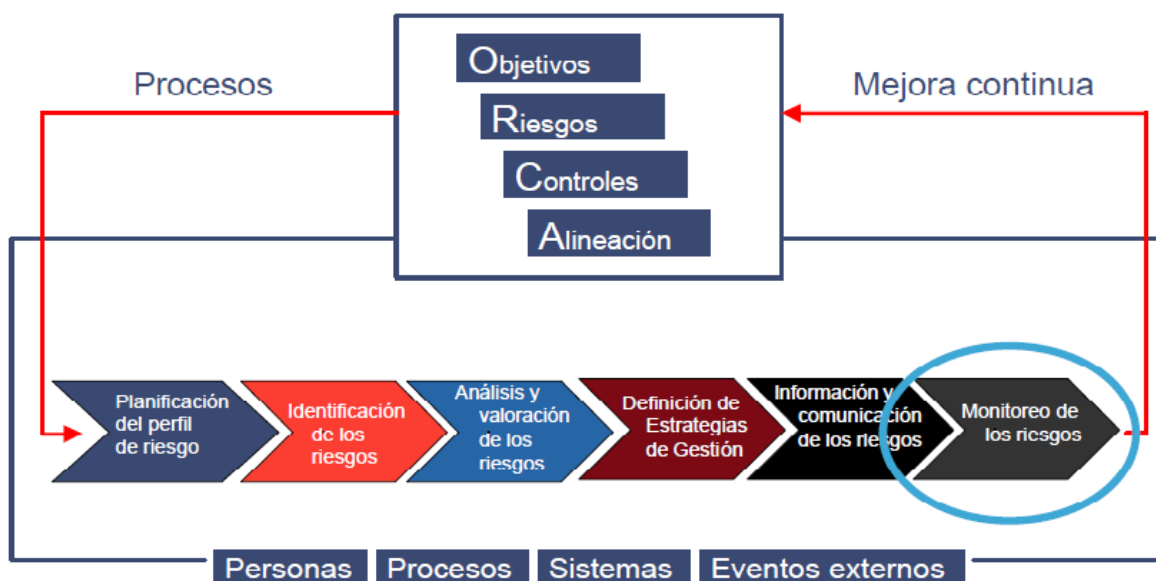
3.3.2 Responsabilidades en la administración del riesgo operativo

La norma establece 3 niveles de responsabilidad en la administración del riesgo operativo, la responsabilidad del directorio es normar, las funciones y responsabilidades del comité de riesgos es asesorar y las funciones y responsabilidades de la unidad de riesgos es supervisar. Dichas responsabilidades se refieren principalmente a:

- La creación de una cultura organizacional
- La implementación de un esquema de gestión de riesgo operativo.
- La definición de un plan de continuidad del negocio

A continuación en la figura 3 se muestra el cuadro del proceso de cómo una organización debe seguir para controlar el riesgo operativo:

FIG. 3 CICLO DEL RIESGO OPERATIVO AMPLIADO



Fuente: PriceWaterHouseCoopers

Elaboración: La autora

3.4 Identificación Tow dow – Bottom up

Es un enfoque estructurado para ayudar a las organizaciones, sin importar su tamaño o misión, a identificar, valorar, gestionar, comunicar y monitorear los riesgos operacionales que retan los objetivos estratégicos, proyectos y actividades del día a día. La solución metodológica posee dos enfoques: Top Down y Bottom Up.

Top Dow.- El enfoque Top Down se centra principalmente en los objetivos estratégicos, así como en los eventos de pérdida y riesgos operacionales que retan los objetivos.

Bottom Up.- El enfoque Bottom Up abarca la identificación de los riesgos en cadenas de valor, procesos y actividades. En las instituciones financieras las Unidades críticas de alto riesgo que requieren evaluación de las cadenas de valor, procesos y actividades son: Operaciones y Banca corporativa.

A continuación se muestra en la figura 4 la integración del Top dow con el Bottom up:

FIG. 4 INTEGRACIÓN DEL TOP DOWN CON EL BOTTOM UP



Fuente: PriceWaterHouseCoopers

Elaboración: La autora

3.4.1 Fases de la metodología de gestión de riesgo operacional a nivel corporativo²³

- **Fase 1: Planificación del perfil de riesgo operacional a nivel corporativo.-** El principal objetivo de esto es entender la naturaleza de los principales riesgos operacionales que enfrenta una organización y las medidas que se pueden adoptar en respuestas a esos riesgos, mediante una visión global. Un perfil de riesgo operacional es definido como la visión consolidada de un conjunto de riesgos operacionales con la representación del impacto en el negocio y la frecuencia de ocurrencia de cada riesgo. Los propósitos del perfil de riesgos son:

²³ PriceWaterHouseCoopers, Riesgo Operacional un enfoque práctico, 2007.

- Proveer a la alta gerencia un entendimiento de los riesgos de la organización en el cumplimiento de sus objetivos y la forma como responde a esos riesgos.
- Fortalecer la cultura de riesgo y control
- Identificar un conjunto de estrategias de gestión (mejoras tempranas) que permitan minimizar el impacto de los riesgos, su frecuencia de ocurrencia o ambos
- Definir o ajustar el apetito de riesgo, niveles de tolerancia y límites de exposición al riesgo
- Proveer insumos para la planificación del negocio o toma de decisiones
- Proveer información de la gestión de riesgos a organismos reguladores, accionistas, aseguradores y otros.

Adicionalmente en esta fase mencionamos los tipos de perfil de riesgo operacional:

Perfil de Riesgo Operacional Corporativo; provee una visión consolidada de los riesgos identificados en la organización, basados en los objetivos estratégicos y riesgos operacionales de alto nivel:

- Perfil de Riesgo Inherente, antes de establecer cualquier estrategia de gestión de riesgo
- Perfil de Riesgo Residual, una vez que se han considerado los controles de gestión de riesgo
- Perfil de Riesgo Administrativo, los factores que generan este riesgo son: la falta de capacitación de personal operativo en agencias; un mal uso del sistema de información; tecnología crediticia limitada.

Perfil de Riesgo Operacional Detallado, provee el portafolio de riesgos de procesos de una unidad de negocio o de apoyo específica.

- **Fase 2: Identificación de los riesgos operacionales.**- En esta fase se determina los riesgos operacionales a nivel corporativo a los cuales se encuentra expuesta la organización, considerando tanto factores

internos como externos que puedan afectar adversamente la implantación de estrategias y el logro de objetivos del negocio. Para realizar esto se necesita recolectar información como la citada a continuación:

- Objetivos y metas del negocio
- Leyes, normas y regulaciones en general
- Políticas y procedimientos
- Mapa de procesos / Áreas involucradas
- Hallazgos de auditoría interna y externa, si existen
- Informes de auditoría interna y externa, si existen
- Datos históricos de pérdidas operacionales, si existen
- Data externa de pérdidas y/o tendencias del sector financiero
- Auto-evaluaciones de riesgo y controles, si existen
- Información sobre futuros cambios, si existen

- **Fase 3: Análisis y valoración de riesgos operacionales.-** Realizar un análisis y valoración de los riesgos operacionales, que permita comprender el perfil de riesgo y dirigir de manera más efectiva los recursos para la gestión de los riesgos identificados.

Cálculo del riesgo inherente: El riesgo inherente es el que enfrenta una organización antes de cualquier actividad de gestión de riesgo y es igual a:

$$\text{Riesgo inherente} = \text{Impacto} * \text{Frecuencia de Ocurrencia}$$

Cálculo del riesgo residual:

El riesgo residual es el que resulta después que la gerencia ha implantado efectivamente acciones para mitigar el riesgo inherente

$$\text{Riesgo residual} = \text{Impacto residual} * \text{Frecuencia de ocurrencia residual}$$

Cálculo del riesgo administrativo:

Para evaluar el riesgo administrativo es necesario la:

- Evaluación y control financiero: análisis de corte transversal; sistemas de control financiero; indicadores financieros

- Sistema de evaluación vertical: balance general; estado de resultados
 - Sistema de evaluación Dupont
 - Camel: capital de activos; administrativo; rentabilidad; liquidez
 - Perfil: Protección; estructura financiera; rendimientos; calidad de activos; servicios.
- **Fase 4: Determinación de las estrategias de gestión de riesgos operacionales**

En esta fase se determina la estrategia de gestión de los riesgos operacionales identificados y evaluados, para lo cual se deberá definir, evaluar y seleccionar las acciones para reducir el riesgo a niveles aceptables. Para esto tenemos las siguientes opciones: evitar, reducir, transferir o aceptar el riesgo; con esto es necesario priorizar los riesgos con los siguientes elementos:

- ✓ Validar los objetivos corporativos del negocio y las políticas de gestión de riesgo operativo
- ✓ Evaluar si el nivel de riesgo residual excede los límites de tolerancia para cada riesgo operativo, si existen tales límites
- ✓ Regulaciones
- ✓ Evaluar los controles existentes operacionales

De la misma manera hay que establecer técnicas para determinar la viabilidad de las estrategias de gestión de los riesgos operacionales de la siguiente manera:

- Determinar el efecto de la estrategia de gestión del riesgo sobre el impacto y la frecuencia de ocurrencia
- Análisis costo-beneficio
- Identificación de posibles oportunidades

Integración de las actividades de control con la estrategia de gestión del riesgo:

- ✓ En la selección de las actividades de control, se deberá considerar cómo integrar a una o varias estrategias de gestión de riesgo

- ✓ En algunos casos una sola actividad de control puede estar contenida en múltiples estrategias de gestión de riesgo y, en otros casos, múltiples controles son necesarios para una sola estrategia de gestión de riesgo
- ✓ Podría encontrarse que las actividades de control existentes son suficientes para asegurar que la nueva estrategia de gestión de riesgo se ejecute efectivamente

- **Fase 5: Información y comunicación del estado de gestión de los riesgos operacionales**

Es necesario desarrollar una estructura y proceso de información y comunicación del estado de gestión de los riesgos operacionales que permita comunicar el estatus de los riesgos operacionales

Directrices para informar el estado de gestión de los riesgos operacionales:

- ✓ Realizar una profunda evaluación de riesgos operacionales
- ✓ Proveer análisis y sumario del avance del plan de implantación de las estrategias de gestión de los riesgos operacionales a la Alta Gerencia
- ✓ Desarrollar un método efectivo de recolección, registro y análisis de incidentes / eventos de pérdidas operacionales
- ✓ Estimar las pérdidas esperadas por la materialización de los riesgos operacionales potenciales
- ✓ Determinar los Indicadores Clave de Riesgo (KRI)
- ✓ Incluir recomendaciones, responsabilidades y cronogramas para revisar y mitigar los riesgos potenciales
- ✓ Elaborar reportes periódicos donde se reflejen los riesgos operacionales prioritarios

La comunicación con entes internos debe proveer al personal y a la organización lo siguiente:

- ✓ La importancia y relevancia de la gestión de los riesgos operacionales

- ✓ La alineación de la gestión de los riesgos con los objetivos de la organización
- ✓ El apetito y la tolerancia al riesgo operacional
- ✓ Un lenguaje común de riesgo operacional
- ✓ Las funciones y responsabilidades del personal de la organización en el apoyo a la gestión de los riesgos operacionales

Adicionalmente la organización también debe mantener comunicación con sus entes externos tales como clientes, proveedores, auditores y reguladores, le permitirá a la organización:

- ✓ Proporcionar una importante información para evaluar los productos y servicios en términos de riesgo operativo
- ✓ Obtener información para mejorar la calidad de los productos y servicios
- ✓ Anticipar a las tendencias del mercado, problemas u oportunidades
- ✓ Mantener estrechas y frecuentes relaciones con clientes y proveedores externos
- ✓ Alinear a los proveedores con los límites de tolerancia al riesgo

La comunicación se la puede realizar y mantener mediante: correos electrónicos, comunicaciones corporativas, informes especiales, discusiones grupales por correo electrónico, sitios de intranet, internet, llamadas en conferencia, folletos, trípticos o carteleras informativas, Comités / reuniones regulares, convenciones internas y conferencias.

- **Fase 6: Monitoreo de los riesgos operacionales**

Establecer un efectivo proceso de seguimiento de los riesgos operacionales, lo cual permitirá velar por la implantación de las estrategias

de gestión y asegurar la detección, comunicación y gestión de los eventos de pérdida o incidentes de riesgos operacionales

Métodos de monitoreo:

- Monitoreo continuo
- Auto-evaluaciones separadas
- Análisis de eventos de pérdida operacional
- Medición de la cultura de riesgo y control

▪ **Monitoreo Continuo**

El monitoreo continuo consiste en una vigilancia constante e ininterrumpida de las estrategias de gestión de los riesgos operacionales. Entre las ventajas de este método se enuncian las siguientes:

- ✓ Es altamente efectivo en el seguimiento de aquellos riesgos operacionales presentes en actividades operativas de alta recurrencia o de naturaleza regular para el negocio
- ✓ Es ejecutado en tiempo real
- ✓ Es el método más efectivo de monitoreo, ya que se puede identificar rápidamente cualquier desviación

▪ **Auto-evaluaciones separadas**

Consiste en que las unidades de negocio y apoyo monitoreen el estado de la gestión de los riesgos operacionales en un momento determinado (por ejemplo: trimestral, semestral o anualmente), o cuando ocurran eventos, tales como:

- ✓ Reestructuración o fusión de unidades de negocio y/o apoyo
- ✓ Incremento en el volumen de transacciones
- ✓ Nuevas tecnologías
- ✓ Cambios culturales y organizacionales
- ✓ Nuevos productos
- ✓ Eventos externos

- **Análisis de eventos de pérdida operacional**

Procedimientos para asegurar que los eventos de pérdida operacional son detectados y comunicados oportunamente, procedimientos para responder y respaldar los eventos de pérdida operacional.

- **Medición de la cultura de riesgo y control**

- ✓ Proporciona una visión global de la integración del control interno y la gestión de riesgo
- ✓ Provee información para desarrollar acciones que contribuyan con el fortalecimiento de la cultura de riesgo y control
- ✓ Provee información sobre los atributos clave de una efectiva y sólida gestión integral de riesgos
- ✓ Permite establecer un indicador para medir la evolución de la organización en el ámbito de la cultura de gestión de riesgo y control
- ✓ Permite obtener un entendimiento del Ambiente de Control que rodea a la organización.

3.5 CORRE (Control de los Recursos y los Riesgos Ecuador)

El CORRE²⁴ toma como base los informes enunciados MICIL (Marco Integrado de Control Interno Latinoamericano), COSO (Committee of Sponsoring Organization) Y COSO II; sin embargo, su presentación se fundamente en COSO II, porque incluye a los dos anteriores COSO Y MICIL. Además, procura que su adaptación a la realidad ecuatoriana y la simplificación de los contenidos, facilite su comprensión y aplicación. COSO está basado en un concepto de control interno, el cual se lo define como un proceso, efectuado por el consejo de administración, la dirección y el resto de personal de una entidad, diseñado con el objeto de proporcionar un grado de seguridad razonable en cuanto a la consecución de objetivos dentro de las siguientes categorías: honestidad y responsabilidad, eficacia y eficiencia en las operaciones, fiabilidad de la información, salvaguarda de los recursos; y, cumplimiento de las leyes y normas.

²⁴ Proyecto Anticorrupción ¡SI se Puede!, 2006

Adicionalmente el CORRE tomo en cuenta los 8 componentes de COSO II que son:

- ✓ Ambiente Interno de Control
- ✓ Establecimiento de Objetivos
- ✓ Identificación de Eventos
- ✓ Evaluación de Riesgos
- ✓ Respuesta a los Riesgos
- ✓ Actividades de Control
- ✓ Información y Comunicación
- ✓ Supervisión y Monitoreo

Todos los componentes del CORRE, tienen como base el ambiente interno de control y, dentro de éste, la integridad y los valores éticos. Se logrará eficiencia y eficacia en el CORRE, si los ocho componentes funcionan de manera integrada en toda la organización, bajo el liderazgo del consejo de administración o de la máxima autoridad, como principal responsable de su diseño, aplicación y actualización, en las instituciones públicas y privadas.

A continuación se describirá cada uno de los componentes que toma en cuenta el CORRE:

✓ **Ambiente Interno de Control**

El ambiente interno de control (o entorno de control como lo denomina el informe COSO), se explica de la siguiente forma: “El entorno de control marca las pautas de comportamiento de una organización y tiene una influencia directa en el nivel de compromiso del personal respecto al control. Constituye la base de todos los demás elementos del control interno, aportando disciplina y estructura. Entre los factores que constituyen el entorno de control se encuentran la honradez, los valores éticos y la capacidad del personal; la filosofía de la dirección y su forma de actuar; la manera en que la dirección distribuye la autoridad y la responsabilidad y organiza y desarrolla profesionalmente a sus

empleados, así como la atención y orientación que proporciona el consejo de administración.”.

La base del CORRE está en los valores, la conducta ética, la integridad y la competencia del personal. Este es un elemento que debe ser cuidado en forma permanente, dentro y fuera de la organización, principalmente con el ejemplo de las más altas autoridades. No es suficiente la emisión de un código de ética y los valores institucionales. Es indispensable que el personal de la entidad, los clientes y terceras personas relacionadas los conozcan y se identifiquen con ellos, para que se logren los objetivos basados en los principios antes señalados. Los valores éticos se complementan con la filosofía y el liderazgo, el establecimiento de objetivos, estrategias, políticas y procedimientos para las operaciones de la organización, con especial énfasis en el capital humano.

Los siguientes factores integran el componente Ambiente Interno de Control:

- ❖ Integridad y Valores Éticos
- ❖ Filosofía y Estilo de la Alta Dirección
- ❖ Consejo de Administración y Comités
- ❖ Estructura Organizativa
- ❖ Autoridad Asignada y Responsabilidad Asumida
- ❖ Gestión del Capital Humano
- ❖ Responsabilidad y Transparencia

✓ **Establecimiento de objetivos**

Los objetivos deben establecerse antes que la dirección pueda identificar potenciales eventos que afecten a su consecución. El consejo de administración debe asegurarse que la dirección ha establecido un proceso para fijar objetivos y que los objetivos seleccionados están en línea con la misión/visión de la entidad, además de ser consecuentes con el riesgo aceptado.

Es a partir de los objetivos que se facilita la gestión de los riesgos empresariales mediante la identificación de los eventos externos e internos; la evaluación de los riesgos; la respuesta a los riesgos; y, el diseño de actividades de control.

Los siguientes factores integran este componente:

- ❖ Objetivos Estratégicos
- ❖ Objetivos Específicos
- ❖ Relación entre Objetivos y Componentes del CORRE
- ❖ Consecución de Objetivos
- ❖ Riesgo Aceptado y Niveles de Tolerancia

✓ **Identificación de eventos**

La gestión de riesgos corporativos es un proceso efectuado por el consejo de administración de una entidad, su dirección y personal restante, aplicable a la definición de estrategias en toda la empresa y diseñado para identificar eventos potenciales que puedan afectar a la organización, gestionar sus riesgos dentro del riesgo aceptado y proporcionar una seguridad razonable sobre el logro de los objetivos. Esta definición recoge los siguientes conceptos básicos de la gestión de riesgos corporativos:

- ✓ Es un proceso continuo que fluye por toda la entidad.
- ✓ Es realizado por su personal en todos los niveles de la organización.
- ✓ Se aplica en el establecimiento de la estrategia.
- ✓ Se aplica en toda la entidad, en cada nivel y unidad, e incluye adoptar una perspectiva del riesgo a nivel conjunto de la entidad.
- ✓ Está diseñado para identificar acontecimientos potenciales que, de ocurrir, afectarían a la entidad y para gestionar los riesgos dentro del nivel de riesgo aceptado.
- ✓ Es capaz de proporcionar una seguridad razonable al consejo de administración y a la dirección de una entidad.

✓ Está orientada al logro de objetivos”.

Se entiende por riesgo a la posibilidad de que un evento ocurra y afecte adversamente el cumplimiento de los objetivos. Los riesgos también siempre se clasifican de alguna manera; en general, en cuatro grandes tipos: el riesgo de reputación, el riesgo de mercado, el riesgo de crédito y el riesgo operacional con sus divisiones.

Al identificar eventos, la dirección reconoce que existen incertidumbres, por lo que no sabe si alguno en particular tendrá lugar y, de tenerlo, cuándo será, ni su impacto exacto.

La dirección considera inicialmente una gama de eventos potenciales, derivados de fuentes internas o externas, sin tener que centrarse necesariamente sobre si su impacto es positivo o negativo.

Los eventos abarcan desde lo evidente a lo desconocido y sus efectos, desde lo que no trae mayores consecuencias a lo muy significativo.

Este componente será tratado con los siguientes elementos:

- ❖ Factores Externos e Internos
- ❖ Identificación de Eventos
- ❖ Categorías de Eventos

✓ **Evaluación de los Riesgos**

La evaluación de los riesgos permite a una entidad considerar la forma en que los eventos potenciales impactan en la consecución de objetivos. La dirección evalúa estos acontecimientos desde una doble perspectiva probabilidad e impacto y normalmente usa una combinación de métodos cualitativos y cuantitativos. Los impactos positivos y negativos de los eventos potenciales deben examinarse, individualmente o por categoría, en toda la entidad. Los riesgos se evalúan con un doble enfoque: riesgo inherente y riesgo residual.

El Riesgos Inherente es aquél al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto; es decir, siempre existirán haya o no controles, debido a la naturaleza de las operaciones. El riesgo residual es el que permanece después de que la dirección desarrolle sus respuestas a los riesgos.

Este componente incluye los siguientes factores:

- ❖ Estimación de Probabilidad e Impacto
- ❖ Evaluación de Riesgos
- ❖ Riesgos Originados por los Cambios

✓ **Respuesta a los Riesgos**

La dirección para decidir la respuesta a los riesgos evalúa su efecto sobre la probabilidad e impacto del riesgo, así como los costos y beneficios, y selecciona aquella que sitúe el riesgo residual dentro de la tolerancia del riesgo establecida. En la perspectiva de riesgo global de la entidad (cartera de riesgos), la dirección determina si el riesgo residual global concuerda con el riesgo aceptado por la entidad.

- ❖ Categoría de Respuestas
- ❖ Decisión de Respuestas

✓ **Actividades de Control**

Las actividades de control son las políticas y procedimientos establecidos por la dirección y otros miembros de la organización con autoridad para emitirlos, como respuesta a los riesgos que podrían afectar el logro de los objetivos. Los procedimientos son las acciones de las personas para implantar las políticas, directamente o a través de la aplicación de tecnología, y ayudar a asegurar que se llevan a cabo las respuestas de la dirección a los riesgos.

Las actividades de control pueden ser clasificadas por la naturaleza de los objetivos de la entidad con la que están

relacionadas: estrategia, operaciones, información y cumplimiento.

Debido a que cada entidad tiene su propio conjunto de objetivos y enfoques de implantación, existirán diferencias en las respuestas al riesgo y las actividades de control relacionadas.

Cada entidad está gestionada por personas diferentes que tienen criterios individuales diferentes en la aplicación de controles. Es más, los controles reflejan el entorno y sector en que opera una entidad, así como su dimensión y complejidad de organización, la naturaleza y alcance de sus actividades y sus antecedentes y cultura. Por esta razón las actividades de control no pueden generalizarse y deberán ser la respuesta a la medida de las necesidades de los objetivos y los riesgos de cada organización.

El componente actividades de control establece los siguientes factores:

- ❖ Integración con las Decisiones sobre Riesgos
- ❖ Principales Actividades de Control
- ❖ Controles sobre los Sistemas de Información

✓ **Información y Comunicación**

El componente dinámico del CORRE es la “información y comunicación”, ya que se comunica el ambiente de control interno con la supervisión, con la evaluación del riesgo y las actividades de control, conectando en forma ascendente a través de la información y descendente mediante la calidad de comunicación generada por la supervisión ejercida.

Es necesario identificar, procesar y comunicar la información relevante en la forma y en el plazo que permita a cada funcionario y empleado asumir sus responsabilidades. Dichos informes contemplan, no solo, los datos generados en forma interna, sino también la información sobre las incidencias,

actividades y condiciones externas, necesarias para la toma de decisiones y para formular los informes financieros y de otro tipo.

Es importante el establecimiento de una comunicación eficaz en un sentido amplio, que facilite una circulación de la información (formal e informal) en varias direcciones, es decir ascendente, transversal, horizontal y descendente. La dirección superior debe transmitir un mensaje claro a todo el personal sobre la importancia de las responsabilidades de cada uno en materia de compartir la información con fines de gestión y control.

Los informes deben contener datos relevantes para posibilitar la gestión eficaz de la gerencia y reunir los siguientes atributos:

- ⇒ Cantidad suficiente para la toma de decisiones.
- ⇒ Información disponible en tiempo oportuno.
- ⇒ Datos actualizados y que corresponden a fechas recientes.
- ⇒ Los datos incluidos son correctos.
- ⇒ La información es obtenida fácilmente por las personas autorizadas.

Los principales factores que integran el componente información y comunicación son:

- ❖ Cultura de Información en todos los Niveles
 - ❖ Herramienta para la Supervisión
 - ❖ Sistemas Estratégicos e Integrados
 - ❖ Confiabilidad de la Información
 - ❖ Comunicación Interna
 - ❖ Comunicación Externa
- ✓ **Supervisión y Monitoreo**

“Resulta necesario realizar una supervisión de los sistemas de control interno, evaluando la calidad de su rendimiento. Dicho seguimiento tomará la forma de actividades de supervisión

continua, de evaluaciones periódicas o una combinación de las anteriores.

La supervisión continua se inscribe en el marco de las actividades corrientes y comprende unos controles regulares efectuados por la dirección, así como determinadas tareas que realiza el personal en el cumplimiento de sus funciones. El alcance y la frecuencia de las evaluaciones puntuales se determinarán principalmente en función de una evaluación de riesgos y de la eficacia de los procedimientos de supervisión continua.

Las deficiencias en el sistema de control interno, en su caso, deberán ser puestas en conocimiento de la gerencia y los asuntos de importancia serán comunicados al primer nivel directivo y al consejo de administración.” Cita del Informe COSO.

El CORRE diseñado y aplicado en la ejecución de las operaciones de una organización evoluciona con el paso del tiempo y de igual manera los cambios en los métodos para ejecutar las operaciones. Procedimientos que fueron eficaces en un determinado momento, pueden perder su eficacia o simplemente dejan de aplicarse por ser innecesarios, sin que se introduzcan los mecanismos de reemplazo requeridos.

El componente del CORRE denominado supervisión y monitoreo permite evaluar si éste continúa funcionando de manera adecuada o es necesario introducir cambios. El proceso de supervisión comprende la evaluación, por los niveles adecuados, sobre el diseño, funcionamiento y manera como se adoptan las medidas para actualizarlo o corregirlo.

El componente supervisión y monitoreo se integra de los siguientes factores:

- ❖ Supervisión Permanente
- ❖ Supervisión Interna
- ❖ Evaluación Externa

La evaluación del CORRE constituye un proceso en sí mismo. Son los directivos de línea o función de apoyo quienes llevan a cabo las actividades de supervisión y dan meditada consideración a las implicaciones de la información que reciben. Hay que establecer políticas y procedimientos para identificar qué información se necesita a un nivel determinado para tomar decisiones en forma eficaz. En todo caso, los altos directivos deberían ser informados de las deficiencias de control interno y de la gestión de riesgos que afecten a la entidad o a las unidades específicas de manera significativa.

Los supervisores definen los procedimientos de información para sus subordinados. Las partes interesadas a las que hay que comunicar las deficiencias a veces proporcionan directrices concretas respecto a lo que debería comunicarse.

Se dispone de una variedad de metodologías y herramientas de evaluación, incluyendo listas de comprobación, cuestionarios, cuadros de mando y técnicas de diagramas de flujo.

La condición para el éxito del modelo CORRE es que todos los componentes funcionen en forma coherente e interrelacionados y que sean aplicados en toda la organización para alcanzar los objetivos previstos, con el menor riesgo posible.

Esta información explica en forma concreta que el componente, Ambiente Interno de Control resulta esencial para el referido modelo CORRE, adicionalmente especifica que es fundamental la conducta ética permanente en el trabajo de todo el personal de una institución, especialmente aplicado en la alta dirección, refiriéndose a la filosofía y estilo de la alta gerencia, la cual es un componente muy importante, para cumplir con responsabilidad y de esta manera reflejar una correcta imagen institucional.

CAPITULO IV

4. METODOLOGIA COSO Y SIMULACION MONTECARLO

4.1 Introducción

En la actualidad, la banca privada cumple un papel protagónico en el sistema financiero ecuatoriano, es considerado como una herramienta estratégica para la reactivación productiva, económica y social del país. Esta se encuentra en un proceso de cambios estructurales necesarios para afrontar el devenir del actual régimen constitucional.

En ese contexto la banca privada ha tenido que incursionar en nuevos productos como las microfinanzas, crédito con bonos, créditos a proveedores, confirming, leasing, cajeros automáticos, crédito para insumos, compra de tierras, compra autos, etc.

Las situaciones citadas, más los cambios en la constitución política del país, las innovaciones tecnológicas, apertura de nuevas oficinas y agencias, de cada uno de los bancos en el país representan un considerable aumento de su riesgo operativo.

Cabe destacar que la finalidad de una banca privada es fundamentalmente incrementar su rentabilidad económica sin dejar de lado el servir con responsabilidad a sus clientes y brindar sus servicios a todos los sectores de la sociedad, ser competitivo sin dejar de ser austero, ser el ejecutor de ambiciosos programas y a su vez cumplir con estándares internacionales sobre riesgos financieros y operativos que precautelen los intereses de las instituciones.²⁵

En la perspectiva de los desafíos planteados, sumados a la globalización de los sistemas financieros, la banca privada debe implementar procesos, esquemas y una serie de metodologías tendientes a gestionar su riesgo operativo, que se encuentra presente en todos los niveles y subniveles de la organización, aceptando que el riesgo operacional es el riesgo de todo, con excepción del riesgo de crédito y de mercado

²⁵ Institución Financiera, Desarrollo Organizacional y Proyectos – Fabrica de ideas para la innovación y la productividad.

4.2 Implementación del riesgo operativo

A partir de la emisión de la resolución de la Junta Bancaria JB-2005-834 de 20.10.2005, los bancos inician la gestión de este tipo de riesgo, mediante la inclusión de planes estratégicos con objetivos trazados sobre el riesgo operativo, cada banco conformó un grupo de trabajo, con el propósito de iniciar el tratamiento específico de los temas relacionados con el riesgo operativo y posteriormente se constituyó como departamento en cada institución.

Las disposiciones transitorias de la resolución JB-2005-834, contemplan plazos para cumplir algunos requerimientos, por lo que la banca privada con la asesoría de expertos en riesgos, elaboraron, el diagnóstico o autoevaluación inicial y el proyecto del plan de implementación del riesgo operativo.

La SBS dispuso que en abril 2006 se presente una autoevaluación del riesgo operativo y un plan de implementación que debía culminar en octubre 2008 y a partir de noviembre 2008, se estaría iniciando con la fase de estabilización o mejora.

A continuación se presenta la descripción sobre los componentes del plan de implementación, con el objeto de ampliar la comprensión de la situación del riesgo operativo:

❖ Factores y administración del riesgo operativo

Para la presente investigación se ha tomado en cuenta como base una institución con las siguientes características: Institución privada grande a nivel nacional que cuenta con una participación de los activos de US\$6.008M y un patrimonio de US\$561M en el sistema financiero nacional, los mismos que tienen una representatividad del 28% y del 27%²⁶ respectivamente; donde el Gobierno Corporativo es el que desarrolla las actividades de la institución, basándose en el conjunto de políticas y normas que gobiernan las relaciones entre la Junta de Accionistas, el Directorio, sus funcionarios, empleados, clientes y proveedores, las cuales permiten dirigir y controlar la institución. Este sistema es un proceso dinámico que tiene por objeto facilitar el establecimiento de objetivos

²⁶ Superintendencia de Bancos y Seguros (SBS), Boletín Abril 2011.

estratégicos de la institución, que son del interés tanto de los accionistas como de toda la organización, además de supervisar su cumplimiento; apoyar el control de la administración por parte del Directorio y establecer las responsabilidades del mismo.

La administración de la institución comprende que la excelencia en la gestión del riesgo, es uno de los elementos primordiales de la estrategia competitiva, que garantiza la sostenibilidad, crecimiento y fortalecimiento a largo plazo, por este motivo la gerencia adecuada de la variable riesgo y su comprensión global, constituye una de las directrices sobre las que se fundamenta la permanente agregación de valor al capital económico de los accionistas, y, por lo tanto sus mecanismos internos de decisión hacen uso de técnicas que buscan identificar, cuantificar, controlar y evaluar los diferentes riesgos de forma homogénea y consistente. A continuación se describe brevemente los factores que comprenden el riesgo operativo en la institución:

- ❖ **Factor procesos.-** Dependiendo de la estructura y del tamaño los bancos privados con las características descritas en el párrafo anterior disponen aproximadamente de 796 procesos levantados²⁷ (Ver Anexo 2), este número puede cambiar por las características propias de las instituciones financieras y de los procesos identificados por las mismas.
- ❖ **Factor personas.-** Las políticas, procesos y procedimientos de la administración del capital humano se han ido formalizando con la identificación de cada evento de riesgo ocurrido, para lo cual se han utilizado flujogramas de los procesos identificados. La debilidad de este factor está en que buena parte del personal desconozca los objetivos institucionales y sus responsabilidades, tales como el plan de regularización impuesto por el ente de control, a los cuales están sometidas las instituciones, sin que se lo haya difundido adecuadamente, existiendo la delegación de actividades, sin una clara responsabilidad, prueba de ello es el incumplimiento de dicho plan, situación reflejada en cada uno de los balances.

²⁷ De acuerdo a la tipología de la institución que se ha utilizado en el desarrollo del presente documento.

Para facilitar la identificación de los eventos de riesgo ocurrido se han determinado las áreas de la institución las cuales para la simulación y cuantificación se las ha denominado segmentos 1, 2, 3, etc. (Ver Anexo 3)

- ❖ **Factor tecnología de la información.-** los bancos han realizado esfuerzos para desarrollar el aspecto tecnológico, se ha implantado un sistema bancario integral que soluciona necesidades emergentes, incorporando seguridades lógicas, implantado controles para mitigar cada evento registrado que aseguran integridad, disponibilidad, pertinencia, oportunidad y confidencialidad de la información.
- ❖ **Factor eventos externos.-** las instituciones financieras han desarrollado un plan de seguridad integral que considera algunos eventos externos, sin embargo no se ha identificado las áreas y procesos críticos que deberán ser atendidas prioritariamente en caso de producirse un evento externo ya que estos están considerados como eventos catastróficos, los mismos que no ocurren con la misma frecuencia que los no catastróficos, pero de ocurrir uno de estos eventos provocaría una gran pérdida en la institución.
- ❖ **Administración del riesgo operativo.-** la banca ha asignado todos sus procesos a un departamento el cual identifica el eventos de riesgo, fallas e insuficiencias, conformación de bases de datos, elaboración de matrices, captura de eventos, los bancos poco a poco han ido adquiriendo políticas que les permita administrar el riesgo operativo.
Los bancos privados de las características descritas anteriormente disponen de una gerencia con una unidad de riesgos operativos independiente²⁸.

4.2.1 Metodología COSO

En el contexto internacional, quien regula las normas y medidas internacionales es el Comité de Supervisión Bancaria de Basilea BCBS. El tema de los riesgos no es nuevo, data desde 1949 con la definición de

²⁸ Mas adelante con la base de datos se explica el manejo del riesgo operativo en la institución que se ha utilizado para el desarrollo de la tesis

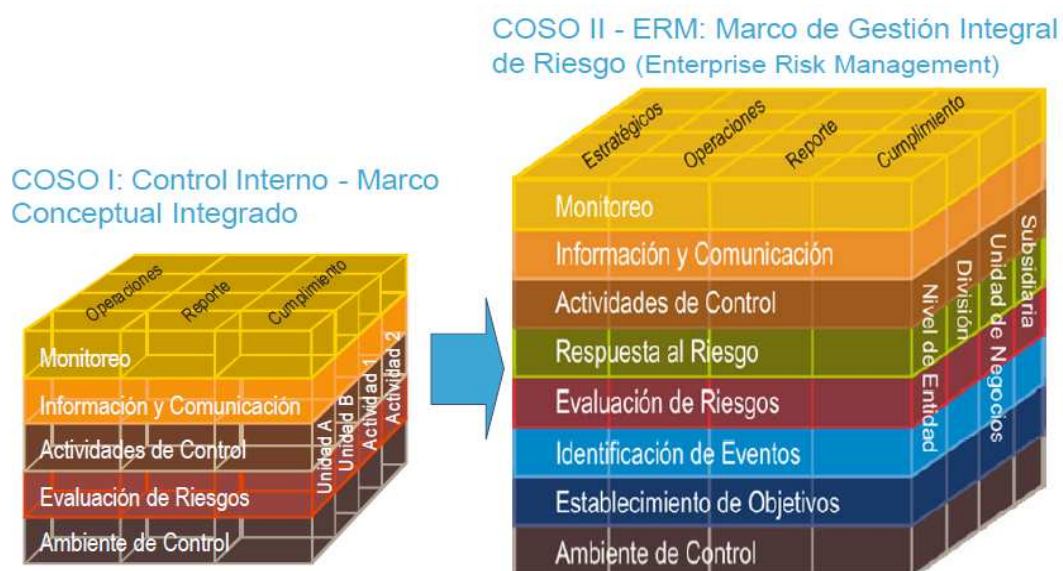
control interno, en 1987 la emisión de Basilea I, en 1992 la publicación del informe COSO; debido a la preocupación y al aumento del interés en la gestión de riesgo durante la segunda mitad de los años 90, el comité de las organizaciones que patrocinaban la Comisión de Treadway (COSO) determinó que había una necesidad de un marco común de Gestión Integral de Riesgo. En el 2001 la Comisión contrató a PricewaterhouseCoopers para desarrollar un marco para evaluar y mejorar la gestión de riesgo en las organizaciones, es allí donde se crea el COSO - ERM este se crea ampliando a COSO I para la gestión integral de riesgo pero no para sustituir el marco de control interno. En Septiembre de 2004 se publicó el estudio ERM (Enterprise Risk Management) Integrated Frameworken.

Para el desarrollo de este documento se aplicará la metodología COSO-ERM aplicada al Riesgo Operativo, la cual como se explicó anteriormente, toma en cuenta todos los componentes necesarios para un adecuado desarrollo de las diferentes actividades que realiza una institución; esta también fue tomada en cuenta y como base para el desarrollo del Control de Recursos y los Riesgos en el Ecuador.

4.2.1.1 COSO-ERM

Es un proceso realizado por la junta directiva, la gerencia y demás personal de la entidad basado en el establecimiento de estrategias para toda la empresa, diseñadas para identificar eventos potenciales que puedan afectar a la entidad, y gerenciar los riesgos dentro del apetito de riesgo para proporcionar una seguridad razonable referente al logro de los objetivos del negocio. A continuación se muestra unos cuadros comparativos del Coso I y II en la figura 5 donde se puede observar la evolución de los mismos:

FIG. 5 COSO I (Control Interno-Marco Conceptual Integrado) y COSO II- ERM: Marco de Gestión Integral de Riesgo



Fuente: PriceWaterHouseCoopers
Elaboraci\u00f3n: La autora

Los objetivos del ERM son:

- ✓ Estrat\u00e9gico: Relacionados con las metas de alto nivel; asimismo est\u00e1n alineados y dan apoyo a la misi\u00f3n del negocio
- ✓ Operacional: Relacionados con la efectividad y eficiencia de las operaciones de la entidad o empresa o corporaci\u00f3n, lo cual incluye su rendimiento y rentabilidad. Usualmente, var\u00edan seg\u00fan las opciones adoptadas por la gerencia en cuanto a estructura y rendimiento.
- ✓ Reporte o presentaci\u00f3n de resultados: Relacionado a la confiabilidad y efectividad de la estructura de l\u00edneas de reporte.
- ✓ Cumplimiento: Relacionado con el apego de la organizaci\u00f3n a las leyes y regulaciones.

En la Figura 6 se muestra los componentes del COSOS-ERM

FIG. 6

Componentes del COSO-ERM



Fuente: PriceWaterHouseCoopers
Elaboración: La autora

El ERM permite:

- Alinear las estrategias y el apetito del riesgo de la organización
- Interrelacionar el crecimiento, riesgo y rentabilidad (creación de valor).
- Mejorar la toma de decisiones sobre respuestas al riesgo
- Minimizar pérdidas y sorpresas operacionales
- Identificar y gestionar el riesgo en toda la empresa
- Proveer respuesta integral ante múltiples riesgos
- Aprovechar oportunidades derivadas de eventos potenciales de riesgo

Es importante que una institución alcance el ERM ya que esta metodología está enfocada al aumento de la participación del mercado (desarrollando fortalezas competitivas y defina argumentas de venta poderosos con los productos de la institución que ayuden a crear nuevas formas de generación de valor; innovando el proceso de comercialización, incluyendo los procesos de supervisión y seguimiento; además de un servicio y atención personalizado continuo), y a que la gestión integral de riesgos permita crear valor a sus accionistas y que por medio de esta gestión se pueda generar un retorno cuantificable de la inversión.

Ahora se explicará los beneficios que se puede lograr con el COSO-ERM en las diferentes áreas que conforman la empresa:

Junta Directiva:

- Base para mejorar gobierno corporativo, permitiendo un monitoreo más efectivo del desempeño
- Aumenta la reputación como empresa transparente y bien administrada
- Participación proactiva en la gerencia del riesgo

Auditoría Interna

- Reduce las sorpresas
- Consistente estrategia del manejo de riesgo hacia la organización con políticas y procedimientos formales
- Mejora la responsabilidad y la conducta de la gerencia
- Mejorar los mecanismos para la toma de decisiones
- Colocación inteligente de recursos en objetivos clave
- Mejora las herramientas para monitorear y controlar los riesgos
- Impulsa un estilo de gerencia proactivo

Comité Ejecutivo

- Aumenta el sentido de responsabilidad sobre los controles
- Mejora las herramientas para monitorear y controlar los riesgos
- Enfoque en áreas de alto riesgo

Clientes y Proveedores

- Optimiza los controles y procesos, mejorando el desempeño operacional
- Anticipación y respuesta proactiva a los cambios en las necesidades y preferencias de los clientes

- Mejora la administración de los acuerdos
- Mejora las relaciones con proveedores de calidad y se eliminan los de bajo desempeño

Empleados

- Mejora en la comunicación de las metas y objetivos
- Mejor entendimiento de los riesgos y adecuadas herramientas para mitigarlos
- Establecen un marco de medición del desempeño y las recompensas
- Mejoras en el desempeño, por medio de evaluaciones, manejo, medición y monitoreo de los riesgos y controles

Leyes

- Aumenta la reputación como una empresa transparente y bien administrada
- Fiel cumplimiento de las regulaciones

Entorno

- Provee a la empresa de un marco para identificar y manejar cualquier riesgo concernientes a temas de salud, seguridad y del medio ambiente
- Mejora la reputación como empresa transparente y bien administrada.

A continuación se explicará y detallará los componentes del COSO-ERM:

4.2.1.1.1 Ambiente de control.- Enmarca el tono de la organización, influenciando la conciencia del riesgo en su personal.

Es la base del resto de los componentes y provee disciplina y estructura. Se refiere al establecimiento de un entorno que estimule el control de las actividades del personal.

Este componente establece:

- Una filosofía de gestión integral de riesgo
- Nivel de riesgo que la alta gerencia asume (Apetito de riesgo)
- Rol supervisorio de la junta directiva en la gestión integral de riesgo
- La integridad y los valores éticos
- Una estructura de gestión integral de riesgos: Sistemas de delegación de autoridad, roles y responsabilidades y líneas de reporte

- Estándares de recursos humanos: habilidad y competencia de los empleados

La filosofía de la gestión de Riesgo representa la creencia y las actitudes compartidas de cómo la entidad considera los riesgos desde la estrategia hasta la implementación; Refleja los valores de la entidad, construye la cultura de riesgo e integra la gestión integral de riesgo con los diferentes procesos; Afecta directamente a los componentes de la gestión integral de riesgo, incluyendo cómo se identifican los eventos, los tipos de riesgos que son aceptados y cómo se manejan; La gerencia refuerza la filosofía de gestión integral de riesgo no sólo con palabras sino también con las acciones diarias

La cultura y control de riesgo son importantes en el ambiente de control ya que la cultura de riesgo fluye desde la filosofía y el apetito de riesgo de la entidad; una gestión integral de riesgo es exitosa y eficiente, cuando la organización mantiene una cultura de riesgo positiva; esto es que toda la entidad tenga conciencia de los riesgos y cumpla con los ocho componentes COSO –ERM.

Para que se cumpla con los puntos anotados al inicio de la explicación del componente hay que medir el riesgo mediante: la Identificación de áreas claves, niveles de cargos y personal que será sujeto a medición; Distribución de cuestionarios e instructivos; recolección de cuestionarios; procesamiento, análisis y elaboración de informe establecimiento de acciones estratégicas.

Adicionalmente la entidad debe tener una estructura organizacional diseñada de acuerdo al tamaño y naturaleza de las actividades de la entidad para que facilite la efectividad de gestión integral de riesgo, defina áreas clave de responsabilidad y establezca líneas de reporte. Además establece el grado en que los individuos y equipos son autorizados para resolver problemas y proveer límites de autoridad, proporciona límites a las asignaciones estableciendo relaciones de reportes y protocolos de autorización, las políticas describen las prácticas apropiadas del negocio, el conocimiento y la experiencia del personal clave y los recursos asociados,

los individuos conocen cómo sus acciones se interrelacionan y contribuyen en el cumplimiento de los objetivos

4.2.1.1.2 Establecimiento de objetivos.- Dentro del marco de la definición de la misión y visión, la gerencia establece las estrategias y objetivos. La gestión integral de riesgo se asegura que la gerencia cuente con un proceso para definir objetivos que estén alineados con la misión y visión, con el apetito de riesgo y niveles de tolerancia. Los objetivos se clasifican en cuatro categorías:

- Estratégicos
- Operacionales
- Reporte o presentación de resultados
- Cumplimiento

Los objetivos estratégicos establecen las metas que deben estar alineadas y dan apoyo a la misión y visión; reflejan las opciones estratégicas elegidas por la gerencia para crear valor a sus accionistas; la gerencia identifica los riesgos asociados con la estrategia y considera sus implicaciones.

Los objetivos relacionados (Operacionales, Reporte, Cumplimiento) ayudan y están alineados con la estrategia seleccionada. Son factores clave de éxito. Cada nivel de objetivo está unido al resto de los objetivos, los objetivos deben ser entendibles y medibles.

Los objetivos seleccionados no definen los objetivos que deben ser elegidos, se asegura que la gerencia cuente con un proceso para definir objetivos y alinearlos con la misión y visión y, además, que sean consistentes con el apetito de riesgo del negocio. Se entiende como apetito de riesgo al máximo nivel de riesgo que los accionistas están dispuestos a aceptar. Adicionalmente se incluye la tolerancia al riesgo la cual indica los niveles aceptables de variación de las metas fijadas.

4.2.1.1.3 Identificación de eventos.- Se identifican eventos potenciales que si ocurren pueden afectar a la entidad.

La base para este componente: evaluación de riesgos y respuesta al riesgo

En este componente se identifican los eventos con impacto negativo (riesgos) y con impacto positivo (oportunidades)

Eventos

- La gerencia identifica los eventos potenciales que afectan la puesta en práctica de la estrategia o el logro de los objetivos, pudiendo tener impactos positivos o negativos
- Incluso los eventos con baja posibilidad de ocurrencia se consideran si el impacto en un objetivo es alto
- Los eventos se identifican en todos los niveles de la organización

Factores Influyentes

- La gerencia reconoce la importancia de entender los factores internos y externos y el tipo de eventos que pueden generar

Técnicas de Identificación de Eventos

La gerencia selecciona técnicas que se ajusten a su filosofía de riesgo y que le permita a la entidad desarrollar capacidades requeridas de identificación de eventos.

- Talleres
- Entrevistas
- Cuestionarios y encuestas
- Análisis de flujo de procesos
- Indicadores principales de eventos y alerta
- Seguimiento de la data de eventos de pérdidas
- Identificación continua de eventos
- Interrelación de eventos que pueden afectar los objetivos

Objetivo de la unidad de negocio: Desarrollo de la campaña promocional de un producto específico

Medición: El número de unidades colocadas por mes por agencia

Meta y Tolerancia: Meta: Colocar 1.000 unidades del nuevo producto por mes por agencia durante campaña promocional. Tolerancia: 900-1.250 unidades colocadas por mes.

Potencial evento: La confianza del cliente disminuye, dando por resultado disminuciones de la aceptación del producto.

4.2.1.1.4 Evaluación de Riesgo.- Permite que una entidad entienda el grado en el cual los eventos potenciales pudieran afectar los objetivos del negocio. Además determina riesgos a partir de dos perspectivas: Probabilidad e Impacto; entre las técnicas se utiliza determinar riesgos y normalmente también se utiliza medir los objetivos relacionados. En la evaluación de riesgos, la gerencia considera eventos previstos e inesperados; los riesgos inherentes y residuales son evaluados.

A continuación se explica el riesgo inherente y residual:

Riesgo Inherente

Es el riesgo en una organización en ausencia de acciones que podrían alterar el impacto o la frecuencia de ocurrencia de ese riesgo.

Riesgo Residual

Es el riesgo que resulta después que la gerencia ha implantado efectivamente acciones para mitigar el riesgo inherente.

Para estimar la probabilidad e impacto hay que evaluar los acontecimientos potenciales se a partir de dos perspectivas: probabilidad e impacto. En la determinación de impacto, la gerencia utiliza normalmente una medida igual, o congruente según lo utilizado para el establecimiento del objetivo. El horizonte del tiempo usado para determinar riesgos debe ser constante con el horizonte del tiempo de la estrategia y de los objetivos. Los métodos de la evaluación serán utilizados por la gerencia de manera que utilicen una combinación de técnicas cualitativas, semi-cuantitativas y cuantitativas. El método utilizado dependerá de la necesidad de precisión y cultura de cada unidad individual y deberán facilitar la evaluación de los riesgos a lo largo de la organización. A continuación se indica en qué consisten las diferentes técnicas de evaluación:

Técnicas Cualitativas

Impacto Vs. Probabilidad

Técnicas Semi-cuantitativa

Se usa un análisis cualitativo asignando valores monetarios al riesgo

Técnicas Cuantitativas

- Técnicas Probabilísticas

- Valor en Riesgo VaR
- Riesgo de Flujo de Caja
- Distribuciones de pérdidas
- Back-testing

- Técnicas no probabilísticas

- Análisis de sensibilidad
- Análisis de escenarios
- Benchmarking

Técnicas Cualitativas

Autoevaluación: Es el proceso en el cual las unidades funcionales de la organización, de forma subjetiva, identifican los riesgos inherentes a sus actividades, evalúan el nivel de control existente y determinan los puntos de mejora que se deben realizar

- Talleres Grupales (Workshops)
- Cuestionarios
- Como resultado de la aplicación de cualquiera de estas técnicas se obtiene el catálogo de riesgos, ponderando la probabilidad de ocurrencia e impacto en los objetivos del negocio.

Las áreas encargadas del manejo del riesgo operativo deben relacionar los eventos presentados y evaluar cómo se correlacionan los mismos, y encontrar la secuencia de los eventos y tomar en cuenta que su interacción crea diferentes probabilidades e impactos.

También mediante la evaluación de riesgos las áreas encargadas podrán considerar las consecuencias positivas o negativas de los eventos potenciales, tanto individualmente como por categoría, en toda la organización.

4.2.1.1.5 Respuesta al Riesgo.- Una vez identificados los riesgos, la gerencia determina como responderá ante ellos, a fin de alcanzar los

niveles de tolerancia al riesgo. Las respuestas incluyen evitar el riesgo, mitigarlo, compartirlo o aceptarlo; en este sentido, la gerencia:

- ✓ Identifica y evalúa posibles respuestas al riesgo y el grado en el cual reducirá el impacto y/o probabilidad de ocurrencia
- ✓ Determina los costos y beneficios de las respuestas al riesgo que permitan ubicarlo dentro de los niveles de tolerancia deseados
- ✓ Identifica nuevas oportunidades de negocio para la organización

Para evaluar las posibles respuestas deben ser evaluadas en función de alcanzar el riesgo residual alineado con los niveles de tolerancia al riesgo y pueden estar enmarcadas en las siguientes categorías: Evitar el riesgo, mitigar el riesgo, compartir el riesgo, aceptar el riesgo.

Evitar el Riesgo

- Reducir la expansión de una línea de productos a nuevos mercados
- Vender una división, unidad de negocio o segmento geográfico altamente riesgoso
- Dejar de producir un producto o servicio altamente riesgoso

Compartir el Riesgo

- Compra de seguros contra pérdidas inesperadas significativas
- Contratación de outsourcing²⁹ para procesos del negocio
- Compartir el riesgo con acuerdos sindicales o contractuales con clientes, proveedores u otros socios de negocio

Aceptar el Riesgo

- Auto-asegurarse (Self-insuring) contra pérdidas
- Aceptar los riesgos de acuerdo a los niveles de tolerancia de riesgo

Mitigar el Riesgo

- Fortalecimiento del control interno en los procesos del negocio
- Diversificación de productos
- Establecimiento de límites a las operaciones y monitoreo
- Reasignación de capital entre unidades operativas

²⁹ Outsourcing, significada servicios de tercerización ofrecidos a una empresa para procesos operativos

Además de evaluar el efecto en la probabilidad de ocurrencia e impacto del riesgo, las respuestas deben ser determinadas para llevar el riesgo residual dentro de los límites de tolerancia; en el análisis del efecto de las respuestas al riesgo, la gerencia puede apoyarse en eventos pasados, tendencias, futuros escenarios, entre otros.

También al evaluar los costos versus beneficios de las respuesta, se debe considerar los costos de diseñar e implantar una respuesta, así como los costos de mantenerla.

Los costos y los beneficios de la implantación de las respuestas a riesgo pueden ser medidos cualitativa o cuantitativamente, típicamente la unidad de medición es consistente con la utilizada en el establecimiento de los objetivos y tolerancia al riesgo. La gerencia debe considerar los riesgos adicionales que pueden resultar de una respuesta, así como también las posibles oportunidades.

4.2.1.1.6 Actividades de Control.- Son Políticas y procedimientos que ayudan a la gerencia a asegurar que las respuestas a los riesgos son ejecutadas, de forma apropiada y oportuna. Estos están presentes en todos los niveles y áreas funcionales de la organización para lograr los objetivos del negocio:

- Incluye un rango de actividades, tales como:
 - Aprobaciones
 - Autorizaciones
 - Verificaciones
 - Conciliaciones
 - Seguridad de los activos
 - Desempeño de las operaciones
 - Segregación de funciones

Políticas y Procedimientos

- Las actividades de control usualmente involucran el establecimiento de una política (lo que debe ser hecho) y los procedimientos para ejecutar la política

- Cuando las políticas están formalmente documentadas pueden ser implementadas amplia, consciente y consistentemente en toda la organización
- Si se identifican desviaciones en el cumplimiento de las políticas y procedimientos deben ser investigadas y tomar las acciones correctivas.

Integración con las respuestas al riesgo

La selección de las actividades de control incluye:

- Considerar su relevancia y lo adecuado para responder ante el riesgo
- Cómo se interrelacionan con otras actividades de control y con los objetivos de la entidad

Ejemplo:

Objetivo: Conocer el cliente objetivo (target) de ventas de un nuevo Producto
Riesgo: Carencia de suficiente conocimiento de factores externos, tales como necesidades potenciales de los clientes
Respuesta: Reducir el riesgo mediante el análisis del comportamiento histórico de los clientes y realizar investigaciones de mercado
Actividad de control: Monitorear el comportamiento de los clientes mediante reportes mensuales y la validación de la data existente

TABLA. 2

Tipos de Actividades de Control

Controles preventivos	Diseñados para evitar riesgos, errores o incidentes antes de su ocurrencia
Controles detectivos	Diseñados para detectar de forma rápida riesgos, errores o incidentes
Controles correctivos	Diseñados para remediar o reducir daños como consecuencia de riesgos, errores o incidentes ocurridos
Revisiones de desempeño del Negocio	Comparaciones del desempeño versus presupuesto, proyecciones y desarrollo del período anterior Por ejemplo: La revisión de informes (por agencia, región y tipo de préstamo) que realiza un gerente de crédito para aprobaciones y cobranzas
Controles físicos	Incluye resguardo de instalaciones, activos físicos, control de acceso físico, conteo periódico y comparación con lo registrado en el sistema Por ejemplo: Realización de arqueos de efectivo en caja y comparar con las cifras presentadas en los sistemas de información
Segregación de funciones	Asignar a diferentes personas las responsabilidades de autorizar, registrar las transacciones y

	mantener la custodia de los activos Por ejemplo: Un asistente no debe liquidar un préstamo y reconciliarlo
Controles de aplicación	Enfocados en el cumplimiento de los objetivos del procesamiento de la información sobre integridad, exactitud, validez y acceso restringido Por ejemplo: Chequeos de existencias y de verificación de cálculos
Controles generales	Incluyen controles sobre la gerencia de tecnología de información, infraestructura de TI, seguridad de los activos de información, adquisición, desarrollo y mantenimiento de software

Elaboración: La autora

4.2.1.1.7 Información y Comunicación.- La información relevante, debe ser identificada, capturada, procesada y comunicada en la oportunidad y forma adecuada.

Los sistemas de información deben apoyar la toma de decisiones y la gestión de riesgo (ERM); la gerencia debe enviar un mensaje al personal resaltando su responsabilidad ante el ERM. El personal debe entender su rol en el ERM así como su contribución individual en relación con el trabajo de otros.

Información

La información debe proveer al personal y a la organización:

- Estrategia y sistemas integrados
- Integración con las operaciones
- Profundidad y puntualidad de la información
- Calidad de la información

- Se puede obtener de fuentes internas y externas

Comunicación

La comunicación interna debe proveer al personal y a la organización en relación al ERM:

- Un lenguaje común de riesgo
- La importancia y relevancia del ERM
- Los objetivos de la organización
- El apetito de riesgo y la tolerancia al riesgo de la organización
- Los roles y responsabilidades del personal y sus funciones de apoyo a la gestión de riesgos
- Los comportamientos aceptables y no aceptables son claramente transmitidos al personal
- Existencia de canales de comunicación internos y externos

Los canales de comunicación externos (ejemplo: proveedores, consumidores y reguladores) proveen información necesaria para mejorar la calidad de productos y servicios, así como anticiparse a las tendencias de mercado, problemas u oportunidades. Adicionalmente la creación de Comités de atención de reclamos o de calidad, convenciones internas de ventas y conferencias de resultados del negocio, líneas internas de denuncias anónimas y políticas, carteleras, publicaciones, e-mails informativos, entre los más importantes.

4.2.1.1.8 Monitoreo. - El ERM es monitoreado, evaluando la presencia y funcionamientos de sus componentes a lo largo del tiempo. La eficacia de los otros componentes del ERM se sigue mediante:

- Actividades de supervisión continua
- Evaluaciones separadas

Actividades de supervisión continua

- Se realizan normal y recurrentemente en cada una de las actividades de la organización
- Son ejecutadas sobre la base de un esquema de tiempo real
- Son más efectivas que las evaluaciones separadas, lo cual hace que el monitoreo continuo pueda identificar rápidamente cualquier desviación

Evaluaciones separadas

- Se enfocan directamente a la efectividad del ERM y las actividades de supervisión continua
- El responsable de la evaluación debe entender las actividades de la entidad y de cada componente del ERM evaluado
- Se debe corroborar el diseño del ERM y los resultados de las pruebas realizadas contra los indicadores establecidos inicialmente por la gerencia.

4.3 Propuesta metodológica para la gestión del riesgo operativo

Observando las normas ecuatorianas y el marco de gestión integral (Coso II – ERM) sobre la aplicación de las mejores prácticas de los controles y evaluación de objetivos para el cumplimiento de los requerimientos del riesgo operativo se tomó como punto de partida el diagnóstico (Ver Anexo 5) efectuado a la situación general de la institución financiera objeto de esta investigación, en donde el riesgo operativo se está desarrollando bajo lo mencionado en los capítulos anteriores de la presente tesis con esta investigación se tiene como objetivo brindar una alternativa para que se tenga claros los lineamientos que deben conformar la estructura de las instituciones financieras sobre las pérdidas por cualquier eventualidad operativa y se ocasione la menor pérdida posible en la misma.

La propuesta metodológica parte del supuesto de que las instituciones de la banca privada con las características antes expuestas operan bajo una organización por procesos, en la que tienen definidas políticas, líneas de negocios, estatutos, reglamentos, manuales, procesos y procedimientos debidamente aprobados por sus directorios, implementados y difundidos, situación que es básica para el tratamiento de la gestión de riesgos y parte de la aplicación de normas de control interno.

Cabe destacar que la finalidad de la banca privada es alcanzar la mayor rentabilidad financiera, siendo competitivos y cumpliendo con los estándares internacionales sobre riesgos financieros y operativos que precautelen los intereses de las instituciones financieras.

Por lo antes mencionado la presente investigación tiene por objeto dar un esquema de las metodologías tendientes ya explicadas en párrafos anteriores, para gestionar el riesgo operativo en todos los niveles y subniveles de las instituciones, aceptando que el riesgo operacional es el riesgo de todo, con excepción del riesgo de crédito y de mercado.

4.3.1 Planteamiento de la propuesta metodológica

El riesgo operativo no es nada nuevo, siempre ha existido, la diferencia está en el enfoque actual de su gestión. La banca privada, frente a sus riesgos ha tomado acciones una vez que el evento se ha producido y las pérdidas se han generado; la metodología que se propone, consiste en adoptar una actitud proactiva en la que una vez **definidos sus objetivos, se debe recolectar adecuadamente la información de los eventos para evaluar el riesgo, realizar un control y mitigación de esos riesgos y revisar la metodología para el cumplimiento de los objetivos de las instituciones y de esta forma tener la menor pérdida posible por este concepto.**

Para la aplicación de la propuesta metodológica y siguiendo lo explicado en el documento se debe:

Identificar de los Riesgos.- Se identifican los eventos de riesgo que tienen mayor incidencia en los resultados de la institución y los factores asociados a los mismos, observando el principio de importancia relativa o materialidad, además se debe tener en cuenta las características propias de cada institución, de tal forma que se pueda reconocer la vulnerabilidad ante los riesgos operativos. Para esto se debe levantar los eventos producidos en cada segmento de la institución (Ver Anexo 3), con los cuales se crea un registro con los eventos de riesgos producidos, a los mismos se los identifica con un código para facilitar la evaluación de cuantas veces se ha producido dicho evento en toda la institución y poder generar una estimación objetiva de las pérdidas ocasionadas, no es posible contar con datos estadísticos que nos puedan orientar con proyecciones porque la cuantificación es un tema complejo y las técnicas para esto aún no son claras. Sin embargo con dichas estimaciones se puede

proporcionar una idea de lo que ocurre con este riesgo y se puede tomar medidas con los procesos identificados para que tengan el mínimo porcentaje de ocurrencia y no generen más eventos de pérdida para la institución.

Para la identificación de un proceso en una institución es necesario establecer los principios para la asignación de las líneas de negocio³⁰, mismas que a continuación se describen:

- a) Todas las actividades deberán asignarse a las líneas de negocio de nivel uno³¹ de forma que a cada una de las actividades le corresponda una sola línea de negocio y no permanezca ninguna actividad sin asignar;
- b) Cualquier actividad bancaria o no bancaria que no pueda asignarse con facilidad al marco de las líneas de negocio, pero que represente una función auxiliar a una actividad incluida en dicho marco, deberá ser asignada a la línea de negocio a la que presta apoyo. Si la actividad auxiliar presta apoyo a más de una línea de negocio, deberá utilizarse un criterio de asignación objetivo;
- c) A la hora de asignar los ingresos brutos, si una actividad no puede ser asignada a una determinada línea de negocio, entonces deberá utilizarse la línea de negocio que genere el requerimiento de capital más elevado. Cualquier actividad auxiliar asociada deberá también asignarse a la misma línea de negocio;
- d) La asignación de actividades a líneas de negocio a los efectos de capital por riesgo operativo deberá ser coherente con las definiciones de líneas de negocio utilizadas en los cálculos de capital regulador en otras categorías de riesgo (es decir, riesgo de crédito y de mercado). Cualquier desviación de este principio deberá motivarse y documentarse con claridad;

³⁰ Para esta investigación y de acuerdo con los datos proporcionados, la institución cuenta con 17 líneas o segmentos como se lo ha establecido en el Anexo...

³¹ Más adelante se explica las categorías de tipos de eventos que conforman el nivel 1.

- e) El proceso de asignación utilizado deberá documentarse con claridad. En particular, las definiciones por escrito de las líneas de negocio deberán ser suficientemente claras y detalladas para que la asignación de líneas de negocio realizada pueda ser reproducida por terceros. Entre otras cosas, la documentación deberá argumentar con claridad cualquier excepción o salvedad existente y deberá conservarse en registros;
- f) La alta dirección es responsable de la política de asignación (que estará sometida a la aprobación del consejo de administración); y
- g) El proceso de asignación a líneas de negocio deberá someterse a examen independiente.

A continuación se muestra en la tabla 3 la asignación de las principales líneas del negocio:

TABLA. 3 ASIGNACION DE LAS LINEAS DE NEGOCIO

Nivel 1	Nivel 2	Grupo de Actividades
Finanzas corporativas	Finanzas corporativos	Fusiones y adquisiciones, suscripción de emisiones, privatizaciones, titulización, investigación, deuda (pública, alto rendimiento), accionistas, sindicaciones. Ofertas públicas iniciales, colocaciones privadas en mercado secundario
	Finanzas de administraciones locales/públicas	
	Banca de inversión	
	Servicios de asesoramiento	
Negociación y ventas	Ventas	Renta fija, renta variable, divisas, productos básicos, crédito, financiación, posiciones propias en valores, préstamo y operaciones con pacto de recompra, intermediación, deuda, intermediación unificada
	Creación de mercado	
	Posiciones propias	
	Tesorería	
Banca minorista	Banca minorista	Préstamos y depósitos de clientes minoristas, servicios bancarios, fideicomisos y testamentarías
	Banca privada	Préstamos y depósitos a clientes privados, servicios bancarios, fideicomisos y testamentarías, asesoramiento de inversiones
	Servicios de tarjetas	Tarjetas de empresa / comerciales, de marca privada y Minoristas
Banca comercial	Banca comercial	Financiación de proyectos, bienes raíces, financiación de exportaciones, financiación comercial, factoring, arrendamiento financiero, préstamos, garantías, letras de cambio
Liquidación de pagos	Clientes externos	Pagos y recaudaciones, transferencia de fondos, compensación y liquidación
Servicios de agencia	Custodia	Cajas de seguridad, certificados de valores, préstamo de valores (Clientes), operaciones de sociedades
	Agencia de empresas	Agentes de emisiones y pagos
	Fideicomiso de empresas	

Administración de activos	Administración discrecional de fondos	Agrupados, segregados, minoristas, institucionales, cerrado, abierto, participaciones accionarias
	Administración no discrecional de fondos	Agrupados, segregados, minoristas, institucionales, de capital fijo, de capital variable
Intermediación minorista	Intermediación minorista	Ejecución y servicio completo

Fuente: Basilea II

Elaboración: La autora

El siguiente paso es **Medir el Riesgo**, para calcular el efecto que generan los eventos de riesgo identificados sobre el valor de los portafolios de inversión y financiación, se debe establecer un mapa de disposiciones y seleccionar herramientas de medición y control que se acomode con mayor precisión a los riesgos asumidos por la institución, estas herramientas deben permitir calcular rápidamente el efecto sobre los resultados, ocasionados por movimientos de los eventos de riesgo, con el fin de hacer más eficientes los procesos de la institución y comprender el perfil del riesgo y dirigir de manera más efectiva los recursos para la gestión de los mismos. Para la institución objeto de esta investigación los cálculos realizados se los muestra en el Anexo N° 4

Posteriormente se debe **Monitorear** los riesgos operacionales definiendo un esquema organizado de reportes que permita contar con información suficiente y adecuada para limitar y neutralizar los eventos de riesgos que puedan afectar a la institución para determinar niveles máximos hasta los cuales está dispuesta admitir pérdida como consecuencia de la fluctuación de estos. Los límites se deberán establecer en función del grado de tolerancia al riesgo por parte de la entidad y el capital que se quiere arriesgar para este riesgo principalmente. Por medio del monitoreo se valora la calidad del desempeño de los modelos de identificación y medición así como el cumplimiento y eficiencia de los límites establecidos.

Con lo mencionado en los párrafos anteriores vamos a explicar e indicar la clasificación de tipos de eventos de pérdida por proceso:

Categoría de tipos de eventos

Fraude Interno.- Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o a soslayar regulaciones, leyes o políticas empresariales (excluidos los eventos de diversidad / discriminación) en las que se encuentra implicada, al menos, una parte interna a la empresa.

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

Relaciones laborales y seguridad en el puesto de trabajo.- Pérdidas derivadas de actuaciones incompatibles con la legislación o acuerdos laborales, de higiene o seguridad en el empleo, del pago de reclamaciones por daños a las personas, o de eventos de diversidad /discriminación.

Prácticas con clientes, productos y negocios.- Pérdidas derivadas del incumplimiento involuntario o negligente de una obligación profesional frente a clientes concretos (incluidos requisitos fiduciarios y de adecuación), o de la naturaleza o diseño de un producto.

Daños a activos materiales.- Pérdidas derivadas de daños o perjuicios a activos materiales como consecuencia de desastres naturales u otros acontecimientos.

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

Ejecución, entrega y gestión de procesos.- Pérdidas derivadas de errores en el procesamiento de operaciones o en la gestión de procesos, así como de relaciones con contrapartes comerciales y proveedores

A continuación se muestra una tabla con los 3 niveles de la clasificación de los eventos de pérdida:

TABLA. 4 CLASIFICACION DETALLADA DE TIPOS DE EVENTOS DE PÉRDIDA POR NIVELES

Nivel 1	Nivel 2	Ejemplos de actividades (Nivel 3)
Fraude interno	Actividades no autorizadas	Operaciones no reveladas (intencionalmente) Operaciones no autorizadas (con pérdidas pecuniarias) Valoración errónea de posiciones (intencional)
	Hurto y fraude	Fraude / fraude crediticio/ depósitos sin valor Hurto / extorsión / malversación / robo Apropiación indebida de activos Destrucción maliciosa de activos Falsificación Utilización de cheques sin fondos Contrabando Apropiación de cuentas / Fingimiento de personalidad / etc. Incumplimiento / evasión de impuestos (intencional) Sobornos / Cohechos Abuso de Información privilegiada (no a favor de la empresa)
Fraude externo	Hurto y fraude	Hurto/ Robo Falsificación Circulación de cheques sin fondos
	Seguridad de los sistemas	Daños por ataques informáticos Robo de información (con pérdidas pecuniarias)
Relación laborales y seguridad en el puesto de trabajo	Relaciones laborales	Cuestiones relativas a remuneración, beneficios sociales, extinción de contratos. Organización de la actividad laboral
	Salud seguridad en el puesto de trabajo	Responsabilidad común (resbalones, etc.) Eventos relacionados con las normas de higiene y seguridad en el trabajo. Indemnizaciones a los trabajadores
	Diversidad y discriminación	Todo tipo de discriminación
Prácticas con clientes, productos y negocios	Adecuación, divulgación de información y Confianza	Abusos de confianza / incumplimiento de pautas Aspectos de adecuación / divulgación de información (know your customer (KYC), etc.)

		<p>Quebrantamientos de la revelación de información sobre clientes minoristas</p> <p>Violación de privacidad</p> <p>Ventas agresivas</p> <p>Confusión de cuentas</p> <p>Abuso de información confidencial</p> <p>Responsabilidad del prestamista</p>
	Prácticas inadecuadas de negocio o de mercado	<p>Prácticas ajenas a la competencia</p> <p>Prácticas inadecuadas de negociación / mercado</p> <p>Manipulación del mercado</p> <p>Abuso de información privilegiada (en favor de la empresa)</p> <p>Actividades no autorizadas</p> <p>Blanqueo de dinero</p>
	Defectos del producto	<p>Defectos del producto (no autorizado, etc.)</p> <p>Errores de los modelos</p>
	Selección, patrocinio y exposición	<p>Ausencia de investigación a clientes conforme a directrices</p> <p>Superación de los límites de exposición frente a clientes</p>
	Actividades de asesoramiento	<p>Litigios sobre resultados de las actividades de asesoramiento</p>
Daños a activos materiales	Desastres y otros acontecimientos	<p>Pérdidas por desastres naturales</p> <p>Pérdidas humanas por causas externas (terrorismo, vandalismo)</p>
Incidencias en el negocio y fallos en el sistema	Sistemas	<p>Hardware</p> <p>Software</p> <p>Telecomunicaciones</p> <p>Interrupción / incidencias en los suministros</p>
Ejecución, entrega y gestión de procesos	Recepción, ejecución y mantenimiento de operaciones	<p>Comunicación defectuosa</p> <p>Errores de introducción de datos, mantenimiento o carga</p> <p>Incumplimiento de plazos o de responsabilidades</p> <p>Funcionamiento erróneo de modelos / sistemas</p> <p>Error contable / atribución a entidades erróneas</p> <p>Errores en otras tareas</p> <p>Fallo en la entrega</p> <p>Fallo en la gestión colateral</p> <p>Mantenimiento de datos de referencia</p>
	Seguimiento y comunicación	<p>Incumplimiento de la obligación de informar</p>

	de informes	Inexactitud de informes externos (con generación de pérdidas)
	Admisión de clientes y documentación	Inexistencia de autorizaciones / rechazos de clientes Documentos jurídicos inexistentes / Incompletos
	Gestión de cuentas de clientes	Acceso no autorizado a cuentas Registros incorrectos de clientes (con generación de pérdidas) Pérdida o daño por negligencia de activos de clientes
	Contrapartes comerciales	Prácticas inadecuadas de contrapartes distintas de clientes Otros litigios con contrapartes distintas de Clientes
	Distribuidores y proveedores	Externalización Litigios con distribuidores

Fuente: Basilea II

Elaboración: La autora

Finalmente hay que **Mitigar** los eventos de riesgo identificados, esto mediante un plan de continuidad que permita gestionar una mejora continua sobre las amenazas identificadas. El plan de continuidad está orientado a asegurar la continuidad del negocio, la satisfacción del cliente y la productividad a pesar de eventos inesperados, este plan 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 contingencia³², un plan de reanudación³³ y un plan de recuperación³⁴

³² 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.

³³ Plan de reanudación.- Especifica los procesos y recursos para mantener la continuidad de las operaciones en la misma ubicación del problema.

³⁴ Plan de recuperación.- Especifica los procesos y recursos para recuperar las funciones del negocio en una ubicación alterna dentro o fuera de la institución.

Las instituciones deben implementar planes de contingencia y de continuidad a fin de garantizar su capacidad de operar en forma continua y minimizar las pérdidas en caso de una interrupción severa del negocio, para esto deberán efectuar adecuados estudios de riesgos y balancear el costo de la implementación de un plan de continuidad con el riesgo de no tenerlo, esto dependerá de la criticidad de cada proceso de la entidad; para aquellos de muy alta criticidad se deberá implementar un plan de continuidad, para otros bastara con un plan de contingencia.

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

- Definición de una estrategia de continuidad de los negocios en línea con los objetivos institucionales;
- Identificación de los procesos críticos del negocio, aún en los provistos por terceros;
- Identificación de los riesgos por fallas en la tecnología de información;
- Análisis que identifique los principales escenarios de contingencia tomando en cuenta el impacto y la probabilidad de que sucedan;
- Evaluación de los riesgos para determinar el impacto en términos de magnitud de daños, el período de recuperación y tiempos máximos de interrupción que puedan ocasionar los siniestros;
- Elaboración del plan de continuidad del negocio para someterlo a la aprobación del directorio u organismo que haga sus veces;
- Realización de pruebas periódicas del plan y los procesos implantados que permitan comprobar su aplicabilidad y realizar los ajustes necesarios; y,
- Incorporación del proceso de administración del plan de continuidad del negocio al proceso de administración integral de riesgos.

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

Los planes de contingencia y de continuidad deberán incluir, al menos, lo siguiente:

- Las personas responsables de ejecutar cada actividad y la información (direcciones, teléfonos, correos electrónicos, entre otros) necesaria para contactarlos oportunamente;
- Acciones a ejecutar antes, durante y una vez ocurrido el incidente que ponga en peligro la operatividad de la institución;
- Acciones a realizar para trasladar las actividades de la institución a ubicaciones transitorias alternativas y para el restablecimiento de los negocios de manera urgente;
- Cronograma y procedimientos de prueba y mantenimiento del plan; y,
- Procedimientos de difusión, comunicación y concienciación del plan y su cumplimiento³⁵.

Al analizar los eventos de riesgo en la institución financiera se identifica las áreas más vulnerables de la misma y con esto aspectos como:

- Criticidad de los recursos de información relacionados con los procesos críticos del negocio
- Período de tiempo de recuperación crítico antes de incurrir en pérdidas significativas
- Sistema de clasificación de riesgos

Este análisis determina el potencial impacto en los procesos de negocio de una interrupción. Las funciones críticas son identificadas y priorizadas, además de estimarse su impacto operativo o financiero en caso de que éstas funciones sean interrumpidas. Los resultados de este análisis dirigirán las prioridades de lo que será desarrollado para el Plan de Continuidad del Negocio con lo cual se podrá:

- Identificar requerimientos de los recursos mínimos para la recuperación
- Establecer objetivos de tiempos de recuperación (segundos, minutos, horas, días semanas)

³⁵ Superintendencia de Bancos y Seguros, Resolución JB-2005-834, Capítulo V.- De la Gestión del Riesgo Operativo. Pág. 261

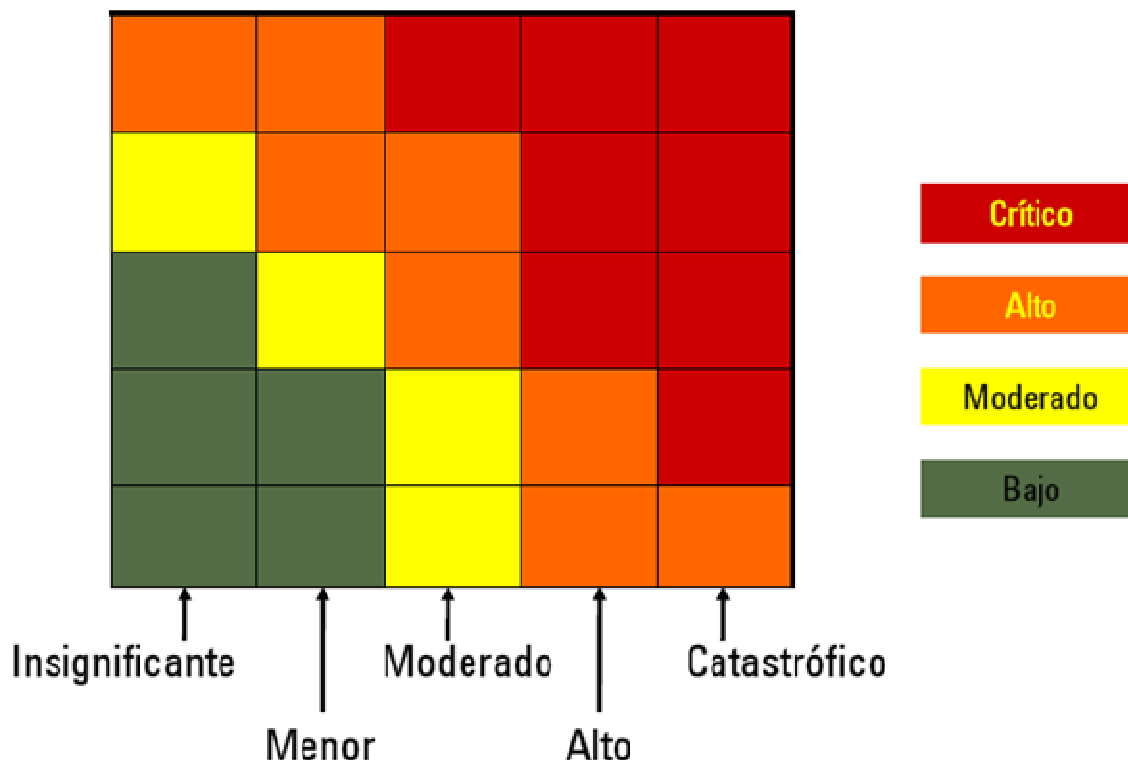
- Establecer objetivos de puntos de recuperación (semanas, días, horas, minutos, segundos)

Es necesario realizar el proceso de pruebas del plan de continuidad del negocio, capacitar al personal con actividades dentro del plan. El plan en sí mismo debe ser una entidad viva y modificable de acuerdo a la dinámica de la propia institución.

Por esto el plan de continuidad del negocio debe incluir un conjunto de decisiones traducidas en acciones específicas que se realizan con el propósito de responder a eventos dados, para mitigarlos (transferir, absorber, reducir o evitar los daños y pérdida que se derivan de la ocurrencia de dichos eventos). La aplicación del plan de acción refleja la naturaleza proactiva de esta metodología. Por esta razón muchos autores manifiestan que *“en la gestión de riesgos en las instituciones financieras se requiere identificar todos los riesgos estrictamente relevantes, ponderar su riesgo inherente en función de su impacto y probabilidad de ocurrencia, evaluar la efectividad de controles existentes y potenciales para mitigar su impacto y tomar decisiones respecto a los riesgos residuales”*, este criterio refuerza la postura, de un plan de acción selectivo (Ver Anexo 6).

Bajo estos criterios el impacto de un evento de riesgo de un proceso puede ser evaluado en una escala de cinco niveles como se muestra en la figura 7 a continuación:

FIGURA N°7 CRITERIOS DE IMPACTO



Fuente: José Lozano. Nuevos desarrollos en Basilea II: Riesgo Operativo. KPMG – México.

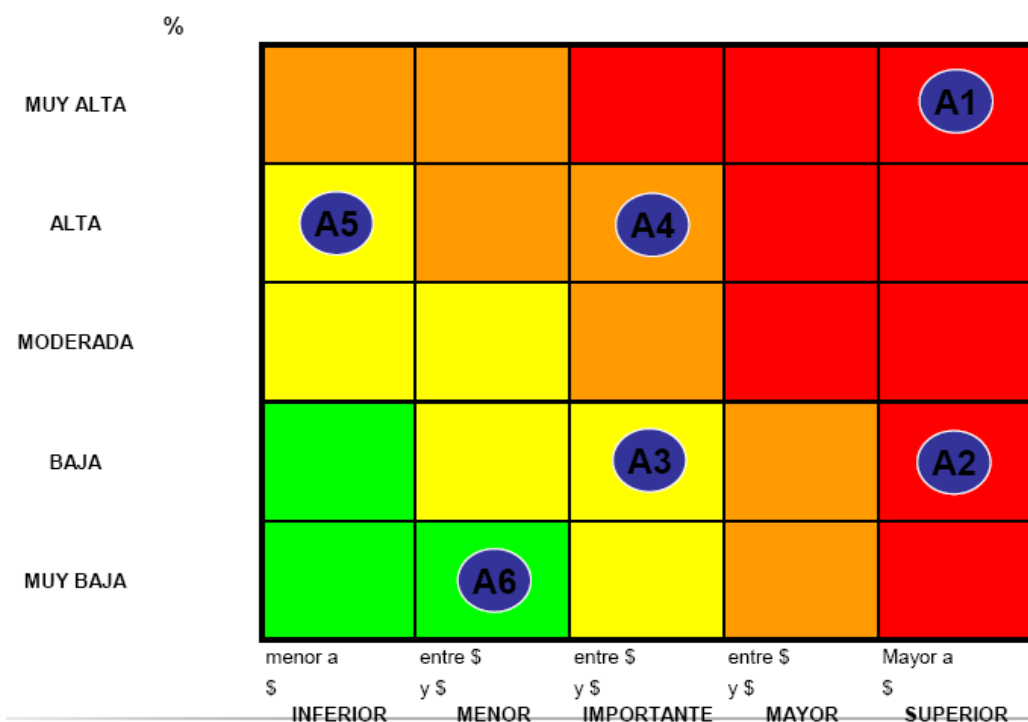
Elaboración: La autora

Para el caso de esta investigación se ha registrado los eventos de riesgo de pérdida producidos en la institución objeto de investigación con códigos y se los ha identificado con el **0** (cero) a los eventos considerados como no catastróficos y con **1** (uno) a los eventos considerados como catastróficos. Un ejemplo de evento catastrófico es el riesgo de pérdida por disminución en el valor de los activos financieros producido por errores o limitaciones en la administración de seguridad de Easy Pagos (Cobros y Pagos) debido a falla en la asignación de perfiles de usuario; un ejemplo de evento no catastrófico es el riesgo de pérdida por disminución en el valor de los activos financieros producido por que se realizaron retiros con cheques clonados debido a fraude externo/asalto/robo. (Ver Anexo 2 y 4).

Para realizar la evaluación del impacto del riesgo de un proceso tomando en cuenta la escala con los cinco niveles indicado en la figura N° 8 y de acuerdo a la estructura de cada institución se establecen los valores de pérdidas que generan a la misma; para la institución objeto de esta investigación y como se

menciono anteriormente los eventos de riesgo se han evaluado como catastróficos y no catastróficos cuyos valores van desde US\$1.39,00 a US\$294.120M. A continuación se muestra el cuadro N° donde se indica un score de riesgo absoluto sin tener en cuenta los controles asociados a este:

FIGURA N° 8 ENFOQUE DE ANALISIS DE RIESGOS (EVALUACION DE RIESGOS)

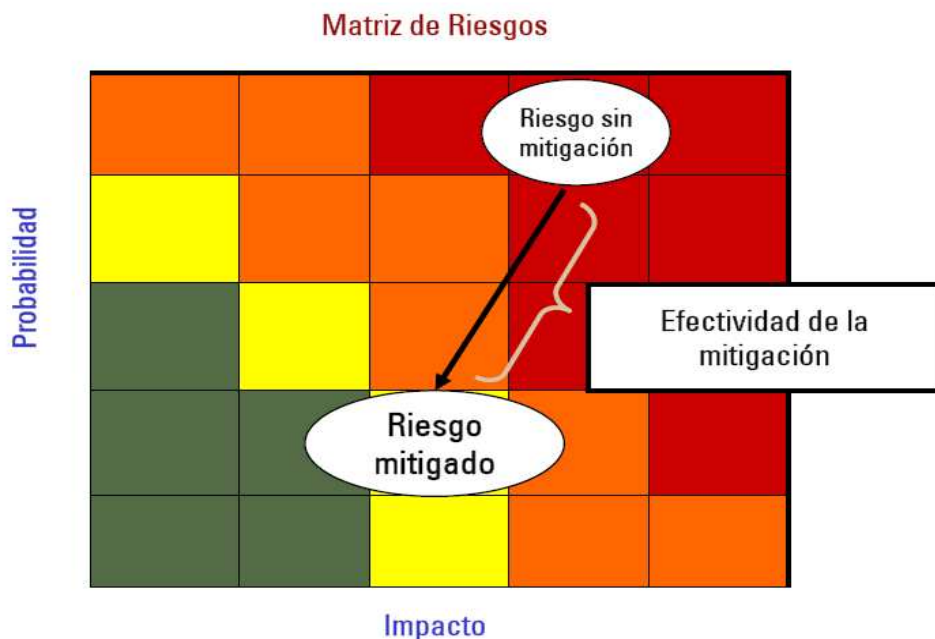


Fuente: José Lozano. Nuevos desarrollos en Basilea II: Riesgo Operativo. KPMG – México.

Elaboración: La autora

La elaboración de una matriz de riesgos esta dado por la probabilidad de ocurrencia de un evento de riesgo y el impacto que pueda tener en la institución financiera, dichos eventos identificados deben ser mitigados. En la figura N° 9 se muestra gráficamente lo mencionado:

FIGURA N° 9 EVALUACION DEL RIESGO DE UN PROCESO



Fuente: José Lozano. Nuevos desarrollos en Basilea II: Riesgo Operativo. KPMG – México.

Elaboración: La autora

Las principales estrategias para mitigar los eventos de riesgo son: evitar³⁶, reducir³⁷, absorber³⁸, transferir³⁹, tal como se muestra en la figura N° 10

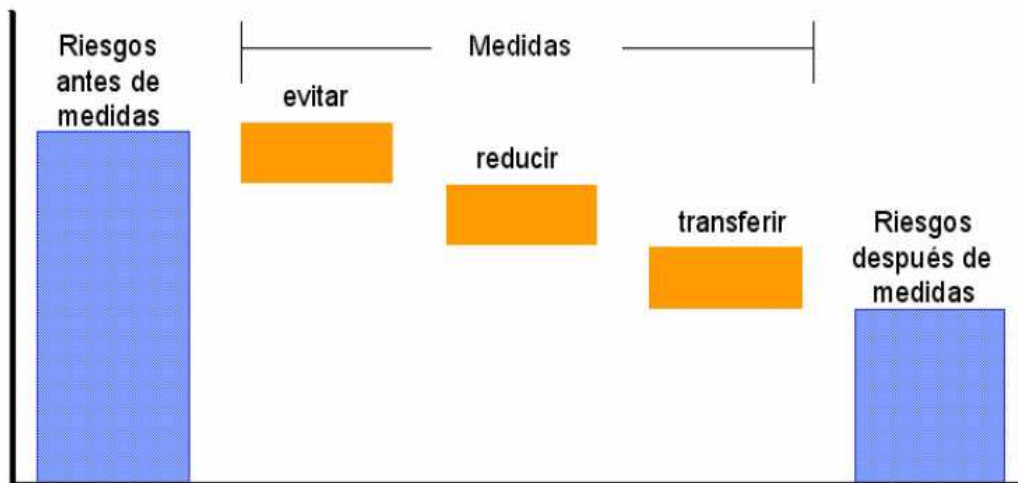
FIGURA N° 10 ESTRATEGIAS DE MITIGACION DE RIESGOS

³⁶ Se toma la determinación de no proceder a formalizar la operación que genera riesgo.

³⁷ Es la que requiere mayor destreza financiera ya que se debe gestionar para reducir a su mínimo nivel optimizando la relación Riesgo – Rendimiento, se requiere conocimiento de técnicas en función de la variabilidad de los riesgos operacionales; igualmente es necesario analizar los instrumentos disponible en el ámbito o aquellas que puedan desarrollarse para realizar coberturas parciales o totales de los riesgos operacionales a los cuales se encuentra expuestos la entidad.

³⁸ Cubrir con sus propios recursos el riesgo al cual se encuentra expuesto la institución.

³⁹ Se refiere a trasladar a un tercero el riesgo al que está expuesto la institución.

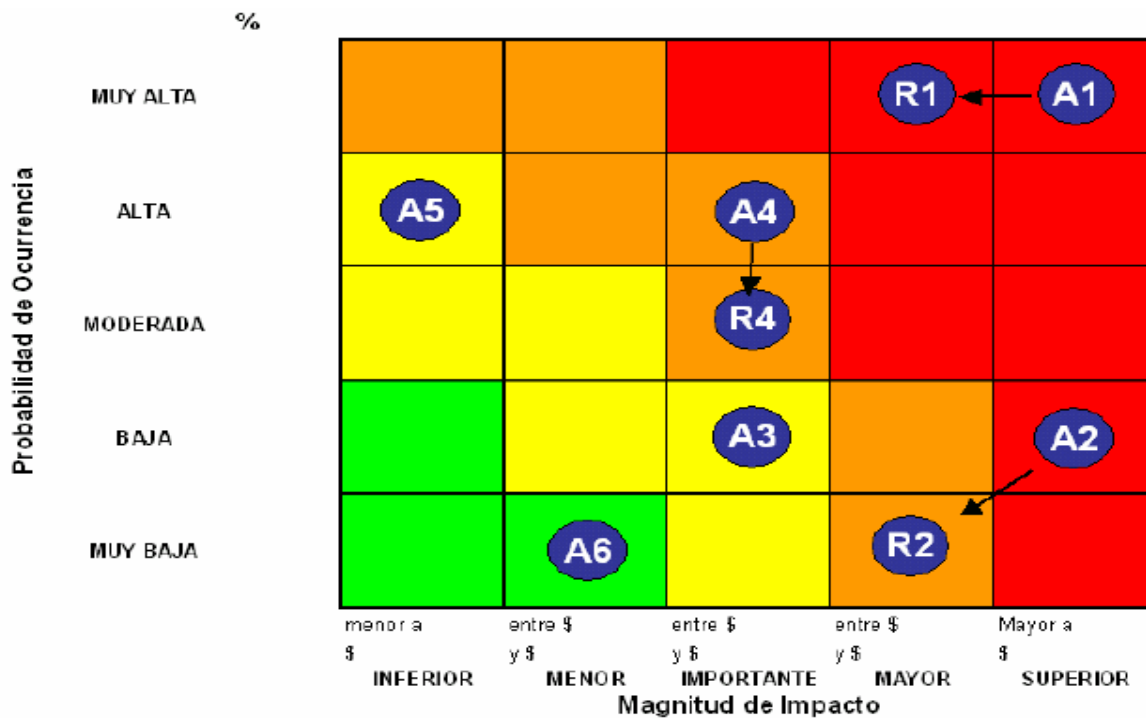


Fuente: José Lozano. Nuevos desarrollos en Basilea II: Riesgo Operativo. KPMG – México.

Elaboración: La autora

Es así que cada evento de riesgo debe tener en cuenta controles asociados a este (riesgo residual), en la figura N° 11 se muestra esto:

FIGURA N° 11 RIESGO RESIDUAL



Fuente: José Lozano. Nuevos desarrollos en Basilea II: Riesgo Operativo. KPMG – México.

Elaboración: La autora

Es común que las instituciones tengan indicadores de seguimientos para identificar los eventos de riesgos, estos pueden ser: la calificación de la auditoría o la Key Performance Indicators (nº de descuadres al mes, nº de reprocesos, nº de reportes regulatorios, multas de las autoridades, errores de captura en los sistemas, nº de retrasos en el envío de la información corporativa) e indicadores de volumen (facturación, transacciones). Sin embargo, muy pocas instituciones registran un quebranto sin antes de haber analizado su naturaleza, causas no informe correspondiente a la dirección.

En la Fig. 12 se muestra una matriz de riesgo en un área de la institución; adicionalmente en la tabla 6 y 7 se presenta las guías para la elaboración de una matriz de riesgos, para aclarar y dar una idea de cómo se puede establecer los parámetros para lo mencionado.

FIG. 12 MATRIZ DE RIESGOS POR PROCESOS

AREAS	LINEA DE NEGOCIO	PROCESO	SUBPROCESO	Nº	RIESGO	1ER NIVEL	2DO NIVEL
INVERSIONES	COMPRA – VENTA	PRENEGOCIACION	Autorización	1	Operación no autorizada	Fraude interno	Actividades no autorizadas
				2	Producto no autorizado	Fraude interno	Actividades no autorizadas
				3	Operador no autorizado	Fraude interno	Robo y fraude
				4	Broker/Dealer no autorizado	Prácticas con clientes, productos o negocios	Prácticas de mercado o de negocio impropias
			Evaluación de riesgos	5	Contrapartida no autorizada	Prácticas con clientes, productos o negocios	Prácticas de mercado o de negocio impropias
				6	Excedido en los límites autorizados	Prácticas con clientes, productos o negocios	Selección, soporte y exposición de clientes

			Documentación legal	7	Documento legal insuficiente	Gestión de ejecución, entrega y procesos	Errores o pérdida de documentos	
				8	Falta de poderes de representación	Prácticas con clientes, productos o negocios	Prácticas de mercado o de negocio impropias	
			Pricing	9	Pricing incorrecto (modelo de valoración incorrecto)	Gestión de ejecución, entrega y procesos	Captura, ejecución y mantenimiento de transacciones	
		LNEGOCIACION	Ejecución		10	Precio fuera de mercado	Fraude interno	Robo y Fraude
					11	(Fraude) Error de entendimiento (contratación telefónica o desacuerdo)	Gestión de ejecución, entrega y procesos	Captura, ejecución y mantenimiento de transacciones
					12	Operación no reportada o falsa (fraude)	Fraude interno	Actividades no autorizadas
					13	Operación no reportada (no intencionada)	Gestión de ejecución, entrega y procesos	Supervisión y reporte de información
			Captura/Registro	14	Error en la introducción de datos	Gestión de ejecución, entrega y procesos	Captura, ejecución y mantenimiento de transacciones	

Fuente: Basilea II

Elaboración: La autora

TABLA. 5

GUIA DE USO PARA LA ELABORACION DE UNA MATRIZ POR PROCESO

NOMBRE	DESCRIPCION
Número	Secuencial dentro del inventario
Tipo de Proceso	Se refiere a la clasificación del macroproceso estratégico, operativo o de soporte
Macroproceso	Nombre del macroproceso con el cual se lo identifica. Los macroprocesos se los puede visualizar en el mapa de procesos
Proceso	Nombre del proceso identificado. Agrupa a los diferentes subprocesos y a su vez es parte de un macroproceso
Subproceso	Corresponde al nombre definido para las actividades realizadas en el subproceso
Proceso crítico	Si/No, indicativo de si el subproceso es crítico y afecta a la continuidad del negocio o no.
Manual de supervisión	Si/No, indica subproceso tiene un manual de supervisión adjunto.
Flujo de proceso	Si/No, indica si se ha presentado el flujo correspondiente al subproceso identificado
Matriz de riesgo	Si/No, indica si para el subproceso ya se ha identificado sus principales riesgos y construido la matriz de riesgo
Objetivo	Objetivo principal que persigue la realización del subproceso
Frecuencia	Frecuencia de ejecución del subproceso, indica la periodicidad del producto (continuo, anual, mensual, ocasional, temporal)

Nivel de ejecución	Recursos humanos que realizan el subproceso
Nivel de supervisión	Recursos humanos que supervisan el subproceso, responsables de la verificación del producto
Áreas ejecutoras	Áreas ejecutoras en las cuales se realiza físicamente el subproceso
Gerencia	Gerencia, funcional a la cual pertenece el área en la que se realiza el subproceso
Gerencia Nacional	Gerencia Nacional, a la cual pertenece la gerencia del área/s en la que se realiza el subproceso
Entradas	Campo en el cual se describen los insumos para llevar a cabo el subproceso
Productos/Servicios	Descripción de los diferentes resultados del subproceso
Medios de entrega	Forma de entrega del producto o servicio final al cliente interno o externo. (electrónico, físico)
Políticas	Referencia a la norma o política que sustenta el subproceso
Tipo de ejecución	Periodicidad de ejecución, diaria, mensual, otra
Clientes internos	Destinatarios finales del producto o servicio producido
Clientes externos	Destinatarios finales del producto o servicio producido, que no se encuentran dentro de la organización
Indicadores de gestión	Si/No indica el subproceso tiene definidos indicadores de gestión para controlar el mismo
Fecha de aprobación	Fecha de aprobación del flujograma del subproceso
Afecta a la contabilidad	Si/No indica si el subproceso ejecutado

	requiere de un registro contable
Tiene operaciones tributarias	Si/No, indica si el subproceso ejecutado tiene impacto tributario

Elaboración: La autora

En la guía de uso anterior se indica detalladamente los parámetros a seguir, en esta se incluye una matriz de riesgos para los procesos, para la cual se muestra una guía de uso para su aplicación:

TABLA. 6

GUIA DE USO: MATRIZ DE RIESGOS

NOMBRE	DESCRIPCIÓN
Proceso	Nombre del proceso identificado. Agrupa a los diferentes subprocesos y a su vez es parte de un macroproceso
No. Actividad	Número de orden de la actividad asignada en el proceso
Descripción de la actividad	Explicar, detallar la actividad desarrollada
Descripción del RIESGO	Explicar, detallar el riesgo al cual está expuesta la actividad
Tipo de EVENTO	Fraude Interno Fraude Externo Prácticas de empleo y seguridad laboral Prácticas con clientes, productos y el negocio

	<p>Daños a los activos físicos</p> <p>Interrupción de operaciones o fallas del sistema</p> <p>Deficiencias en ejecución y gestión de procesos</p> <p>Deficiencias en procesos relacionados con proveedores y 3ros.</p>
FALLAS o insuficiencias	Razón, motivo o circunstancia por la cual se tiene exposición al riesgo. Esto se encuentra en relación directa a la descripción del riesgo
FACTORES DE RIESGO OPERATIVO	<p>Procesos</p> <p>Personas</p> <p>Tecnología de la información</p> <p>Eventos externos</p>
IMPACTO	<p>Grado de afectación de la ocurrencia del evento en los últimos tres años:</p> <p>Insignificante</p> <p>Menor</p> <p>Moderado</p> <p>Alto</p> <p>Catastrófico</p>
PROBABILIDAD	<p>Posibilidad de ocurrencia del evento en los últimos tres años:</p> <p>Muy baja</p> <p>Baja</p> <p>Moderada</p> <p>Alta</p> <p>Muy alta</p>
SEVERIDAD	Resultado de la conjugación de probabilidad e impacto del evento

	Bajo Moderado Alto Crítico
CONTROLES Implementados	Exámenes, inspecciones o análisis de seguimiento efectuados a las actividades
Efectividad del control	Resultados del control implementado medio como: impacto*frecuencia/control
RIESGO RESIDUAL	Riesgo final al cual está expuesta la actividad luego de la aplicación de controles.

Elaboración: La autora

4.4. Desarrollo de Metodologías aproximadas para la cuantificación del Riesgo Operacional

4.4.1 Modelaje para Pérdidas Esperadas en Riesgo Operativo

Modelación de una Pérdida

Existen varias maneras de modelar el comportamiento de una variable aleatoria dependiendo del riesgo. Si "X" es una variable aleatoria que representa pérdida potencial, el valor esperado de "X" es una medida equivalente pura. En otras palabras, el riesgo se puede transferir a un tercero, o puede asumir el riesgo cuya cuantía viene expresada de la siguiente manera:

Si $X \sim f(X, \Theta)^{40}$ y $E(X)$ y $Var(X)$ es el valor esperado y la varianza existen; entonces una medida de riesgo, es igual a $\sigma_x^2 = Var(X)$; siendo $E(X) = \sum XiPi$ y $\sigma_x^2 = E(X - E(X))^2$; en el caso de variables discretas y $E(X) = \int xf(x)dx$ en el caso continuo.

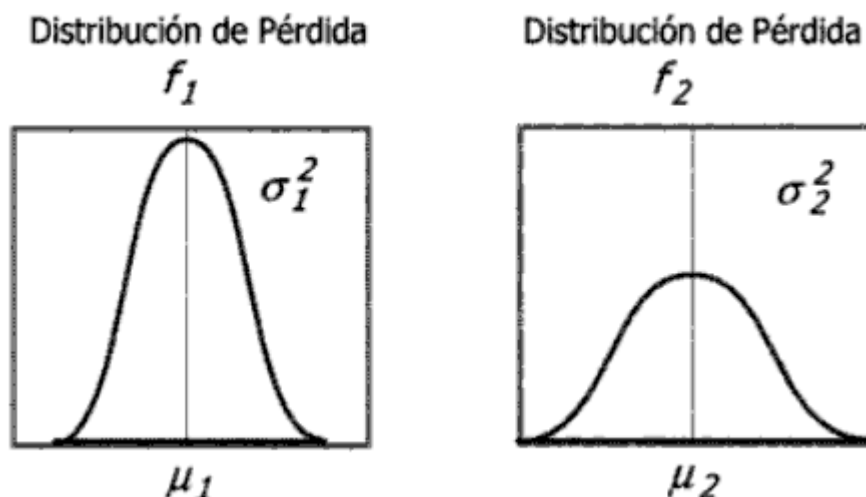
⁴⁰ Esta expresión significa que la variable aleatoria está distribuida según la función de probabilidad f con un parámetro Θ

Otra medida de variabilidad del riesgo viene dado por el Coeficiente de Variación

$$\rho = \frac{\sigma}{\mu} \text{ donde } \sigma = \sqrt{\text{Var}(X)} \text{ y } \mu = E(X)^{41}$$

Aquellas distribuciones de pérdida cuyo Coeficiente de Variabilidad ρ sea muy bajo (no hay reglas específicas, pero empíricamente se pueden considerar como bajos valores de $\rho \leq 30\%$) tiene asociados distribuciones cuyas varianzas son bajas y viceversa; suponiendo una $E(X) = \mu$ fija y conocida para dos distribuciones f_1 y f_2 se obtendría:

FIGURA N°13 DISTRIBUCIONES DE PERDIDA f_1 y f_2



Fuente: Alfonso de Lara Haro. Medición y Control de Riesgos Financieros.

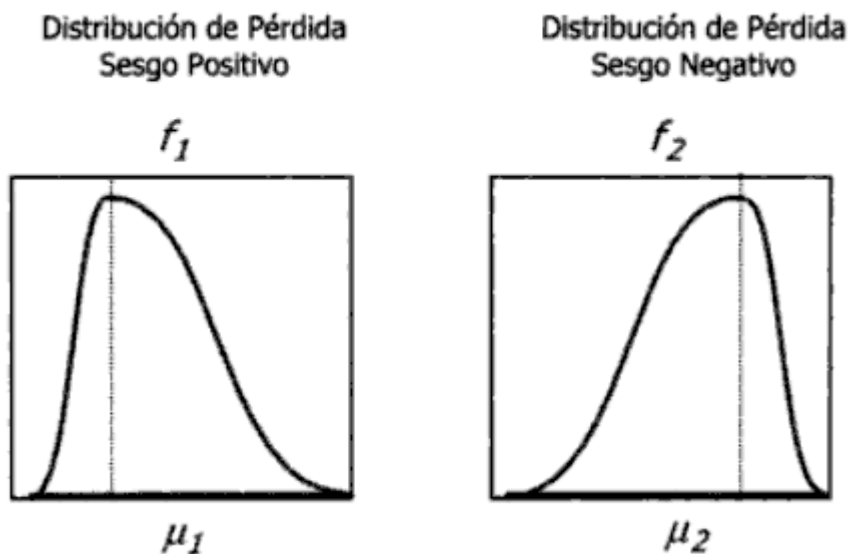
Elaboración: La autora

⁴¹ Evaristo Díz Cruz. Teoría de Riesgo: Riesgo Actuarial, Riesgo Financiero. Global ediciones, pág. 5

Donde $\mu_1 = \mu_2$ y $\sigma_1^2 < \sigma_2^2$ lo cual implica un menor riesgo en f_1 que en f_2 . En el caso anterior, las distribuciones son simétricas, lo cual implica que no existe sesgo alguno.

Por el contrario, otras distribuciones de pérdida son generalmente sesgadas.

FIGURA N° 14 DISTRIBUCIONES DE PERDIDA SESGADAS



Fuente: Alfonso de Lara Haro. Medición y Control de Riesgos Financieros.

Elaboración: La autora

El nivel medio de la pérdida, es mayor en f_2 que en f_1 . La diferencia es que en el primer caso, el nivel de riesgo está concentrado en valores relativamente bajos de la variable aleatoria; pero es de alta densidad.

En la práctica es común observar, para la pro-frecuencia de reclamos de severidad baja, una alta densidad o probabilidad. Por el contrario, los reclamos de severidad alta, generalmente tiene una baja densidad.

Modelos de Probabilidad

Existen varias maneras de expresar y describir la distribución de la probabilidad de una pérdida.

En el primer caso, corresponde con la descripción completa y detallada de la variable aleatoria "X" asociada a la magnitud de la pérdida. Si "X" es una variable aleatoria continua, se deben especificar $f(X)$ o $F(X)$ función de densidad o función de distribución respectivamente.

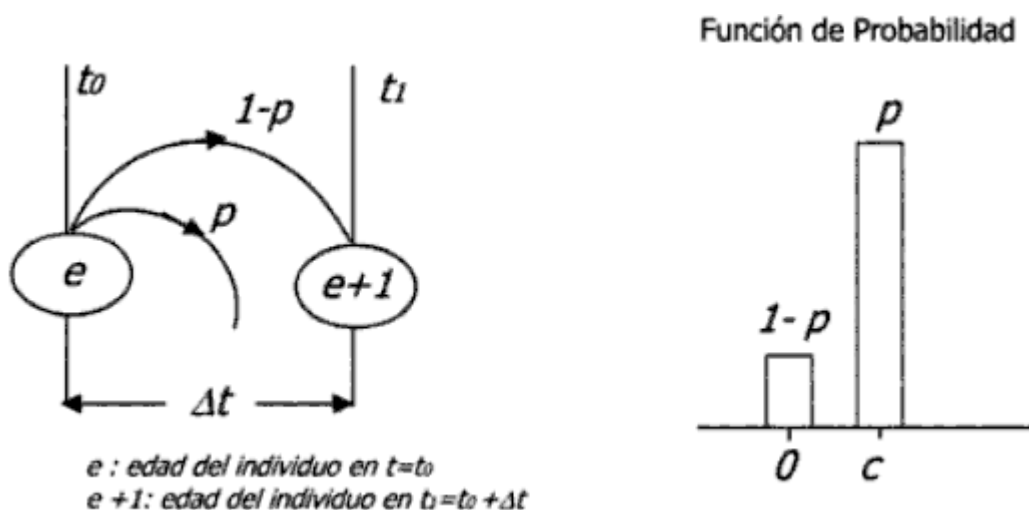
En el caso discreto, la función de probabilidad o la función de distribución deben conocerse⁴². Un caso típico de una distribución de probabilidad discreta se puede representar como sigue:

$$X = \{c \text{ con probabilidad } p \text{ y } 0 \text{ con probabilidad } 1 - p\}$$

Como ***ejemplo*** de esto se pudiera describir en el período de un año $\Delta t = 1$ un beneficio por muerte equivalente a “c” unidades monetarias cuando la probabilidad de muerte dentro del período Δt es p .

Simbólicamente se muestra en la figura N° 15:

FIGURA N° 15 PROCESO MARKOVIANO⁴³



Fuente: Alfonso de Lara Haro. Medición y Control de Riesgos Financieros.

Elaboración: La autora

⁴² O poder ser estimable de alguna manera

⁴³ La probabilidad de que una persona esté viva a la edad ($e+1$), sólo depende de haberlo estado a la edad (e). A esta propiedad se le conoce como markoviana y el proceso de evolución para todas las edades cumpliendo esta prioridad se le conoce como un proceso Markoviano.

La prima o el valor esperado para este beneficio, obviando de momento el valor del dinero en el tiempo, serían:

$$E(X) = cp \div o(1 - p)$$

Donde c es la función de distribución con probabilidad p y o es la función de distribución con probabilidad (1-p), estas deben ser estimables de alguna manera.

$$E(X) = cp$$

Igualmente la varianza $Var(X)$ vendría dado por:

$$\begin{aligned} Var(X) &= E(X - E(X))^2 \\ &= E(X^2 + E^2(X) - 2XE(X)) \\ &= E(X^2) - E^2(X) \\ &= c^2p - (cp)^2 \\ &= c^2p - c^2p^2 \\ &= c^2(p - p^2) \end{aligned}$$

Con un c conocido se podría establecer el máximo nivel de varianza o nivel de riesgo.

La medición efectiva y cuantitativa del riesgo se asocia con la probabilidad de una pérdida futura; la esencia de la administración de riesgos consiste en medir las probabilidades y las pérdidas estimadas en contextos de Incertidumbre para cubrirlas.

Suponiendo que la probabilidad o tasa de que ocurra una pérdida es, \square siendo $X \sim Ber(p)$, lo cual significa que la pérdida ocurre o sencillamente no ocurre. Si el monto de la pérdida, es la variable aleatoria M y es idénticamente nula cuando no ocurre la pérdida, entonces puede establecerse matemáticamente lo que sigue:

$$X = \{1 \text{ si ocurre la pérdida, con probabilidad } p; 0 \text{ si no ocurre la pérdida, con probabilidad } 1-p\}$$

A su vez, la cuantía o severidad viene dada por

$$M = \{B \text{ dado que el pago referido a la pérdida ya ocurrió}; 0\}$$

Este último planteamiento lleva al concepto de probabilidad condicional, acotando formalmente el modelo completo como sigue:

$$P(M|X) = P(M \cap X)/P(X)^{44}$$

⁴⁴ El Teorema de Bayes permite determinar las probabilidades $P(M|X)$ y $P(X|M)$ una en función de la otra, a través del concepto de probabilidad condicional.

Puede existir una descripción completa de la distribución de probabilidad asociada a la cuantía de la pérdida. En la mayoría de los casos en la práctica sólo se conoce $E(M)$ su valor esperado y $Var(M)$ su varianza. Aplicando el concepto de varianza se cumple lo siguiente:

$$Var(M) = E(M^2) - E(M)^2 \text{ y despejando } E(M^2) \text{ se obtiene, } E(M^2) = Var(M) + E(M)^2$$

Si expresamos la variable aleatoria "M" como una mezcla de dos variables aleatorias M_1 y M_2 donde $M_1 = 0$ y $M_2 = B$ con pesos o probabilidades de ocurrencia $\{1-p, p\}$ entonces los dos primeros momentos $E(M)$ y $Var(M)$ de la distribución de pérdida se determinan como sigue:

$$\begin{aligned} E(M) &= (1-p) \cdot E(M_1) + pE(M_2) \\ &= pE(M_2) \\ &= pE(B) \text{ dado que si } M_1 = 0 \Rightarrow E(M_1) = 0 \text{ igualmente} \end{aligned}$$

$$\begin{aligned} E(M^2) &= (1-p) \cdot E(M_1^2) + pE(M_2^2) \\ &= pE(M_2^2) \end{aligned}$$

Luego aplicando el concepto de varianza tenemos:

$$\begin{aligned} Var(M) &= pE(B^2) - (pE(B))^2 \\ &= pE(B^2) - p^2E(B)^2 \end{aligned}$$

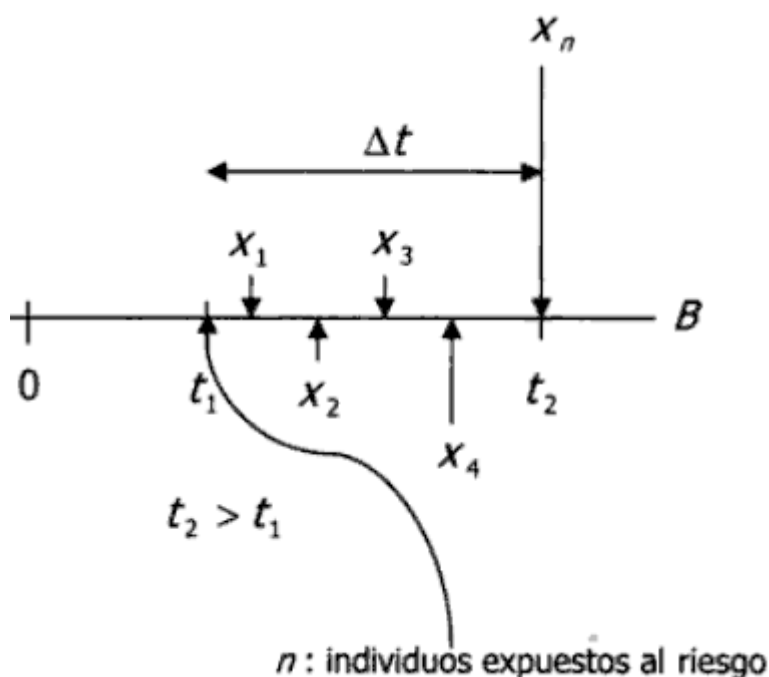
Modelo de Riesgo Individual

El modelo de Riesgo Individual asume que la cartera, portafolio, áreas, individuos expuestos o sometidos al riesgo; digamos que $n > 0$, en un período de tiempo unitario $\Delta t = 1$, están siendo modelados por una variable aleatoria de pérdida individual X_i .

De esta manera se asume independencia y distribuciones de probabilidades idénticas $\forall_i X_i \sim f(X = x)$. Si "S" es la pérdida agregada entonces $S = \sum_{i=1}^n X_i = X_1 + \dots + X_{ni}$ donde "n" es el número total de siniestros⁴⁵

FIGURA N° 16 FLUJO DE PÉRDIDAS

⁴⁵ n: es el número total de siniestros que pudiera también ser una variable aleatoria en ese caso tanto los X_i como los n tendrían asociados sus distribuciones respectivas.



Fuente: Alfonso de Lara Haro. Medición y Control de Riesgos Financieros.

Elaboración: La autora

Lo que interesa es caracterizar la distribución de probabilidad de $S = f(X_1, X_2, \dots, X_n)$ o $f(S = s)$ o su función de distribución $\int_{-\infty}^s f(S) ds$.

Lo anterior pudiera ser muy complicado y hasta matemáticamente intratable, pues dependiendo del tipo de distribución asumido para las X_i la $\sum_{v_i} X_i$ pudiera ser cerrada⁴⁶ o no. Sin embargo es más fácil determinar los momentos de la distribución de pérdida agregada conociendo las $f_{x_i}(x)$.

De nuevo, si $S = \sum_{i=1}^n X_i$ entonces $E(S) = E(\sum_{i=1}^n X_i) = \sum_{i=1}^n E(X_i)$ y $Var(S) = Var(\sum_{i=1}^n X_i) = \sum_{i=1}^n Var(X_i)$ ahora si $X_i \sim f(\mu_i, \sigma_i^2)$ se cumple que $\begin{cases} \mu_i = \mu \text{ entonces} \\ \sigma_i^2 = \sigma^2 \end{cases}$

$E(X_i) = \mu; Var(X_i) = \sigma^2$ por cada $i=1,2,\dots,n$ igualmente.

El coeficiente de variación $P_s = \sigma_s / \mu_s$ siendo $\{\mu_s = E(S); \sigma_s^2 = Var(S)\}$. Haciendo las sustituciones del caso y expresando $P_s = f(\mu, \sigma^2)$ se obtiene $P_s = \frac{\sigma_x}{\mu_x \sqrt{n}}$ el cual $\rightarrow 0$

a medida que $n \rightarrow \infty$. Sin olvidar que $P_x = \frac{\sigma_x}{\mu_x}$ y sustituyendo en la ecuación anterior

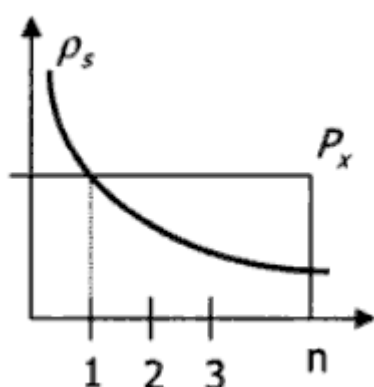
$P_s = \frac{P_x}{\sqrt{n}}$. Esto indica que la variabilidad del portafolio, cartera, etc., es

⁴⁶ El concepto matemáticamente se refiere a la posibilidad de encontrar una distribución para los $\sum X_i$ analíticamente conocida. De no ser posible lo anterior, una de las alternativas es encontrar la distribución empírica a través de la simulación (Simulación Montecarlo).

directamente proporcional al coeficiente de variación de la pérdida individual e inversamente proporcional a la raíz cuadrada del número de individuos expuestos al riesgo.

En el gráfico N° se ve como disminuye el riesgo⁴⁷, cuando el número de individuos aumenta y para un “n” suficientemente grande llega a niveles francamente pequeños. Lo anterior, es una manifestación de la reducción progresiva, más no una eliminación.

FIGURA N°17 EVOLUCION P_s EN FUNCION DE n



Fuente: Alfonso de Lara Haro. Medición y Control de Riesgos Financieros.

Elaboración: La autora

Proceso de Medición (Probabilidad-Severidad)

Se refiere a la medición objetiva de las probabilidades y la severidad de falla con el fin de predecir las pérdidas potenciales, mediante la recopilación de los eventos de riesgos y el modelo de valoración de riesgos donde se define:

- Los factores de evaluación de las categorías de riesgos
- Las relaciones e interdependencias entre riesgos
- Las escalas de valoración para la probabilidad y la severidad
- Combinación de la probabilidad y la severidad
- Valoración de riesgos

Escalas de Valoración de Probabilidad y Severidad

- Nominal: asigna términos lingüísticos a las categorías. Ejemplo: patrones culturales, de uso de la tierra, clasificaciones.

⁴⁷ p es una medida de riesgo.

- Ordinal: escala comparativa. Puede juzgarse como más o menos que. Ejemplo: clasificación como muy alta, media, baja, muy baja ó 1,2,3,4,5 donde el valor numérico no se relaciona con ningún patrón o cantidad si no con una clasificación dada por un analista.
- Intervalo: Intervalos cuantitativos entre unidades de medición de la variable. Ejemplo: utilidad 5', 10', 15'....
- Relacional: similar a la de intervalos pero la medición se hace en relación a un punto de referencia. Ejemplo: pérdidas 5', 10', 15'...(el cero es el punto de referencia).

Combinación de Probabilidad y Severidad

Por lo general el riesgo se expresa a partir de la combinación de sus componentes es decir de la probabilidad y la severidad. En general el riesgo es proporcional a sus componentes por lo tanto una medida de riesgo puede ser expresada esencialmente como se muestra a continuación:

$$Riesgo = P \times S$$

$$Riesgo = P. \alpha \times S. \beta$$

$$Riesgo = EXP(P. \alpha \times S. \beta)$$

Para tratar los riesgos la opción más apropiada es balancear los costos de implementación contra los beneficios derivados de la misma (necesidad de valoración) y ordenar las prioridades hasta cumplir con el presupuesto.

Otros Modelos de Medición

- **Modelos Causales:** Tratan de determinar las causas que originan el evento de riesgo y permiten tratar diferentes tipos de información (aplicaciones econométricas, series de tiempo, análisis multivariante (análisis factorial, análisis discriminante, análisis correlación canónica)).
- **Modelos No Lineales:** Redes neuronales, Logística difusa
- **Técnicas Bayesianas:** Las *Redes Bayesianas* definen las variables que intervendrán en el modelo (diferentes categorías de eventos de pérdida, indicadores de Riesgo por categoría, estimar las probabilidades subjetivas, probabilidades condicionales entre indicadores, probabilidades condicionales por eventos de pérdida dada la relación con los indicadores de riesgo), hacen una revisión de Probabilidades Subjetivas en la Red

Bayesiana (tienen en cuenta la información histórica existente sobre los eventos de pérdida, estiman la distribución de probabilidad de ocurrencia para cada evento de pérdida), establecer la frecuencia aproximada del evento de pérdida, obtienen la distribución de pérdidas totales mediante un método de simulación.

- **Modelos Estocásticos:**
 - Funciones de Probabilidad
 - Teoría del Valor Extremo
 - Modelos de Frecuencia
 - Procesos Estocásticos
 - Simulación Montecarlo

Los limitantes de los modelos son la ausencia de información y la ausencia de relaciones definidas entre indicadores; la solución a esto es la autovaloración y la implementación y resultados del Proyecto Indicadores de Riesgo Operativo.

La similitud entre los modelos explicado anteriormente es que estiman la distribución de la frecuencia y severidad de fallo de la historia, construyen una función de pérdida agregada y obtienen el Valor en Riesgo Operativo como el percentil de la distribución de pérdida agregada.

4.4.2 Medición Cuantitativa del Riesgo Operativo

Se basa en el concepto de VaR (Value at Risk)⁴⁸, aplicado en el sector financiero para cuantificar los riesgos de mercado.

En una institución financiera, los miembros del gobierno corporativo son quienes deben definir dos aspectos fundamentales para el cálculo del VaR: *el nivel de confianza* que desean tener para determinar el VaR, y *el horizonte de tiempo* con que se va a medir⁴⁹. Para el caso de esta

⁴⁸ El VaR es una medida estadística que con un solo dato resume el riesgo de un valor o cartera de valores, de generar pérdidas derivadas de movimientos normales de mercado. Pérdidas superiores al VaR se producen sólo en movimientos anormales de mercado y tienen por tanto una pequeña probabilidad de producirse. El VaR permite una medida homogénea del riesgo asumido. En este sentido agrega todos los factores de riesgo operacional ofreciendo un único dato que es comparable.

⁴⁹ Alfonso de Lara Haro. Medición y Control de Riesgos Financieros. Limusa Noriega Editores. México-2008, pág. 58

investigación se ha utilizado el nivel de confianza del 99% con un horizonte de tiempo de un año.

El VaR no otorga certidumbre con respecto a las pérdidas que se podrían sufrir con un evento de riesgo, sino una expectativa de resultados basada en estadística (series de datos en el tiempo) y en algunos supuestos de los modelos o parámetros que se utiliza para su cálculo. Por ese motivo las instituciones deben en adición al cálculo del VaR, complementar su medición de riesgos con otras metodologías como: el análisis de stress (valores extremos), las reglas prudenciales, los procedimientos y políticas de operación, los controles internos, los límites y las reservas de capital adecuadas; algunas de las citadas anteriormente han sido tomadas en cuenta para elaboración de la presente investigación.

Metodologías para el cálculo del VaR

El Valor en Riesgo se puede calcular mediante dos métodos:

- ✓ Métodos no-paramétricos
- ✓ Métodos paramétricos

- **Métodos no-paramétricos**

Consiste en utilizar una serie histórica de datos de los eventos de riesgo para construir una serie de tiempo simulados o hipotéticos, con el supuesto de que se ha conservado los datos durante el período de tiempo de la serie histórica.

Para aplicar esta metodología los componentes hay que reunir los datos de los eventos de riesgos diarios históricos considerando un período que oscila entre 250 y 500 datos. A partir del histograma de frecuencias de los datos simulados, se calcula el cuantil correspondiente de dicho histograma (primer percentil si el nivel de confianza es de 99%). Existen tres tipos de simulación histórica: crecimientos absolutos, crecimientos logarítmicos y crecimientos relativos.

- **Métodos paramétricos**

Tiene como característica el supuesto de que los datos en cuestión se distribuyen de acuerdo con una curva de densidad de probabilidad normal. En la práctica la mayoría de los datos no siguen un comportamiento estrictamente normal, sino que son aproximados a la curva normal y por tanto los resultados que se obtiene al medir el riesgo son una aproximación. Bajo el supuesto de normalidad y media de rendimiento igual a cero, el modelo paramétrico determina el valor en riesgo de una posición de la siguiente manera:

$$VaR = F \times S \times \sigma \times \sqrt{t}$$

Donde:

F = factor que determina el nivel de confianza del cálculo. Para un nivel de confianza de 99%, $F=2.33$

S = monto total de la inversión o a la exposición total en riesgo

σ = desviación estándar de los rendimientos del activo

t = horizonte de tiempo es que se desea calcular el VaR.

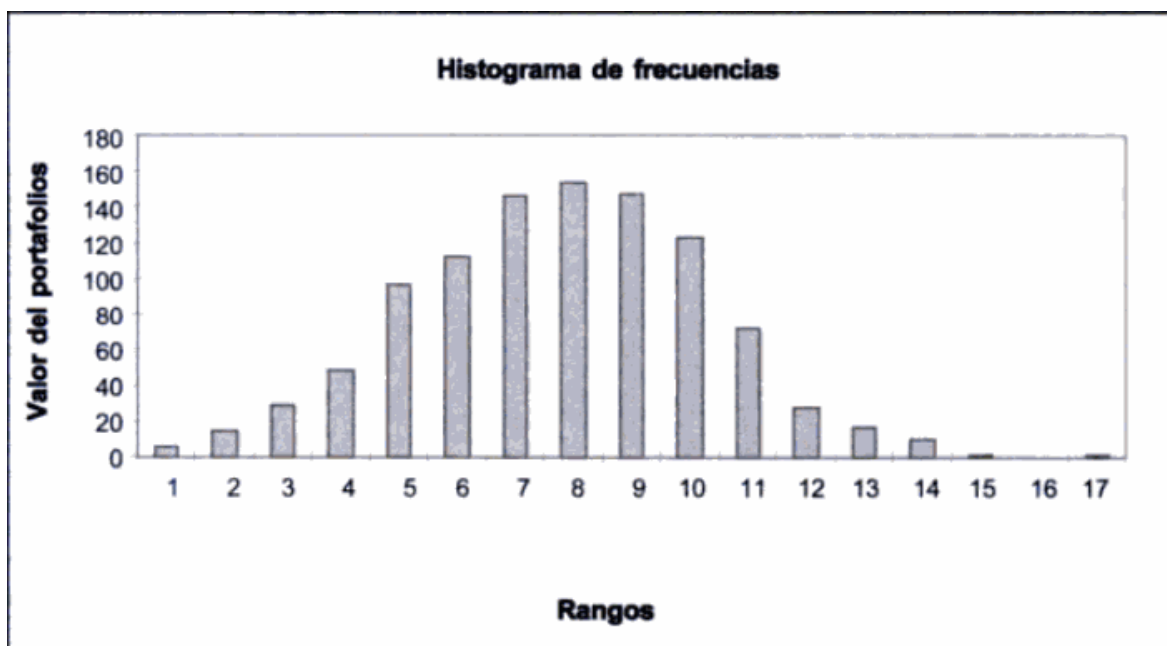
- ❖ **Método paramétrico denominado Simulación Montecarlo**

Consiste en la generación de números para calcular el valor de los escenarios generados con la base de datos obtenida previamente. Un nuevo número aleatorio sirve para generar un nuevo valor con igual probabilidad de ocurrencia que los demás y determinar la pérdida o ganancia en el mismo. Este proceso se repite un gran número de veces (10,000 escenarios) y los resultados se ordenan de tal forma que pueda determinarse un nivel de confianza específico⁵⁰.

Si se hacen 1,000 escenarios y se grafica el histograma de frecuencias, se obtiene una curva de distribución muy cercana a la normal como se muestra a continuación en la figura N° 18. El valor en riesgo simplemente se obtiene calculando el primer percentil del histograma de frecuencia (considerando un nivel de confianza de 99%).

⁵⁰ Alfonso de Lara Haro. Medición y Control de Riesgos Financieros. Limusa Noriega Editores. México - 2008.

FIGURA N°18 HISTOGRAMA DE FRECUENCIAS



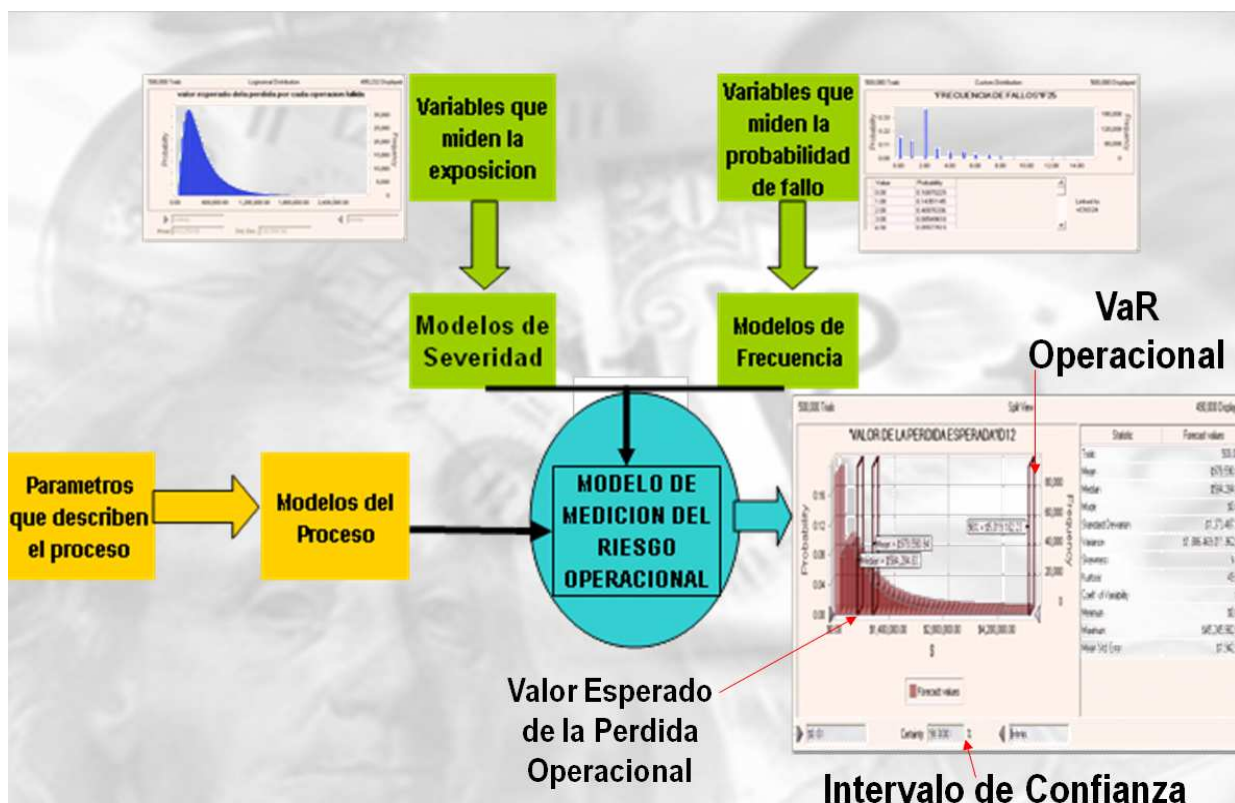
Fuente: Alfonso de Lara Haro. Medición y Control de Riesgos Financieros.

Elaboración: La autora

Basándose en observaciones históricas se modela la distribución de las pérdidas que han tenido la institución por riesgo operacional esta debe ajustarse la curva de distribución de probabilidades más adecuada al valor de las pérdidas históricas. (Distribución Normal, Exponencial, Gamma. Empírica, Lognormal, Weibull, Beta).

A partir de la construcción de un modelo que representa el proceso administrativo, se identifican en el los pasos en los cuales pueden ocurrir fallos; la probabilidad de ocurrencia de tales fallos se incorporan al modelo variables aleatorias independientes; el valor de la pérdida esperada por la ocurrencia de errores en la gestión está afectado por el valor de la operación en curso; el valor de la operación en curso se incorpora como variable continua.

FIGURA N°19 MODELO DE RIESGO OPERACIONAL



Fuente: Camilo Romero. Riesgo Operacional: El reto contemporáneo de la banca internacional.

Elaboración: La autora

- **Determinación de las Funciones de Probabilidad**

La ausencia de información es un fenómeno recurrente en la valoración del riesgo operacional, para proveer una solución inicial al problema a la espera de recolectar la información en la medida en la cual el proceso de implantación de la generación de datos avance se puede aplicar el proceso de autovaloración, esto mediante las preguntas a expertos es posible lograr la asignación de una función de distribución; para ello puede hacerse uso del Método Delphi⁵¹ a

⁵¹ Es una metodología de investigación multidisciplinar para la realización de pronósticos y predicciones. Su objetivo es la consecución de un consenso basado en la discusión entre expertos. Es un proceso repetitivo.

través del cual la opinión de los expertos converge a la caracterización de la variable.

Este Método se desarrolla por etapas:

- ✓ En la primera los expertos expresan su opinión y de esta información se produce las estadísticas que resumen la opinión del grupo.
- ✓ En la segunda etapa, conocidos los resultados de la primera, los expertos retroalimentan y producen un nuevo concepto.
- ✓ El proceso se repite eliminando opiniones extremas hasta arribar a un consenso que puede estar representado por una función de distribución triangular, o por una distribución uniforme.

La aplicación de las pruebas de bondad de ajuste⁵² permite tener una idea de la mejor distribución que describe el fenómeno, cuando se cuenta con datos.

El proceso se puede complementar con la observación de la gráfica de la función de distribución acumulada y los datos observados, adicionalmente comparar los parámetros estadísticos de la muestra con los de la distribución contribuyen a la formación de un concepto adecuado respecto a la distribución que mejor se ajusta. Para el caso de esta investigación la distribución que mejor se ajusto fue la lognormal.

- ✓ Distribución lognormal: una distribución de probabilidad de cualquier variable aleatoria con su logaritmo normalmente distribuido (la base de una función logarítmica no es importante, ya que $\log_a X$ está distribuida normalmente si y sólo si $\log_b X$ está distribuida normalmente). Si X es una

Su funcionamiento se basa en la elaboración de un cuestionario que ha de ser contestado por los expertos. Una vez recibida la información, se vuelve a realizar otro cuestionario basado en el anterior para ser contestado de nuevo.

⁵² Mide el grado de ajuste que existe entre la distribución obtenida a partir de la muestra y la distribución teórica que se supone debe seguir esa muestra.

variable aleatoria con una distribución normal, entonces $\exp(X)$ tiene una distribución lognormal.

Una distribución puede ser modelada como log-normal si puede ser considerada como un producto multiplicativo de muchos pequeños factores independientes. En riesgo operacional existen muchos eventos independientes.

La distribución lognormal tiende a la función densidad de probabilidad $f(x; \mu, \sigma) = \frac{1}{x\sigma\sqrt{2\pi}} e^{-(\ln x - \mu)^2 / 2\sigma^2}$ para $x > 0$, donde μ y σ son la media y la desviación estándar del logaritmo de variable. El valor esperado es $E(X) = e^{\mu + \sigma^2/2}$ y la varianza es $\text{var}(X) = (e^{\sigma^2} - 1)e^{2\mu + \sigma^2}$.

Si $X \sim N(\mu, \sigma^2)$ es una distribución normal, entonces $\exp(X) \sim \text{Log} - N(\mu, \sigma^2)$.

Si $X_m \sim \text{Log} - N(\mu, \sigma_m^2), m = \overline{1 \dots n}$ son variables independientes lognormalmente distribuidas con el mismo parámetro μ y permitiendo que varíe σ , y $Y = \prod_{m=1}^n X_m$, entonces Y es una variable distribuida lognormalmente como: $Y \sim \text{Log} - N(\mu, \sum_m \sigma_m^2)$.

Medición de la Frecuencia

La frecuencia en riesgo operacional se refiere a la periodicidad en que se presente determinado fallo operacional. Las funciones de distribución más aplicadas a estos fenómenos son: Binomial, Poisson, Binomial Negativa y Hipergeométrica.

4.4.3 Metodologías de Medición de Riesgo Operativo Según Basilea

Debido a que los métodos de medición avanzada implican la obtención de información acumulada de años anteriores, es difícil establecer un solo modelo que prediga exactamente el requerimiento de capital que debe mantener un Institución Financiera para cubrir sus pérdidas operativas. Sin embargo, los modelos más acertados son aquellos que incluyen simulaciones de las pérdidas esperadas e inesperadas por medio de

curvas de distribución, considerando dos factores fundamentales: la magnitud o cantidad de las pérdidas (severidad) y el número de veces que ocurren los eventos de riesgo en un período determinado (frecuencia).

A continuación se presenta un modelo de simulación de pérdidas esperadas por Riesgo Operativo que servirá de insumo en el cálculo de requerimientos de capital para las Instituciones Privadas del Sistema Financiero Ecuatoriano. El objetivo de desarrollar un modelo de predicción de pérdidas operativas es observar la metodología que va a presentarse a continuación, para implementar esta herramienta una vez que las entidades del Sistema Financiero cuenten con la información necesaria⁵³ que permita hacer aplicable y consistente el modelo.

Con esto y con lo indicado en párrafos anteriores se ha seguido el siguiente procedimiento:

4.4.3.1 Proceso

- **Paso 1 - Base de datos**

La base de datos es la “piedra fundamental” en la construcción o desarrollo de cualquier modelo de cuantificación. En forma particular, una base de datos poblada de pérdidas operacionales históricas será el input fundamental del modelo de cuantificación de riesgo operacional y permitirá el traspaso de un enfoque cualitativo a un enfoque integral (cualitativo-cuantitativo).

Las entidades deben desarrollar sus bases de datos a partir de un proceso homogéneo de recolección de pérdidas y de asignación de éstas en función de las distintas áreas de negocios y a los diferentes tipos de riesgos; no sólo con el fin de registrar las pérdidas, sino también para entender sus causas.

Poseer la base de datos de pérdidas es uno de los desafíos más relevantes a los cuales se enfrentan las entidades financieras.

- **Paso 2 - Frecuencia de eventos**

⁵³ La creación e implementación de una Base de Datos que recoja los eventos de Riesgo Operacional de las empresas, permitirá que en el futuro se cuente con una herramienta que funcione como insumo principal para el desarrollo de modelos de medición avanzada.

Con la finalidad de modelar la frecuencia de eventos con un horizonte determinado, se utiliza una distribución de conteo que explicita la probabilidad de ocurrencia de una determinada cantidad de eventos para dicho horizonte a partir de la población expuesta, es decir, de las pérdidas registradas por la entidad.

Usualmente, la distribución seleccionada es la distribución de Poisson, dadas sus características que permiten establecer de forma apropiada el número de eventos a partir de la media de la frecuencia de eventos observada en el pasado.

- **Paso 3 - Intensidad de eventos**

Una vez estimada la distribución de frecuencias se debe proceder a estimar la distribución del monto de pérdida (o intensidad) de los eventos. En virtud de eso es necesario estudiar la base de pérdidas operacionales para “ajustar” la distribución paramétrica que mejor se adecue a los datos observados de montos de pérdidas.

En la práctica es usual que se utilicen distribuciones como Lognormal, Pareto y distribuciones de “cola larga”, a efectos de no subestimar ésta por falta de información, dado que en los procesos de cuantificación de riesgo operacional debe prestarse especial atención a la estimación de la “cola” derecha de la distribución de intensidad, ya que allí se encuentran las pérdidas menos frecuentes pero las de mayor impacto para los resultados de la entidad.

- **Paso 4 – Simulación de MonteCarlo**

Por último, con la finalidad de generar la distribución de pérdidas se puede utilizar el método de simulación de MonteCarlo, una técnica que consiste en repetir el siguiente proceso:

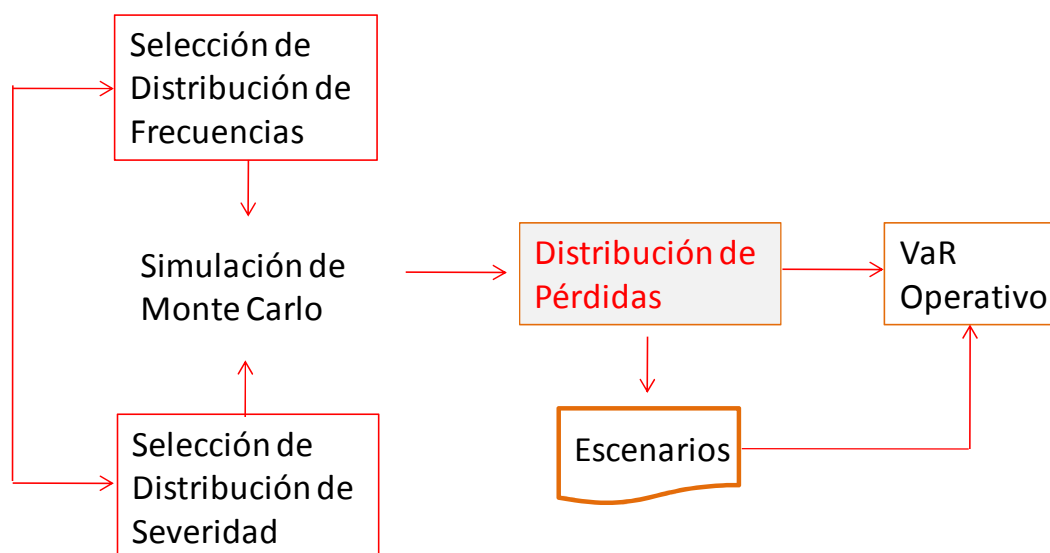
Simular la cantidad de eventos de pérdidas operacionales para el horizonte de tiempo determinado, para cada uno de estos eventos de pérdida se procede a simular el monto de pérdida asociado, luego; la pérdida total para el horizonte de tiempo es la suma de los montos de pérdida de cada uno de los eventos que se simularon en el punto anterior.

De esta manera, el proceso estima la distribución de pérdidas utilizando un número suficiente de escenarios hipotéticos, generados aleatoriamente a partir de las estimaciones de las distribuciones de intensidad y frecuencia.

Cada una de estas repeticiones o escenarios hipotéticos es decir, simulaciones representa las pérdidas operacionales para el período fijado como horizonte de tiempo. La cantidad de repeticiones o iteraciones debe ser elevada a fin de lograr estabilidad en los resultados de las simulaciones y lograr construir la distribución de pérdidas operacionales.

La distribución de pérdidas agregadas puede ser construida a través de la convolución⁵⁴ de las diferentes distribuciones de pérdidas de cada agrupación (correspondientes a cada línea de negocio, tipo de riesgo o a una combinación de ambas).

Bajo el supuesto de correlación perfecta entre las pérdidas de cada agrupación, el requerimiento de capital total para la entidad puede ser determinado a través de la suma del VaR, obtenido de las distribuciones de pérdidas de cada agrupación realizada. El flujograma del proceso es el siguiente:



⁵⁴ Una convolución es un operador matemático que transforma dos funciones f y g en una tercera función que en cierto sentido representa la magnitud en la que se superponen f y una versión trasladada e invertida de g . Una convolución es un tipo. En teoría de la probabilidad, la distribución de probabilidad de la suma de dos variables aleatorias independientes es la convolución de cada una de sus distribuciones de probabilidad.

4.4.3.1.1 Modelo Montecarlo

A continuación y para la institución objeto de la investigación se describe el procedimiento realizado de la simulación para la obtención de los datos.

Inicialmente se recolecto una base de datos observando en la entidad financiera las pérdidas históricas que ha tenido la misma, se clasificaron los riesgos incurridos, dada su naturaleza en catastróficos y no catastróficos

- ✓ Los Eventos Catastróficos son los que por definición, el impacto monetario es sumamente fuerte, pero su probabilidad de ocurrencia sumamente bajo, por ejemplo un desastre natural o el colapso de los servidores del Banco. Eventos muy poco probables pero de alto impacto.
- ✓ Los Eventos No Catastróficos son los que usualmente se observan en el día a día bancario. Son riesgos de menor cuantía pero con frecuencia y probabilidad de ocurrencia mayor que los catastróficos, un descriptivo de los eventos se encuentra en el anexo 2.

Se agrupa los riesgos de acuerdo al segmento y subsegmento de impacto de la perdida, para mejor gestión y control dentro de la institución.

Para determinar la frecuencia, se toma la banda de un año y se contabilizan el número de DIAS en los que ocurre uno o más eventos en este lapso de tiempo, así, si un evento ocurrió un día en el año, su frecuencia será de 1.

Un Comité Experto determina la frecuencia esperada de los eventos catastróficos, ya que no se tienen registros de ocurrencia. Se prioriza el sentido conservador de medir el riesgo

La probabilidad de ocurrencia del evento, viene dada por la división de los días que ocurre el evento en el año entre los días del año. Así

por ejemplo, la probabilidad del evento anterior que ocurrió una vez en el año, será de $1/365 = 0.00274$

Para aquellos riesgos que no se tenga registro de ocurrencia, el Comité experto determinara la probable ocurrencia en el tiempo, así un evento "catastrófico" puede ocurrir una vez cada diez años, por tanto su frecuencia es 0.1 en un año (1/10 años) y su probabilidad es $1/3650$ (1/3650 días)

El porcentaje de Mitigación viene dado por un estudio que se hace por tipo de riesgo, y las acciones concretas que se toman al respecto de cada riesgo, se determina que tanto del riesgo se cubriría con las acciones que se está tomando, mediante una estimación histórica donde aplique o comité experto si es necesario. Ejemplo: si uno de los eventos es robo de clave de uso de banca electrónica, y con un programa de mitigación (entrega de tarjeta de coordenadas de claves a los clientes) se logró mitigar las pérdidas históricas en un 60% a las registradas antes del plan de mitigación. Este sería entonces el porcentaje de mitigación a usar en el modelo.

El Riesgo Residual, viene dado por la diferencia entre el riesgo inherente y el riesgo que se pudo mitigar, es decir el porcentaje del riesgo inherente que no está mitigado.

Se parte de un supuesto, que las pérdidas seguirán una distribución normal. Por tanto, el Default o pérdida total, es la porción de la curva que resta desde la probabilidad de ocurrencia viene dada por $= \text{DISTR.NORM.ESTAND.INV} (1-\text{probabilidad de ocurrencia})$

Dado que en riesgo Operativo, no se tiene un record constante de pérdidas, o dicho de otra manera, puede ocurrir cualquier evento, por cualquier cuantía en cualquier momento en el tiempo, el modelo establece que se genere un aleatorio que caerá dentro de la curva normal de la cual se parte como supuesto.

Se realiza una simulación Montecarlo con 10.000 escenarios en donde, cada vez que un aleatorio genere una distancia al default

mayor al default proveniente de la probabilidad de ocurrencia, registrará como pérdida el valor del riesgo residual del evento.

Los riesgos deben agruparse por tipo y segmento. Sobre estos riesgos agrupados se ajustó curvas de probabilidad usando Crystal Ball para que los aleatorios que se generen en la Simulación Montecarlo estén dentro de éstas, ya que con este programa se puede asignar una función que sea a la medida de los datos recolectados mediante la introducción de la información del histograma de frecuencia construido con los datos observados.

Las medidas de riesgo que se buscan son la Media (Pérdida Esperada⁵⁵) y el percentil 99 (VaR⁵⁶)

Se realizaron 3 simulaciones para dar sostenibilidad al modelo y los datos que se presentan son el promedio de las 3.

4.4.3.1.2 Resultados del Modelo

Para realizar la simulación se utilizó el programa Crystall Ball, el cual con los parámetros antes mencionados, a un nivel de confianza del 99%, y después de haber probado y utilizado varias distribuciones⁵⁷; la que mejor se adapta al supuesto para el resultado es la Lognormal. A continuación se muestra los datos obtenidos de las 3 simulaciones realizadas, los cuales se los puede observar en el Anexo 7.

⁵⁵ Las pérdidas esperadas deben ser cubiertas con provisiones.

⁵⁶ Valor en Riesgo debe ser soportado por el capital de la entidad.

⁵⁷ Distribución Normal, Lognormal, Exponencial, Beta, Gamma, Logistic y T de Student.

FIG. 20 RESULTADOS DEL MODELO MONTECARLO

INSTITUCION	Institución	Eventos Catastróficos	Eventos No Catastróficos	Subsegmento Corporativo	Subsegmento Empresarial	Subsegmento IFIS	Subsegmento Sector Público	Subsegmento Sector Público	Subsegmento Pequeñas Emp.	Subsegmento Microempresa	Subsegmento Jurídico	Subsegmento Manejo de Liq.	Subsegmento Mesa de Diner	Subsegmento Banca Privada	Subsegmento Institucional
	Período 1	4,156,804	517,371	3,639,433	13,422	3,982	596	1,547	3,517,073	11,377	1,263	400	45	4,362	288
VaR 99%	7,763,794	0	6,431,946	177,832	24,290	0	913	5,208,593	47,455	11,263	0	0	4,000	3,843	2,386,895
Período 2	4,146,959	499,488	3,647,470	15,275	3,502	445	1,752	3,524,278	10,661	1,418	337	54	4,169	244	85,335
VaR 99%	8,488,124	0	6,528,740	351,675	23,893	3,075	913	5,526,895	51,364	11,263	0	0	1,500	1,750	2,237,196
Período 3	4,113,364	471,481	3,641,883	13,332	4,915	442	1,545	3,523,119	11,497	1,113	467	41	3,425	348	81,639
VaR 99%	8,577,813	0	6,494,315	177,832	23,893	0	913	5,439,171	51,364	11,263	0	0	4,000	3,843	1,969,220
Promedio	4,139,042	496,113	3,642,929	14,010	4,133	494	1,615	3,521,490	11,178	1,265	401	47	3,985	293	84,018
VaR 99%	8,276,577	0	6,485,000	235,780	24,025	1,025	913	5,391,553	50,061	11,263	0	0	3,167	3,145	2,197,771

Como se mencionó anteriormente los resultados obtenidos para la institución financiera objeto de la presente investigación son de la realización del promedio de las tres simulaciones Montecarlo, de las mismas se sacó un promedio y se registró un valor de pérdida esperada de US\$4.139M, dicho valor correspondería al provisionado por la entidad. Y el 99% de probabilidad de tener pérdidas sería de hasta US\$8.276M. De tal manera que la diferencia entre la pérdida esperada promedio que la institución y el VaR (99%) la entidad debería ser solventando con el patrimonio de la misma, esto según Basilea; por lo que con esto también se estaría probando la capacidad financiera de la institución para enfrentar los posibles eventos operacionales. Cabe señalar que en los casos donde el resultado del VaR es 0 es porque se ha tomado en cuenta el concepto de percentil: *El Percentil 0 es el menor valor de la muestra y el Percentil 100 el mayor valor, técnicamente es el percentil i -ésimo, donde la i toma valores del 1 al 100. **El i % de la muestra son valores menores que él y el $100-i$ % restante son mayores.*** Debido a que esta es una medida de posición no central nos muestra donde están acumulados (por debajo) los datos desde el porcentaje en el que queremos referirnos. En el caso de esta muestra, como en el de otras variables del modelo, la gran mayoría de los datos se encuentran concentrados en el valor de 0 (Ver Anexo 7). Esta altísima concentración se debe a que la probabilidad de ocurrencia de los eventos en los sectores registrados con este resultado especial es sumamente baja, y dada la construcción del modelo, solo se registrará una pérdida cuando el aleatorio cumpla con las características que haga que la probabilidad se cumpla y por tanto se registre una pérdida. Como esto ocurre muy pocas veces, se ha aplicado el concepto antes mencionado; si queremos el percentil al 99% (VaR:99%), encontramos que el valor donde se ubican el 99% de los datos, es 0. No se relaciona con el valor de la media, ya que esta es una medida de tendencia central. Lo que si podemos acotar es que la media no nos dice mucho en este caso ya que la simulación claramente se sesga a 0 por la gran cantidad de datos en este valor, no obstante es lo correcto por la probabilidad de ocurrencia tan baja.

Es así que:

- ✓ Si las pérdidas ocasionadas por un determinado tipo de evento de Riesgo Operacional tienen una severidad elevada, el parámetro de la distribución también será alto, lo cual implica que las pérdidas operativas máximas que experimentará la Institución Financiera por ese tipo de Riesgo de Operación serán mayores y por tanto requerirán de un monto mayor de capital para ser cubiertas.
- ✓ En el caso de frecuencia, si la distribución para un determinado tipo de evento de Riesgo Operacional tiene un parámetro alto, significa que este tipo de eventos ocurren con una frecuencia mayor. Por tanto, el número de pérdidas será más alto, lo que hará que el requerimiento de capital aumente para cubrir las mismas.
- ✓ Existen eventos de Riesgo Operacional que presentan una gran severidad y poca frecuencia, generalmente estas características se ajustan a los fraudes internos y externos, ya que este tipo de eventos generalmente son ocasionales, sin embargo, cuando suceden, la magnitud de la pérdida es muy alta para una Institución. Al contrario, existen eventos de riesgo que ocurren frecuentemente, sin embargo, su severidad es poco significativa, éste es el caso de fallas en los sistemas de operaciones, fallas en tecnología, etc.

Se debe tomar en cuenta que cada institución debe contar con sus propias distribuciones de pérdida según los valores experimentados a través del tiempo y la gestión que efectúa sobre sus riesgos operativos, por lo que se esperaría que la adopción de fórmulas y distribuciones genéricas sobreestime o minimice las pérdidas operativas reales. Lo más acertado sería escoger la curva que se adapte a la distribución de las pérdidas que la Institución Financiera haya experimentado en años anteriores, de acuerdo al tipo de Riesgo de Operación.

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

- El análisis de los acuerdos de Basilea I y II han permitido marcar parámetros bajo los cuales las instituciones financieras privadas del sistema financiero puedan tener una aplicación adecuada del riesgo de operación.
- El Gobierno Corporativo en una institución es fundamental ya que es el que regula principios, normas, diseño, integración y funcionamiento de las áreas de la entidad siendo el principal responsable de definir a tiempo todos los asuntos relevantes tanto financieros, de desempeño y administrativos de la institución.
- Las instituciones financieras deben tener claros los procesos con los que cuenta para el giro del negocio, así como también debe definir cada área de la entidad para que de alguna manera se facilite el levantamiento de los eventos de riesgo.
- La introducción del Riesgo Operacional dentro del Sistema Financiero Nacional permitió crear una cultura de riesgo dentro de las instituciones que lo conforman, con el fin de lograr un trabajo más ordenado y controlar la ejecución de procesos y políticas. También adoptaron métodos y técnicas que permitan administrar y controlar las pérdidas provenientes del mismo, esto a su vez ayudan a proveer seguridad a las instituciones financieras en el manejo del tema.
- El Proceso de Medición (Probabilidad – Severidad) es importante para la institución financiera y se refiere a la medición objetiva de las probabilidades y la severidad de falla con el fin de predecir las pérdidas potenciales. Para esto es fundamental recopilar Información de riesgos, definir los Factores de Evaluación de las Categorías de Riesgos, definir relaciones e interdependencias entre riesgos.
- El utilizar herramientas y metodologías para el cálculo de las pérdidas operativas de una institución financiera privada no significa contar con un gasto

adicional, al contrario, esto permite retribuir la inversión realizada en controles, ya que se contará con el capital necesario que cubra estas pérdidas y al mismo tiempo se logrará reducir el Riesgo Operacional.

- La medición cuantitativa del Riesgo Operativo se basa en el concepto de VaR (Value at Risk), aplicado en el sector financiero, esto se obtiene mediante observaciones históricas donde se modela la distribución de las pérdidas que ha tenido la organización por riesgo operacional, debiendo ajustarse la curva de distribución de probabilidades más adecuada al valor de las pérdidas históricas, que para la presente investigación la más adecuada es una Lognormal.
- Los resultados del modelo indican cual va a ser la pérdida máxima que podría enfrentar una Institución Financiera, en base a las pérdidas que ha venido experimentando a través del tiempo y con ello se podrá establecer el capital necesario para poder cubrir la misma.
- Si bien los modelos no predicen con exactitud las posibles pérdidas operacionales en las que puede incurrir una Institución Financiera, esta es la forma más acertada de aproximar las mismas, lo que permite contar con un capital estimado que podría cubrirlas en el futuro.

RECOMENDACIONES

- Se recomienda a la administración de las instituciones financieras que para identificar los eventos de riesgo, las posibles fallas o insuficiencias en las actividades y realizar una estimación de su impacto y frecuencia, se debería organizar talleres en los que participen los diferentes actores y usuarios de los procesos, con la finalidad de tener estimativos de la realidad.
- Las instituciones deben tener muy claro las metodologías que van aplicar y tomar conciencia técnica de los métodos planteados, si bien es cierto es difícil cuantificar un riesgo operacional extremo, se puede provisionar de alguna manera un evento y tener una alerta continua en la organización para que todos sus procesos sean adecuados y se produzcan las mínimas fallas.

- Se recomienda la creación de mapas o matrices para clasificar y categorizar los riesgos de acuerdo a su importancia, por magnitud y frecuencia, de tal forma que se pueda identificar procesos y áreas con debilidades, las cuales requerirían de mayor atención.
- Una eficiente gestión del Riesgo Operacional exige una colaboración permanente del Gobierno Corporativo de la institución para la revisión y aprobación de las políticas, procesos y controles; además el área encargada del cumplimiento del riesgo operativo en cada institución será la encargada del control y revisión del cumplimiento en la administración del riesgo de operación y de toda la organización en general, con el fin de contar con una cultura a nivel organizacional, que facilite la administración y el monitoreo del riesgo operativo.
- Es fundamental que las instituciones financieras cuenten con programas de medición que faciliten las estimaciones y ofrezcan herramientas complementarias para el análisis, para el desarrollo de la presente investigación se utilizó el programa Crystall Ball, el cual cumple con lo antes mencionado.

BIBLIOGRAFIA

- Navarrete Enrique, “Requerimientos de Capital y Ponderaciones de Riesgo para carteras de Microfinanzas”, México 2006.
- Banco de Pagos Internacionales, Prácticas sanas para la Administración y supervisión del Riesgo Operativo, 2003
- Vizuite Moraima, Administración del Riesgo Operativo y de Mercado en Ecuador frente a otras experiencias internacionales, Tesis-Quito, 2006.
- Romero Carla, Impacto del Riesgo Operativo dentro del Contexto del nuevo acuerdo de Capital, Tesis-Quito, 2005.
- Price Waterhouse Coopers, “Seminario-Taller Gestión de Riesgo Operativo”, Ecuador 2006.
- Soler José; Stakung Kim; Ayuso Alfonso; Botin Emilio; Escrig Miguel y Falero Bernardo, Gestión Riesgos Financieros, Banco Interamericano de Desarrollo. Grupo Santander, 1999.
- Gujarati Damodar, Enometría, McGraw-Hill, tercera edición. Colombia, 2002.
- Moreno Alvarez Ismael, Gestión del Riesgo Operacional en Entidades Financieras, 2005.
- ASBA, “Nuevo Acuerdo de Capital de Basilea”, 2001.
- Superintendencia de Entidades Financieras y Cambiarias, Basilea II: Hacia un nuevo esquema de medición de Riesgos. España, 2003.
- Losano José María, “Nuevos Desarrollos en Basilea II: Riesgo Operativo”. México 2003.
- BBVA, Basilea II: Impacto en las entidades financieras. España 2000.
- Guijarro Maria de Lourdes y Battaini Victor, “Un nuevo reto para la Banca
- Ecuatoriana: Basilea II, Revista EKOS N° 118, febrero 2004

- Velasteguí, Iván, documentos de propiedad del profesor de riesgo operativo en la maestría de finanzas y gestión de riesgos, Universidad Andina Simón Bolívar, Quito, 2008
- Llerena Endara, Valeria, Introducción del Riesgo Operacional dentro del Sistema Financiero Ecuatoriano, Quito, 2006
- Boletín Económico-AIFE-Asociación de Instituciones Financieras del Ecuador, Estado de la gestión del riesgo operativo, No.10, Junio 2006.
- Lozano José. Nuevos desarrollos en Basilea II: Riesgo Operativo. KPMG – México, 2004
- Evaristo Díz Cruz. Teoría de Riesgo: Riesgo Actuarial, Riesgo Financiero. Global ediciones, 2008.
- Alfonso de Lara Haro. Medición y Control de Riesgos Financieros. Limusa Noriega Editores. México-2008
- Páginas Web

www.superban.gov.ec/pages/c_bancos_boletines.htm

www.superban.gov.ec/pages/resoluciones_ib.htm

www.monografías.com/trabajos12/coso

www.riesgooperativo.blogspot.com

www.latinriskonline.com

ANEXOS