Universidad del Azuay

Departamento de Posgrados

Maestría en Auditoría Integral y Gestión de Riesgos Financieros, Versión III

Alternativas para mitigar el riesgo operativo que afrontan las empresas del sector privado de la Ciudad de Cuenca durante el año 2017 en función del control interno. Aplicación de una herramienta metodológica.

Tesis previa a la obtención del título de Magíster en Auditoría Integral y Gestión en Riesgos Financieros

Autora: María Augusta Guillén Paredes

Directora: CPA. Ximena Catalina Abril Fajardo Msc.

Cuenca, Ecuador

2020

Dedicatoria

Este artículo dedico a mis Padres quienes desde un comienzo me animaron a cursar la Maestría en Auditoría Integral y Gestión de Riesgos Financieros. Además por brindarme su apoyo económico y emocional durante estos dos años, tiempo en el cual he podido fortalecer conocimientos y aprender nuevos temas que de seguro serán útiles a lo largo de mi vida profesional.

Este trabajo lo dedico a mi persona porque es una muestra de cumplir lo que uno se propone. De igual manera es una razón de satisfacción personal por toda la dedicación, responsabilidad y compromiso durante el tiempo de estudio considerando que todo esfuerzo tiene su recompensa.

Agradecimientos

A Dios y a María Auxiliadora por bendecirme y darme la oportunidad de cumplir mis metas y anhelos personales.

A mis padres, por brindarme su apoyo tanto emocional como económico y motivarme a ser una persona competitiva en el ámbito profesional.

A mi esposo por convertirse en el pilar emocional y ser la persona incondicional en mi etapa de maestrante.

A mi Directora de tesis, Magíster Ximena Abril Fajardo, por su orientación y guía en el desarrollo de este artículo y por estar siempre presta a brindarme un momento de su tiempo para la revisión y corrección durante el avance del mismo.

A los directivos de la prestigiosa Universidad del Azuay por ofrecer programas de posgrados en los cuales se pueden fortalecer conocimientos, aclarar inquietudes y poner en práctica nuevos conocimientos, los cuales permiten ser una profesional competitiva.

Resumen

El presente trabajo desarrolla un sistema de mitigación de riesgo operativo dirigido a organizaciones que ofrecen servicios de telecomunicaciones, desarrollo de ingeniería y tecnología el mismo que se encuentra ajustado al análisis del COSO ERM, ISO 31000 e ISO37001.

En la primera parte se detalla el listado de arte que sustenta la metodología para la identificación, mitigación, evaluación y control de riesgo, que, ha permitido delimitar sistemas de control en función del riesgo.

Posteriormente, se realiza un diagnóstico cualitativo de las debilidades y riesgos potenciales a las que está expuesta y que puede afectar la operatividad de esta organización.

Se plantea un método de cuantificación de frecuencia e impacto sobre el patrimonio, que permitirá a estas organizaciones adoptar decisiones por medio del control interno a fin de identificar, mitigar, evaluar y controlar el riesgo, mediante la utilización del COSO ERM, ISO 31000 e ISO 37001. Estas estrategias serán dirigidas a mantener límites aceptables y cumplir con los lineamientos y objetivos de la entidad.

Finalmente se definirá un plan de acción a través de formatos que permitan administrar el riesgo en la mejora continua de procesos y maximización de la seguridad frente a factores internos y externos mediante análisis de la ISO 37001.

Palabras Claves

Gestión de riesgo, matriz de riesgo, gestión anti soborno, mitigación de riesgo

Abstract y Keywords

This work project develops an operational risk mitigation system aimed at organizations that offer telecommunication services, engineering development, and technology, adjusted to the analysis of the COSO ERM, ISO 31000, and ISO37001.

The first part details the states of the arts that supports the methodology for the identification, mitigation, evaluation, and control of risk, which has made it possible to delimit control systems according to risk.

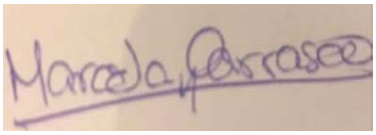
Subsequently, a qualitative diagnosis is made of the potential weaknesses and risks to which it is exposed and which may affect the operation of this organization.

Quantifying frequency and impact on assets is proposed, which will allow these organizations to make decisions through internal control to identify, mitigate, evaluate, and control risk using COSO ERM, ISO 31000 and ISO 37001. These strategies will be aimed at maintaining acceptable limits and meeting the entity's guidelines and objectives.

Finally, an action plan will be defined through formats that allow managing the risk in the continuous improvement of processes and maximizing security against internal and external factors through analysis of ISO 37001.

Keywords:
Risk management, risk matrix, anti-bribery management, risk mitigation

Translated by



Marcela Carrasco

Índice de contenido

Índice de Tablas

Índice de Figuras

Guillén Paredes María Augusta
"Trabajo de Graduación"
C.P.A Ximena Catalina Abril Fajardo, Msc.
Abril 2020

Introducción

Hoy en día, las organizaciones buscan tener un marco de referencia que les permita la implementación de estándares más elevados de control interno, administración y gestión de riesgos y a través de éstos, mejorar el desempeño de quienes forman parte de la empresa y a la vez mitigar riesgo operativo. La normativa COSO ERM, publicada por primera vez en el año 1992 tuvo por objeto ayudar a las entidades a evaluar y mejorar los sistemas de control interno de toda la organización; es decir, desde los empleados hasta los altos mandos con la finalidad de proporcionar seguridad razonable que refleje una información transparente, fiable y útil para que los miembros de la organización puedan tomar acciones correctivas. La organización en la cual se lleva a cabo la presente investigación, brinda servicios de telecomunicaciones, investigación y desarrollo en ingeniería y tecnología, además ofrece consultorías técnicas, capacitaciones y otros tipos de enseñanza a estudiantes, investigadores, docentes y demás personas interesadas en el área económica ofertada. Por lo tanto, este estudio permitirá analizar y comparar la aplicación de las tres normativas: COSO ERM, ISO 31000 e ISO 37001 con otros países de Latinoamérica entre ellos Perú, Colombia y Chile y así poder discutir la forma de aplicación en cada nación y encontrar similitudes o diferencias con la aplicación en Ecuador.

Además, esta investigación propone una herramienta metodológica basada en COSO ERM y apoyada en la herramienta tecnológica @ Risk, la cual ayude a identificar los factores críticos de riesgo, en relación a las personas, procesos, tecnología y factores externos e internos los cuales puedan generar eventos de riesgo operativo y establecer un control interno que servirá para la toma de decisiones en futuras correcciones.

De igual manera se incluirá la ISO 31000 que indica directrices y principios para la gestión de riesgo y la ISO 37001 que ayuda a la empresa a combatir el soborno y promover una cultura empresarial ética. De esta manera, se propondrá a dicha organización la implementación de éstos controles para que así mejore la capacidad de prevenir, detectar y llevar a cabo el tratamiento de riesgo relacionado con el soborno.

Este trabajo está divido en cuatro secciones. En la primera de ellas, se desarrolla el estado del arte para la elaboración de tema en estudio. En la segunda sección se redacta la metodología empleada para la consecución de los resultados. La tercera sección describe los resultados obtenidos dentro de la investigación. En la sección cuarta se presenta la discusión sobre los resultados obtenidos, además las conclusiones y bibliografía utilizada. Como

resultado obtendremos una propuesta que servirá de base para mitigar el riesgo operativo que afrontan las empresas del sector privado dentro de la Ciudad de Cuenca.

Estado de arte

Existen varias definiciones que describen fundamentos teóricos en los que se basa la presente investigación y que están relacionados directamente con temas de riesgos, control interno y aplicación de normativas vigentes a nivel operativo de las empresas privadas que, según la investigación en desarrollo, brinden servicios de tecnologías de la información, capacitaciones, consultorías y enseñanza en temas de telecomunicaciones.

Según (Sánchez Sánchez, 2015) en relación a la metodología de gestión de riesgo operacional COSO ERM, indica que el propósito del método es "efectuar una adecuada administración de riesgos que permitiera identificar, evaluar y responder adecuadamente a los riesgos presentados, de modo que se estuviese preparado para enfrentar situaciones que limiten el logro de los objetivos del negocio" (pág. 43).

Es importante que la organización entienda que la administración de riesgos, no solo conlleva a cumplir principios contables y legales, sino también saber manejar y tratar los riesgos operacionales para que éstos se mitiguen y no afecten de manera negativa a la organización.

La ISO 31000 es "la norma internacional para la Gestión de Riesgos. Al proporcionar principios y Guía exhaustivos, esta norma ayuda a las organizaciones en sus análisis y evaluaciones de riesgos" (bsi., 2020)

La entidad debe gestionar los riesgos de forma eficaz para al momento que se presenten situaciones de incertidumbre puedan aplicar buenas prácticas en las operaciones diarias y así tener éxito en dicha misión.

Otra norma internacional que se integra con los procesos de gestión y controles es la ISO 37001 sistemas de gestión anti-soborno, la cual indica que "el diagnóstico de riesgo genera el input para la planificación, diseño e implementación del Sistema de Gestión. Este sistema es apoyado por tecnologías capaces de medir, controlar y prevenir comportamientos humanos indebidos o inadecuados. La definición e implementación de procesos, procedimientos y controles son claves para el éxito del sistema" (México, 2016).

La norma de sistemas de gestión anti-soborno, garantiza a los altos mandos, socios, personal interno y demás partes interesadas, que la entidad toma medidas para la prevención, enfrentamiento o mitigación del soborno. Además, al obtener la certificación ISO 37001, la organización en estudio adquiere mayor prestigio, costo mercantil, maximiza las ganancias o minimiza pérdidas financieras, a la vez que crea una cultura anti-soborno y se vuelve competitiva.

Es relevante considerar la teoría de Porter sobre "la estrategia empresarial es la búsqueda deliberada de un plan de acción que desarrolle la ventaja competitiva de una empresa y la

acentúe de forma que ésta logre crecer y expandir su mercado reduciendo la competencia, para que la teoría de la estrategia tenga éxito, una empresa debe crear una propuesta de valor diferencial que satisfaga las necesidades de un conjunto seleccionado de clientes" (Vidal, 2011, pág. 2).

La teoría de Porter también indica que "la ventaja competitiva no se puede entender si se examina la empresa en su conjunto. La ventaja nace de muchas actividades discretas que ejecuta al diseñar, fabricar, comercializar, entregar y apoyar su producto, es decir, la cadena de valor" (Vidal, 2011, pág. 3).

Tanto directivos, coordinadores y empleados de la organización, deben tener claro el proceso a seguir para brindar el servicio para que al analizarlo puedan encontrar fallas o déficit en ciertas etapas y así disminuir el riesgo de perder fiabilidad y posicionamiento en el mercado tanto nacional como internacional.

Materiales y métodos

El objeto de estudio definido para esta investigación constituye la medición del riesgo operativo para mejorar los procesos financieros de esta organización; este proceso de análisis de datos inicia con la fase de recopilación primaria, que consiste en desarrollar una metodología a través del análisis descriptivo que se basa en las normas COSO ERM, ISO 31000 e ISO 37001 vigentes y aplicables en todo tipo de instituciones en el Ecuador, inclusive las que se encuentran debidamente reguladas por el Ministerio de Educación.

En este estudio, se llevará a cabo el método cuantitativo recopilado mediante una investigación de campo y bibliografía documental; además, se pondrá en práctica el método deductivo; es decir se analizará desde lo general a lo más específico con la finalidad de encontrar riesgos concretos.

Se realizará un estudio comparativo con artículos científicos referentes al control interno COSO ERM de los países de Perú, Colombia y Chile, lo que permitirá determinar observaciones respectivas para la siguiente fase.

Posteriormente, se identificará los procesos críticos en base a la información obtenida de la matriz elaborada a través de entrevistas, reuniones y cuestionarios efectuados a las áreas que intervienen en cada proceso, la finalidad es consolidar resultados de manera consistente y fiable, reconociendo así procedimientos significativos dentro de la organización.

Finalmente se dará una interpretación y evaluación de la información obtenida como resultado de la herramienta metodológica @Risk, de manera que se pueda establecer comparaciones con la información obtenida, para su posterior conclusión y plan de mitigación que permitirá disminuir el riesgo operativo.

Resultados

El propósito de la identificación de eventos de riesgos operativos es evitar impactos financieros a través de controles adecuados, evaluando la separación de funciones de carácter incompatible entendidas como tareas que maneja una sola persona y que podría permitir la realización u ocultamiento de fraudes, errores y otros eventos de riesgo operativo.

Tabla 1: Eventos de riesgo operativo

Eventos de riesgo operativo

Tipo de evento	Fallas o insuficiencias	Factores de Riesgo Operativo
Fraude Interno		
Falsificación o Clonación.	Corresponde a la alteración, falsificavión o suplantación de firmas o documentos.	Personas Tecnología
Robo y asalto.	Corresponde al ingreso de sujetos no identificados a la empresa con el objeto de apoderarse de documentación relevante de la entidad.	Personas Tecnología
Fraude Externo		
Robos y asaltos.	Corresponde a la apropiación de documentos de usuarios realizados por sujetos no identificados, utilizados para realizar fraude.	Personas Proceso
Falsificación o clonación.	Se relaciona la falsificación o suplantación de firmas en documentos por parte de terceros.	Personas Tecnología
Daños o fallas de equipo por terrorismo.	Corresponde a daños o destrucción de activos fijos como muebles, equipo de oficina, cómputo, maquinarias por actos por parte de terceros destinados a destruir en perjuicio de la empresa.	Personas Eventos externos
Interrupción del negocio por fallas en la Tecnología de la Información.		
Falta de fiabilidad en generación de datos.	Corresponde a la desconfianza de los resultados obtenidos por el sistema.	Tecnología de Información
Diseño de aplicativos que afectan a otros módulos.	Corresponde a la incapacidad de operar en otros aplicativos por la puesta en marcha de uno nuevo.	Tecnología de Información
Manipulación de información por terceros.	Corresponde a la falta de validación, restricciones o bloqueos por perfil de usuario.	Tecnología de Información
Deficiencias en la ejecución de procesos, en el procesamiento de operaciones y en las relaciones con proveedores y terceros.		
Falta de difusión de políticas y funciones.	Proceso de operaciones bajo inconsistencia de políticas institucionales.	Personas
Incumplimiento de proveedores.	Corresponde a una mala selección del proveedor o pedidos realizados con poca anticipación.	Personas Eventos externos

Fuente: (Superintendencia de Bancos y Seguros, 2020, pág. 265.1)

Elaborado por: Superintendencia de Bancos y Seguros de Ecuador

En la tabla 1 se puede analizar el tipo de evento que pertenece al riesgo operativo, las fallas o insuficiencias de cada suceso y el tipo de factores de riesgo operativo que están involucrados en cada uno de los eventos.

Para realizar la gestión de riesgo operativo se diseña una matriz que permitirá evaluar la probabilidad e impacto de los riesgos a los que la organización está expuesta. Los procesos que se considerarán críticos serán aquellos cuyos resultados sean significativamente altos,

es decir, los procesos de riesgo alto se ubicarán en un rango de 500 a 600 puntos, en cambio el rango entre 200 y 400 puntos serán considerados riesgo medio y los inferiores a 200 puntos serán calificados como riesgo bajo. Los parámetros de calificación se indican en la tabla 2.

Tabla 2: Calificación del impacto

Calificación del Impacto	
0	Nulo
1	Bajo
2	Medio
3	Alto
4	Crítico

Fuente: propia
Elaborado por: autora

Por otro lado, es importante considerar la frecuencia puesto que es una medida que caracteriza la ocurrencia del evento en la entidad; por lo tanto, se requiere otorgar un indicador y el nivel de atributo para seleccionar las categorías en relación a la probabilidad de que el riesgo se materialice. Se puede observar en la tabla 3.

Tabla 3. Frecuencia

Frecuencia	
0	Nulo
1	Bajo
2	Medio
3	Alto
4	Crítico

Fuente: propia
Elaborado por: autora

Al utilizar una herramienta informática que brinde información relevante para una auditoría y por ende una adecuada toma de decisiones, es importante dar una calificación de entrada para tener un claro conocimiento de los porcentajes establecidos para cada atributo dado. Ver tabla 4

Tabla 4: Calificación de entrada

Calificación de entrada	
0,25	Bajo
0,50	Bueno
0,75	Satisfactorio
1,00	Óptimo

Fuente: propia
Elaborado por: autora

La ponderación que se dé a los elementos, es un factor considerable, pues se otorga un valor específico a cada parámetro para poder desarrollar el trabajo de estudio. Tabla 5.

Tabla 5: Ponderación del elemento

Elemento	Ponderación
Talento Humano	35
Área Financiera	25
Planificación	15
Área Técnica	15
Usuarios	10

Fuente: propia
Elaborado por: autora

De igual manera, en la tabla 6 se indican factores determinantes que se ponderarán dentro de la organización, los cuales se analizarán en el presente estudio.

Tabla 6: Factores determinantes

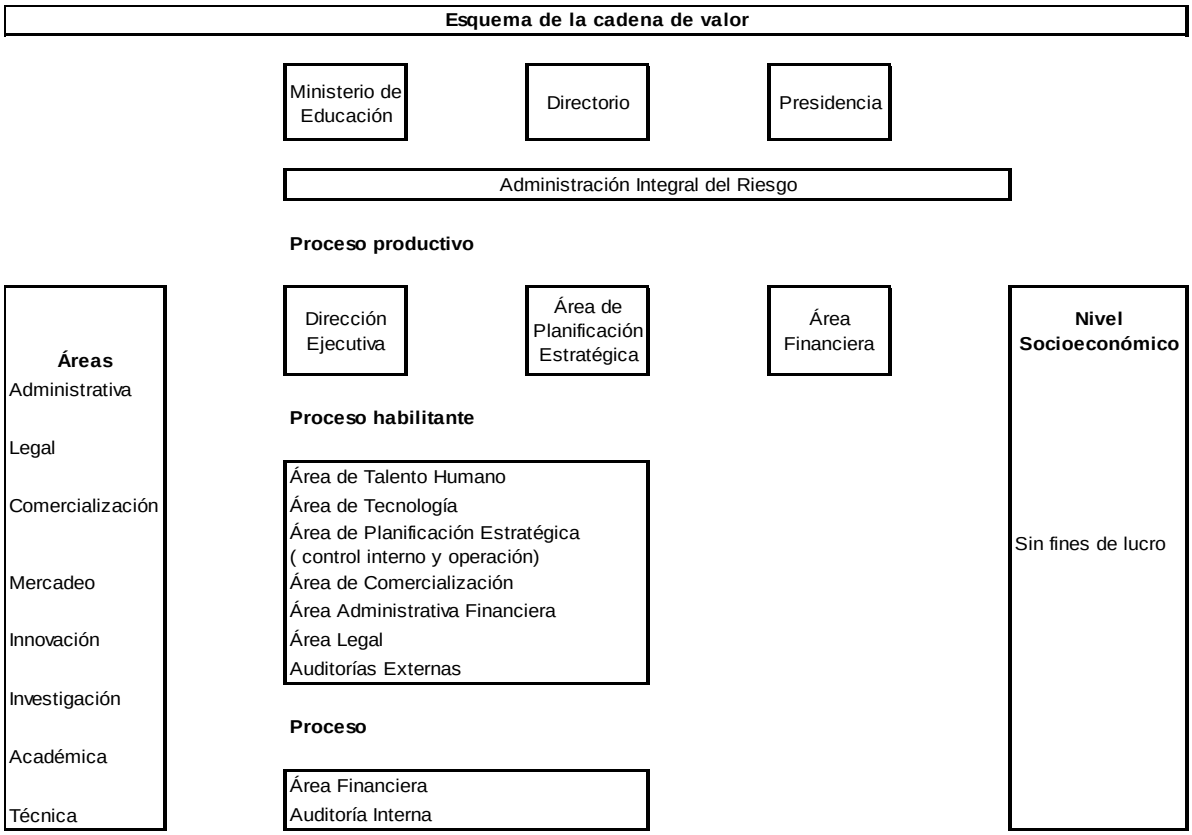
Factores Determinantes	Ponderación
Insuficiencia de proveedores	25
Inversión efectuada	20
Costo de la Inversión	20
Contratos de responsabilidad y Obligatoriedad	25
Existencia de mauales y políticas institucional	10

Fuente: propia
Elaborado por: autora

Es importante, considerar instrumentos que permitan entender si una empresa tanto del sector privado como público da valor a los productos o servicios que ofrece en sus actividades económicas. Por lo tanto, en esta investigación se tomará en cuenta “La Cadena de Valor” de Michael Porter, con la cual se analizará cada activad, estableciendo una ponderación del impacto en caso de fallas dentro de la institución, las actividades estratégicas relevantes y así comprender el costo y fuentes de diferenciación que existen en una organización.

El conjunto de actividades que desempeña la empresa tales como: diseñar, producir, ofertar al mercado y entregar o brindar sus productos y servicios se pueden representar en un esquema de la cadena de valor.

Tabla 7: Esquema de la cadena de valor



Fuente: propia
Elaborado por: autora

Toda empresa al desarrollar su actividad económica, tiene implícito el riesgo operativo debido a que interactúan personas, plataformas tecnológicas y procesos indicados en manuales internos o señalados por la alta dirección, provocando alta complejidad por la diversidad de causas que lo originan y el grado de dificultad con el cual se cuantifica.

Los tipos de eventos de pérdidas analizados son:

Tabla 8: Nivel de Riesgo por Tipo de Evento

Nivel de riesgo por tipo de evento

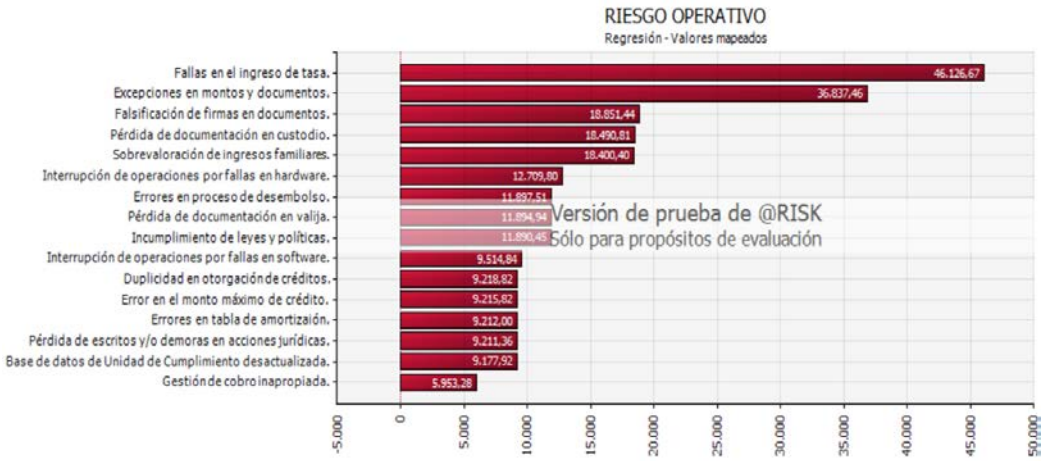
Nro	Riesgo	Tipo de Debilidad	Peso	Factor de riesgo	Nivel de riesgo	Porcentaje	Perfil de riesgo
1	Excepciones en montos y excepciones de documentos no regularizables (garantías, pólizas en trámite, firmas de clientes, etc.	* Falta de automatización de los procesos. * Debilidades en el control interno	0,70 0,30	Procesos Procesos	$56.249,65	14%	Riesgo Alto
2	Falla en el ingreso de rubros	* Errores en el diseño de los aplicativos * Falta de capacitación * Negligencia	0,70 0,20 0,10	Tecnología Información Personas Personas	$70.311,45	17%	
3	Errores en el cálculo automático de la tabla de amortización.	* Negligencia (Descuido u olvido) * Errores en el diseño de laos aplicativos	0,20 0,80	Personas Tecnología Información	$14.072,50	3%	Riesgo Bajo
4	Incumplimiento de políticas, normas, leyes y lineamientos internos y los establecidos por organismos de control.	* Políticas inadecuadas	1	Procesos	$17.918,10	4%	
5	Errores en ingresos de datos del cliente que invalide la generación automática del Certificado de Depósito y se otorgue el crédito sin abono al primer pago.	* Falta de capacitación * Negligencia	0,8 0,20	Personas Personas	$8.964,30	2%	
6	Duplicidad en la otorgación de créditos.	* Errores en el diseño de los aplicativos	1	Procesos	$14.072,50	3%	
7	Mal cálculo automático del monto máximo a otorgar en crédito.	* Errores enel diseño de los aplicativos	1	Tecnología informa	$14.072,50	3%	
8	Mal ingreso en el proceso de desembolso que no son procesados por el IT Bank.	* Falta de capacitación * Debilidades en el control interno	1	Personas Procesos	$17.918,10	4%	
9	Inadecuado mantenimiento de software.	* Mal funcionamiento de software * Incumplimiento de contratos de terceros	0,50 0,50	Tecnología información Eventos Externos	$17.318,05	4%	
10	Inadecuado mantenimiento de hardware.	* Mal funcionamiento del hardware * Incumplimiento de contratos de terceros	0,50 0,50	Tecnología información Eventos Externos	$23.078,80	6%	
11	Pérdida de documentación en valija.	* Falta de automatización de los procesos * Fraude externo / asalto / robo	0,80 0,20	Procesos Eventos Externos	$17.918,10	4%	
12	Falta de actualización de la base de datos especializada para la identificación de Cliented involucrados en negocios ilícitos.	* Información desactualizada	1	Procesos	$14.072,50	3%	
13	Falsificación de firmas en documentos.	* Debilidades en el control interno * Fraude externo / asalto / robo	0,90 0,10	Procesos Eventos Externos	$28.131,75	7%	Riesgo Medio
14	Pérdida de documentación en custodio: garantías , cheques en blanco, liquidaciones de compra, documentos de retenciones, contratos y convenios comerciales u otros.	* Debilidades en el control interno * Falta de automatización en los procesos	0,50 0,50	Procesos Procesos	$26.883,95	7%	
15	Cobertura de garantía no conforme a las políticas y objetivos institucionales.	* Errores en el diseño de los aplicativos * Falta de capacitación	0,80 0,20	Procesos Personas	$8.964,30	2%	Riesgo Bajo
16	Sobrevaloración en ingresos familiares	* Información desactualizada	1	Procesos	$28.131,75	7%	Riesgo Medio
17	Falta de cobertura legal en cobro de CDs no pignorados (no establecidos como garantía.	* Fraude externo / asalto / robo	1	Eventos Externos	$8.964,30	2%	Riesgo Bajo
18	Pérdida de escritos y / o demoras en el proceso de aprobación para demandar.	* Falta de automatización de los procesos	0,70 0,30	Procesos Eventos Externos	$14.072,50	3%	
19	Errores en ingreso de datos del cliente que imposibilite la gestión de cobranza y falta de actualización de información.	* Proceso no documentado	1	Procesos	$8.964,30	2%	
	TOTAL				**$410.079,40**	**100%**	

Fuente: propia
Elaborado por: autora

Al analizar la tabla 8 de nivel de riesgo por tipo de evento, se puede observar que el **52%** del impacto se concentra en los siguientes eventos de riesgo: excepciones en montos y documentos con el 14%, fallas en el ingreso de tasa (17%), falsificación de firmas en documentos (7%), pérdida de documentos en custodio (7%) y sobrevaloración de ingresos familiares (7%).

Para mejor interpretación, con base en las políticas y límites de tolerancia al riesgo, la corporación define los rangos de probabilidad e impacto en los siguientes:

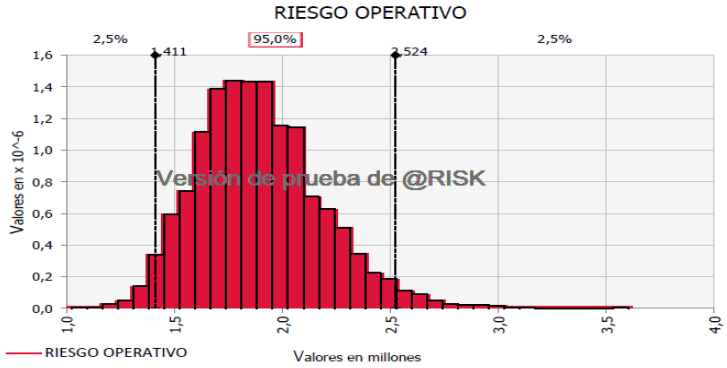
Figura 1: Simulación de Montecarlo por Riesgo Operativo



Fuente: propia
Elaborado por: autora

Por otro lado, en la figura 1 se puede ver el porcentaje de la pérdida asciende al 46.94% del patrimonio, es decir $1’814.105 dólares. (Figura 1).

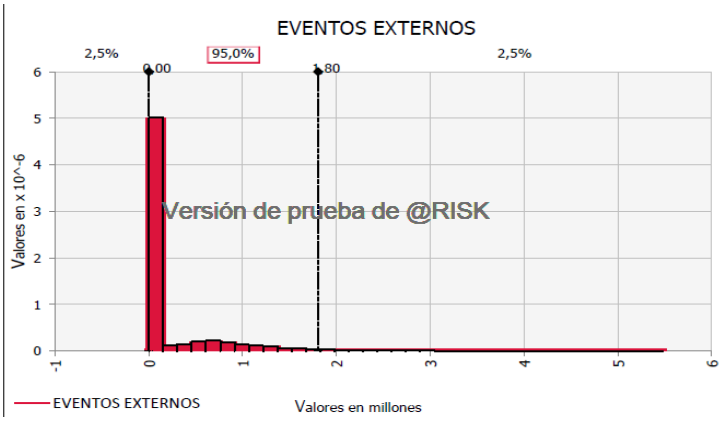
Figura 2: Simulación de Montecarlo por Riesgo Operativo



Fuente: propia
Elaborado por: autora

La pérdida esperada excede el objetivo de la institución ya que representa el 10,61 % del patrimonio técnico, representando una afectación del 46.94% del patrimonio (Figura 2).

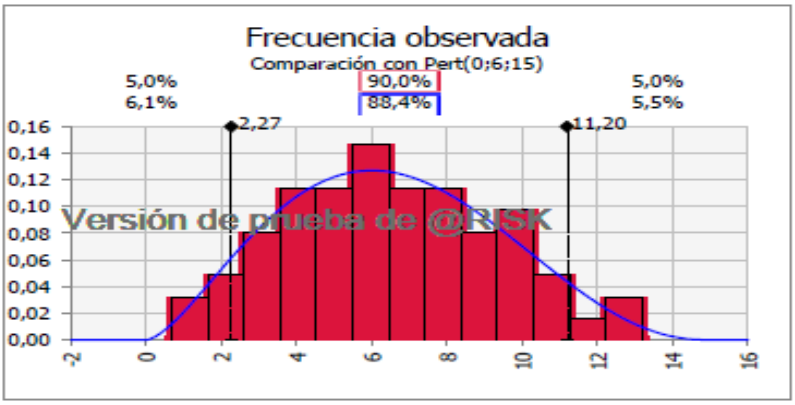
Figura 3: Simulación de Montecarlo por Eventos Externos



Fuente: propia
Elaborado por: autora

La pérdida máxima de eventos externos significaría el 95% sobre el patrimonio, lo que correspondería a un 0.007% es decir, hablamos de incendios, apagones de energía eléctrica, vandalismo, terrorismo o robo (Figura 3).

Figura 4: Frecuencia con datos aleatorios - Fraude Interno

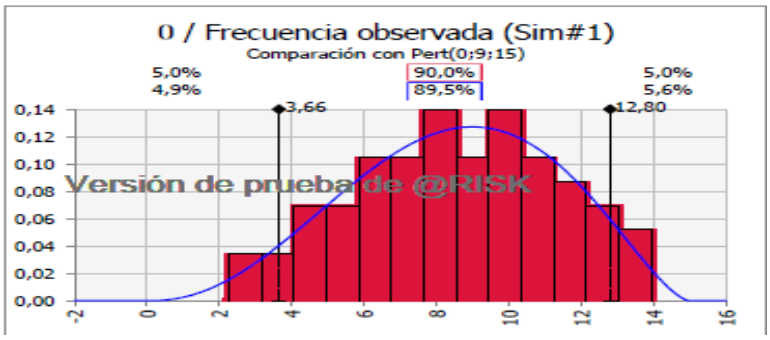


Fuente: propia
Elaborado por: autora

Se muestra la diferencia entre frecuencias observadas y pronosticadas. Este proceso se ha elaborado a través de datos aleatorios con una muestra de distribución Poisson o binomial; en el estudio el valor estadístico corresponde a una distribución Poisson. Dicha función se encuentra caracterizada por un parámetro Lambda λ que representa el número de sucesos ocurridos en el año. La mayor frecuencia se registra con el cliente, producto, negocio, activos fijos y problemas en el sistema que provocan dificultades leves y materialización del riesgo.

Se observa en la figura 4 que con un nivel de significancia del 90% el efecto sobre el patrimonio corresponde al 0.07%

Figura 5: Frecuencia con datos aleatorios - Fraude Externo



Fuente: propia
Elaborado por: autora

Los eventos externos están relacionados con fallas tecnológicas y deficiencias en la ejecución por procesos de supervisión, está relacionada con una distribución binomial cuyo nivel de significancia es del 90% como se muestra en la figura 5 y el efecto sobre el patrimonio corresponde al 0.03%.

Discusión

Al observar los resultados obtenidos en este análisis, se puede indicar que según lo planteado por Porter con relación a la cadena de valor, se vislumbró la importancia de establecer un mapa de procesos dentro de las organizaciones específicamente en el Departamento Administrativa Financiera, porque identifica cuáles son las actividades que generan valor, lo que permitirá trabajar en la mitigación del riesgo operativo, puesto que nos indica el norte de cómo direccionarnos por las diferentes áreas y procesos en apoyo de la normativa de gestión de riesgo COSO ERM y normas estandarizadas como la ISO 31000 e ISO 37001. Es por eso que la gestión del riesgo operativo ayudará a controlar, identificar, mitigar y evaluar el riesgo que se puede originar al interior de una organización, permitiendo de este modo evaluar mediante la calidad y la cantidad del riesgo la disminución del riesgo residual y evitarnos posibles pérdidas al interior de una organización.

A través de la matriz se consideró otro evento del riesgo como la ejecución, entrega y gestión de procesos atado a datos cualitativos y cuantitativos, así como relaciones con la contraparte tal como proveedores, excepciones en montos y documentos no regularizados, fallas de ingresos por rubros, falsificación de firmas en documentos, pérdida de documentos en custodio y sobrevaloración de ingresos familiares, evidenciando si se incurre en prácticas involuntarias. Por esta razón, es de vital importancia considerar el riesgo operativo a través del COSO ERM, la norma ISO 31000 de Gestión de Riesgos Operacionales y la norma 37001 de sistemas de gestión anti-soborno pues está demostrado que se deberá desarrollar,

implementar y mejorar constantemente esta cadena de valor junto con la matriz nivel de riesgo por tipo de evento, porque su propósito es integrar el proceso de gestión a través de la planificación, políticas, procesos, estructuras organizacionales, capacitación, desarrollo tecnológico, que serán los pilares fundamentales de calidad para la mitigación del riesgo. Además, se aplicó la distribución Poisson, la cual relaciona deficiencias en operaciones, prácticas relacionadas con el usuario, productos y servicios, productos en el sistema, eventos asociados con excepciones en montos y documentos no regularizados, falla en ingresos de rubros, falsificación de firmas en documentos, pérdidas de documentación en custodio, sobrevaloración de ingresos familiares, que provocan interrupciones leves y cuya ejecución se realiza con mayor frecuencia.

Los eventos relacionados con fallas tecnológicas y deficiencias en la ejecución se han asociado con la distribución binomial.

Para efectuar un análisis de probabilidad e impacto de los riesgos inherentes, se han evaluado los controles en cada proceso los mismos que están reflejados en el matriz nivel de riesgo por el tipo de evento y mediante los cuales se pueden observar ciertos riesgos como: fallas en los controles, errores humanos, segregación de funciones lo que posibilita errores de verificación.

La debilidad de los sistemas y factor humano tienen un riesgo menor por lo tanto generan un menor impacto monetario dentro de la organización.

La mayor parte de los procesos de riesgo alto presenta buenos y satisfactorios controles, lo que implica una mitigación de controles a los que se encuentra expuesta la institución, solo una mínima proporción de los procesos con riesgo alto están cubiertos por controles óptimos, es decir son efectivos para mitigar la ocurrencia de problemas de la institución.

El nivel medio presenta ineficiencias en sus verificaciones por lo que se buscará cristalizar dichos controles para evitar riesgos que afecten el desarrollo eficiente de las operaciones.

En la encuesta realizada se detectó que no se gestiona de manera integral el riesgo dentro del departamento administrativo financiero, puesto que para ello se necesita trabajar duramente con el área de procesos en cuanto a levantamiento de información in situ, además es muy importante implantar políticas estrictas y normas estandarizadas como las ISO 31001 y 37001 las cuales están relacionadas con la gestión del riesgo operativo y sistema de gestión anti-soborno con la finalidad de analizar situaciones de fraude, permitiendo así disminuir el mismo y evitar pérdidas inesperadas.

Cabe destacar que el desempeño de este servicio es de calidad y permite bienestar y satisfacción de sus usuarios y se deberá considerar la evaluación de quejas, recomendaciones y sugerencias logrando gestionar adecuadamente el riesgo y lograr fidelizar a los usuarios.

Así mismo al evidenciarse pérdidas, es importante reforzar las políticas de recuperación y la necesidad de mitigar el riesgo a través de un proceso de evaluación, seguimiento y control de la parte administrativa financiera y cuidado de los procesos.

Se concuerda entonces con (Lizarzaburu Bolaños, Barriga , Kurt , & Noriega, 2019) quienes en su artículo indican “la necesidad de establecer políticas procedimientos y metodologías para gestionar diferentes tipos de riesgos como crédito, mercado, liquidez, operativo, reputacional y legal. Así mismo, busca mejorar la operatividad de la empresa mediante herramientas que hagan posible identificar, evaluar, mitigar y monitorear diferentes riesgos a los que se encuentra expuesta la organización” (pág. 81-84).

Por tal motivo, la metodología COSO ERM es un facilitador del proceso de la gestión de riesgos, que permite a los administradores de las empresas operar más eficazmente en un ámbito pleno de riesgo, aumentando la capacidad (Sánchez Sánchez, 2015, pág. 45)

Según las citas referenciales a la gestión de riesgos operativos y COSO ERM se puede apreciar que en los países de Colombia y Perú al igual que en Ecuador, las empresas del sector privado dan importancia a la gestión de riesgos puesto que genera un valor agregado tanto en la parte económica como reputacional de la entidad. De igual manera, se analizan las consecuencias de pérdida y el tipo de factor interno o externo que causa el conflicto ya que se ven afectadas las estrategias y objetivos de la entidad.

En cuanto a la norma estandarizada internacional ISO 31000 la cual guía a la organización en el tema de gestión de riesgos y al no delimitarse el sector ni tipo de empresa en el que se utiliza la norma, el país de Chile aplica dicha norma tanto en instituciones de servicio como en las comercializadoras o de producción.

“En Chile, el 90% de las organizaciones son conscientes de la necesidad del desarrollo e implementación de un plan de gestión de riesgos. Su aplicación trae mejoras en el desempeño económico, su reputación, resultados ambientales, de seguridad y salud laboral” (Escuela Europea de Excelencia., 2020).

Gracias a la concientización que tienen las empresas de Chile sobre la norma 31000 la cual aporta principios y lineamientos para la gestión de riesgos de un modo global, este país puede evolucionar favorablemente en los mercados internacionales permitiendo a las organizaciones incorporar procesos de elevado nivel para evaluar y limitar los riesgos en todas sus operaciones. No queda duda entonces que implementar la norma 31000 y dar cumplimiento en la organización, fortalecerá el proceso administrativo financiero y se podrá gestionar de una mejor manera el riesgo, convirtiéndolo de una amenaza a una oportunidad.

La empresa en Ecuador tiene acceso a certificarse en la norma ISO 31000 pero al no obligar su implementación se llega a la conclusión que existen al momento un bajo número de empresas que aplican la ISO en mención.

La norma ISO 37001 que hace referencia a sistemas de gestión anti-soborno, “es una herramienta flexible y está diseñada para adecuarse a todo tipo y tamaño de empresas, tanto del sector público como del privado o sin fines de lucro y al tipo de soborno involucrado” (Lizarzaburu Bolaños, Barriga , Kurt , & Noriega, 2019, pág. 91).

Los países de Latinoamérica en los últimos años han sufrido incumplimiento de la norma ISO37001 puesto que se han escuchado tantos casos de corrupción, soborno, dolo… por parte de los mismos empleados de organizaciones privadas o instituciones públicas. Por esta razón es considerable implementar la norma en mención para que la entidad evite tener mala reputación, desconfianza, pérdida del dinero, problemas legales y en tal caso adopte buenas prácticas y luchen cada vez contra el soborno, cualidad que debe predominar en la cultura empresarial a nivel mundial.

Finalmente se indica que las normas COSO ERM, ISO 31000 e ISO 37001, son herramientas que al implementarlas en la organización nos ayudarán a ser más críticos, gestionar los riesgos evitando cualquier tipo de mala práctica que pongan en apuros a la entidad. Por lo tanto, se debe recordar que un factor importante es conocer y saber llegar al cliente, socio o proveedor con la oferta del servicio o producto, pensando siempre en crear un mejor modelo para la corporación.

Por otro lado, el plan de mitigación del riesgo, que se encuentra adjunto en el anexo 2 puede ser reforzado con capacitaciones que coadyuven a disminuir los controles y permitirá detectar errores para una excelente aplicación de una acción correctiva, misma que ayudará a la mejora en el proceso administrativo del riesgo.

Conclusiones

Se demostró que la gestión por procesos aplicado con las normas COSO ERM e ISO 31000, permiten ordenar, clasificar, procesar, evaluar el riesgo operativo dentro de una organización que ha permitido visualizar posibles técnicas que permitan el cumplimiento del objetivo dentro de esta institución y a través de la ISO 37001 se controlará las buenas prácticas para evitar cualquier tipo de chantaje, soborno y acto de corrupción en general dentro de la organización.

La aportación principal de este trabajo, consistió en desarrollar una cadena de valor que permitió identificar claramente los procesos gobernantes, unidades de apoyo, procesos que integran diferentes departamentos con sus respectivas actividades instaurando así una debida estructura organizacional la cual visualizó las áreas y las personas que levantan este tipo de servicios.

Así mismo con el fin de evaluar el riesgo operativo se aplicó un análisis de las normas COSO ERM, ISO 31000 e ISO 37001 para la gestión tanto de riesgos como de sistemas anti-soborno, que proporcionaron un análisis y evaluación del mismo detectando errores en su debido momento para la aplicación de una acción correctiva inmediata que permita gestionar

los respectivos controles para mitigar el riesgo inherente dentro de los diez y nueve riesgos detectados de los cuáles se encontró dos riesgos altos por falta de controles en la debida diligencia de los documentos y tres riesgos medios sobre el cual se aplicará un debido proceso los mismos que nos permitirán gestionar de manera inmediata la priorización de los riesgos.

Por otro lado, la implementación de la ISO 37001 referente a sistemas de gestión anti-soborno en la organización, ayuda a combatir el soborno, promueve una cultura y garantiza la toma medidas para prevenir, enfrentar o disminuir las malas prácticas que se originen tanto en el ambiente interno como externo de la entidad.

En conclusión, una vez realizado este estudio en la organización, se pudo resolver que se debería trabajar con esquemas atados a la gestión de la administración del riesgo y a través de la cual se pudo disminuir el porcentaje de las pérdidas de la organización, demostrando así que la gestión de riesgo operativo es de vital importancia para el desarrollo de esta institución.

Trabajo futuro

Debido a la aplicación de un buen análisis para mitigar el riesgo operativo, sería adecuado desarrollar e implementar el estudio en función de la Ley Orgánica de Prevención, Detección y Erradicación del Delito de Lavado de Activos y Del Financiamiento de Delitos para poder estimular una cultura de riesgos que fortalezcan la imagen y reputación organizacional.

Bibliografía

Alberto, S. C. (Agosto de 2018). Las Prácticas de Gestión y Sustentabilidad Económica y Ética, en Municipios De Sexta Categoría En Colombia. Colombia.

bsi. (25 de enero de 2020). Obtenido de https://www.bsigroup.com/es-ES/ISO-31000-Gestion-de-Riesgos/

Delgado, Carlos (2011). Auditoría de Gestión – Gestión de Riesgo Empresarial [diapositivas]. (Material de enseñanza). Lima: PUCP, Diplomatura de Especialización en Auditoría.

Escuela Europea de Excelencia. (25 de Enero de 2020). Obtenido de https://www.escuelaeuropeaexcelencia.com/2015/12/norma-iso-31000-chile/

Lizarzaburu Bolaños, E. R., Barriga , G., Kurt , B., & Noriega, E. (2019). Gestión Integral de Riesgos y Antisoborno: Un enfoque operacional desde la perspectiva iso 31000 e iso 37001. *Universidad y Empresa*, 81-82.

Mena, D. (2014). Aplicación Práctica del Marco Integrado de Control Interno – COSO, según CIA, CRMA, CFE, Ecuador

Menéndez Alonso , E. (s.f.). *Google Académico.* Recuperado el 05 de Noviembre de 2019, de https://books.google.es/books?id=x3lMo4yEiegC&pg=PT236&dq=comit%C3%A9+de+basilea+riesgo+operativo&hl=es&sa=X&ei=IjZBVdyPNYWVNpfsgZAG&ved=0CDAQ6AEwAw#v=onepage&q=comit%C3%A9%20de%20basilea%20riesgo%20operativo&f=false

Rivas, Márquez, G. (2011). Modelos contemporáneos de control interno. Fundamentos

teóricos. Observatorio Laboral Revista Venezolana, 4(8), 115-136. https://doi.org/Observatorio Laboral Revista Venezolana Vol. 4, Nº 8, julio-diciembre, 2011: 115-136

Rodrigo Estupiñán Gaitán, B. W. (2015). *Administración de riesgos E.R.M. y la auditoría interna.* Bogotá: Ecoe Ediciones.

Sánchez Sánchez, L. R. (2015). Coso ERM y la Gestión de Riesgos. *QUIPUKAMAYOC Revista de la Facultad de Ciencias Contables*, 43.

Superintendencia de Bancos y Seguros. (25 de 01 de 2020). Obtenido de http://www.riesgooperacional.com/docs/documentos/ecuador/Ecuador%20Riesgo%20operativo%20ultima%20actualizacion.pdf

Vidal, I. (septiembre de 2011). El Principio del Valor Compartido. Barcelona, España.