UNIVERSIDAD POLITECNICA SALESIANA

SEDE QUITO

CARRERA: ADMINISTRACIÓN DE EMPRESAS

Tesis previa a la obtención del Título de: INGENIERO COMERCIAL

TEMA:

ANÁLISIS DE LA ADMINISTRACIÓN DE RIESGO OPERATIVO EN LA BANCA PRIVADA EN EL PERÍODO 2005-2009.

AUTOR

SANTIAGO ADOLFO SÁNCHEZ AVILES

DIRECTOR

ING. PEGRO HUMBERTO MONTERO TAMAYO

Quito, Febrero del 2012

Declaración de responsabilidad

Los conceptos desarrollados, análisis realizados y las conclusiones del presente trabajo son de exclusiva responsabilidad del autor.

Quito, Febrero del 2012

(f) _____

Santiago Sánchez A.

CI. 1717138000

DEDICATORIA

A mis padres quienes han hecho de mí un hombre de bien, qué mediante su sabiduría y concejos me han sabido transmitir valores como: responsabilidad, disciplina, respeto, perseverancia y dedicación, de tal manera, cada palabra, cada concejo han sido imprescindibles para poder estar preparado para enfrentar cualquier adversidad que se pudiere acontecer tanto en mi vida personal como profesional.

Por consiguiente, es para mí muy grato dedicar este logro a quienes han sido mi motor y pilares fundamentales en todos estos años de carrera profesional y han estado ahí cuando más lo he necesitado.

Pienso que cualquier meta u objetivo que nos tracemos en la vida se consigue con: esfuerzo, constancia, dedicación y sacrificio, no obstante debemos tener una inspiración la cual nos motive e incentive a seguir adelante y nunca a darnos por vencidos, es por ello que, mi inspiración fueron mis padres de quienes me siento muy orgulloso y sin ellos no hubiese sido posible conseguir este reconocimiento académico muy importante en mi vida del cual me llevo gratos recuerdos y me llena de total satisfacción a nivel profesional y como persona por todas las vivencias y conocimientos que aprendidos a lo largo de mi carrera.

AGRADECIMIENTOS

Indudablemente quisiera primero dar gracias a Dios quien me dio la: salud, sabiduría, apoyo incondicional, y me guio durante todos estos años de formación profesional.

A mis mentores en las diferentes asignaturas quienes me brindaron sus sabios conocimientos y estuvieron conmigo a lo largo de mi carrera.

A la Universidad Politécnica Salesiana que me formo con valores y principios cristianos, y siempre me brindo su respaldo.

Finalmente a mi Director de carrera quien está al pendiente por los intereses de los estudiantes y esta salvaguardando nuestro bienestar.

INDICE GENERAL

ÍNDICE DE CONTENIDO

ÍNDICE DE GRÁFICOS

ÍNDICE DE CUADROS

ÍNDICE DE ANEXOS

RESUMEN EJECUTIVO

En los últimos años las entidades han venido trabajando en incluir al Riesgo Operativo en los procedimientos y políticas internas, pero cabe señalar que el principal inconveniente que tuvieron las entidades en considerar al RO. como un riesgo imprescindible en sus procesos fue el desconocimiento del tema, es decir que, este factor de riesgo ha sido generarador de grandes pérdidas cuantitativas.

El Riesgo operativo es uno de los riesgos más relevantes que una entidad financiera, el cual se deberá tomar en cuenta en todos los procesos organizacionales de la misma.

En este trabajo de tesis se proporcionará a una entidad financiera las pautas necesarias de una correcta administración y gestión del Riesgo Operativo (RO).

Se detallará los requisitos cualitativos como cuantitativos que una entidad debe contar para implementar el RO.

Adicionalmente se analizará todos los componentes esenciales que conforman el Riesgo Operativo (Personas, Procesos Internos, Tecnología de Información, Eventos Externos), además de cada una de las etapas que lo conforman (Identificación, medición control).

Se realizara el análisis de la normatividad de Basilea II respecto a los requerimientos que una entidad financiera debe cumplir para la implementación del Riesgo Operativo .

Se realizara una matriz de riesgo la misma que es una herramienta indispensable para verificar y evaluar la eficiencia y calidad de los procesos de una entidad.

Durante el periodo 2005-2009 se analizará el cuestionario emitido por la SBS(Superintendencia de Bancos y Seguros) siendo este el organismo regulador de la implementación de RO en el Ecuador.

Mediante este análisis se verificará el porcentaje de implementación y ejecución que cuenta las entidades financieras y se tendrá un criterio claro de la evolución del RO. en el periodo sujeto a la investigación.

Se diseñará un manual de Riesgo Operativo (RO) con todos los requisitos que debe contener y la manera de ejecución lo cual proporcionara las directrices que debe contar este manual y las entidades podrán basarse para acoplarlas a su propio perfil de riesgo.

Se evaluará experiencias internacionales y se comparará con nuestro país, y finalmente se abordará la realidad nacional de los fraudes y riesgos operativos que se dan en el país y se dará las pautas necesarias de como mitigarlos.

CAPITULO I

1.1 Antecedentes del Riesgo Operativo

Iniciaría remontándome a la fecha de Octubre del año 2005, en donde la Superintendencia de Bancos del Ecuador emitió una resolución sobre gestión de riesgo operativo, aplicable a todas las instituciones financieras.

La resolución establece que antes de determinar cargos de capital por riesgo operativo, las instituciones financieras deberían desarrollar un ambiente apropiado de gestión de riesgo operativo.

Esto implica asegurar una gestión efectiva de los procesos institucionales, estos abarcan: recursos humanos y tecnología de la información, estableciendo y validando planes de contingencia y de continuidad de negocio. Una vez que estos aspectos cualitativos sean alcanzados, las instituciones tendrían la capacidad para moverse hacia requerimientos cuantitativos de capital, como establece el Nuevo Acuerdo de Capital.

Se requirió a las instituciones supervisadas presentar su evaluación y un plan para poner en práctica las nuevas provisiones de gestión de riesgo operativo a la Superintendencia de Bancos y Seguros, dentro de seis meses después de la fecha de emisión de la resolución. El plan de puesta en práctica, aprobado por la junta directiva de la institución, debería incluir una lista (un programa) detallada de actividades y una lista de la gente responsable de su ejecución.

La gestión del Riesgo Operativo basada en los planteamientos propuestos por el Comité de Supervisión Bancaria de Basilea y en sus diversas publicaciones, se ha convertido en un elemento importante con implicaciones significativas sobre las instituciones financieras (IFIS), como para el caso de la exigencia futura por parte de los órganos supervisores de modelos de identificación, medición, control y reporte del riesgo operativo por distintas vías.

El riesgo operativo relacionado con procesos, RR.HH., sistemas y eventos externos presenta una importancia significativa en las empresas, cualquiera sea su naturaleza (financiera o no financiera). Su incorporación mejora sustancialmente el enfoque de negocio corporativo y permite una mejora en el cumplimiento de los objetivos de negocio.

En estos últimos años, producto de situaciones no deseadas, se ha empezado a prestar mayor atención a este riesgo que se puede presentar por la complejidad y diversidad de actividades bancarias; los cambios tecnológicos y su uso; el comercio electrónico; las fusiones, escisiones y consolidaciones; el uso de colaterales y derivados y; el outsourcing (subcontratación externa) por citar algunos casos.

Dado que el trabajo de gestión de un negocio genera repercusiones en cifras e indicadores de las empresas y finalmente en su propia viabilidad, la observancia de aspectos relacionados con el tema engloban conceptos tales como la estrategia, el negocio, los procesos, las personas, los sistemas, el control, entre otros y en el entendido que se cumple con el objetivo de gestión corporativa del riesgo (GCR), como etapa final dentro de la estrategia institucional, donde destaca el riesgo operativo como aquel de mayor importancia entre los riesgos que enfrentan las IFIS(Instituciones Financieras).

Este contexto ha motivado a las empresas a seguir los lineamientos propuestos por BIS (Supervisión Bancaria de Basilea) o por las mejores prácticas en la gestión corporativa para que aquellas conformen un adecuado ambiente de gestión de riesgos para la administración de los mismos.

Las instituciones financieras deben poseer adecuados mecanismos de identificación, gestión y control para su desempeño eficiente y eficaz en el marco operacional.[1]

Procesos

Se debe tener claramente definidos los procesos en una organización de conformidad con la estrategia y políticas adoptadas por cada entidad agrupándoles de la siguiente manera:

Procesos Gobernantes.

Estos se encargan fundamentalmente de dar las directrices a los demás procesos para cumplir así los objetivos organizacionales previstos institucionalmente como son: la planificación estratégica, la estructura organizacional y la administración integral de riesgos.

Procesos productivos fundamentales u Operativos

Estos son vitales ya que permiten ejecutar efectivamente las políticas y estrategias relacionadas a la calidad de los productos o servicios en una entidad.

[1] PÉREZ, Marissela, y otros, *Riesgo Operacional,* 1era. Edición, Editorial McGraw-Hill, Ecuador, 2006

Mediante la grafica se puede visualizar los componentes esenciales del Riesgo Operativo

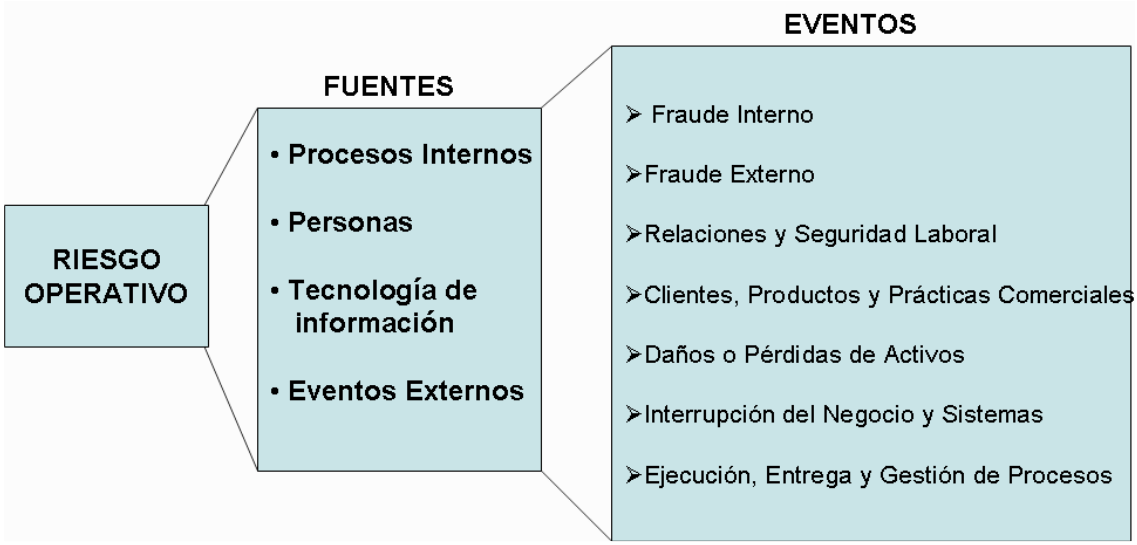


Grafico 1 Componentes del Riesgo Operativo

Fuente: MENDOZA, Álvaro y CASTILLO Mario, Riesgos Financieros, Julio 2005

1.2 Problemática de la investigación

Mediante el análisis se determinó que las entidades únicamente se enfocan en los dos primeros riesgos mas no en el operativo el cual es uno de los más relevantes e involucrara a toda la organización como se demuestra en la grafica.

Mediante la grafica se determinara los diferentes tipos de riesgos que existen en una entidad financiera:

Grafico 2 Diferentes tipos de Riesgo

Fuente: MENDOZA, Álvaro y CASTILLO Mario, Riesgos Financieros, Julio 2005

El criterio de la problemática es que el riesgo operacional ha sido el último de los riesgos objeto de tratamiento por el sector financiero, después de mercado y crédito, los mismos que han sido sujetos de análisis.

Las pérdidas operacionales pueden ser directas (quebranto financiero), indirectas (pérdida de reputación, clientela, etc.) y de coste de oportunidad (falta de capacidad para acometer negocios). Inicialmente estaban incluidas las indirectas y el coste de oportunidad, pero su grado de incertidumbre y la dificultad de estimación de tales pérdidas hicieron que se quitasen de la definición (coherente con la exclusión del reputacional / estratégico), entre los factores que dificultan el cálculo y asignación de riesgo operativo son las pérdidas sufridas en los últimos años y los eventos repetitivos de gran severidad.

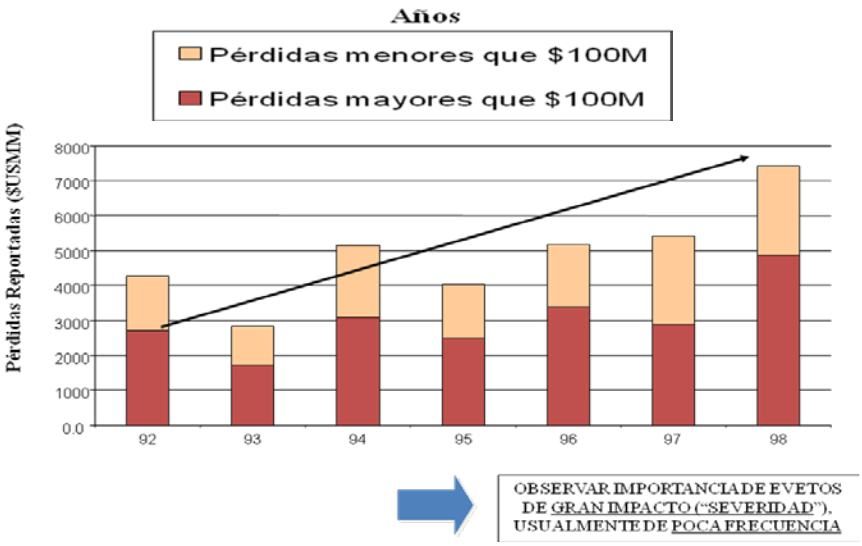


Grafico 3 Pérdidas reportadas por eventos de Incidencia

Fuente: ERNEST, Y, Perdidas por eventos de reincidencia, Septiembre, 2008

CONCEPTUALIZACIÓN DEL PROBLEMA

DESCRIPCIÓN	CAUSA	EFECTO
Por qué se da procesos inadecuados y repetitivos en una entidad financiera.	Falta de control en los procesos internos departamentales y no se ha delegado aun responsable de cada área.	Retraso en los objetivos organizacionales y perdidas cuantitativas
Por qué no se evalúa los procesos organizacionales y se generan perdidas inesperadas	Debido a la falta de revisión de cada procedimiento y manual operativo y la previsión de riesgos	Impacto financiero y errores inmersos en cada procedimiento
Por qué las entidades desconocen del riesgo operativo y dejan relegado este factor de riesgo	Falta de conocimiento partiendo de la alta gerencia	Se obtiene una inadecuada administración financiera que afecta a la rentabilidad de cada entidad

Cuadro 1 Conceptualización del problema

Fuente: el autor

Las renombradas pérdidas sufridas por fallas operacionales durante los últimos años en las Instituciones financieras han alarmado debido a grandes pérdidas, citaré algunos ejemplos:

El caso Barinas con pérdidas operativas cercanas a 850 millones de dólares el caso Daiwa Bank, con pérdidas operativas cercanas a 1000 millones de dólares, el caso Sumitomo Bank con pérdidas por riesgo operacional de 2.600 millones de dólares.

El caso de la caída del mayor banco de la República Dominicana (Baninter), que además de producir una crisis financiera también tuvo un fuerte impacto en la economía del país, es por ello que de esta problemática nace la necesidad de la investigación cuyo enfoque es el de analizar y concientizar de la responsabilidad de una correcta administración del riesgo operativo (RO).[2]

En Ecuador no se tiene reportes documentados ni evidencia de primera mano que corroboren perdidas de gran magnitud como consecuencia de Riesgo Operativo, sin embargo muchas entidades asumen que, el riesgo Operativo ha sido un riesgo generador de perdidas y en la actualidad las entidades están dándole la importancia del caso.

No obstante y pese a lo anterior, la toma de conciencia en el sector financiero esclusivamente la banca privada ha reconocido la importancia que amerita el riesgo operativo en una entidad las mismas que actualmente se encuentran en proceso de implementación y su status actual esta dado en:

[2] ERNEST, YOUNG, *Gestión del Riesgo Operacional en Entidades Financieras,* Quito, 26 de Septiembre de 2008

- Conciencia creciente en la Alta Dirección

- Responsabilidad principal asignada a los responsables de áreas de negocio/productos (y no a una unidad especifica de RO). De hecho, sólo el 60% de estas entidades tenía un responsable para riesgo operacional para el conjunto del banco (La cifra no es representativa del sistema financiero en general).

- Cuando se realizó el proceso inicial sobre de la implementacion del RO.(Riesgo Operativo),Los bancos reconocieron estar en una fase inicial en la gestión del Riesgo Operacional, sin haber llegado a la fase de medición de este tipo de riesgo. Sin embargo, la mayoría controlaba indicadores de riego, analizaba la experiencia de pérdidas y las calificaciones de auditoría interna.

Uno de los puntos sobre los que ha habido problemas es la misma definición. La última versión provisional pone el acento en las causas últimas generadoras de RO:

Es el riesgo de incurrir en pérdidas como consecuencia de deficiencias o fallos de los:

- Procesos internos
- Recursos humanos o
- Sistemas, o bien derivado de
- Circunstancias externas

➢ Las entidades no están obligadas a enfocarse únicamente en esta definición de los fallos organizacionales exactamente. Lo importante es la detección de todos los posibles factores de riesgo en cada una de los procesos, productos y actividades de la entidad.

- Cabe reiterar que las perdidas operacionales más relevantes están dadas principalmente en:

- Pérdidas o quebrantos financieros en una entidad.

- Perdida reputacional que afecta la imagen institucional

1.3 Justificación

Algunos hechos explican el aumento de la importancia del RO:

- El aumento del e-commerce, que genera nuevos tipos de riesgo de tipo operacional (piratería informática, fiabilidad sistemas, seguridad transacciones)

- Grandes procesos de fusión en los últimos años, con lo que ello supone a nivel de integración de sistemas, RRHH, organización, etc

- El aumento en la utilización de técnicas de mitigación de riesgos puede llevar aparejado mayor RO (legal)

- Mayor uso del outsourcing: supone transferencia de cierto tipo de riesgos, pero supone una pérdida de control sobre ciertas actividades que implican a su vez aumento de RO

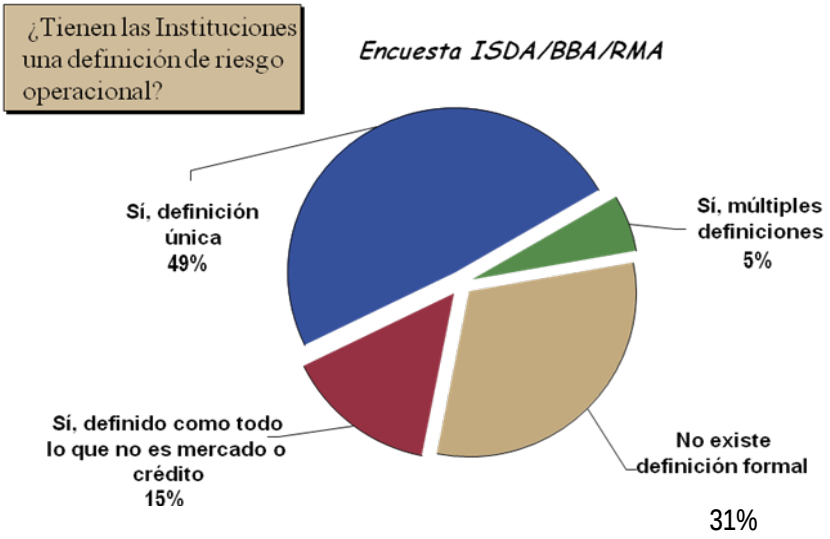


Grafico 4 Conocimiento de la Banca sobre Riesgo Operativo

Fuente: ISDA, Encuesta sobre conocimiento Riesgo Operativo

Mediante la investigación se busca reflejar la importancia y la relevancia que posee el riesgo operativo dentro de una entidad, centrándonos en la realidad nacional, la misma que refleja la falencia de la implementación del riesgo operativo, el mismo que abarca a toda la empresa no únicamente está dado en un departamento sino de manera global en toda la organización.

De esta manera el objetivo del análisis está canalizado a concientizar al sistema financiero sobre las pérdidas que este riesgo podría generar si no se tiene claro la importancia que este riesgo amerita dentro de una organización, además permitirá a cada entidad provisionarse su propio perfil de riesgo, obteniendo así aportar a la banca privada los lineamientos necesarios para una correcta administración del riesgo operativo, permitiendo así minimizar el impacto sobre el capital de cada institución financiera, exclusivamente me enfocaré al segmento de la banca privada ecuatoriana exclusivamente en los 24 bancos privados que la conforman. Sobre la implementación del riesgo operativo dentro de la organización, proporcionándoles directrices y

parámetros explícitos sobre el mecanismo que se debe seguir para tener las etapas para incorporar el Riesgo operativo dentro de una entidad, teniendo muy claro los lineamientos necesarios a seguir en cada etapa que involucra la implementación del riesgo operativo en una entidad.

Durante los últimos años se han podido determinar algunos inconvenientes por los cuales las entidades financieras no han podido acoplarse en su totalidad con la integración total del RO. en sus procesos organizacionales.

Mediante la grafica se describirá algunos de los inconvenientes más importantes:

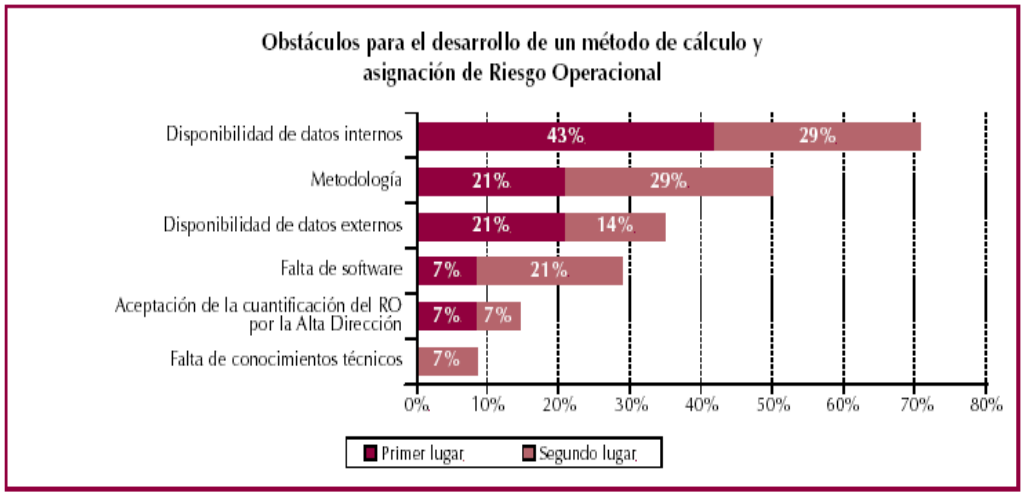


Grafico 5 Inconvenientes para la Implementación del Riesgo Operativo

Fuente: ERNEST, YOUNG, Gestión del Riesgo Operacional, Septiembre, 2008

Es por ello que, los beneficios en la Banca Privada estarán dados mediante un diagnostico situacional de cómo se encuentran actualmente el proceso de implementación del riesgo operativo acorde al perfil de cada entidad, y se proporcionará los parámetros y pautas necesarias para concientizar, fomentar e informar sobre la importancia del riesgo operativo y cómo administrarlo con eficiencia y eficacia, manteniendo así la continuidad del negocio.

A continuación se mostrara las etapas que conforman el Riesgo Operativo, estas etapas deben ser partes activas en los procesos organizacionales de una entidad financiera.

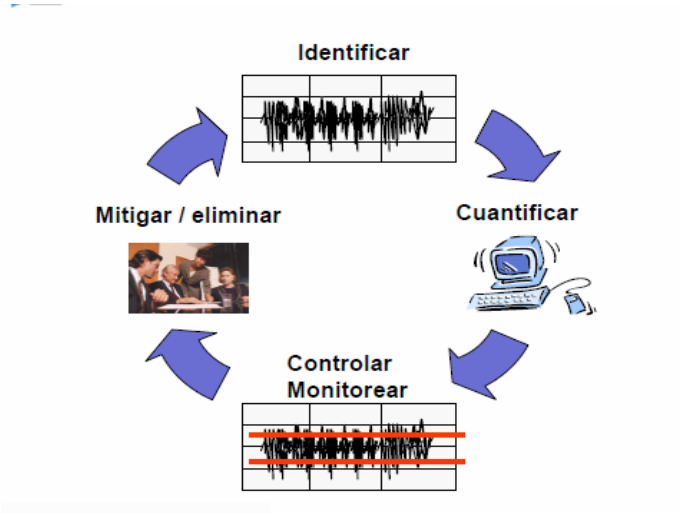


Grafico 6 Etapas del Riesgo Operativo

Fuente: ERNEST, YOUNG, Modelo Cualitativo de Riesgo Operacional, Septiembre, 2008

MARCO DE GESTIÓN DEL RIESGO OPERACIONAL

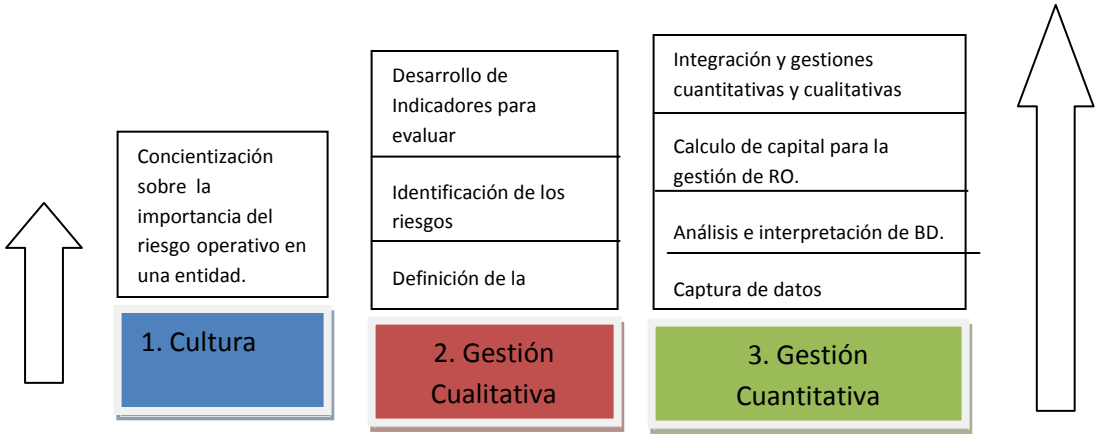


Grafico 7 Marco de Gestión del Riesgo Operativo

Fuente: el Autor

CULTURA

Las entidades Financieras mediante el convencimiento de la alta dirección de los beneficios y de la necesidad de implementar un marco que administre el riesgo operacional.

GESTIÓN CUALITATIVA

Las entidades Financieras identifican tres aspectos relevantes en la gestión del riesgo operacional: Identificación de riesgos, modelo organizativo de acuerdo al perfil de riesgo de cada entidad y las herramientas de gestión utilizadas como son cuestionarios de evaluación de cada área crítica que se encuentra inmerso el riesgo operativo.

GESTION CUANTITATIVA

Con la gestión cuantitativa se busca la creación de una base de datos por medio de la cual se podrá cuantificar las pérdidas operacionales que se den en las distintas áreas expuestas en este riesgo operacional en toda la organización.

El mecanismo que se llevará a cabo para la realización de este tema de investigación previo a la obtención del título de Ing. Comercial será la siguiente:

- Diagnostico de la problemática.

- Fundamentación Teórica, términos de la investigación y demás generalidades de interés.
- Justificación de la investigación con un panorama grafico porcentual y conceptual.

- Identificación correcta del manejo del riesgo operativo y análisis real nacional de la banca privada ecuatoriana.

- Parámetros de procesos de implementación del riesgo operativo en una entidad financiera.

- Problemática e inconvenientes que retrasan la implementación del riesgo operativo en los procesos organizacionales.

- Normatividad impuesta por la SBS (Superintendencia de Bancos y Seguros, cuestionario de evaluación al sistema financiero).

- Proceso actual de cómo se encuentra la implementación del riesgo operativo en la banca privada de manera estadística proporcionando un status actual.

- Lineamientos del proceso de implementación.

- Cuestionarios aplicables delimitando los factores esenciales del riesgo operativo.[3]

[3] RODRIGUEZ, Noberti, *Riesgo Operativo Ceo*-2da. Edición, Editorial Isma,Buenos Aires-Argentina, 2007

1.4 Objetivos

Objetivo General

Proporcionar un conocimiento sólido a la banca privada Ecuatoriana sobre la relevancia de implementar el riesgo operativo en una entidad generando una cultura enmarcada en la concientización, además los procedimientos y lineamientos que se debe seguir para prevenir, identificar, controlar y mitigar los factores internos y externos de riesgo que corroboran producir grandes pérdidas organizacionales, utilizando el riesgo operativo como una herramienta canalizadora de la eficiencia y eficacia en la optimización de los recursos.

Contribuyendo así, en generar un incremento en la productividad y disminución de pérdidas inesperadas por diversos factores y por falta de supervisión y control.

SISTEMATIZACIÓN

1.-OBJETIVO ESPECIFICO

Diseñar un análisis basado en la implementación del RO. en su etapas y componentes principales para medir la eficiencia de cada procedimiento de una entidad, mediante herramientas de control y evaluación como matrices de riesgo y un manual aplicable a los requerimientos establecidos por los organismos de control, generando a su vez una mejora de procedimientos de control, obteniendo así mitigar este factor de riesgo.

2.-OBJETIVO ESPECIFICO

Realizar un análisis minucioso de las fuentes principales que abarca el riesgo operativo como lo son: los procesos internos, eventos externos, el personal, y la tecnología. y que podrían generar la disminución de la solvencia y rentabilidad de la organización.

3.-OBJETIVO ESPECIFICO

Proporcionar por medio de la presente investigación una fuente de información y conocimiento respecto a los beneficios de la implementación y administración del riesgo operativo en la banca privada ecuatoriana.

CAPITULO II

2.1 Teorías en Relación al Producto

Definición de Riesgo Operativo

Se entiende por riesgo operativo a la posibilidad de ocurrencia de pérdidas financieras por deficiencias o fallas en los procesos internos, en la tecnología de información, en las personas o por ocurrencia de eventos externos adversos. Esta definición incluye el riesgo legal, pero excluye el riesgo estratégico y el de reputación.

Las empresas de cualquier sector de negocios tienen diferentes niveles de exposición al Riesgo Operacional dependiendo del perfil de riesgo que esté sujeta la entidad.

El riesgo operacional, operativo o de operación se basa en la posibilidad de falencias en algunos procesos de que dan principalmente en: procesos estratégicos más relevantes de una entidad.

El riesgo de operación incluye el riesgo legal, aunque no se refiere a la posibilidad de pérdidas originadas en cambios inesperados en el entorno político, económico y social seno aspectos netamente legales y de cumplimiento.[4]

[4] SAENZ,Jordan ," Economía de la Empresa", *Revista Europea de Dirección*, año 2008, No.2, Georgia,18 de Septiembre de 2008,p.68.

En BASILEA II, el riesgo operativo se define como el riesgo de pérdida debido a la inadecuación o a fallos de los procesos, el personal y los sistemas internos o bien a causa de acontecimientos externos.

A continuación se citaran algunos conceptos de riesgo operativo para conceptualizar y entender el enfoque que este tiene en una entidad financiera:

- Se dice de riesgo operativo que es, el impacto y probabilidad de que un evento no deseado pueda afectar el logro de metas y objetivos de una entidad.

Existen diversas definiciones que se han dado al concepto de riesgo operativo, pero entre ellas, a continuación se menciona la emitida por el Comité de Basilea, la cual señala que:

El riesgo operativo es el que proviene de fallas de información en los sistemas o en los controles internos que pueden provocar una pérdida inesperada. Este riesgo se asocia con errores humanos, fallas en los procesos e inadecuados sistemas y controles"
Por lo que se acaba de exponer, se infiere que el riesgo operativo puede definirse como sigue:

- El riesgo de pérdida como resultado de procesos, gente y sistemas inadecuados o fallas en procesos internos, gente y sistemas de eventos externos.[5]

[5] Comité de Basilea, *Sanas prácticas de la Gestión y supervisión del Riesgo Operativo*, Suiza, Febrero 17 del 2003, p.45.

El hecho de dar una definición es vital, porque supone un gran avance hacia el consenso y la homogeneización de términos. Basilea II ha venido a aportar, en este sentido, un punto de partida básico y un marco de referencia a la hora de tratar este riesgo.

De acuerdo con José Antonio Núñez y José Juan Chávez, en su artículo "Riesgo operativo: esquema de gestión y modelado del riesgo", del riesgo operativo se pueden destacar las siguientes características:

1-Es antiguo y está presente en cualquier clase de negocio.

2- Es inherente a toda actividad en que intervengan personas, procesos y plataformas tecnológicas.

3- Es complejo, como consecuencia de la gran diversidad de causas que lo originan.

4- Las grandes pérdidas que ha ocasionado en varias empresas, muestran el desconocimiento que de él se tiene y la falta de herramientas para gestionarlo.[6]

[6] NUÑEZ, José y CHAVEZ José J.,"Esquema de gestión y modelado del riesgo", *Gestión del Riesgo Operativo*, año 2007, No.3, Quito 20 de Julio de 2007, p.47.

De tal manera y de acuerdo a los diversos criterios detallados anteriormente se formulará uno general, el cual resumirá lo más esencial del Riesgo Operativo para así entenderlo de mejor manera:

El Riesgo Operativo es trascendental en una entidad ya que abarca y afecta a todos sus recursos tanto humanos, procesos internos, tecnológicos y eventos externos, en donde no existe una adecuada planificación, organización, dirección y control de los mismos generando así errores involuntarios no identificados ni mitigados oportunamente, los mismos que son generadores de perdidas financiaras lo que afectan a la rentabilidad e imagen de la entidad impidiendo así lograr los objetivos organizacionales.

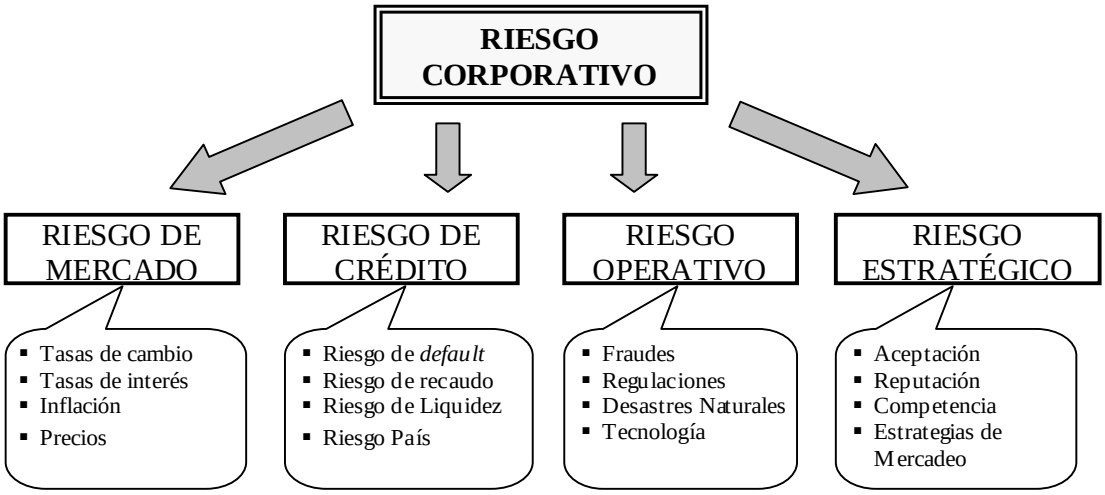


Grafico 8 Riesgos Corporativos
Fuente: MENDOZA, Álvaro y CASTILLO Mario, Riesgos Financieros, Julio 2005

En el gráfico claramente determino los distintos riesgos a nivel corporativo y particularmente el riesgo operativo el mismo que es sujeto de análisis en esta investigación. El cual tiene entre sus componentes aquellos factores internos y externos que conforman una entidad financiera y son parte activa de sus procesos organizacionales.

2.1.1 Proceso de la Administración del Riesgo Operativo

La administración adecuada del riesgo operativo juega un papel de vital importancia dentro de una entidad finaciera.[3]

A continuación se definirá el proceso que implica la administración del riesgo operativo dentro de una entidad el mismo que lograra prever pérdidas cuantiosas involuntarias como efecto de un desconocimiento del tema.

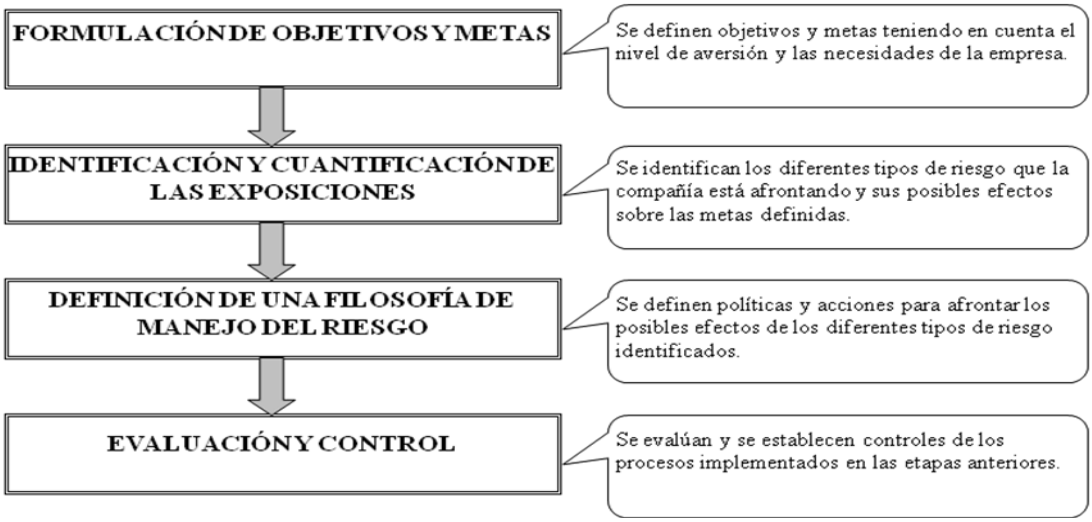
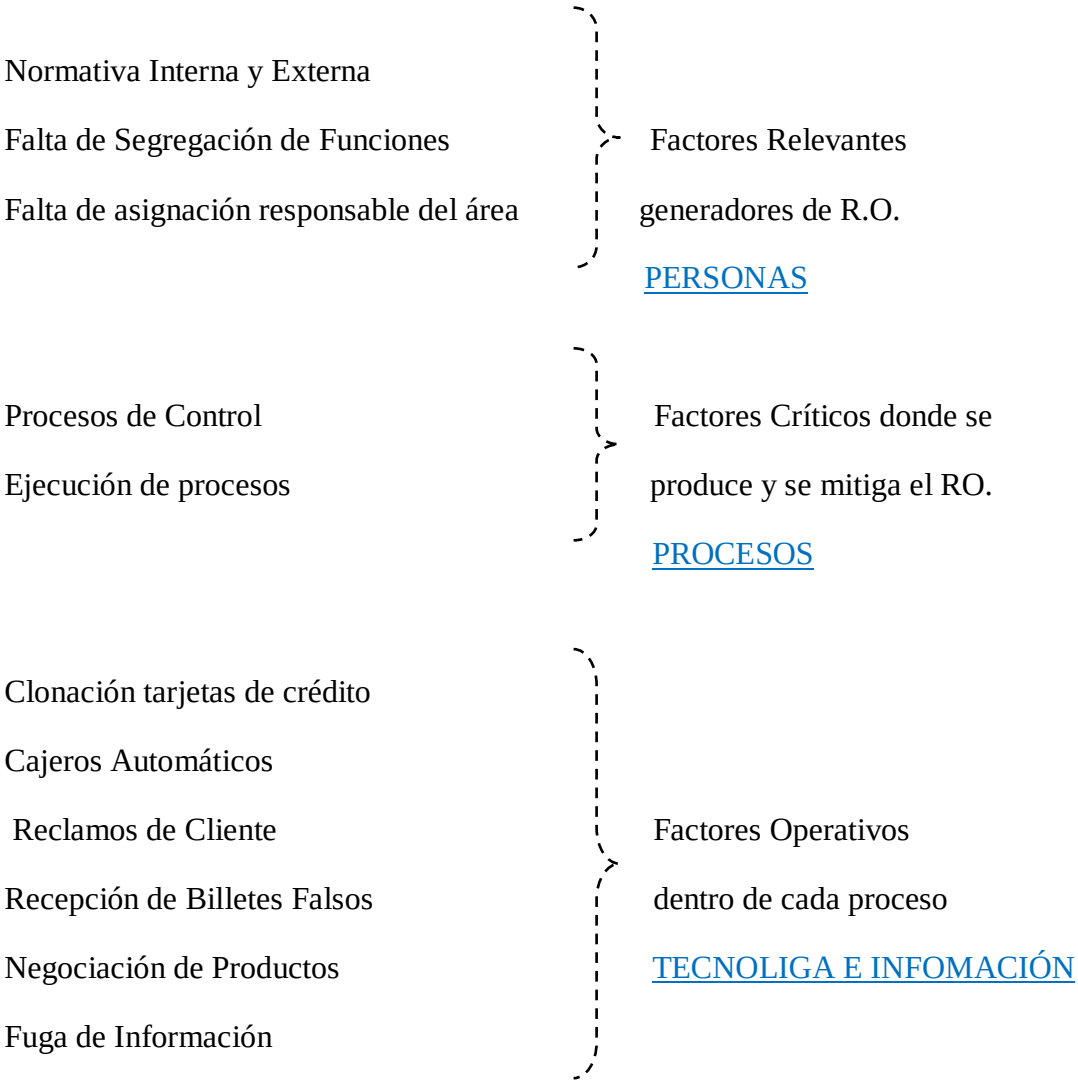


Grafico 9 Proceso de la Administracion del Riesgo Operativo

Fuente: MENDOZA, A., y CASTILLO Mario, "*Riesgos Financieros"*, Julio 2005.

2.1.2 Factores más frecuentes para generar Riesgo Operativo



Personas.- No se ha revisado correctamente desde la alta gerencia el organigrama estructural para asignación del responsable de cada área y sus funciones en la supervisión, control y evaluación de cada proceso donde están inmersos los procesos estratégicos.

Procesos.- No se han realizado una correcta supervisión ni la evaluación respectiva de la efectividad respecto a la optimización de cada recurso dentro de los procesos productivos vigentes de la entidad cuyo objetivo será identificar errores en la ejecución de los procesos.

Tecnología e Información.-No se cuenta con las medidas de seguridad apropiadas para evitar la encriptación, y la tecnología para poder repeler factores de fraude los mismos que se realizan de forma cotidiana en la entidad y contribuyen a generar grandes pérdidas.

2.1. 3 Requisitos Cuantitativos y Cualitativos para Implementar el Riesgo Operativo en una Entidad Financiera

Requisitos Cualitativos

Existencia de unidad independiente de RO dentro del área de riesgos, que realice la codificación e implementación de la gestión de este tipo de riesgo (incluye elaboración de manuales de procedimiento y manuales metodológicos).

- Involucración alta dirección, es decir se requiere al apoyo de gerencia en los procesos de RO.

- Integración del RO en la gestión diaria de la entidad. Inclusión del RO en el cálculo del Capital neto y en el precio de las operaciones de una entidad.

- Reportar con regularidad los diferentes niveles de exposiciones y pérdidas por RO

- Las metodologías de cuantificación deben estar perfectamente documentadas

- Revisión por parte de auditoría interna y externa de los sistemas de medición, tanto a nivel de unidades de negocio como la unidad de RO.

❖ Los auditores externos y el regulador deben verificar que los sistemas internos de validación de los modelos funcionan y que los flujos de datos y los procesos asociados a la medición son trasparentes y accesibles.

➢ Es importante señalar que es imprescindible en una entidad implementar una área de riesgo la cual sería la encargada de llevar un control integral de cada una de las áreas de la organización en donde se verificaría todos los procesos. Y a la vez se encargará de dar todos los lineamientos y herramientas mediante manuales de procedimientos muy puntuales de cómo de debe desarrollar el control y supervisión en cada departamento**.**

Requisitos Cuantitativos

- El banco debe demostrar que la metodología utilizada, y en particular la función de distribución de pérdidas, recoge los eventos de poca frecuencia y alta severidad característicos de algunos de los eventos de pérdida del RO. No incluye hechos catastróficos.

- Las entidades deben contar con un requerimiento mínimo de capital.

- La medición del RO debe tener en cuenta tanto datos internos como externos, realizar análisis de escenarios y utilizar factores de riesgo que comprendan las características propias de la entidad así como sus sistemas de control interno.[7]

- Cabe señalar que las bases de datos (información interna) son herramienta fundamental en la detección y mitigación del RO, y es la labor de las entidades contar con estas bases de datos las mismas que deben ser alimentadas progresivamente con el fin de verificar la frecuencia e incidencia de los eventos generadores de perdidas.

- Existen toda una serie de requisitos sobre los Datos Internos, que son un aspecto crucial en el desarrollo de metodologías de gestión de riesgos.

[7] SMITHSON, Charles W.," *Managing Financial Risk*". 3ª Edición, Editorial McGraw-Hill, Págs. 550-573

2.2 Categorización de eventos de pérdida por Riesgo Operativo según Basilea II

Generalidades del acuerdo de Basilea II

En 1988, el comité de supervisión bancaria de Basilea estableció el primer acuerdo de capital, es decir, Basilea I. El centro de dicho documento era el riesgo crediticio de los bancos, a los cuales se les pedía prever un mínimo de capital en caso de insolvencia de los deudores. No fue sino hasta 1996, que se incluyó el riesgo de mercado.

Es en 2004 con el acuerdo de Basilea II, cuando se intenta trabajar de una manera más integral acerca de la solvencia y seguridad del sector financiero. Una de las innovaciones en este acuerdo es la inclusión de requerimientos de capital por riesgo operativo. Si bien es cierto que el riesgo operativo existe en todas la funciones de las entidades financieras, desde el primer instante de su vida, y su gestión ha sido importante para disminuir el fraude y desarrollar controles internos, sólo recientemente se ha desarrollado un interés formal por parte de los reguladores, consultores, académicos e instituciones financieras. Lo anterior es debido básicamente a las enormes pérdidas de las entidades financieras registradas por errores operacionales en el mercado.

A continuación se detallará las pérdidas más cuantiosas registradas como consecuencia de factores de Riesgo Operativo:

Banco Barings y Daiwa Bank en 1995, Sumimoto Bank en 1996 y Allied Irish Bank en 2000.

El acuerdo de Basilea II no sólo es la búsqueda de cumplimiento de reglas por parte de las entidades financieras, sino pretende incentivar un estándar de mayor calidad en la gestión y control de riesgos y capital, y es a la vez, un reflejo de un clima de atención por parte de los reguladores a los sistemas de control interno y a la cultura de control. La gestión del riesgo operativo es ahora una práctica constante y tan importante como la gestión del riesgo crediticio o del mercado.

A su vez el Comité identifica los principales eventos de riesgo operativo, los cuales están relacionados con: el fraude interno y externo; las relaciones laborales y seguridad en el puesto de trabajo (ejemplo: solicitud de indemnizaciones por parte de los empleados, infracción de las normas laborales de seguridad e higiene, organización de actividades laborales, acusaciones de discriminación, responsabilidades generales, etc.); las prácticas con los clientes, productos y negocios (abusos de confianza, abuso de información confidencial sobre el cliente, negociación fraudulenta en las cuentas del banco, lavado de dinero, etc.); los daños a activos materiales (terrorismo, vandalismo, terremotos, incendios, inundaciones, etc.); las alteraciones en la actividad y fallos en los sistemas (fallos del hardware o del software, problemas en las telecomunicaciones, interrupción en la prestación de servicios, etc.); la ejecución, entrega y procesamiento (errores en la introducción de datos, fallos en la administración de las garantías, documentación jurídica incompleta, etc.).

Indudablemente todo ello no es algo nuevo, sino que siempre ha sido una parte importante del esfuerzo de los bancos por evitar el fraude, mantener la integridad de los controles internos, reducir los errores en las operaciones, etc. Sí resulta relativamente nueva la consideración de la gestión del Riesgo Operativo como una práctica integral comparable a la gestión del Riesgo del crédito o Riesgo de Mercado. En este sentido, son cada vez más las instituciones convencidas de que los programas de gestión integral del riesgo operativo proporcionan seguridad y solidez.[8]

[8] Comité de Basilea, *Sanas prácticas de la Gestión y supervisión del Riesgo Operativo*, Suiza, Febrero 17 del 2003, p.56.

Fraude Interno

Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o incumplir regulaciones, leyes o políticas empresariales en las que se encuentra implicada, al menos, una parte interna a la empresa; no se consideran los eventos asociados con discriminación en el trabajo. Esta categoría incluye eventos como: fraudes, robos (con participación de personal de la empresa), sobornos, entre otros.

- Este fraude está enfocado en las clientes internos es decir el talento humano ya que se ha determinado que muchos de los factores que contribuyen a incrementar el factor de riesgo están dados por el personal que trabaja en la entidad por el incumplimiento de sus obligaciones profesionales, por lo que recomendaría realizar de manera eficiente los procesos de incorporación ya que este es el encargado de la selección, evaluación e inducción del personal**.**

Fraude Externo

Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o soslayar la legislación, por parte un tercero. Esta categoría incluye eventos como: robos, falsificación, ataques informáticos, entre otros.

- Este fraude hace referencia a agentes externos que afectaría directamente a cambios regulatorios, desastres naturales, reestructuración corporativa, outsourcing además de ataques on line por lo que recomendaría contar con tecnología de punta misma que servirá para contrarrestar estos eventos externos disminuyendo así este factor generador de RO.

Relaciones laborales y seguridad en el puesto de trabajo

Pérdidas derivadas de actuaciones incompatibles con la legislación o acuerdos laborales, sobre higiene o seguridad en el trabajo, sobre el pago de reclamaciones por daños personales, o sobre casos relacionados con discriminación en el trabajo. Clientes, productos y prácticas empresariales.

Pérdidas derivadas del incumplimiento involuntario o negligente de una obligación profesional

Frente a clientes concretos (incluidos requisitos fiduciarios y de adecuación), o de la naturaleza o diseño de un producto.

- Daños a activos materiales

- Pérdidas derivadas de daños o perjuicios a activos físicos como consecuencia de desastres naturales u otros eventos de fuentes externas.

- Interrupción del negocio y fallos en los sistemas

- Pérdidas derivadas de incidencias o interrupciones en el negocio y de fallas 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. Esta categoría incluye eventos asociados con: captura de transacciones, ejecución y mantenimiento, monitoreo y reporte, entrada y documentación de clientes, gestión de cuentas de clientes, contrapartes de negocio, vendedores y proveedores.

2.3 Componentes del Riesgo Operativo

Procesos Internos

Posibilidad de pérdidas financieras relacionadas con el diseño inapropiado de los procesos críticos, o con políticas y procedimientos inadecuados o inexistentes que puedan tener como consecuencia el desarrollo deficiente de las operaciones y servicios o la suspensión de los mismos.

En tal sentido, podrán considerarse entre otros, los riesgos asociados a las fallas en los modelos utilizados, los errores en las transacciones, la evaluación inadecuada de contratos o de la complejidad de productos, operaciones y servicios, los errores en la información contable, la inadecuada compensación, liquidación o pago, la insuficiencia de recursos para el volumen de operaciones, la inadecuada documentación de transacciones, así como el incumplimiento de plazos y presupuestos planeados.[9]

Personas

Posibilidad de pérdidas financieras asociadas con negligencia, error humano, sabotaje, fraude, robo, paralizaciones, apropiación de información sensible, lavado de dinero, inapropiadas relaciones interpersonales y ambiente laboral desfavorable, falta de especificaciones claras en los términos de contratación del personal, entre otros factores. Se puede también incluir pérdidas asociadas con insuficiencia de personal o personal con destrezas inadecuadas, entrenamiento y capacitación inadecuada y/o prácticas débiles de contratación.

[9] CÁCERES Michael y MATURANA J., *Riesgo Operacional*,1era.Edición,Editorial McGraw-Hill, Ecuador, Marzo 2008

Tecnología de Información

Posibilidad de pérdidas financieras derivadas del uso de inadecuados sistemas de información y tecnologías relacionadas, que pueden afectar el desarrollo de las operaciones y servicios que realiza la institución al atentar contra la confidencialidad, integridad, disponibilidad y oportunidad de la información.

Las instituciones pueden considerar de incluir en ésta área, los riesgos derivados a fallas en la seguridad y continuidad operativa de los sistemas TI (Tecnología de Información), a errores en el desarrollo e implementación de dichos sistemas y su compatibilidad e integración, problemas de calidad de información, inadecuada inversión en tecnología y fallas para alinear la TI con los objetivos de negocio, con entre otros aspectos. Otros riesgos incluyen la falla o interrupción de los sistemas, la recuperación inadecuada de desastres y/o la continuidad de los planes de negocio.[10]

Eventos Externos

Posibilidad de pérdidas derivadas de la ocurrencia de eventos ajenos al control de la empresa que pueden alterar el desarrollo de sus actividades, afectando a los procesos internos, personas y tecnología de información. Entre otros factores, se podrán tomar en consideración los riesgos que implican las contingencias legales, las fallas en los servicios públicos, la ocurrencia de desastres naturales, atentados y actos delictivos, así como las fallas en servicios críticos provistos por terceros. Otros riesgos asociados con eventos externos incluyen: el rápido paso de cambio en las leyes, regulaciones o guías, así como el riesgo político o del país.

[10] OJEDA, Elvia. "Riesgo Operativo XXIII",Ponencia presentada en el Congreso AMA Argos, Buenos Aires,24 de Agosto del 2008

2.4 Gestión del Riesgo Operativo y sus Etapas

Como principio general, las entidades financieras deben contar con una estrategia aprobada por el Directorio estableciendo principios para la identificación, medición, control, monitoreo y mitigación del riesgo operativo.

Las estrategias y políticas deberían ser implementadas por la Función de Gestión de Riesgo, responsable de identificar y gestionar todos los riesgos. La Función de Gestión de Riesgo puede incluir sub-unidades especializadas por riesgos específicos.

- Las entidades financieras deberían desarrollar su propio enfoque y metodología para la gestión de riesgos, de acuerdo con su objeto social, tamaño, naturaleza y complejidad de operaciones y otras características. La implementación del sistema de gestión de riesgo operativo debería considerar todas las etapas de gestión de riesgo, incluyendo la identificación, evaluación, medición, monitoreo y control.

Marco estratégico

El modelo de riesgos debe ser acorde con las grandes directrices emitidas desde la alta dirección, sobre todo en lo que respecta el "apetito" por el riesgo de la entidad. Algunas entidades son claramente más conservadoras que otras, lo que se traduce en carteras de clientes diferentes, políticas comerciales diferentes, niveles de rating (Calificación de solvencia y acogida en el mercado de una entidad).

Identificación

La identificación efectiva del riesgo considera tanto los factores internos como externos que podrían afectar adversamente el logro de los objetivos institucionales.

- Fase inicial de un modelo, donde, para un grado variable de detalle, se van analizando los diferentes procesos y subprocesos, en los cuales se deben ir identificando los posibles eventos de pérdida para la entidad

La fase de identificación atraviesa por varios pasos:

- Establecimiento de las diferentes AN (Aéreas del negocio) y sub-AN que van a ser objeto de identificación. Las mismas que son establecidas por BIS (Banco Mundial o Centro Financiero Global).

- Definición, dentro de cada de estas áreas, de los procesos y actividades generadores de riesgo.

- Para cada uno de esos productos y actividades, análisis de los riesgos y su riesgos asociados. Asimismo, se deben establecer unos controles que deben ser verificados por la unidad de control.

- Finalmente, el diseño de un modelo de datos, que deberá contemplar no sólo la recolección de información relativa a las pérdidas operacionales, sino adicionalmente un conjunto de indicadores de riesgo que permita realizar la evaluación cualitativa de los procesos operativos y de la estructura de controles existente.

En el proceso de identificación se suelen utilizar las denominadas auto-evaluaciones, que siguen los siguientes pasos:

Elaboración de cuestionarios de auto-evaluación para cada una de las líneas de negocio y áreas de soporte, que repase de forma exhaustiva las categorías de riesgos (personas, sistemas, procesos, externos).

El objetivo del mismo será:

- Obtener información sobre el impacto y frecuencia de los riesgos identificados.

- Obtener información sobre la existencia y efectividad de los controles existentes y la posibilidad de establecer controles adicionales.

- Determinación de personas responsables dentro de cada área de responder los cuestionarios

- Entrenamiento y formación de las personas implicadas en el proceso de auto-evaluación

- El resultado de un cuestionario no deja de ser una valoración subjetiva de la persona entrevistada, por lo que es importante que los cuestionarios estén bien definidos y sean llevados a cabo con rigor y por personas imparciales.

- El campo “controles” deberá identificar los controles existentes y una valoración sobre su efectividad.

Los campos de frecuencia e impacto de los eventos de riesgo deberán estimar claramente una evaluación cuantitativa y cualitativa de la situación de riesgo de una entidad.

Evaluación

Para todos los riesgos operativos materiales que han sido identificados, la entidad debería decidir si usa procedimientos apropiados de control y/o mitigación de los riesgos o asumirlos.

Para aquellos riesgos que no pueden ser controlados, el banco debería decidir si los acepta, reduce el nivel de actividad del negocio expuesta o se retira de esta actividad completamente.

Todos los riesgos materiales deberían ser evaluados por probabilidad de ocurrencia e impacto a la medición de la vulnerabilidad de la entidad a este riesgo. Los riesgos pueden ser aceptados, mitigados o evitados de una manera consistente con la estrategia y el apetito al riesgo institucional. Cuando sea posible, la entidad debería usar controles internos apropiados u otras estrategias de mitigación, como los seguros.

- En la evaluación se debe realizar como herramienta fundamental un cuestionario integral de acuerdo a todos los componentes descritos en este capítulo, el cuestionario será analizado e interpretado para posteriormente desarrollar el modelo más acorde de acuerdo a los requerimientos de la entidad.

Medición

Las entidades financieras deberían estimar el riesgo inherente en todas sus actividades, productos, áreas particulares o conjuntos de actividades o portafolios.

- Se debe usar técnicas cualitativas basadas en análisis expertos, técnicas cuantitativas que estiman el potencial de pérdidas operativas a un nivel de confianza dado o una combinación de ambos.

Monitoreo

Un proceso efectivo de monitoreo es esencial para una gestión adecuada del riesgo operativo. Un monitoreo regular de las actividades puede ofrecer la ventaja de detectar rápidamente y corregir deficiencias en las políticas, procesos y procedimientos de gestión del riesgo operativo.

El monitoreo regular también fomenta la identificación temprana de cambios materiales en el perfil de riesgo, así como la aparición de nuevos riesgos.

- El alcance de las actividades de monitoreo incluye todos los aspectos de la gestión del riesgo operativo en un ciclo de vida consistente con la naturaleza de sus riesgos y el volumen, tamaño y complejidad de las operaciones. (de cada departamento en sus procesos).

Control

Después de identificar y medir los riesgos a los que está expuesta, la entidad financiera debería concentrarse en la calidad de la estructura de control interno.

- El control del riesgo operativo puede ser conducido como una parte integral de las operaciones o a través de evaluaciones periódicas separadas, o ambos. Todas las deficiencias o desviaciones deben ser reportadas a la gerencia**.**

Reporte

Debe existir un reporte regular de la información pertinente a la alta gerencia, al directorio, al personal y a partes externas interesadas, como clientes, proveedores, reguladores y accionistas. El reporte puede incluir información interna y externa, así como información financiera y operativa.

Para considerar la existencia de un apropiado ambiente de gestión de riesgo operativo, las instituciones controladas deberán definir formalmente políticas para un adecuado diseño, control, actualización y seguimiento de los procesos.[11]

- Es conveniente que mediante la alta gerencia se defina los parámetros necesarios, a manera de normatividad o política interna en el mapa de procesos, para diseñar un manual de procedimientos y a su vez dar el respectivo seguimiento a cada una de las áreas de la entidad en donde se determinara las falencias en los procesos internos.

[11] ERNEST, YOUNG, *Gestión del Riesgo Operacional en Entidades Financieras*, Quito,10 de Noviembre del 2003,p.36

Conclusiones Relevantes

Los registros históricos son fuente básica requerida para el análisis del riesgo operativo, es necesario la mayor cantidad de datos disponibles y un flujo constante de esta información en las distintas actividades de la organización, y las personas responsables de ejecutar los procesos para así lograr las efectividad de la gestión de riesgos.

Existen dos grupos principales de riesgo que se pueden conocer en una entidad:

Cuantitativos

Incidencias de eventos de perdidas esto se obtiene de la información histórica.

Cualitativos

Estos son riesgos potenciales que se basan en juicio de expertos, entre los riesgos potenciales que debemos conocer se detallan los siguientes:

Organigramas Funcionales

Revela las divisiones de la organización y sus relaciones permitiendo entender al analista más claramente si la persona o área esta segregada correctamente su función y permitiendo así evitar el riesgo operativo.[8]

Procesos Operativos

Permite conocer al administrador como se realizan las actividades por área específica.

2.5 Componentes de una Matriz de Riesgo

Diagramas de Flujo

Mediante estos el administrador podrá visualizar si se cumple con todo el proceso o existen factores que impiden concluirlo.[12]

Además debemos conocer la tipología del riesgo el cual se clasifica en:

- Riesgo de Proceso(Operativo)
- Riesgo Legal
- Riesgo Humano
- Riesgo Tecnológico
- Riesgo de Contraparte(proveedor)
- Riesgo de Desastres naturales

[12] OJEDA, Elvia. "Riesgo Operativo XXIII",Ponencia presentada en el Congreso AMA Argos, Buenos Aires,24 de Agosto del 2008

- Por su fuente se clasifican en:

  - Errores Humanos
  - Incumplimiento
  - Diseño
  - Abuso
  - Planeación
  - Fallas

  Son componentes de una matriz de riesgo operativo

  - Seguridad
  - Experiencias

- Por su frecuencia esto es por cada riesgo ya clasificado se asigna una ocurrencia a cada uno de ellos esas se clasifican en:

  - ✓ Casi nulo
  - ✓ Raro
  - ✓ Probable

  Son componentes de una matriz de riesgo operativo

  - ✓ Casi seguro

  - ❖ Por la severidad, aquí se estima el impacto en caso de materializarse el riesgo y se clasifica en:

    - Insignificante
    - Moderado
    - Fuerte

    son componentes de la matriz d riesgo operativo

    - Significante

CAPITULO III

3.1 Análisis de la implementación del Riesgo Operativo en la Banca privada Ecuatoriana Durante el Periodo 2005-2009

Antecedentes

Inicialmente se enfocará mediante la gráfica, como ha ido evolucionando el proceso de implementación del riesgo operativo en la banca privada ecuatoriana, claramente se indica como el ciclo se ha ido desarrollando, de acuerdo a las etapas que una entidad debe atravesar para conseguir los objetivos trazados inicialmente por parte de la SBS, que es lograr que el riesgo operativo y su gestión forme parte activa en sus procesos organizacionales de las entidades financieras.

Como por ejemplo la planificación de la continuidad del negocio, implementación de un sistema de gestión y controles para la seguridad de la información, conformación de una base de datos para monitorear y controlar el riesgo operativo, y aquellos que signifiquen cambios en la cultura organizacional, estos son los objetivos que se prevé en la etapa de mejoramiento.

Proceso de Implementación del Riesgo Operativo en los últimos años

Grafico 10 Proceso de Implementación del Riesgo Operativo

Fuente: MENDOZA, Á. y CASTILLO Mario, Riesgos Financieros, Julio 2005.

Mediante resolución JB-2005-834 de 20 de octubre del 2005 se emite la normatividad por parte de la SBS la cual inicia su proceso en abril del 2006, mientras que en el 2007 aun se encuentra en desarrollo aun el proceso de implementación.

ETAPA DE IMPLEMENTACIÓN.- Significa la ejecución de proyectos de mejoramiento continúo de la entidad

En Diciembre del 2006 y de acuerdo a lo manifestado con el acuerdo de Basilea II se toma en cuenta por primera vez al riesgo operativo y se inicia el proceso de incorporación en una entidad financiera, a partir de esta fecha en adelante las entidades han venido tratando de familiarizarse cada vez más con el riesgo operativo, pero no se ha tenido el éxito deseado, ya que para el año 2008 en adelante se preveía que las entidades contarían con su requerimiento de capital mínimo en función de las pérdidas acumuladas sufridas por defectos de control y mitigación del riesgo antes mencionado.

Para el año 2009 y afínales del 2010 la SBS evalúa al sistema financiero el porcentaje de implementación de RO. en sus proceso organizacional lo cual indica avances significativos.

La Superintendencia de Bancos del Ecuador, que es el organismo regulador encargado de supervisar al sistema financiero ecuatoriano, emitió un cuestionario en Noviembre del 2010 enmarcado a los requerimientos de riesgo operativo que consta en el acuerdo de Basilea II, el objetivo de este cuestionario es reflejar el status actual de implementación del riesgo operativo en el sistema financiero, para efectos de la investigación se analizara únicamente a la banca privada.

Los resultados establecidos por la norma han sido evaluados, ponderando el avance que ha tenido cada entidad y están representados de manera independiente a los componentes que conforman el riesgo operativo para interpretarlos y entenderlos a cada uno de ellos.

3.1.1 Análisis Cuestionario emitido por la Superintendencia de Bancos respecto a la Implementación de Riesgo Operativo

PROCESOS

DISPOSICIONES NORMATIVAS			ASPECTOS A CUMPLIRSE		
(Sección II): FACTORES DEL RIESGO OPERATIVO			REQUERIDO EN EL PROCESO DE IMPLEMENTACION DE RO.	ENTIDAS QUE CUENTAN CON LO SOLICITADO	PORCENTAJE DE IMPLEMENTACÓN
PROCESOS	¿La entidad ha identificado los procesos con los que cuenta bajo los parámetros definidos en la norma de Riesgo Operativo?	Cuenta con un inventario y/o mapa de procesos de toda la entidad.	25	17	68%
		Los procesos están agrupados en: gobernantes, productivos y de	25	18	72%
		Tiene identificadas las líneas de negocios de acuerdo con el	25	18	72%
		Ha identificado los procesos críticos propios de la entidad y los provistos por terceros en función de criterios formalmente establecidos.	25	17	68%
		Los procesos están debidamente diseñados (detalle del tipo de procesos, secuencia lógica de las actividades, responsables y áreas involucradas).	25	16	64%
	¿La entidad ha definido políticas y procedimientos para la administración de procesos?	Ha definido responsables de los procesos.	25	15	60%
		Cuenta con políticas y procedimientos para el levantamiento, diseño y descripción de los procesos.	25	18	72%
		Cuenta con políticas y procedimientos de difusión y comunicación de los procesos a nivel de toda la organización.	25	18	72%
		Cuenta con políticas y procedimientos de medición y gestión de procesos, es decir: indicadores de gestión.	25	9	36%
		Existen políticas y procedimientos para el seguimiento permanente de la gestión de los procesos que permita la actualización y mejora continua de los mismos.	25	17	68%
PORCENTAJE IMPLEMENTADO EN PROCESOS			250	163	65%

Cuadro 2 Análisis componente Procesos

Fuente: SBS, Cuestionario emitido al sistema financiero, evaluación de implementación RO, 2010

Analizando este componente que hace referencia a los procesos de una entidad financiera y de acuerdo a la evaluación establecida por la Superintencia de Bancos se determina de forma clara los procesos más relevantes de una entidad como los son: los procesos gobernantes, productivos y de apoyo estos son el pilar fundamental para una correcta administración del riesgo operativo.

Además se evalúa las líneas de negocio, si estas están direccionadas correctamente para un segmento de mercado específico, y se verifica el flujograma de procesos de cada una de ellas para poder determinar si existe una correcta distribución y secuencia lógica en sus procesos.

De igual manera se debe identificar al responsable de cada proceso ya que es el encargado de mantener informado a la alta gerencia de cualquier anomalía que podría retrasar el proceso al cual ha sido asignado cada responsable, y buscar así soluciones oportunas.

Consecuentemente las entidades deben vigilar el cumplimento de los procesos, mediante sus procedimientos y someterlos a una mejora continua por lo que se recomienda desarrollar políticas para identificar, diseñar, medir, analizar, actualizar y controlar los procesos para que estos trabajen en armonía para maximizar la efectividad organizacional.

Adicionalmente se recomienda utilizar indicadores de gestión tales como son el de desempeño, eficiencia, efectividad y calidad del servicio para evaluar a cada proceso y emitir un informe respectivo el mismo que debe realizarse de manera trimestral para efectos de control.

Es por ello que de los 25 bancos privados del ecuador de acuerdo a cada pregunta de la evaluación el 65 % de las entidades cuentan con este componente de riesgo operativo en sus procesos de acuerdo a los lineamientos antes descritos.

PERSONAS

(Sección II): FACTORES DEL RIESGO OPERATIVO			REQUERIDO EN EL PROCESO DE IMPLEMENTACION	ENTIDAS QUE CUENTAN CON LO SOLICITADO	PORCENTAJE DE IMPLEMENTACÓN
PERSONAS	La entidad ha definido procedimientos para la Administración del Capital Humano bajo los parámetros definidos en la norma de riesgo operativo?	La administración del capital humano cuenta con políticas y procedimientos para cada uno de los procesos de incorporación, permanencia y desvinculación del personal.	25	17	68%
		Cuenta con un Código de Ética / Código de Conducta formalmente establecido y difundido en todos los niveles de la	25	18	72%
		Los procesos de incorporación, permanencia y desvinculación están ajustados a las disposiciones legales garantizando condiciones laborales idóneas.	25	16	64%
		Cuenta con análisis para la determinación del personal necesario y las competencias idóneas para el desempeño de	25	15	60%
		Cuenta con una base de datos actualizada de su capital humano (número de personas, formación académica y experiencia, fechas de selección, reclutamiento y selección, eventos de capacitación, cargos que ha desempeñado, evaluaciones de desempeño, fechas y causas de separación del personal, entre	25	14	56%
PORCENTAJE IMPLEMENTADO EN PERSONAS			125	80	64%

Cuadro 3 Análisis

Componente Personas

Fuente: SBS, Cuestionario emitido al sistema financiero, evaluación de implementación RO, 2010

Analizando este componente del riesgo operativo que hace referencia al talento humano y de acuerdo a la evaluación por parte de la Superintendencia de Bancos las preguntas hacen referencia a aspectos relacionados con el personal y sus procesos principales como son: incorporación, permanencia y desvinculación.

En los procesos de incorporación abarcan aspectos como: el reclutamiento, contratación e inducción del personal. En el proceso de permanencia se considera: la capacitación del personal, y por último el proceso de desvinculación que hace referencia a la terminación laboral, aspectos legales cuyo objetivo es dar terminado un contrato.

En este componente de Riesgo Operativo se debe considerar los siguientes factores: selección, determinación de competencia, planes de carrera, motivación, ambiente organizacional, ambiente organizacional, terminación de la relación laboral, evaluación del desempeño, estos factores deben ser considerados al momento que una entidad diseñe sus políticas internas.

Se recomienda que las entidades fomenten las competencias del personal mediante: cursos, seminarios y demás conocimientos para que el personal desarrolle habilidades y se convierta en especialista en riesgo operativo ya que muchas entidades no existe personal especializado en este factor de riesgo.

Por último es de vital importancia que las entidades deben cuenten con bases de datos actualizadas de su personal actual y sus competencias para tener un panorama claro del personal que se cuenta este aspecto es enfocado claramente en la evaluación.

Es por ello que de los 25 bancos privados del ecuador de acuerdo a cada pregunta de la evaluación el 64 % de las entidades cuentan con este componente riesgo operativo en sus procesos de acuerdo a los lineamientos antes descritos

Tecnología de la Información

Analizando este componente referente a la tecnología, y de acuerdo a lo establecido por la evaluación de la SBS determina que las entidades deben contar con tecnología adecuada y actual para que puedan soportar adecuadamente todas las operaciones y

procesos que implica la gestión de riesgos como por ej.: bases de datos donde se requiere que la información sea lo más optimo posible es por ello que las entidades deben planificar sus requerimientos actuales y futuros de tecnología que establezcan requisitos tales como: seguridad integra de la información, confidencialidad y no exista la encriptación (alteración de información por persona no autorizado)

Cabe señalar que este componente es vital para mantener controles y registros detallados de los eventos ocurrentes y repetitivos de falencias en los distintos procesos.

TECNOLOGIA DE LA INFORMACIÓN

(Sección II): FACTORES DEL RIESGO OPERATIVO			REQUERIDO EN EL PROCESO DE IMPLEMENTACION DE RO.	ENTIDAS QUE CUENTAN CON LO SOLICITADO	PORCENTAJE DE IMPLEMENTACIÓN
TECNOLOGÍA DE INFORMACIÓN	¿La entidad cuenta con una planificación estratégica de Tecnología de Información (TI) que considere planes a largo y corto plazo acordes con la misión y las estrategias de negocio de la organización?	Planificación estratégica de la tecnología de información, aprobada y respaldada por un procedimiento formal.	25	17	68%
		Plan operativo anual y presupuesto aprobados formalmente.	25	17	68%
		Cuenta con una estructura orgánico - funcional de TI acorde con los servicios que brinda, así como con un comité directivo que supervise sus servicios.	25	17	68%
		Existe un manual de políticas y procedimientos de tecnología de información aprobado formalmente, difundidos y comunicados.	25	18	72%
		Cuenta con un plan de entrenamiento y capacitación anual para el personal de TI acorde con las necesidades para la ejecución de sus funciones, y considera un plan de entrenamiento anual para usuarios de los servicios de información.	25	16	64%
	¿La entidad ha definido procedimientos para garantizar que las operaciones de TI satisfagan los requerimientos de la entidad?	Los usuarios y la función de tecnología de información cuentan con acuerdos escritos que describan los niveles de servicio en términos cualitativos y cuantitativos y responsabilidades de ambas partes.	25	13	52%
		El área de TI ha definido procedimientos para la administración de incidentes y problemas incluyendo su registro, análisis y solución oportuna.	25	16	64%
		El área de TI ha establecido y documentado procedimientos para las operaciones de tecnología de información.	25	17	68%
		El área de TI ha establecido procedimientos para soporte a usuarios, dentro de una función de Help Desk o Mesa de Control y Ayuda.	25	17	68%
		Existen procedimientos para la administración de activos de tecnología que incluyan su registro, clasificación, control y responsables de su uso y mantenimiento.	25	16	64%
	¿La administración de servicios tecnológicos provistos por terceros considera los criterios de contratación institucionales, responsabilidades y monitoreo de la prestación del servicio para garantizar que satisface los requerimientos de la entidad?	Los servicios de TI provistos por terceros se administran de acuerdo con las políticas institucionales de contratación de servicios.	25	18	72%
		Los contratos de servicios de TI provistos por terceros definen la propiedad de la información así como las responsabilidades de cada parte.	25	18	72%
		La entidad ha designado una contraparte técnica que sea responsable de administrar las relaciones con terceros.	25	17	68%
		Los contratos consideran la transferencia de conocimiento y entrega de documentación técnica y de usuario, así como la aceptación del usuario (si aplica).	25	18	72%
		Se ha definido un procedimiento formal y continuo de monitoreo sobre la prestación de servicio de terceros, con el fin de asegurar el cumplimiento de los acuerdos del contrato.	25	17	68%
	¿La entidad cuenta con un sistema de administración de seguridad de la información que garantice su integridad, disponibilidad y confidencialidad?	La entidad cuenta con políticas y procedimientos de seguridad de la información aprobadas formalmente, difundidas e implementadas; incluyendo aquellas relacionadas con servicios de transferencia y transacciones electrónicas, si aplica.	25	13	52%
		La entidad ha identificado los requerimientos de seguridad relacionados con la tecnología de información y ha implementado los controles necesarios para minimizar el impacto de las vulnerabilidades e incidentes de seguridad.	25	17	68%
		La entidad cuenta con un sistema de administración de las seguridades de acceso a la información y niveles de autorización de accesos para ejecución de las funciones de procesamiento.	25	16	64%
		La entidad dispone de un plan de evaluación del desempeño del sistema de administración de la seguridad de la información que permita tomar acciones para mejorarlo.	25	15	60%
		La entidad cuenta con condiciones físicas y ambientales necesarias para garantizar la seguridad de la información y el correcto funcionamiento del entorno de la infraestructura de tecnología de información.	25	17	68%
	¿La entidad cuenta con políticas y procedimientos para la adquisición, desarrollo, implementación y mantenimiento de las aplicaciones que garanticen que éstas satisfacen los requerimientos del negocio?	La entidad dispone de una metodología para la administración del ciclo de vida de desarrollo, mantenimiento y/o adquisición de aplicaciones incluyendo procedimientos para migración de información si aplica.	25	16	64%
		La entidad cuenta con un procedimiento de monitoreo para evaluar el cumplimiento de la metodología del ciclo de vida de desarrollo de sistemas.	25	17	68%
		La entidad tiene procedimientos formales para administración de versiones que garanticen el registro, evaluación y autorización de los cambios previo a su implantación y la revisión posterior contra los resultados planeados.	25	17	68%
		La entidad considera la ejecución de un plan de entrenamiento de las nuevas implementaciones efectuadas, a los usuarios involucrados y al grupo de operaciones de la función de TI.	25	17	68%
		La entidad cuenta con procedimientos formales que garanticen que la documentación técnica y de usuario se mantiene actualizada y disponible para los usuarios.	25	17	68%
	¿La entidad cuenta con políticas y procedimientos que garanticen una adecuada administración, monitoreo y documentación de la infraestructura tecnológica?	Cuenta con procesos para adquirir, implementar y actualizar la infraestructura tecnológica de acuerdo con las estrategias tecnológicas establecidas.	25	16	64%
		Dispone de políticas y procedimientos formales para la administración del desempeño y la capacidad de los recursos de TI que incluya su revisión periódica, el desempeño actual y el pronóstico de las necesidades futuras.	25	17	68%
		Existen políticas y procedimientos de administración de configuraciones de la infraestructura tecnológica que permita garantizar una mayor disponibilidad, minimice los problemas de producción y los resuelva más rápido.	25	17	68%
		Ha efectuado un levantamiento de la documentación correspondiente a la infraestructura tecnológia incluyendo bases de datos, redes de datos, software de base y hardware.	25	18	72%
		Ha establecido políticas formales y controles para detectar y evitar la instalación de software no autorizado o no licenciado, así como instalar y actualizar periódicamente aplicaciones de detección y eliminación de virus informático y demás software malicioso.	25	16	64%
PORCENTAJE IMPLEMENTADO EN TECNOLOGIA			750	498	66%

Cuadro 4 Análisis componente tecnología de la Información

Fuente: SBS, Cuestionario emitido al sistema financiero, evaluación de implementación RO, 2010

Análisis de Preguntas Relevantes de este Componente

¿La entidad cuenta con una planificación estratégica de Tecnología de Información (TI) que considere planes a largo y corto plazo acordes con la misión y las estrategias de negocio de la organización?

¿La entidad ha definido procedimientos para garantizar que las operaciones de TI satisfagan los requerimientos de la entidad?

¿La entidad cuenta con un sistema de administración de seguridad de la información que garantice su integridad, disponibilidad y confidencialidad?

¿La entidad cuenta con políticas y procedimientos para la adquisición, desarrollo, implementación y mantenimiento de las aplicaciones que garanticen que éstas satisfacen los requerimientos del negocio?

¿La entidad cuenta con políticas y procedimientos que garanticen una adecuada administración, monitoreo y documentación de la infraestructura tecnológica?

Las preguntas detalladas anteriormente están direccionadas a verificar y dar cumplimiento aspectos fundamentales como son: una correcta planificación estratégica de la tecnología, (esta planificación debe ser incluida en el plan operativo anual) , manejo de información restringido a terceros, esto implica que la información debe ser de carácter estrictamente laboral y debe haber un contrato de por medio en el cual se describa la confidencialidad de la información, (se recomienda que el contrato sea monitoreado, para garantizar su cumplimiento).

Además se evalúa: el desempeño de la tecnología adquirida para esto la entidad deberá diseñar políticas y procedimientos de implementación y control: en los procedimientos de implementación se recomienda incorporar capacitaciones al personal sobre la tecnología adquirida para garantizar una correcta administración de la misma, en el

proceso de control se debe realizar reportes periódicos del impacto que ha tenido la nueva tecnología en el mejoramiento de los procesos internos.

Por último se recomienda que la entidad este informada de los cambios tecnológicos y tendencias a nivel nacional e internacional para efectivizar sus procesos en futuras adquisiciones.

Es por ello que de los 25 bancos privados del ecuador de acuerdo a cada pregunta de la evaluación el 66 % de las entidades cuentan con este componente riesgo operativo en sus procesos de acuerdo a los lineamientos antes descritos

ADMINISTRACIÓN DEL RIESGO OPERATIVO

(Sección III): ADMINISTRACIÓN DEL RIESGO OPERATIVO			REQUERIDO EN EL PROCESO DE IMPLEMENTACION DE RO.	ENTIDAS QUE CUENTAN CON LO SOLICITADO	PORCENTAJE DE IMPLEMENTACÓN
ADMINISTRACIÓN DEL RIESGO OPERATIVO	¿La entidad ha definido un esquema formal para la administración del riesgo operativo acorde con la administración integral de riesgos, que permita: identificar, medir, controlar y monitorear las exposiciones al mencionado riesgo?	Ha identificado formalmente por línea de negocio los eventos de riesgo operativo, agrupados por tipo de evento y, las fallas o insuficiencias en los factores de riesgo operativo.	25	15	60%
		Ha conformado bases de datos centralizadas, suficientes y de calidad con información sobre los eventos de riesgo operativo y de fallas o insuficiencias en los factores de riesgo operativo conforme lo dispuesto en la resolución JB-2005-834; que sean alimentadas de acuerdo con procedimientos formales que involucran a toda la organización.	25	14	56%
		Cuenta con niveles de control formalmente establecidos y validados periódicamente para asegurar un adecuado sistema de control interno que mitigue los eventos de riesgo operativo.	25	14	56%
		Auditoría Interna realiza periódicamente pruebas orientadas a determinar el cumplimiento de las políticas, procedimientos y requerimientos regulatorios para la administración del riesgo operativo.	25	16	64%
		Cuenta con esquemas organizados de reportes para la gestión del riesgo operativo.	25	15	60%
PORCENTAJE IMPLEMENTADO ENADMINISTRACIÓN DEL RO.			125	74	59%

Cuadro 5 Análisis Administración del Riesgo Operativo

Fuente: SBS, Cuestionario emitido al sistema financiero, evaluación de implementación RO, 2010

Analizando este componente que hace referencia a la administración del Riesgo Operativo, y de acuerdo con lo establecido por la evaluación de la SBS, determina que para una correcta administración integral del Riesgo Operativo se debe establecer un sistema de gestión que permita: identificarlo, medirlo controlarlo y monitorearlo.

De acuerdo a la evaluación de este componente, las preguntas enfocadas están precisando, si las entidades han determinado sus líneas de negocio esto abarca la etapa de identificación con esta etapa permitirá a la alta gerencia tener una idea clara los diferentes tipos de exposición entre los más relevantes son: fraude interno, externo, y priorizar a cada uno de estos, permitiendo modificar controles, planes de contingencia para preservar la continuidad del negocio.

La siguiente etapa es la de medición esta abarca otra pregunta de la evaluación la cual hace referencia a las bases de datos las mismas que deben ser alimentadas y actualizadas de manera eficiente, oportuna y progresiva de manera que a futuro permita estimar las perdidas esperadas e inesperadas atribuibles a este riesgo.

- Las bases de datos deben estar conformadas por línea de negocio: por evento de RO., fallas por factores de RO., frecuencia que se repite cada evento, efecto de pérdida.

- Cabe señalar que esta norma no está orientada a desarrollar de metodologías para estimación de capital que se requiere para el RO.

- En la etapa de control se debe crear políticas y procedimientos regulatorios de RO. que están sujetos a auditorías internas las mismas que tendrán como objetivo la supervisión.

- En la etapa de monitoreo consta una pregunta de la evaluación que hace referencia a reportes de control, los mismos que deben detallar evaluación del grado de cumplimiento de los procesos, tipo de evento, indicadores de gestión de cada proceso.

- Es por ello que de los 25 bancos privados del ecuador de acuerdo a cada pregunta de la evaluación el 59 % de las entidades cuentan con este componente riesgo operativo en sus procesos de acuerdo a los lineamientos antes descritos

RESPONSABLE DE LA ADMINISTRACION DEL RIEGO OPERATIVO

(Sección V): RESPONSABILIDADES EN LA ADMINISTRACIÓN DEL RIESGO OPERATIVO			REQUERIDO EN EL PROCESO DE IMPLEMENTACION DE RO.	ENTIDAS QUE CUENTAN CON LO SOLICITADO	PORCENTAJE DE IMPLEMENTACÓN
RESPONSABILIDADES EN LA ADMINISTRACIÓN DEL RIESGO OPERATIVO	¿Se han definido y establecido formalmente las funciones para una adecuada administración del riesgo operativo, enmarcadas en lo establecido en la resolución JB-2005-834?	Definición de responsabilidades del directorio u organismo que haga sus veces, en cuanto a la administración del riesgo operativo.	25	17	68%
		Definición de funciones y responsabilidades para el comité de administración integral de riesgos, en cuanto a la administración del riesgo operativo.	25	17	68%
		Definición de funciones y responsabilidades para unidad de riesgos, en cuanto a la administración del riesgo operativo.	25	17	68%
		Las funciones y responsabilidades para la administración del Riesgo Operativo han sido difundidas y comunicadas al personal involucrado (nivel directivo, ejecutivo y operativo).	25	16	64%
		El Comité de Administración Integral de Riesgos mantiene reuniones periódicas con la unidad de riesgos para tratar temas relacionados con la administración del riesgo operativo y son formalizadas en actas.	25	16	64%
PORCENTAJE IMPLEMENTADO EN RESPONSALBLE DE LA ADM. DEL RO.			125	83	66%

Cuadro 6 Análisis componente responsable de la Administración del RO.

Fuente: SBS, Cuestionario emitido al sistema financiero, evaluación de implementación RO, 2010

En este componente y de acuerdo con lo establecido por la SBS, manifiesta que entre las principales funciones de este organismo sea este la unidad de riesgos debe crear una cultura organizacional enmarcada en principios y valores de comportamiento ético que propicie la gestión eficaz del riesgo operativo en todos sus componentes y etapas de control.

Por consiguiente el enfoque de evaluación focaliza directamente lo antes expuesto, determinando al responsable de la administración del riesgo operativo, sus funciones principales además quien liderara los planes de contingencia, adicionalmente emitir informes del área legal

- Es por ello que de los 25 bancos privados del ecuador de acuerdo a cada pregunta de la evaluación el 66 % de las entidades cuentan con este componente riesgo operativo en sus procesos de acuerdo a los lineamientos antes descritos

CONTINUIDAD DEL NEGOCIO

(Sección IV): CONTINUIDAD DEL NEGOCIO			REQUERIDO EN EL PROCESO DE IMPLEMENTACION DE RO.	ENTIDAS QUE CUENTAN CON LO SOLICITADO	PORCENTAJE DE IMPLEMENTACÓN
CONTINUIDAD DEL NEGOCIO	¿La entidad ha definido un proceso formal para la administración de la continuidad del negocio que permita mantener activa sus operaciones esenciales en caso de desastres?	Ha definido un proceso formal y permanente para administrar la continuidad del negocio alineado al cumplimiento de los objetivos institucionales y a la estrategia de la entidad.	25	14	56%
		Ha identificado los principales escenarios de contingencia tomando en cuenta el impacto y la probabilidad de que sucedan.	25	13	52%
		Ha defindio un plan de continuidad del negocio y éste se encuentra formalizado, difundido e implementado.	25	13	52%
		Ha definido un plan de emergencia para la evacuación y reubicación del personal y de recursos de TI, que permita reanudar las operaciones de la entidad con los recursos necesarios (procedimientos, instalaciones, suministros, mobiliario, equipos, etc) para su ejecución.	25	12	48%
		Ha efectuado pruebas periódicas del plan y de los procesos implantados para verificar su aplicabilidad y hacer los ajustes necesarios.	25	13	52%
	¿La entidad ha definido un plan de continuidad del negocio (BCP) que permita garantizar su capacidad para operar en forma contínua y minimizar las pérdidas en caso de interrupciones severas del negocio?	⊟ BCP incluye acciones a ejecutar antes, durante y después de ocurrido el incidente, recursos necesarios así como los responsables de ejecutar cada actividad, procedimientos de capacitación y difusión al personal involucrado.	25	16	64%
		⊟ BCP incluye un plan de recuperación de desastres que permita la reubicación de las operaciones en un nuevo lugar, es decir cuenta con una alternativa de recuperación en un sitio distinto a la ubicación física primaria.	25	16	64%
		⊟ BCP considera procedimientos formales de respaldo para los programas, datos y documentación necesarios para la ejecución del plan de continuidad.	25	16	64%
		⊟ BCP incluye un plan de reanudación que permita regresar las operaciones a la normalidad en la instalación original.	25	16	64%
		⊟ BCP incluye políticas y procedimientos para la realización de pruebas periódicas del plan y los procesos implantados que permitan comprobar su aplicabilidad y realizar los ajustes necesarios.	25	15	60%
PORCENTAJE IMPLEMENTADO EN CONTINUIDAD DEL NEGOCIO			250	144	58%

Cuadro 7 Análisis componente continuidad del negocio

Fuente: SBS, Cuestionario emitido al sistema financiero, evaluación de implementación RO, 2010

Analizando este componente que hace referencia a la continuidad del negocio y de acuerdo con lo establecido por la SBS manifiesta que se debe crear estrategias de continuidad del negocio, identificar los procesos críticos del negocio incluido los que están provistos por terceros, un plan de continuidad deberá incluirlas personas responsables de ejecutar cada actividad (telefonos, mail), acciones a ejecutar, acciones a realizar, un cronograma y procedimientos de prueba, y por último la difusión, comunicación y concienciación del plan de cumplimiento.

Cabe señalar puntualmente que la continuidad del negocio es de vital importancia para una entidad financiera ya que de este dependerá que la entidad se proyecte a futuro y prevea posibles eventos externos los cuales afectarían su rentabilidad.

Para esto es indispensable que exista un proceso el cual se encargue de la continuidad del negocio y un plan referente a la continuidad del negocio donde se ejecutara los procedimientos necesarios en caso de una desastre, (este proceso implica capacitación del personal involucrado, reanudación actividades, planes de contingencia entre otros), en estos procesos se debe realizar pruebas, además medir su aplicabilidad y poder realizar las correcciones del caso si así se lo requiere.

- Es por ello que de los 25 bancos privados del ecuador de acuerdo a cada pregunta de la evaluación el 58 % de las entidades cuentan con este componente riesgo operativo en sus procesos de acuerdo a los lineamientos antes descritos

3.2 Ejemplo de una Matriz de Riesgo Operativo

Mediante este ejemplo se explicara una matriz de riesgo. y todo el pasos que se debe realizar para implementarla en una entidad, la matriz variara de acuerdo a cada línea de negocio y sus procesos.

El ejemplo detalla: El proceso de Emisión de una Póliza Individual

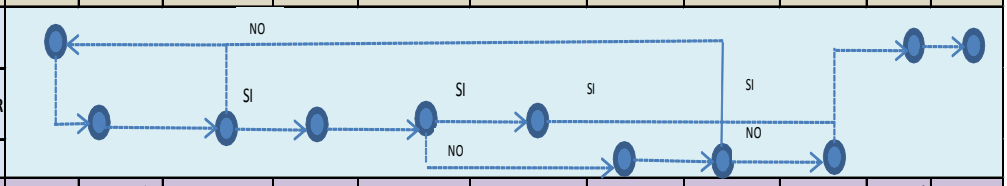
	PROCESO PARA LE EMISIÓN DE PÓLIZAS										
ACTIVIDADES	Entrega de solicitudes de seguros al analista	Recibe solicitudes y valida la información necesaria	Esta completa la solicitud y su documentación	Captura de informacion de la solicitud en el Sistema	¿Esta la suma asegurada dentro de los limites de suscripcion autorizados?	SI.-Cambia estatus de solicitud "P" NO.-Toma la solicitud al Gerente de Suscripción	Recive solicitud y documentación para realizar la póliza	¿Requiere información adicional para realizar la suscripción?	SI.-Cambia estatus de solicitud "P" NO.-Toma la solicitud al Gerente de	Imprime y arma las Pólizas	Entrega Pólizas
AGENTE											
ANALISTA SUSCRIPTOR											
GERENTE SUSCRIPTOR											
RIESGO OPERATIVO IDENTIFICADO	No llenar totalmente la solicitud	Se recive la solicitud sin toda la documentación requerida,s	Deja pasar la solicitud sin todos los documentos requeridos	Error de captura de información en el sistema		Emite póliza con suma asegurada superior al limite establecido por el analista				impresión lote de pólizas de un día diferente al de	
CONTROLES		Realizar la debida supervisión por un supervisor		Hojas de validación		Automatización de limites de suma asegurada				Rediseño del Sistema	

Grafico 11 Proceso de Emisión de una Póliza en una Entidad Financiera

Fuente: Autor

Mediante la grafica se puede visualizar todos los procesos requeridos para la emisión de una póliza individual y los responsables de cada uno de ellos, aquí podemos determinar cuál es la falencia en este proceso, mediante un análisis minucioso identificamos los factores de riesgo operativo y en lo posterior los controles que debemos efectuar para mitigarlos.

Por consiguiente las entidades deben tener esta matriz por cada línea de negocio que posean y entregar a la unidad correspondiente de riesgos para que allí se tomen las medidas correctivas pertinentes.

MATRIZ INICIAL GENERALIDADES

No. De Riesgo	Descripción del Riesgo	Origen	Tipo	Fuente
EM01	Recibir solicitud sin tener todos los datos llenos	Interno	Riesgo Humano	Errores, Experiencia
EM02	Error en la captura de información del sistema	Interno	Riesgo Humano	Errores
EM03	Autorizar emisión con suma asegurada fuera del limite de suscripción	Interno	Riesgo Humano	Experiencia, Abuzo
EM04	Imprimir un lote de pólizas de un dia diferente al de	Interno	Riesgo Tecnológico	Fallas

Cuadro 8 Matriz Inicial de identificación.

Fuente: Autor

Mediante esta tabla se detalla mediante los riesgos identificados en el proceso principal: el origen, tipo, fuente del riesgo operativo categorizándolos a cada uno de estos de acuerdo a su descripción.

MATRIZ FRECUENCIA-IMPACTO

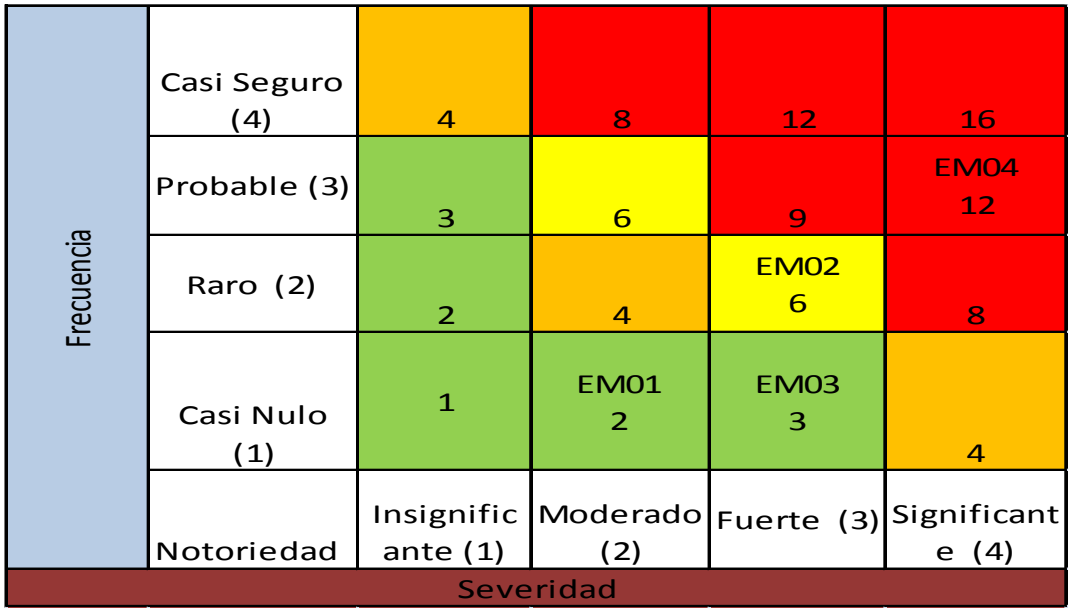
No. De Riesgo	Descripción del Riesgo	Frecuencia	Severidad	Peso
EM01	Recibir solicitud sin tener todos los datos llenos	Casi nula	Moderado	2
EM02	Error en la captura de información del sistema	Raro	Fuerte	6
EM03	Autorizar emisión con suma asegurada fuera del limite de suscripción	Casi nula	Fuerte	3
EM04	Imprimir un lote de pólizas de un dia diferente al de	Probable	Significante	12

Cuadro 9 Matriz Frecuencia e Impacto

Fuente: Autor

Mediante esta tabla se categorizara a cada factor de riesgo operativo con su frecuencia de incidencia, es decir, que tan repetitivo es este error y su impacto que genera en el proceso y en el cumplimiento de objetivos trazados por la línea de negocio.

MATRIZ PRIORIDAD DE GESTION



Cuadro 10 Matriz Prioridades de Gestión

Fuente: Autor

Mediante la tabla final se encuentran resaltados de acuerdo al grado de prioridad los riesgos del proceso, los que tienen el color rojo son los que requieren atención inmediata, es decir, se los debe gestionar inmediatamente, mientras que los restantes se los debe gestionar de acuerdo a lo requerido.

Para cada riesgo se determina una o varias actividades de control a realizar:

- Modificación al sistema
- Capacitación al personal
- Reporte con cifras de control
- Redefinir funciones

MATRIZ CONTROL

No. De Riesgo	Descripción del Riesgo	CONTROL
EM01	Recibir solicitud sin tener todos los datos llenos	Supervisión
EM02	Error en la captura de información del sistema	Hoja de Validación
EM03	Autorizar emisión con suma asegurada fuera del limite de suscripción	Automatizacion de control de limites de sumas aseguradas por usuarios del sistema
EM04	Imprimir un lote de pólizas de un dia diferente al de emisión	Solicitar que el sistema permita marcar pólizas que ya se imprimierón

Cuadro 11 Matriz Control

Fuente: Autor

- Periódicamente se deben revisar los procesos para validar si el riesgo identificado ha disminuido en su calificación de frecuencia y severidad.

- Se deben generar indicadores de Riesgo Operativo, los cuales permitan dar un seguimiento periódico de la evolución del nivel de riesgo, además de alertar de situaciones graves y el impacto en el nivel de riesgo con las acciones correctoras.

Entre los indicadores más relevantes de Riesgo Operativo tenemos:

- Estadísticas de actividad

- Bases de datos de incidencias y eventos de perdida

- Reporte de cifras de control

- Reportes para análisis de conciliaciones

- Grado de implementación de recomendaciones de los auditores

Cada uno de estos indicadores deberán ser supervisados de manera progresiva ya que si los verificamos a tiempo identificaríamos los factores de riesgo que podrían incurrir en pérdidas inesperadas y que afectarían directamente a la entidad.

- La mitigación y eliminación de riesgo se irá presentando de acuerdo a la continuidad que tengamos en la supervisión y control de cada riesgo.

- Las matrices de riesgo, los controles e indicadores son base de información indispensable que debe reunir el área o la unidad de riesgos para diseñar modelos de Riesgo Operativo que mas se ajuste a su perfil de riesgo

- El objetivo de la administración de riesgos es detectarlos oportunamente y evitar que se materialicen, esto se consigue únicamente con una oportuna gestión y controles adecuados.

- Se deben realizar bases de datos de incidencias de eventos de perdidas.

- Con estas bases de datos se podrá diseñar un modelo probabilístico para estimar el Riesgo Operativo.

3.3 Análisis Macroentorno

3.3.1 Experiencias Internacionales sobre Riesgo Operativo

Experiencia en Colombia

Entre los avances académicos desarrollados en Colombia sobre riesgo operacional, se considera los siguientes aspectos relevantes en los estudios realizados recientemente, por investigadores.

El estudio es el Diseño de una metodología para la identificación y la medición del riesgo operativo en instituciones financieras.

- Teniendo en cuenta la escasez de información histórica sobre los eventos de pérdida debidas al riesgo operativo que se presenta en la mayoría de las entidades financieras colombianas, este trabajo desarrolla una metodología que permite, no sólo identificar las principales fuentes de riesgo operativo, sino también cuantificar la exposición al mismo y calcular las provisiones que debe realizar la entidad para cubrir cualquier evento de pérdida que se pueda presentar.

- Finalmente, utilizando simulación de Montecarlo se obtiene la distribución de las pérdidas totales para la línea de negocio seleccionada en el banco durante el horizonte de tiempo definido para el análisis y se calcula la provisión que debe hacer la entidad financiera para cubrir los posibles eventos de pérdida debidos al riesgo operativo.

- La gestión integral del riesgo financiero, y en particular del riesgo operacional, se ha convertido en los últimos años en un gran reto para los operadores e investigadores en finanzas, ante los conocidos grandes desastres financieros de muchas entidades, mucha parte de ellos atribuidos causas operacionales.

- La Superintendencia Financiera de Colombia, como ente regulador en el ámbito nacional, en los últimos años ha concentrado sus esfuerzos en la implementación de los sistemas de administración de riesgo de crédito y riesgo de mercado; pero empieza a incursionar en la normativa relativa a riesgo operacional, como ya lo ha hecho en algunos aspectos de riesgo operacional en las entidades aseguradoras.

- No sólo la emergente regulación internacional, y la inminente normativa nacional, sino también, y fundamentalmente, el propósito de mejorar continuamente los procesos de toma de decisiones en las instituciones, han motivado en los últimos años el interés por la investigación en el campo del riesgo financiero y, específicamente, en identificación, valoración y gestión del riesgo operacional

- Uno de los problemas cruciales para la cuantificación del riesgo operacional ha sido, indudablemente, la escasez de datos confiables. Pero ante la convicción creciente de la necesidad de cuantificar ese riesgo, las entidades han iniciado serios procesos de recolección de datos, y se considera que con el transcurrir del tiempo será un problema superado, y los modelos de medición avanzada tomarán plena vigencia y aplicación.

- Entretanto, sigue siendo un gran reto la formulación de un modelo con una complejidad manejable y con las características de complejidad, exactitud, y satisfacción de los estándares generales, cualitativos y cuantitativos planteados por el Nuevo Acuerdo de Basilea. Eso puede explicar el porqué, incluso hasta el año 2005, grandes entidades financieras en el ámbito internacional, estaban manejando el Método Estándar de Basilea II, para cuantificar su riesgo operacional.[13]

Análisis Comparativo con Ecuador

- Un aspecto que nos menciona en Colombia es la problemática que muchas entidades poseen actualmente es la falta de información historial la cual se la obtiene de los procesos y de bases de datos que cada entidad debe seguir diseñando y alimentando estas deben estar clasificadas por líneas de negocio, es decir por cada proceso que la entidad cuente.

- En ecuador se ha evidenciado carencia de bases de datos de eventos repetitivos generadores de perdidas y de un departamento de Riesgo Operativo.

[13]WHITTINGTON R y PANY K., *Auditoria Un Enfoque Integral*, Editorial MC Graw Hill.Bogotá, 2007

Experiencia Internacional Argentina

- Los Bancos muestran un avance significativo respecto al último relevamiento realizado durante el año 2006 (enfocado al grado de desarrollo de estructuras organizativas y sistemas para la medición del RO y que evidenciaba que la mayor parte del sistema financiero argentino estaba todavía en una etapa primaria y salvo casos particulares, no se observaba, a esa fecha, el desarrollo de sistemas integrales de administración del Riesgo Operacional).

- La última encuesta abarcó aspectos relacionados con la estructura existente para la gestión del riesgo, el diseño de las políticas, la asignación de responsabilidades, los sistemas tecnológicos utilizados, entre otros aspectos. Se relevaron también toda una serie de aspectos relacionados con la recolección y uso de datos internos sobre eventos y perdidas por RO.

- La encuesta fue completada por casi todas las entidades financieras de Argentina durante el mes de abril de 2009.

- En definitiva, las entidades argentinas tienen por delante un largo camino por recorrer para alcanzar un nivel de gestión del riesgo operacional con un grado de madurez similar al que existe en algunos de los países de la región. Esto, sin duda, implicará altas inversiones de tiempo, dinero y recursos humanos.

- Las normativas que los reguladores emitan en los próximos años acelerarán en muchos casos la implantación de un marco adecuado para la gestión del riesgo operacional. Sin embargo serán aquellas entidades que comprendan el verdadero valor de administrar este riesgo como una herramienta de gestión las que podrán considerar el dinero utilizado en su implementación como una inversión y no como un gasto.

- Un elemento fundamental para que las entidades puedan pasar de un enfoque cualitativo a un marco de gestión integral del riesgo operacional la creación de una base de datos de pérdidas operacionales. Este paso representa uno de los mayores desafíos a los cuales se enfrentan las entidades de la Argentina y Latinoamérica.

- Por otra parte, y dadas las particularidades de nuestro mercado, si bien es posible observar en el sector interés en complementar su información interna con datos externos, existen dificultades para poder lograrlo, tanto por cierto recelo de parte de las entidades en compartir informaciones de estas características.

- El desarrollo de una adecuada gestión cualitativa implica tres aspectos: la identificación de riesgos, el modelo organizativo y las herramientas de gestión utilizadas. El primer paso consiste en la elaboración de un mapa de procesos de la entidad que sirva para detectar los riesgos y controles existentes, así como también para realizar una valoración en términos de severidad y frecuencia de los eventos de pérdidas.

- A nivel organizativo, resulta vital la creación de una unidad independiente, responsable por riesgo operacional, dado que ésta será la que genere los mecanismos para una adecuada administración del riesgo , la organización, sobre la cual podemos poner especial atención en las unidades de negocio como responsables últimos por los riesgos operacionales, ya que el área encargada de la gestión de este riesgo sólo tiene responsabilidades asociadas con definiciones de políticas, utilización y selección de herramientas, diseño de tableros de reporte, así como de sugerir planes de acción y realizar actividades de seguimiento de los riesgos identificados.[14]

Análisis comparativo con Ecuador

- Algo de vital importancia es la creación de una unidad de riesgo operativo responsable de la administración y cumplimiento de lo establecido en el manual de riesgos diseñado por cada entidad, adicionalmente crear una cultura de riesgo operativo enmarcada en las directrices de la gestión de riesgos.

- En relación a Ecuador en Argentina no se cuenta con un responsable encargado de reportar a la gerencia del perfil de riesgo de una entidad financiera.

[14] HERNANDEZ R, Metodología de la Investigación. RO, Editorial Dunken, Argentina,2008

3.4 Comité de Basilea

El Comité de Basilea fue creado en 1.975, en la ciudad de Basilea (Suiza), por el grupo de los diez (G10), que corresponde a los diez países más industrializados: Alemania, Bélgica, Canadá, Estados Unidos, Francia, Gran Bretaña, Holanda, Italia, Japón y Suecia. Su objetivo era uniformizar los criterios que se utilizan en la supervisión de las instituciones financieras de carácter internacional en sus respectivos países.

A Través de Basilea II se pretende introducir nuevas disciplinas y procesos de control que afectarán la gestión y la cultura de las entidades.

El Nuevo Acuerdo de Capital Basilea II busca generar una base mucho más sólida respecto de la regulación prudente del capital, la supervisión y la disciplina de mercado, pero a la vez, trata de perfeccionar la gestión del riesgo en general y la estabilidad financiera. Igualmente, le señala claras ideas al supervisor en lo que se refiere a modelos de gestión y cuantificación del riesgo operativo. Pero quizás, el elemento más importante de acuerdo al tema aquí tratado, es la inclusión de requisitos de capital por riesgo operacional, que cuantifica en un rango del 5% al 15% de los activos totales ponderados, en función del riesgo o riesgos de la entidad.

- Para esto utilizaremos el método de Indicador Básico el cual considera un rango del 5% como porcentaje mínimo y un 15% como porcentaje máximo tomando como referencia los requerimientos que se tenga de riesgo de crédito y mercado es un promedio de los tres últimos años para luego multiplicar este porcentaje por los ingresos netos anuales positivos de la Institución.

3.4.1 Ejemplo calculo requerimiento mínimo de capital para Riesgo Operativo en una Entidad Financiera

CALCULO REQUERIMIENO MINIMO DE CAPITAL PARA RO.				
	2008	2009	2010	PROMEDIO
RIESGO DE CREDITO	5%	8%	12%	8,33%
RIESGO DE MERCADO	6%	9%	14%	9,67%
PROMEDIO TRES ULTIMOS AÑOS				9,00%
PORCENTAJE REQUERIDO PARA RO.	9%	Este porcentaje multiplicado por los ingresos netos anuales de la entidad		

Cuadro 12 Ejemplo Calculo Requerimiento Mínimo de Capital para RO.

Fuente: el Autor

Con este ejemplo determinamos el **Capital Mínimo requerido** para el año 2011 mediante Basilea II.

De esta manera el capital de los bancos será el suficiente para protegerse de los diversos riesgos que podría incurrir y podría afectar la continuidad del negocio.

3.4.2 Análisis Normatividad Basilea II

Componentes Esenciales de Basilea II

Basilea II cuenta se estructura en tres pilares fundamentales:

Pilar I. Requerimientos mínimos de capital: Establece el capital mínimo de las entidades de crédito, dado los diferentes niveles de riesgos asumidos en la gestión de riesgo de crédito, de mercado y operativo.

El capital mínimo exigido a cada entidad debe ser del 5% de la suma de la evaluación de los riesgos de crédito, de mercado y operacional, lo importante es que se ha considerado dentro de este esquema a riesgo operacional como un riesgo importante, de similar tratamiento y evaluación, que afecta al capital de la institución.

En este pilar nos explica que las entidades deben contar con un nivel patrimonial suficiente para amortiguar las pérdidas que le pueden generan los riesgos de sus operaciones estos riesgos son: crediticios, mercado, operativos en donde cada uno de estos juega un papel importante para determinar el capital mínimo requerido para cada uno de estos.

Pilar II. Proceso de Supervisión bancaria: Se enmarca dentro de las relaciones permanentes que debe existir entre las entidades financieras y el órgano responsable de la supervisión bancaria. Cuatro principios marcan el camino de estas relaciones:

- las entidades deberán contar con un esquema adecuado para evaluar su requerimiento de capital (gestión integral de riesgo) y contar con una estrategia coherente para su mantenimiento.

- El organismo supervisor deberá juzgar los procesos y estrategias de las entidades para verificar su cumplimiento satisfactorio de cada proceso.

- los supervisores podrán exigir un cumplimiento por encima del capital mínimo.

- Además la posibilidad de intervención inmediata y con prontitud cuando el capital requerido esté por debajo del mínimo, exigiendo medidas correctivas eficaces.

En este pilar nos explica la necesidad de una entidad financiera de evaluar su posición de capital frente a sus riesgos globales. Los supervisores son los encargados directos de adoptar las medidas correctivas necesarias a los resultados de las evaluaciones, ver las necesidades de capital de la entidad para enfrentar los posibles riesgos que se presenten

Pilar III. Disciplina de mercado: Establece requisitos para la divulgación de información sobre los riesgos y su gestión para que los participantes y agentes del mercado conozcan el perfil de riesgo de las entidades a nivel particular.

En este pilar nos explica la necesidad de los bancos entreguen información al mercado para que este pueda evaluar los niveles de riesgo, además evalúa la adecuación de capital y la forma que cada banco tiene para administrarlos, para estos los bancos deben contar con políticas de trasparencia de información aprobada por la alta gerencia.

Esta información debe contener la estructura del capital, esto hace referencia a la clase, componentes y características del capital lo que reflejara al mercado la capacidad de la entidad para absorber perdidas financieras.

- Basilea II, empezó a diferenciar el tratamiento que se le daba al riesgo operativo en el sector financiero.

- Nos define el riesgo operativo como el riesgo de pérdida resultante de una falta de adecuación o un fallo de los procesos, el personal y aún de los sistemas internos, o bien de acontecimientos externos que en suma o de manera particular afectan el normal funcionamiento de una entidad financiera.

- El Comité de Supervisión Bancaria de Basilea señala que el método utilizado para la gestión de riesgos operativos que elija cada banco dependerá de varios factores, como son su tamaño y sofisticación así como la naturaleza y complejidad de sus actividades, pero hace notar que pese a estas diferencias es importantes considerar que para una adecuada gestión de riesgos, sea cual sea el tamaño y ámbito de actuación del banco;

Se recomienda que la entidad cuenten con estrategias claramente definidas y se realice un seguimiento de cada una de ellas por parte de la Alta Gerencia.

Además se debe proporcionar una sólida cultura de gestión del riesgo operativo, control interno, segregación de funciones, planes de contingencia para asegurar así la continuidad del negocio.

Adicionalmente se debe contar con una comunicación efectiva por parte de cada área de la organización y transmitir la información que consideren relevante a una unidad encargada de cada proceso y esta a su vez a la alta gerencia.

Principios de Riesgo Operativo

Desarrollo de un Ambiente apropiado de Gestión de Riesgos

Principio No. 1.- Responsabilidad Alta Gerencia*:* El Directorio debe ser consciente de responsabilidad de los principales aspectos de los riesgos de operación del banco, como una categoría de riesgo distinta que debe ser gestionada, y debe aprobar y revisar periódicamente el esquema de gestión del riesgo operativo del banco.

El esquema debe proporcionar una definición a nivel corporativo del riesgo operativo y establecer los principios sobre la manera como los riesgos de operación serán identificados, evaluados, monitoreados, y controlados o mitigados.

La entidad debe contar con un proceso de evaluación de suficiencia de capital total de acuerdo a su perfil de riesgo y una estrategia para mantener sus niveles de capital.

Principio No. 2.- Aseguramiento efectivo del control: El Directorio debe asegurar que el esquema de gestión del riesgo operativo del banco esté sujeto a una auditoría interna efectiva e integral por parte de personal competente, operativamente independiente y apropiadamente entrenado. La función de auditoría interna no debe ser directamente responsable de la gestión de los riesgos de operación.

Los supervisores deben evaluar las estrategias respecto a la suficiencia de capital de una entidad, aquí los supervisores deben intervenir si no están de acuerdo con resultados del capital de supervisión. y de cualquier proceso que involucre a la gestión de riesgo operativo.

Principio No. 3.- Gestión integral de toda la Organización: La Alta Gerencia debe tener la responsabilidad de implementar el toda la organización esquema de gestión del riesgo operativo aprobado por el Directorio. El esquema debe ser implementado en toda la organización bancaria, y todos los niveles del personal deben entender sus responsabilidades con relación a la gestión de los riesgos de operación. La alta gerencia también debe tener la responsabilidad de desarrollar políticas, procesos y procedimientos para la gestión de los riesgos de operación en todos los productos, actividades, procesos y sistemas del banco. La gestión de riesgos implica: Identificación, Evaluación, Monitoreo, y Mitigación/ Control.

Los supervisores deben velar por el cumplimiento de los procesos del riesgo operativo, así como exigir el capital mínimo para riesgo operativo.

Gestión de riesgos: identificación, evaluación, monitoreo y Mitigación/control

Principio No. 4.- Tanto para las actividades actuales como las nuevas*:* Los bancos deben identificar y evaluar el riesgo operativo inherente a todos los productos, actividades, procesos y sistemas relevantes.

- Los bancos también deben asegurar que antes de introducir o emprender nuevos productos, actividades, procesos y sistemas, el riesgo operativo inherente a los mismos esté sujeto a procedimientos de evaluación adecuados.

Principio No. 5.- Gestión permanente sistemática y proactiva*:*

Los bancos deben implementar un proceso para monitorear regularmente los perfiles de riesgos de operación y su exposición material a pérdidas. Debe existir un reporte permanente de información pertinente a la Alta Gerencia y al Directorio que apoye la gestión proactiva de los riesgos de operación

Principio No. 6.- Coherencia entre estrategias y objetivos*:*

Los bancos deben tener políticas, procesos y procedimientos para controlar o mitigar los riesgos de operación significativos. Los bancos deben evaluar la viabilidad de estrategias alternativas de control y limitación de riesgos, y deben ajustar su perfil de riesgo operativo empleando estrategias apropiadas, de conformidad con su apetito y perfil integral de riesgo.

Principio No. 7.- Existencia de planes de Contingencia*:*

Los bancos deben implementar planes de contingencia y de continuidad del negocio a fin de garantizar su capacidad para operaren forma continua y minimizar las pérdidas en caso de una interrupción severa del negocio.

En los principios de la gestión de riesgos se debe contar con manuales internos participando así conjuntamente con la alta gerencia para tener claro responsables de los procesos donde se especificara la función de cada uno sus limitantes además los incidentes de tecnología de información.

Papel de los Supervisores

Principio No. 8.- Supervisión obligada a todo tipo de entidades*:*

Los supervisores bancarios deben exigir a todos los bancos, sin importar su tamaño, que implementen un esquema eficaz para identificar, evaluar, monitorear y controlar o mitigar los riesgos de operación, como parte de un enfoque integral para la gestión de riesgos.

Principio No. 9.- Supervisión, periódica e independiente*:*

Los supervisores deben llevar a cabo, de manera directa o indirecta, una evaluación periódica independiente de las políticas, procedimientos y prácticas de un banco relacionadas con los riesgos de operación.

Los supervisores deben asegurarse de contar con mecanismos apropiados de reporte que les permitan mantenerse informados de los avances en los bancos.

- En estos principios los supervisores deben contar con un reporte detallado y explicito de cada proceso de la entidad con su respectivo responsable, para que este reporte sea sujeto a análisis para rediseñar algún proceso si así este lo requiere y ver q se cumpla los objetivos estratégicos previstos

Papel de la Divulgación

Principio No. 10.-. Transparencia y divulgación*:*

Los bancos deben hacer suficiente divulgación pública para permitir que los participantes del mercado evalúen su enfoque para la gestión de los riesgos de operación.

3.5 Análisis Microentorno

3.5.1 Riesgo Legal

Es la posibilidad de pérdida en que incurre una entidad al ser sancionada u obligada a indemnizar daños como resultado del incumplimiento de normas o regulaciones y obligaciones contractuales.

El riesgo legal surge también como consecuencia de fallas en los contratos y transacciones, derivadas de actuaciones malintencionadas, negligencia o actos involuntarios que afectan la formalización o ejecución de contratos o transacciones.

3.5.2 Riesgo Reputacional

Es la posibilidad de pérdida en que incurre una entidad por desprestigio, mala imagen, publicidad negativa, cierta o no, respecto de la institución y sus prácticas de negocios, que cause pérdida de clientes, disminución de ingresos o procesos judiciales.[15]

Los riesgos antes mencionados deben ser incluidos en el concepto de riesgo operativo y tal manera que incurren en factores externos.

SARO (Sistema de Administración de Riesgos Operativos)

Es el conjunto de **elementos** tales como:

1. políticas,
2. procedimientos,
3. documentación,
4. estructura organizacional,
5. registro de eventos de riesgo operativo,
6. órganos de control,
7. plataforma tecnológica,
8. divulgación de información y
9. capacitación.

y **etapas** mediante las cuales las entidades

1. identifican,
2. miden,
3. controlan y
4. monitorean el riesgo operativo.

[15] Comite de Basilea, *Gestión de Riesgo Operativo*, Suiza 26 de Octubre del 2006, p.64.

- ✓ Algunas entidades han identificado actualmente al SARO para tener un control más completo y preciso de estimaciones del Riesgo Operativo, en donde el pilar fundamental es la tecnología ya que se trabaja con software como cristal ball, risk simulador.

3.6 Conclusiones

- Como se puede apreciar, la norma sobre riesgos de operación no está orientada a exigir de las entidades controladas la aplicación, por el momento, de métodos cuantitativos de estimación de requerimientos de capital por el riesgo operativo, sino, más bien, busca promover y guiará a las entidades controladas en el desarrollo de un apropiado ambiente de gestión de este riesgo a través de la aplicación de prácticas sanas de gestión conforme con las recomendaciones del Comité de Supervisión Bancaria de Basilea, las cuales son perfectamente aplicables en nuestro país; y de esta forma contribuir a la solidez y seguridad del sistema financiero mediante una administración adecuada del riesgo operativo que deben llevar a cabo las instituciones controladas y una supervisión preventiva con enfoque de riesgos que debe aplicar el organismo de control.

- Una adecuada administración del riesgo operativo en nuestro país es que se las entidades deben contar con gerencias eficaces que satisfagan las necesidades del cliente y estar al tanto de las tendencias y cambios que ocurren rápidamente, así también como de contar con la información confiable integra y oportuna.

- Se debe dar la importancia que amerita el riesgo operativo y priorizarlo para obtener resultados a corto y largo plazo, logrando así identificar a tiempo las factores que podrían incurrir a este riego y previniendo perdidas inesperadas a futuro.

- Las entidades deben concientizar y elaborar presupuestos en el plan operativo anual para invertir en generar una cultura del Riesgo Operativo dentro de sus políticas y manuales internos

- Las entidades deben contar con el personal calificado y especialistas en temas de Riesgo Operativo y conjuntamente con la unidad de riesgo en la entidad la misma que receptara las matrices de RO, indicadores y demás controles para diseñar alternativas claras y oportunas.

CAPITULO IV

4.1 Diseño de la Propuesta

Mediante la propuesta se enfocara principalmente en definir los componentes y estructura principal que debe contener un manual de RO, adicionalmente se abordara los aspectos más importantes donde se debe tener mayor responsabilidad y control. con este maual integral las entidades financieras podrán basarse para modelar, reforzar o diseñar el suyo de acuerdo a su perfil de riesgo.

4.1.1 Objetivos de la propuesta

Proporcionar a las entidades financieras un concepto claro de la importancia que tiene el Riesgo Operativo en los procesos organizacionales. Este involucra a todos los componentes o recursos esenciales de una entidad como son: recursos humanos, procesos internos, tecnológicos y eventos externos, los cuales deben formar parte activa en un manual de riesgo operativo el mismo que debe ser lo más explicito y concreto posible conteniendo todos los puntos detallados anteriormente y lo mas importante es que sea aplicado para obtener los resultados previstos como es mitigar el riesgo operativo.

4.2 Proceso de Diseño de la Propuesta

Para el diseño de la propuesta se enfocará en el diseño de un manual de riesgo operativo, el mismo que aportará las pautas necesarias para que una entidad cuente con todos los lineamientos necesarios para entender y saber estructurar de manera correcta un manual de RO. Para poder implementarlo en sus procesos organizacionales.

Cabe señalar que un manual de riesgo operativo se ajustara a los requerimientos de una entidad financiara y a su perfil de riesgo, por lo que, este esta sujeto a cambios de acuerdo a políticas y procedimientos internos de cada entidad.

A continuación se describirá la tabla de contenido.

4.2.1 Diseño Manual de Riesgo Operativo

TABLA DE CONTENIDO

A continuación se ampliara cada punto a fin de tener claro el concepto de cada uno de ellos, a fin de integrarlos en el diseño del manual de RO.

1.-DESCRIPCION

En la descripción del manual se debe registrar en número de la circular que fue emitida por la Superintendencia de Bancos y seguros del Ecuador. Siendo esta el organismo regulador al cual debe ser presentado cada manual de la banca privada.

Ejemplo:

Gestión del Riesgo Operativo
(Resolución No JB-2005-834 de 20 de octubre del 2005)

2.-OBJETIVO

El objetivo general y el más importante del sistema de la gestión del riesgo operativo (SARO), se basa en establecer las políticas procedimientos y metodologías para monitorear, medir y controlar el riesgo operativo.

Por tanto las entidades financieras deben formulara un objetivo de acuerdo al cumplimento de una gestión eficaz de la administración de RO. Es decir, los procedimientos que se van a modificar.

Por ejemplo: si existe inconvenientes en un área puntual de la entidad, se debe trazar como objetivo general mejorar el procedimiento y eficacia en el proceso en función a la aplicación de políticas y metodologías de gestión de riesgo como el monitoreo y seguimiento del área en conflicto.

3.-ALCANCE.-

En el alcance se debe identificar y medir los eventos de riesgo, es decir en qué procesos se ha detectado falencias, para de esta manera tomar las medidas correctivas del caso, como son controles y monitoreo de cada área

En el alcance se debe analizar los procesos más relevantes como son:

Grafico 12 Procesos Principales de una Entidad Financiera

Fuente: el Autor

En el alcance se debe indicar el plan de continuidad del negocio el mismo que es vital para administrar correctamente la gestión de riesgo a pesar de eventos que afecten a la entidad.

En el plan de continuidad debe incluir:

- **Plan de contingencia**
  Direcciona a un plan alternativo cuando sucede un evento inesperado.

- **Plan de Reanudación**
  Especifica procesos y recursos para mantener la continuidad de las operaciones

- **Plan de Recuperación**
  Su objetivo es buscar las funciones del negocio especificando procesos y recursos

EJEMPLO RESPECTO A LA SITUACIÓN EN ECUADOR

Los sistemas de Información de un Banco

Cuando existe un riesgo informático pueden ser afectados severamente los sistemas de información de una entidad, esto se da por virus hackers o eventualidades externas. Este es un factor de RO. que suele darse con mucha frecuencia en una entidad financiera y genera muchas problemáticas entorno a esto, por lo cual una entidad debe contar con un plan de contingencia y este a su vez abarca el plan de reanudación y recuperación.

Lo inicial que se debe hacer es:

- Realizar es un Análisis de Impacto al Negocio. Éste es básicamente un informe que nos muestra el coste ocasionado por la interrupción de los procesos de negocio.

- Una vez obtenido este informe, la entidad debe clasificar los procesos de negocio en función de su criticidad y lo que es más importante: establecer la prioridad de recuperación, es decir, se debe enfocar en los puntos más críticos que fueron afectados.

- Seguido de esto se debe seleccionar una estrategia como por ejemplo en la tecnología de información estar más a la vanguardia de los cambios tecnológicos implementando y reforzando las seguridades informáticas de una entidad.

- Antes de ponerlo en marcha se debe realizar pruebas piloto de que tan seguro es la seguridad informática, esto se lo hace desde enlaces foráneos por parte del departamento informático para simular posibles a tentados al sistema de la entidad y además se detectara al directo culpable del atentado.

- Finalmente se debe evaluar la eficiencia del plan que fue ejecutado para salvaguardar las sistemas informáticos de la entidad y si se requiere realizar algún ajuste, deberá ser notificado oportunamente al Supervisor encargado.

El Plan de Continuidad de Negocio abarca todos los sectores de Negocio, dado con más énfasis en aquellos donde la Disponibilidad de la Información es su mayor activo, a partir del 11 de Septiembre de 2001, los Planes de Continuidad de Negocio cobraron importancia abarcando con mayor cobertura a Compañías del Sector Financiero y sus asociados, donde hoy en día tiene su mayor aplicación. No hay importancia del tamaño de la empresa o institución, un plan de continuidad puede ser aplicado tanto a empresas grandes, medianas, pequeñas e incluso micro empresas. Como todo proceso, la aplicación de un plan de continuidad involucra determinados pasos obligatorios para garantizar la funcionalidad del mismo, estas fases son: 1) Fase de Analisis y Evaluacion de Riesgos 2) Selección de Estrategias 3) Desarrollo del Plan 4) Pruebas y Mantenimiento del Plan.[16]

[16] Secretaria de Riesgos, *Plan de continuidad del Negocio*, Quito 23 de Septiembre del 2010, p.88.

4.-DEFINICION DEL SARO

El Sistema de Administración del Riesgo Operativo "SARO" es el conjunto de elementos tales como las políticas, procedimientos, documentación, estructura organizacional, registro de eventos de riesgo operativo, órganos de control, plataforma tecnológica, divulgación de la información y capacitación, mediante los cuales la entidad identifica, mide, controla y monitorea el Riesgo Operativo.

Mediante el SARO la entidad debe contar con un sistema o plataforma para medir y cuantificar las incidencias de errores en cada proceso.

El departamento de riesgos es el encargado de alimentar bases de datos con incidencias de errores de cada proceso para emitir un informe a la gerencia y tomar las medidas correctivas del caso.

5.-POLITICAS ADOPTADAS PARA LA ADMINISTRACION DEL SISTEMA DE RIESGO OPERATIVO SARO.

Las entidades deberán diseñar políticas las cuales hagan cumplir las normatividades internas y externas de control del riesgo operativo.

A continuación se detallara las Politicas que se implementara en este manual:

Política de Procesos

Definir claramente el procedimiento a cumplir, debe ser claro y especifico, de igual manera al responsable del área y las metas que se desea cumplir.

Es necesario para efectivizar esta política elaborar un registro en el cual se explique claramente lo siguiente:

FORMATO DE REGISTRO DE PROCESOS

NOMBRE DE LA ENTIDAD

DEPARTAMENTO DE :……

FECHA DE APROBACIÓN:…… FECHA DE ACTUALIZACIÓN……

TIPO DE PROCESO…….

IMPORTANCIA DEL PROCESO……..

DIAGRRAMA DEL PROCESO

……	……..
RESPONSABLE DEL AREA	**REVISADO POR DEPARTAMENTO DE RIESGOS**

Cuadro 13 Formato Registro de Procesos

Fuente: el Autor

- En el departamento se indicará el área a la cual pertenece el registro.

- En fecha de aprobación se indicara la fecha que se aprobó el procedimiento.

- En la fecha de actualización se indicara la fecha en la que se revisó y evaluó el procedimiento por parte del departamento de Riesgo.

- En el Tipo de proceso e importancia del mismo se categorizara en: Gobernantes, Productivos, Apoyo. Con el objetivo de gestionar de acuerdo a la prioridad del proceso.

- En el diagrama o mapa de proceso se detallara como está conformado, esta información debe ser lo más clara posible a fin de comprender como está el proceso y medir su eficacia.

Política de Personal

Las instituciones controladas deben administrar el capital humano de forma adecuada, e identificar apropiadamente las fallas o insuficiencias asociadas al factor “personas”, tales como: falta de personal adecuado, negligencia, error humano, nepotismo de conformidad con las disposiciones legales vigentes.

Las entidades deben tener en consideración tres procesos importantes:

Proceso de Incorporación

En este proceso se debe evaluar la necesidad de la vacante y se debe definir claramente sus funciones principales y capacitar al nuevo empleado de acuerdo a lo requerido.

Proceso de Permanencia

En este proceso la entidad debe proporcionar a sus empleados capacitaciones para incrementar sus competencias y su vez desarrollar mayor eficiencia en las funciones que realicen lo que minimiza errores involuntarios.de igual manera se debe medir el desempeño de cada trabajador de acuerdo a las competencia que haya adquirido en procesos de capacitación.

Proceso de Desvinculación

Corresponde a la salida del personal, la preparación de finiquitos y la terminación de la relación laboral.

Las instituciones controladas mantendrán información actualizada del capital humano, que permita una adecuada toma de decisiones por parte de los niveles directivos y la realización de análisis cualitativos y cuantitativos de acuerdo con sus necesidades.

Dicha información deberá referirse al personal existente en la institución; a la formación académica y experiencia; a la forma y fechas de selección, reclutamiento y contratación; información histórica sobre los eventos de capacitación en los que han participado; cargos que han desempeñado en la institución; resultados de evaluaciones realizadas; fechas y causas de separación del personal que se ha desvinculado de la institución.

El objetivo de cada una de las políticas de este manual son para efectos de control y evaluación de cada proceso de cada línea de negocio de una entidad financiera

Cabe señalar que estos registros podrían sufrir variaciones de acuerdo a políticas y procedimientos de control de cada entidad.

Es necesario para efectivizar esta política elaborar de un registro en el cual se explique claramente lo siguiente:

FORMATO DE REGISTRO DE PERSONAL

NOMBRE DE LA ENTIDAD

NOMBRE DEL EMPLEADO …….

FECHA DE INGRESO:…… **FECHA DE SALIDA**……

MOTIVOS……

CARGO……

OBJETIVOS Y FUNCIONES PRINCIPALES DEL PUESTO…….

AREA DE TRABAJO……

TITULO ……

COMPETENCIAS ……

HABILIDADES ……

CURSOS Y CAPACITACION …… **FECHAS:**……

EVALUACIONES DE DESEMPEÑO…… **FECHAS:**……

…… ……

RESPONSABLE DEL AREA **REVISADO POR DEPARTAMENTO DE RIESGOS**

Cuadro 14 Formato Registro de Personal

Fuente: el Autor

Se debe analizar como puntos críticos el motivo de la salida del personal, ya que con esto se tendrá en cuenta los aspectos que se debe reforzar de acuerdo a las funciones como la restructuración del cargo.

Política en Tecnología de la Información

Las entidades deben contar con tecnología de información que garantice captura procesamiento, almacenamiento y transmisión de la información de manera ágil, oportuna y confiable.

Para ello las entidades deben contar con políticas y procedimientos bien definidos al respecto.

Entre las más importantes, se detalla las principales políticas que las entidades deberían contar:

- Un plan funcional acorde con el plan estratégico institucional ya que en este consta el presupuesto que se asignara en la adquisición de nueva tecnología.

- Un plan operativo que detalle los objetivos y alcance por la adquisición de nueva tecnología.

- Un procedimiento de clasificación y control de activos de tecnología de información, que considere por lo menos, su registro de: identificación, así como los responsables de su uso y mantenimiento, especialmente de los más importantes.

Es necesario mara efectivizar esta política elaborar un registro en el cual se explique claramente lo siguiente:

FORMATO DE REGISTRO DE TECNOLOGIA DE INFORMACIÓN

NOMBRE DE LA ENTIDAD

AREA …… **TECNOLOGIA DE LA INFORMACIÓN**

DEPARTAMENTO : ……..

FECHA DE APROVACION:…… **FECHA DE ADQUISICIÓN** ……

TECNOLOGIA QUE SE ADQUIERE ……
NECESIDAD DE ADQUISICION ……
OBJETIVOS PREVISTOS A CUMPLIR ……

CAPACITACION INFORMATIVA AL PERSONAL ……. **FECHA:** ……
OBJETIVOS DE LA CAPACITACIÓN …… **TIEMPO DE DURACIÓN:** ……

CAPACITADOR:……
RESPONSABLE DE MANTENIMIENTO DE EQUIPO ADQUIRIDO…….
RESPONSABLE DIRECTO EN USO DEL EQUIPO ……

…… …… ……

JEFE RESPONSABLE DEL AREA **GERENCIA** **REVISADO POR DEPARTAMENTO DE RIESGOS**

Cuadro 15 Formato Registro Tecnología de la Información

Fuente: el Autor

- En fecha de adquisición se indica cuando se adquirió la tecnología esta es importante para en lo posterior realizar actualizaciones.

- Los objetivos claramente especificados, es decir, lo que se desea cumplir y optimizar con respecto a la adquisición ejemplo de esto: agilización y optimización de procesos.

- La capacitación es de vital importancia ya que se informará a los empleados designados para la utilización de esta tecnología la respectiva información y capacitación de cómo proceder a utilizarla.

- En el responsable directo se señala puntualmente la persona que se encargara del uso eficiente del equipo

- En el responsable de mantenimiento se señalara la persona que tendrá como responsabilidad tener en óptimas condiciones el equipo de acuerdo a requerimientos específicos del sistema.

- Adicionalmente y unas de las partes principales respecto a tecnología de información es la parte enfocada a seguridades y autorizaciones, es decir, que solo el personal debidamente autorizado deberá tener acceso al sistema claves, licencias, etc. ya que se podría suscitar problemas respecto a hackers o eventualidades externas que podrían afectar significativamente a los sistemas de información.

- Se recomienda actualizar de manera continua claves y demás aspectos relevantes de seguridad informática a fin de minimizar este factor de riesgo.

6.- OBJETIVOS ESPECIFICOS DEL SISTEMA SARO

- Identificar en todos los procesos cada uno de los eventos de riesgo, establecer un perfil de riesgo operativo para la entidad y asegurar que los controles se ajusten en la medida que se desarrolle la cultura de prevención de riesgos.

- Establecer las metodologías de identificación, registro y valoración de los riesgos operativos.

- Establecer los métodos y procedimientos para registrar los eventos de riesgo operativo.(esto se da mediante bases de datos que registren el evento y su reincidencia en una base de datos).

- Divulgar el sistema, respecto de lo que se trata, la mejor manera es capacitar a los funcionarios en cada una de las etapas que se implementen.

- Asegurar que cualquier evento de riesgo sea registrado en la bases de datos.

- Velar porque el riesgo sea controlado y minimizado progresiva y permanentemente.

- Asegurar la actualización y verificación del sistema de acuerdo con las mejoras tecnológicas y de procesos que podrían garantizar la mejora de los procesos

7. ESTRUCTURA ORGANIZACIONAL

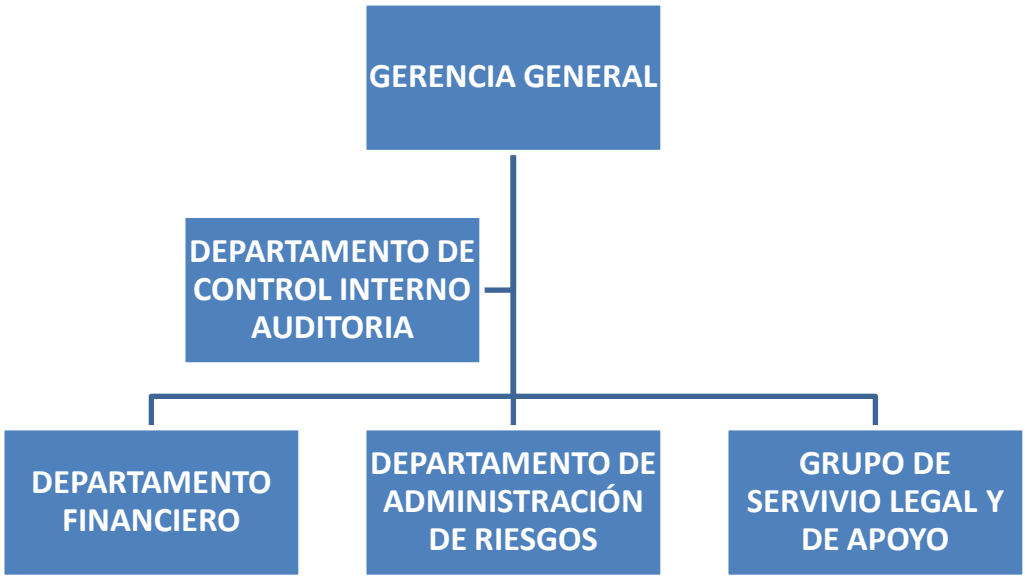


Grafico 13 Estructura Organizacional de una Entidad

Fuente: el Autor

En la estructura organizacional inicialmente se debe crear el departamento de riesgo el mismo que trabajara directamente con la gerencia reportando mediante informes las incidencias y novedades de la gestión de riesgos de cada área y proceso de la entidad.

Adicionalmente el departamento de riesgos trabajara con el departamento de control interno o auditoría para coordinar revisión y planificaciones de evaluación y control de cada departamento que cuente la entidad para estar al tanto de las actividades, desempeño y gestión que se realiza.

El departamento financiero es el encargado de asignar un presupuesto el mismo que servirá para ser canalizado en compras o financiamiento de algún requerimiento que emita el departamento de riesgos y sea previamente evaluado y aprobado por gerencia.

Por último el departamento legal es el encargado de respaldar y dar cumplimiento a las ordenanzas y mandatos legales que se debe cumplir.

8.- COMITÉ INTEGRAL DE RIESGOS

El comité de riesgos se encarga de supervisar y controlar los sistemas de administración de riesgos de una entidad al igual se encarga de la aprobación de políticas y procedimientos internos.

Cabe señalar que el encargado de revisar el plan de continuidad del negocio es el comité de riesgos para poder tener un panorama claro de cómo proceder en caso de suscitarse eventualidades externas

9.- FUNCIONES

Del Representante Legal

El Representante legal es el funcionario responsable de:

- Diseñar y someter a aprobación de la Junta Directiva el presente Manual de Riesgo Operativo así como sus actualizaciones.

- Velar por el cumplimiento efectivo de las políticas establecidas por la Junta Directiva.

- Adelantar un seguimiento permanente de las etapas y elementos constitutivos del SARO que se llevan a cabo en la entidad.

- Verificar el cumplimiento de las funciones asignadas al Departamento de Administración de Riesgos y en particular las concernientes al Sistema SARO.

- Desarrollar y velar porque se implementen las estratégicas con el fin de establecer el cambio cultural en la administración de los riesgos de la entidad.

- Adoptar las medidas relativas al perfil de riesgo, teniendo en cuenta el nivel de tolerancia al riesgo, fijado por la Junta Directiva.

Del Departamento de Administración de Riesgos

El Departamento de Administración de Riesgos debe cumplir con las siguientes funciones:

- Definir los instrumentos, metodologías y procedimientos tendientes a que la entidad administre efectivamente su riesgo operativo, en concordancia con los lineamientos, etapas y elementos, mínimos previstos en esta norma.

- Desarrollar e implementar el sistema de reportes, internos y externos, del riesgo operativo de la entidad.

- Administrar el registro de eventos de riesgo operativo.

- Coordinar la recolección de la información para alimentar el registro de eventos de riesgo operativo.

- Evaluar el impacto de las medidas de control potenciales para cada uno de los eventos de riesgo identificados y medidos.

- Establecer y monitorear el perfil de riesgo individual y consolidado de la entidad, y presentar los informes correspondientes a la Alta Dirección.

- Realizar el seguimiento permanente de los procedimientos y planes de acción relacionados con el SARO y proponer sus correspondientes actualizaciones y modificaciones.

- Desarrollar los modelos de medición del riesgo operativo.

- Coordinar con el área administrativa el desarrollo de los programas de capacitación de la entidad relacionados con el SARO.

- Realizar seguimiento a las medidas adoptadas para mitigar el riesgo inherente, con el propósito de evaluar su efectividad.

- Reportar semestralmente al Representante Legal la evolución del riesgo, los controles implementados y el monitoreo que se realice sobre el mismo

De la Oficina de Control Interno

La Oficina de Control Interno es la encargada de evaluar periódicamente la efectividad y cumplimiento de todas y cada una de las etapas y los elementos del SARO con el fin determinar el grado de eficiencia y las oportunidades de mejora encontradas. De su gestión debe informar tanto al Departamento de Administración de Riesgos como a la Presidencia

10. METODOLOGIA Y PROCEDIMIENTO

El desarrollo del modelo de metodología que se estableció en esta investigación respecto a la Administración del Riesgo Operativo comprendió los siguientes pasos de evaluación:

- Entrevista con la alta dirección: A través de la cual se estableció la severidad máxima aceptable y de ocurrencia para los eventos de riesgo en la entidad.

- Identificación de riesgos principales (altos, medios y bajos) en cada uno de los procesos que conforman el mapa de procesos de la entidad.

- Determinación de posibles impactos del riesgo operativo (insignificante, menor, moderado, mayor o catastrófico).

- Determinación de la probabilidad de ocurrencia de los eventos (Rara, improbable, posible, probable y casi cierta)(matriz de riesgo).

- Desarrollo de registro de eventos de riesgo en una base de datos diseñada por procesos.

- Entrevista con los responsables de cada uno de los procesos para identificar en forma detallada los eventos de riesgo en cada una de las etapas de los procesos, así como para valorarlos e identificar los controles.

- Análisis de escenarios sobre la continuidad del negocio en materia de:

  -Instalaciones físicas

  -Personas

  -Procesos

  -Infraestructura tecnológica

Se explicara cada etapa para dar las pautas necesarias a una entidad de los lineamientos que debe seguir en cada etapa de mitigación y control del Riesgo operativo

Fase de Identificación

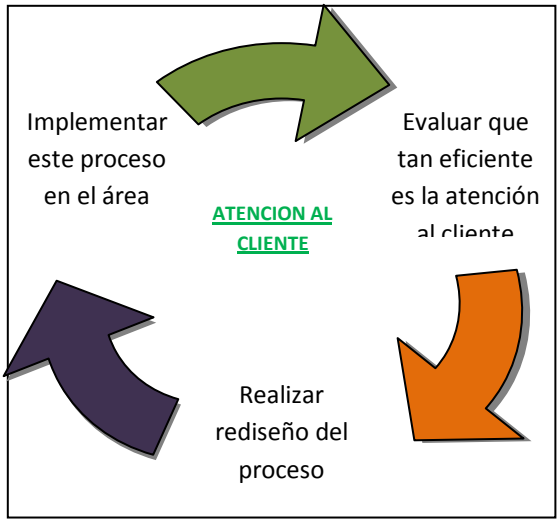
Las entidades financieras utilizarán datos internos, debiendo establecer un proceso para registrar y consignar en forma sistemática la frecuencia, severidad, categorías y otros aspectos relevantes de los eventos de pérdida por riesgo operacional.

El registro de esos eventos contribuirá a reducir los incidentes, las pérdidas y a mejorar la calidad del servicio y de los productos.

Aquí se hace hincapié en que se debe alimentar de manera progresiva las bases de datos con los eventos generadores de Riesgo Operativo para de esta manera tomar las correcciones del caso obteniendo así la mejora continua de los procedimientos y procesos internos de la entidad.

Fase de Seguimiento

Las entidades financieras deberán contar con un proceso de seguimiento eficaz a los efectos de facilitar la rápida detección y corrección de las posibles deficiencias que se produzcan en sus políticas, procesos y procedimientos de gestión del riesgo operacional. Este proceso deberá insertarse en las actividades habituales de la entidad financiera.
Por ejemplo se evaluara el proceso de atención al cliente:



17

[17] ESPINOSA J.,*Metodología de la Investigación RO.*,2da Edición, Editorial Mc Graw-Hill, Quito-Ecuador, 2008

Grafico 14 Ciclo de evaluacion de un Proceso

Fuente: WHITTINGTON R., Auditoria Un Enfoque Integral, 2008

En el diagrama podemos darnos cuenta que es indispensable la evaluación de cada área de la entidad, seguido de esto realizar la rectificaciones que se pudieron identificar en la evaluación, y por ultimo implementar en el proceso que estamos realizando el seguimiento, de esta manera el proceso será progresivo.

Fase de Control y Mitigación

Las entidades deberán establecer procesos y procedimientos de control mediante un sistema que asegure el cumplimiento de las políticas internas reexaminando con una frecuencia mínima anual las estrategias de control y reducción de riesgos operacionales.

En este punto se enfoca principalmente en el cumplimiento de manuales o procedimientos para cada área específica de la entidad.

Se recomienda que las entidades cuenten con controles internos para que den cumplimiento a lo establecido por el manual de procedimientos que debe contar cada área de la entidad.

Este manual de debe contener las directrices y parámetros necesarios para poder controlar los factores de riego que podrían surgir en una entidad.

Un ejemplo de esto seria la aprobación de créditos de consumo, mediante el manual de procesos la persona o responsable encargado deberá cumplir al pie de la letra lo que manifiesta este proceso es decir no podrá dar un crédito si el cliente no cumple con

algunos requisitos esenciales para que sea aprobado aquí existe un control y mitigación de un posible riesgo operativo que se podría suscitar.

Evaluación

Para todos los riesgos operativos materiales que han sido identificados, la entidad debería decidir si usa procedimientos apropiados de control y/o mitigación de los riesgos o asumirlos.

Para aquellos riesgos que no pueden ser controlados, el banco debería decidir si los acepta, reduce el nivel de actividad del negocio expuesta o se retira de esta actividad completamente.[1]

- Todos los riesgos materiales deberían ser evaluados por probabilidad de ocurrencia e impacto a la medición de la vulnerabilidad de la entidad a este riesgo.

- Los riesgos pueden ser aceptados, mitigados o evitados de una manera consistente con la estrategia y el apetito al riesgo institucional. Cuando sea posible, la entidad debería usar controles internos apropiados u otras estrategias de mitigación, como los seguros.

11.-PLAN DE CONTINUIDAD DEL NEGOCIO

El Plan de Continuidad del Negocio debe contener:

- ✓ Objetivo
- ✓ Alcance
- ✓ Estructura para contingencia(luego del proceso principal sigue lo contigente)
- ✓ Roles y responsabilidades(funciones principales)
- ✓ Línea de sucesión(el backup del jefe responsable)
- ✓ Procedimientos generales(procedimientos principales)
- ✓ Procedimientos alternos para trabajar bajo contingencias(procedimientos alternos)
- ✓ Procedimientos de mantenimiento

El Plan de Continuidad del Negocio debe estar en funcionamiento en los términos y plazos establecidos por la Superintendencia de Bancos SBS.

Adicionalmente el Plan de Continuidad del Negocio debe ser objeto de revisión y actualización por lo menos cada año.

12.-REPORTES

El Departamento de Administración de Riesgos responde y es responsable por la preparación y remisión de los informes a la Presidencia y a la Junta Directiva, además es responsable por dar cumplimiento a los reportes sobre el avance en la implementación del SARO.

La Oficina de Control Interno debe informar los resultados de las evaluaciones sobre la efectividad y el cumplimiento de todas y cada una de las etapas del SARO, informes que deberá presentar al Departamento de Administración de Riesgos, a la Presidencia y al Comité de Auditoría.[1]

Debe existir un reporte regular de la información pertinente a la alta gerencia, al directorio, al personal y a partes externas interesadas, como clientes, proveedores, reguladores y accionistas. El reporte puede incluir información interna y externa, así como información financiera y operativa.

Este reporte debe ser entregado al departamento de riesgos para que este evalué el tipo de riesgo y las medidas correctivas a tomar.

Además debe especificar al responsable de cada área el cual especificara como se encuentra su estatus actual de los procesos que le han sido asignados y su evaluación de los mismos.

4.3 Resumen y Análisis de la Propuesta

Mediante la investigación se proporcionó al sistema bancario la relevancia y la importancia del Riesgo Operativo en una entidad financiara mediante todos los procesos vitales que se realizan internamente y las eventualidades de carácter externo.

El plan de continuidad del negocio es parte fundamental en la gestión de riesgo operativo ya que por medio de este la entidad puede ejecutar su procedimiento de contingencia y contrarrestar los posibles factores de riesgo operativo que se pudieren sucintar, o a su vez factores de índole externa.

Todas las entidades deben diseñar su plan de contingencia de acuerdo a lo establecido por la SBS, además que cada plan de contingencia debe proporcionar criterios claros y explícitos de cómo una entidad financiera deberá proceder en casa de cualesquier eventualidad.

Mediante la grafica se detalla claramente la correcta administración y gestión el Riesgo Operativo en una entidad.

GESTION CORRECTA DEL RIESGO OPERATIVO

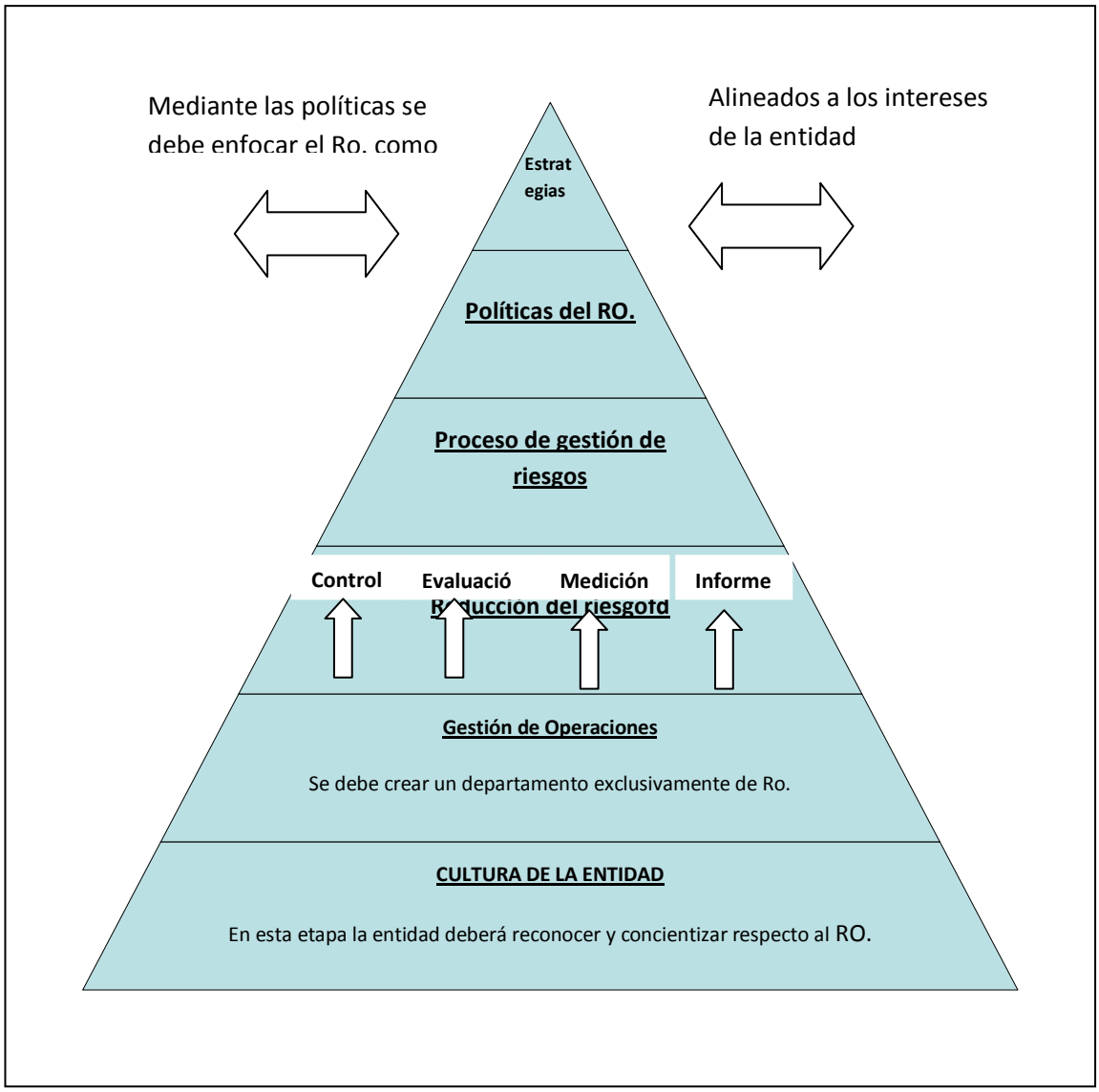


Grafico 15 Correcta Administracion del Riesgo Operativo

Fuente: PricewaterhouseCooppers2006

- ✓ Mediante la cultura la alta gerencia informara sobre la importancia que tiene el Riesgo Operativo en su entidad.

- ✓ Cada departamento o área de la entidad debe realizar la revisión y evaluación de sus procesos y si encuentran errores que reinciden y su frecuencia es ocurrente se debe reportar al departamento de riesgo y diseñar una base de datos donde consten estos riesgos

- ✓ Es fundamental que este ciclo de control evaluación, medición y control este de manera permanente

- ✓ Mediante las políticas se creara la cultura organizacional y además servirán como herramienta regularizadora de los objetivos que se prevé cumplir.

- ✓ Los políticas contaran con lineamientos enfocados a la correcta administración del RO. un ejemplo de esto son los manuales de procedimientos.

- ✓ La ventaja de una gestión eficaz respecto a la administración del riesgo operativo son el rediseño de las estrategias y la toma de decisiones será más acertada.

4.4 Fraudes y Riesgos Informáticos en Ecuador

El fraude es el engaño del cual se vale una persona para conseguir un objeto de procedencia ajena en perjuicio de otra, y de acuerdo con la legislación penal ecuatoriana vigente, se indica una acción tendiente a alcanzar un lucro u obtener ilícitamente una cosa a través del aprovechamiento de un error cometido por otras personas.

En cuanto al engaño, es cuando un sujeto despliega una serie de maquinaciones y artificios con la finalidad de hacer que una o varias personas, tengan una falsa apreciación de la realidad para lograr la entrega de cosas o derechos patrimoniales ajenos.

Como ha venido Evolucionando

Según un estudio realizado en los Estados Unidos, aproximadamente el 27% de los fraudes se cometen hoy en día contra bancos, el 29% contra individuos y el resto contra empresas (21%), Gobiernos (19%) y otros.

Por otra parte, sólo un 10% de todos los casos son reportados a las autoridades, ya sea porque la empresa no sabe cómo proceder ante el fraude, o bien porque quiere evitar exponer un fraude ante la opinión pública.

Virus Roba Información en Cajeros Automáticos de Todo el Mundo

Alrededor del mundo, la red de cajeros automáticos (ATM) está siendo afectada por un virus capas de recolectar información de las tarjetas de crédito, para utilizarla en fraudes, lo que podría empeorar a medida que este virus se vuelve más sofisticado.

Cajeros Automáticos (ATM) alrededor del mundo están siendo infectados con malware que puede recolectar la información de la tarjeta de crédito de una persona para utilizarla en fraudes, situación que podría verse empeorada a medida que este código malicioso se convierte en mas sofisticado, de acuerdo a una investigación de seguridad.[1]

A continuación se mostrara la manera como se apropian de la información de la tarjeta de crédito al momento de insertar en la ranura del cajero automático.

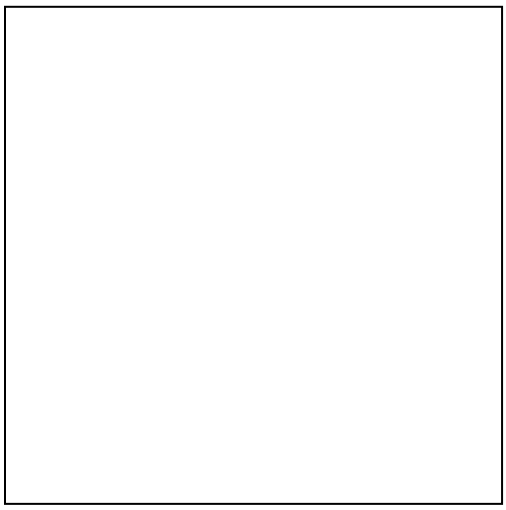


Grafico 16 Fraudes en Cajeros Automáticos

Fuente: PricewaterhouseCooppers2006

Riesgos Informáticos que se encuentra en la actualidad en las Entidades Financieras en Ecuador

Cabe señalar que se detecto este software malicioso a principios de este año por lo que a venido a formar parte de uno de los riesgos más eminentes y nocivos en la actualidad, por lo que está afectando de manera significativa a las entidades financieras.

La información sobre malware (software malicioso) es alarmante ya que este virus es sofisticado debido que:

El virus registra información de la cinta magnética en la parte posterior de las tarjetas, así como también el número de identificación de las personas conocido como (PIN).

Esta información puede imprimirse en un recibo del cajero al insertar una tarjeta especial que genera una interfaz de usuario.

- Para instalar el malware, una persona necesita tener acceso al interior del cajero automático o a un puerto a través del cual el software pudiera ser cargado. Esto significa que personas de la institución deberían estar involucradas o que cyber criminales han logrado desbloquear un ATM (Modo de Transferencia),para poder instalar el software.

- Con esto se pude evidenciar que el riesgo humano y fraude interno está comprobado en las instituciones financieras.

Clonación de tarjetas de Crédito

La técnica más usual es el 'skimming' es un método para el robo de datos mediante la clonación de las tarjetas de crédito de los consumidores sin que éstos lo sospechen, y se realiza tanto en cajeros automáticos como en los propios establecimientos.

Como funciona este fraude

En los cajeros, los estafadores suelen colocar un lector de tarjetas magnéticas en la ranura donde el cliente debe insertar la tarjeta. El dispositivo "lee" la información de la banda magnética y la transmite a otro aparato, donde quedan almacenados los datos. De esta manera los criminales pueden crear un duplicado de sus tarjetas clónicas sin que el cliente lo sepa.

En ocasiones los delincuentes colocan cámaras de vídeo en los cajeros para grabar el código de seguridad (PIN) del usuario mientras éste lo teclea. Por este motivo es muy importante tapar el código en este momento.

El Skimming también se practica en discotecas, restaurantes, tiendas… Para ello, cuando los empleados estafadores solicitan la tarjeta al cliente para cobrar, no sólo utilizan el habitual dispositivo de pago que todos conocemos (TPV) sino que, además, pasan la tarjeta por un pequeño lector de bandas magnéticas, que les permite obtener y guardar todos los datos.[1]

4.4.1 Análisis como mitigar los Riesgos Informáticos

Para efectos de control de este fraude se solicita a los clientes de entidades financieras tomar en consideración que, los fraudes están inmersos, pero se pueden controlar a tiempo, mediantes las medidas preventivas necesarias y trabajando conjuntamente con los funcionarios responsables de salvaguardar los intereses y buena imagen de una entidad financiera:

- Verificar al momento de insertar una tarjeta sea esta de crédito o debito si no existe dispositivos adaptados.

- Informar al gerente o persona encargada del departamento de auditoría o riesgos de cualquier anomalía que podría suscitarse por ejemplo, se ha detectado que en cajeros automáticos han generado billetes falsos por lo que esto nos hace suponer que los mismos funcionarios identificaron y depositaron el billete.

- Actualizar claves de más información importante de manera mensual y pemanente, por lo que evitara así que su clave sea clonada.

4.4.2 Recomendaciones Para los Organismos de Control

Recomendaciones para la Superintendencia de Bancos y organismos de control Bancario

.

- Que las sanciones para Funcionarios, empleados o clientes que confabulen para un fraude sean más severas en caso de demostrarse que han sido participes de un fraude interno o externo.

- Capacitar a los Auditores, y que estos a su vez realicen revisiones sorpresas, con el propósito de observar novedades importantes que acontecen en cada entidad.

- En relación a la Auditoría externa, se debe controlar que éstas ejecuten su trabajo de una forma eficiente, realizando pruebas muy puntuales y esquematizadas en aquellas áreas con tendencia histórica de manipulación o fraude.

- Se recomienda crear un sistema integrado en el cual trabaje con la SBS y sea totalmente confidencial y se puede informar de cualquier sospecha o fraude de algún funcionario y la SBS procede s intervenir a la entidad y al empleado que se tiene sospechas e informar inmediatamente para realizar el seguimiento

RECOMENDACIONES PARA INSTITUCIONES FINANCIERAS

Las siguientes son recomendaciones generales para el tratamiento integral de los actos ilícitos y fraudes internos en las instituciones financieras:

- Establecer una política y procedimientos basados en el concepto de "Tolerancia cero". de esta manera que, los funcionarios sabrán a qué atenerse en caso de participar en fraudes y demás ilícitos.

- Que las sanciones por incumplimiento de la política de "Tolerancia Cero" sean mucho más severas, aplicando la separación inmediata del individuo de la Institución Financiera y en caso de fraudes comprobados se apliquen sanciones penales contra empleados y la denuncia de sus cómplices externos.

- Promover e incentivar una cultura y conciencia de prevención y seguridad, mediante la utilización de volantes infamativos, es mucho mejor prever que sufrir percances.

- Desarrollar y difundir la ética profesional, como valores de la entidad para fortalecer la integridad de la institución y la honorabilidad de los empleados en todos los niveles jerárquicos de la institución.

- Revisar e implementar controles duales en procesos operativos críticos.

- Llevar a cabo auditorías periódicas y eventualmente sorpresivas a cada entidad.

- Investigar oportunamente y a profundidad los actos ilícitos detectados y reportados.

- Diseñar programas de capacitación y sensibilización en materia de prevención y detección de actos ilícitos internos.

- Implantar un buzón confidencial efectivo, donde los empleados puedan informar sus sospechas sin necesidad de sentirse comprometidos o identificados como soplones o comprometidos con sus compañeros.

- Realizar una investigación de antecedentes efectiva en los procesos de selección y contratación de personal.

- Preparar al departamento de Recursos Humanos, para que sea más cuidadoso y selectivo para contratar personal y que esté debidamente capacitado.

- Que Auditoría Interna, adopte políticas de revisiones permanentes, en todos los niveles susceptibles de posibles fraudes.

- Actualizar los manuales de procedimientos y funciones, en razón de los cambios jerárquicos, tomando en consideración las necesidades internas de la institución.

- Implementar la entrega de reportes semanales de las actividades diarias de cada uno de los empleados a su jefe inmediato, el cual entrega este reporte al departamento de riesgos y a la gerencia con la finalidad de presionar la eficiencia y desvirtuar y controlar las posibles ventajas para los fraudes.

- Mejorar la seguridad privada en todas las dependencias donde se desarrollen las actividades financieras cotidianas.

- Se recomienda que los Bancos mantengan archivos con datos históricos de los fraudes de los cuales han sido objeto, con el propósito de crear medios para evitarlos.

- Se propone que en cada Banco Privado Ecuatoriano se implemente un Departamento de Análisis estadístico ya que éste, brindaría una información veraz y exacta de cada anomalía, para facilitar así la toma de decisiones en la implementación de medios objetivos y eficaces.

5. Conclusiones y Recomendaciones

Como principio general, las entidades deben contar con una estrategia que establezca principios para la identificación, medición, control, monitoreo y mitigación del riesgo operativo.

Las estrategias y políticas deberían ser implementadas por la Función de Gestión de Riesgo, responsable de identificar y gestionar todos los riesgos. Estos pueden incluir sub-unidades especializadas por riesgos específicos

Las entidades deberían desarrollar su propio enfoque y metodología para la gestión de riesgos, de acuerdo con su objeto social, tamaño, naturaleza y complejidad de operaciones y otras características.

Como conclusión, el modelo del riesgo operativo es un ciclo en el que se implementan mejoras que responden a los cambios en el entorno y en la organización y los principales puntos de acción que se deben de seguir, y son los siguientes:

- Identificar el riesgo
- Medir (cuantitativa y cualitativamente)
- Analizar
- Prevenir
- Mitigar, transferir, cambiar
- Comunicar y Monitorear

- Todas estas etapas deben trabajar independientemente pero al mismo tiempo se debe generar sinergia ya que todas juntas generan el objetivo que se trazo inicialmente en esta investigación, que es dar a conocer la importancia del Riesgo Operativo en una entidad financiera y las pautas para mitigarlo y minimizar su impacto.

- Respecto al manual de Riesgo Operativo se debe poner en práctica y cumplir a cabalidad las disposiciones que se encuentran en este. Ese es su el objetivo principal.

- Respecto a los delitos y fraudes informáticos, las entidades deben controlar con mayor detalle a sus funcionarios sobre todo aquellos operativos que están encargados del dinero como son cajeros, asistentes en bóveda y demás funcionarios activos en este proceso.

CONCLUSIONES RELEVANTES

De acuerdo al análisis que se realizo a las entidades financieras se determino que:

- El inicio de la implementación del riesgo operativo se efectuó en Abril del 2006 en esta fecha se comenzó con el proceso de implementación del riesgo operativo como parte de sus procedimientos organizacionales.

- Durante el año 2009 y finales del 2010 la SBS realizó una evaluación al sistema financiero para medir el porcentaje de implementación de RO. en sus procesos organizacionales lo cual mediante la investigación se determino que la mayoría de las entidades en un porcentaje de rango de: 58%-66% han implementado el riesgo operativo en todos sus componentes principales como son: procesos, personas, tecnología de información, continuidad del negocio, responsable de administración del RO y administración del mismo. Lo que indica que se empieza a generar una cultura enmarcada y correctamente direccionada a este factor de Riesgo tan importante para una entidad financiera.

- En la actualidad cada entidad financiera a diseñado su propio perfil de riesgo, es decir, cada entidad a diseñado su propio manual de riesgo operativo de acuerdo a sus políticas y requerimientos internos.

- Durante el periodo comprendido en los años: 2007-2008 las entidades mantuvieron realizando la implementación del riesgo operativo, rigiéndose a lo impuesto por Basilea y la normatividad emitida por la SBS,pero aun existía

muchas falencias en este proceso como falta de supervisión y control en cada area y actualización de registros de cada componente del RO.

- Se determino que las entidades no cumplían con los requerimientos mínimos de capital para preservar la continuidad del negocio, por lo que se recomendó realizar el método del indicador simple el cual determinaría el capital mínimo que deben contar las entidades para cubrir esta necesidad de riesgos y cumpliendo así lo impuesto por BASILEA II. realizando así una correcta gestión de implementación del RO.

- Se diseño un ejemplo de matriz de Riesgo la cual se la debe diseñar en cada línea de negocio que cuente la entidad, esta matriz debe ser diseñada por el departamento de RO. el cual debe ser creado dentro del organigrama estructural de una entidad. Este departamento debe trabajar conjuntamente con el área de control interno para velar por el cumplimiento de lo antes expuesto.

- Se diseño una metodología explicativa del diseño de un manual de RO. y el proceso que se debe seguir durante la implementación de este manual, y de cómo realizar una eficiente administración y gestión de este factor de riesgo, tomando en consideración las etapas cruciales que este debe atravesar para lograr mitigar el impacto que tiene el Riesgo Operativo en una entidad financiera, brindando así los lineamientos necesarios y requeridos en la investigación.
- Se enfoco principalmente la supervisión y control que debe contar cada área de una entidad financiera para que se pueda evaluar cada proceso a fin de detectar inconsistencias y errores en los procedimientos.

En la actualidad las instituciones financieras están más familiarizadas con la importancia del riesgo operativo, pero en muchos de los casos se pudo evidenciar que no cuentan con procedimientos necesarios de control como lo es registros de cada componente de Riesgo Operativo, estos registros se encuentran dentro de un manual de RO. y aportaran la información requerida para tener un completo control de lo que sucede a nivel interno y reflejaran la situación real que se encuentra una entidad financiera como consecuencia de este factor de riesgo.

Se determino que para dar cumplimiento a la gestión de riesgo operativo es imperativo la creación de un departamento enfocado a este riesgo y se requiere el apoyo de la alta gerencia para la toma de decisiones en aspectos de mejora implementación que se determine en la gestión de riesgos.

RECOMENDACIONES

- Se recomienda que las entidades cuenten con una unidad de riesgos la misma que se encargara de realizar el seguimiento y tomara medidas correctivas.

- Se recomienda realizar un proceso de gestión de Riesgo Operativo la cual implica la cultura organizacional, esto debe ser direccionado por la alta gerencia conjuntamente con la unidad de riesgos, a las distintas áreas de la entidad.

- Se recomienda realizar mapas de riesgos en donde se identificara claramente como se encuentra actualmente el proceso, donde existen falencias y como se lo puede mejorar, cabe señalar que debe existir el responsable de cada área el mismo que se encargara de elaborarlo y comunicarlo a ala alta gerencia, para su toma de decisiones.

- Se recomienda diseñar y reforzar procesos de control interno en donde se conceptualizara y se dará cumplimiento a políticas y normatividades de la entidad

- Además se recomienda que la alta gerencia diseñe manuales de procedimientos en cada área indistinta de sus procesos.

- Adicionalmente se recomienda realizar cuestionarios de auto evaluación el mismo que reflejara como se encuentra la entidad en su gestión de riesgos.

- Se recomienda a las entidades realizar campañas informativos a los usuarios y entregar al momento que realicen sus transacciones.

Las entidades deben partir enfocándose principalmente en la deficiencia en su estructura organizacional, la cual debe ser reestructurada para depurarla, corrigiendo así las falencias que se detecten entre los aspectos más puntuales que deben ser analizados tenemos:

❖ Ausencia o debilidad de una adecuada separación entre las áreas de negocio y las áreas de control.

Se debe identificar cada área de la entidad claramente y en cada una de estas evaluar sus procesos para verificar la eficiencia de de los mismos.

Además debe existir un responsable de elaborar el informe de esta evaluación este informe será analizado por la alta gerencia para toma de decisiones.

❖ Ausencia o debilidad de una adecuada división del trabajo (funciones, responsabilidades, interconexiones) para las actividades de registro, tratamiento, almacenamiento, transmisión, producción, seguridad, y control.

Se recomienda asignar el trabajo de acuerdo a cada área.las funciones deben centrarse únicamente en su proceso para efectivizar los resultados previstos.

Para analizar los procesos y funciones se recomienda iniciar revisando el diagrama estructural.

Para implementar correctamente la gestión del riesgo operativo en una entidad financiera se recomienda:

- Primero se debe diseñar y aprobar las políticas y procedimientos por parte de la alta gerencia, entre las políticas se recomienda solicitar un informe detallado de cada área respecto a sus procesos y al cumplimiento de los mismos.

- Como podemos constatar el Riesgo Operativo está inmerso en todo el organigrama de una entidad por lo que se lo debe gestionar de manera prioritaria.

- Se recomienda crear un área exclusivamente de Riesgos para direccionar y administrar de manera correcta a cada área de la entidad de acuerdo a sus requerimientos de riesgo en sus procesos. De igual manera esta área será encargada de recopilar toda la información que se encuentra en bases de datos y es proporcionada por cada departamento de la entidad.

- Por último el responsable de cada área debe difundir a sus subordinados la cultura de Riesgo Operativo mediante charlas para comprometer y concientizar respecto a la importancia que este riesgo en sus procesos.

- Adicionalmente se recomienda a las entidades siempre prever es decir identificar a tiempo el riesgo que afecta a una línea de negocio para solucionar inmediatamente y evitar así perdidas inesperadas cuantiosas que podrían generar perdidas en la entidad.

- Como recomendación principal y la más importante es que , las entidades financieras deben gestionar, aplicar e implementar el Riesgo Operativo en todos sus procesos organizacionales y además, dar cumplimiento a las políticas y procedimientos que constan en el manual de Riesgo Operativo, ya que aplicando todos sus componentes y etapas las entidades lograran minimizar y mitigar el impacto que tiene el RO. en una entidad.

- Adicionalmente se recomienda entregar reportes e información de esta índole a la Súper Intendencia de Bancos la cual analizará, medirá y evaluará la gestión de cada entidad.

Anexos 1 Definiciones sobre Riesgo Operativo

Las definiciones deben constar en el manual de Riesgo Operativo (RO) para tener un criterio claro de los términos que estamos utilizando y saber el contenido e interpretación de las disposiciones que se debe cumplir.

Plan de contingencia

Conjunto de acciones y recursos para responder a las fallas e interrupciones específicas de un sistema o proceso.

Plan de continuidad del negocio

Conjunto detallado de acciones que describen los procedimientos, los sistemas y los recursos necesarios para retornar y continuar la operación, en caso de interrupción.

Riesgo

Es la posibilidad de que un evento ocurra y afecte en forma adversa el cumplimiento de objetivos.

Riesgo Operativo (RO)

Se entiende por Riesgo Operativo, la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos. Esta definición incluye el riesgo legal y reputacional, asociados a tales factores.

Riesgo Legal

Es la posibilidad de pérdida en que puede incurrir la entidad al ser sancionada u obligada a indemnizar daños como resultado del incumplimiento de normas o regulaciones y obligaciones contractuales.

El riesgo legal surge también como consecuencia de fallas en los contratos y transacciones, derivadas de actuaciones malintencionadas, negligencia o actos involuntarios que afectan la formalización o ejecución de contratos o transacciones.

Riesgo Reputacional

Es la posibilidad de pérdida en que puede incurrir la entidad por desprestigio, mala imagen, publicidad negativa, cierta o no, respecto de la institución y sus prácticas de negocios, que cause pérdida de clientes, disminución de ingresos o procesos judiciales.

Riesgo Inherente

Nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles.

Riesgo Residual

Nivel resultante del riesgo después de aplicar los controles.

Evento

Incidente o situación que ocurre en un lugar particular durante un intervalo de tiempo determinado.

Eventos de Pérdida

Son aquellos incidentes que generan pérdidas por riesgo operativo a las entidades.

Fraude Interno

Actos que de forma intencionada buscan defraudar o apropiarse indebidamente de activos de la entidad o incumplir normas o leyes, en los que está implicado, al menos, un empleado o administrador de la entidad.

Fraude Externo

Actos realizados por una persona externa a la entidad, que buscan defraudar, apropiarse indebidamente de activos de la misma o incumplir normas o leyes.

Relaciones laborales

Actos que son incompatibles con la legislación laboral, con los acuerdos internos de trabajo y, en general la legislación vigente.

Clientes

Fallas negligentes o involuntarias de las obligaciones frente a los clientes y que impiden satisfacer una obligación profesional frente a éstos.

Daños a activos físicos

Pérdidas derivadas de daños o perjuicios a activos físicos de la entidad.

Fallas tecnológicas

Pérdidas derivadas de incidentes por fallas tecnológicas.

Ejecución y administración de procesos

Pérdidas derivadas de errores en la ejecución y administración de los procesos.

Factores de riesgo

Se entiende por factores de riesgo, las fuentes generadoras de eventos en las que se originan las pérdidas por riesgo operativo.

Son factores de riesgo el recurso humano, los procesos, la tecnología, la infraestructura y los acontecimientos externos.

Dichos factores se deben clasificar en internos o externos, según se indica a continuación.

Anexos 2 Clasificación de los Factores de Riesgo Operativo

INTERNOS

Recurso Humano

Es el conjunto de personas vinculadas directa o indirectamente con la ejecución de los procesos de la entidad.

Se entiende por vinculación directa, aquella basada en un contrato de trabajo en los Términos de la legislación vigente, bien sea celebrada por la misma entidad o a través de un tercero.

La vinculación indirecta hace referencia a aquellas personas que tienen con la entidad una relación jurídica de prestación de servicios diferente a aquella que se origina en un contrato de trabajo.

Procesos

Es el conjunto interrelacionado de actividades para la transformación de elementos de entrada en productos o servicios, para satisfacer una necesidad.

Tecnología

Es el conjunto de herramientas empleadas para soportar los procesos de la entidad. Incluye: hardware, software y telecomunicaciones.

Infraestructura

Es el conjunto de elementos de apoyo para el funcionamiento de una organización. Entre otros se incluyen: edificios, espacios de trabajo, almacenamiento y transporte.

EXTERNOS

Son eventos asociados a la fuerza de la naturaleza u ocasionados por terceros, que escapan en cuanto a su causa y origen al control de la entidad.

Indicadores de riesgo

Alarmas tempranas en los sistemas, procesos, productos, gente y el ambiente externo.

La Unidad de Riesgo Operativo

Se entiende por Unidad de Riesgo Operativo el área designada por el Representante Legal de la entidad, que debe coordinar la puesta en marcha y seguimiento del SARO

Manual de Riesgo Operativo

Es el documento que contiene las políticas, objetivos, estructura organizacional, estrategias, los procesos y procedimientos aplicables en el desarrollo, implementación y seguimiento del SARO.

Pérdidas

Cuantificación económica de la ocurrencia de un evento de riesgo operativo, así como los gastos derivados de su atención.

Perfil de Riesgo

Resultado consolidado de la medición de los riesgos a los que se ve expuesta una entidad.[1]

BIBLIOGRAFIA

CÁCERES Michael y MATURANA J., *Riesgo Operacional*,1era.Edición,Editorial McGraw-Hill, Ecuador, Marzo 2008

Comite de Basilea, *Gestión de Riesgo Operativo*, Suiza 26 de Octubre del 2006, p.64.

Comité de Basilea, *Sanas prácticas de la Gestión y supervisión del Riesgo Operativo*, Suiza, Febrero 17 del 2003, p.45

Comité de Basilea, *Sanas prácticas de la Gestión y supervisión del Riesgo Operativo*, Suiza, Febrero 17 del 2003, p.56

ERNEST, YOUNG, *Gestión del Riesgo Operacional en Entidades Financieras*, Quito, 26 de Septiembre de 2008

ERNEST, YOUNG, *Gestión del Riesgo Operacional en Entidades Financieras*, Quito,10 de Noviembre del 2003,p.36

ESPINOSA J.,*Metodología de la Investigación RO.*,2da Edición, Editorial Mc Graw-Hill, Quito-Ecuador, 2008

FRANKLIN B.,*Auditoria Administrativa*,-1era Edición, Editorial Interamericana, Quito-Ecuador,2008

HARRIS, JC, "Enfoque Integral de Riesgos", Fraudes Corporativos,No.4, Quito,13 de

Marzo del 2009

HERNANDEZ R, Metodología de la Investigación. RO, Editorial Dunken, Argentina,2008

MALDONADO.M., *Estudio de Fraudes*, Tesis *ESPOL*, Quito, 24 de Abril de 2009

NUÑEZ, José y CHAVEZ José J.,"Esquema de gestión y modelado del riesgo", *Gestión del Riesgo Operativo*, año 2007, No.3, Quito 20 de Julio de 2007, p.47.

OJEDA, Elvia. "Riesgo Operativo XXIII",Ponencia presentada en el Congreso AMA Argos, Buenos Aires,24 de Agosto del 2008

ORMAECHEA J. *,Auditoría y Control Interno-2da.*Editorial Amazon,Madrid-España,2007

PÉREZ, Marissela, y otros, *Riesgo Operacional,* 1era. Edición, Editorial McGraw-Hill, Ecuador, 2006

RODRIGUEZ, Noberti, *Riesgo Operativo Ceo*-2da. Edición, Editorial Isma,Buenos Aires-Argentina, 2007

SAENZ,Jordan ," Economía de la Empresa", *Revista Europea de Dirección*, año 2008, No.2, Georgia,18 de Septiembre de 2008,p.68.

Secretaria de Riesgos, *Plan de continuidad del Negocio,* Quito 23 de Septiembre del 2010, p.88.

SMITHSON, Charles W.," *Managing Financial Risk"*. 3ª Edición, Editorial McGraw-Hill, Págs. 550-573

WHITTINGTON R y PANY K., *Auditoria Un Enfoque Integral*, Editorial MC Graw Hill.Bogotá, 2007

REFERENCIAS ELECTRONICAS

FERNANDEZ y MARTINEZ,Riesgo Operacional Conceptos y Mediciones, Agosto 2009, www.sbif.cl/sbifweb/servlet/Biblioteca?indice=C.D.A&idContenido=10553

Comité de Basilea, nuevo acuerdo de capital, enero del 2010, http://www.bis.org/publ/bcbsca03_s.pdf

SuperIntendencia de Bancos, Riesgo Operativo, noviembre del 2010, www.sbs.gov.ec