Universidad & Empresa
ISSN: 0124-4639
ISSN: 2145-4558
univesidadyempresa@urosario.edu.co
Universidad del Rosario
Colombia

Lizarzaburu Bolaños, Edmundo R.; Barriga, Gabriela; Burneo, Kurt; Noriega, Eduardo
Gestión Integral de Riesgos y Antisoborno: Un enfoque operacional desde la perspectiva ISO 31000 e ISO 37001
Universidad & Empresa, vol. 21, núm. 36, 2019, Enero-Junio, pp. 79-118
Universidad del Rosario
Colombia

DOI: https://doi.org/10.12804/revistas.urosario.edu.co/empresa/a.6089

Disponible en: http://www.redalyc.org/articulo.oa?id=187258177005

Gestión Integral de Riesgos y Antisoborno: Un enfoque operacional desde la perspectiva ISO 31000 e ISO 37001

Edmundo R. Lizarzaburu Bolaños*
Gabriela Barriga**
Kurt Burneo***
Eduardo Noriega****

Fecha de recibido: 21 de septiembre de 2017
Fecha de aprobado: 3 de mayo de 2018

Para citar: Lizarzaburu Bolaños, E. R, Barriga G., Burneo, K., & Noriega, E. (2019). Gestión Integral de Riesgos y Antisoborno: Un enfoque operacional desde la perspectiva ISO 31000 e ISO 37001. *Universidad & Empresa, 21*(36), 79-118.
DOI: http://dx.doi.org/10.12804/revistas.urosario.edu.co/empresa/a.6089

* Ph.D. en Management por la Universidad Carlos III de Madrid. Magíster en Investigación por la Universidad ESAN. Program of Negotiation PON, Harvard University (2012). Postgrado en Administración de Riesgos por el Tecnológico de Monterrey. Global MBA de Thunderbird y EGADE del Tecnológico de Monterrey (2008). Maestría en Dirección y Evaluación Financiera de USMP y Especializaciones en Riesgos, Finanzas, Proyectos y Calidad. Ingeniero Industrial (2000), Pontificia Universidad Católica del Perú. Profesor e Investigador de la Universidad ESAN (Perú). Acreditado por Concytec (DINA – REGINA). Correo electrónico: elizarzaburub@gmail.com

** Bachiller en Administración de Empresas, Universidad Peruana de Ciencias Aplicadas (Perú). Investigadora y Consultora en operaciones y gestión financiera. Bachiller en Administración por la Universidad Peruana de Ciencias Aplicadas. Diploma de Especialización en comercio internacional, banca y finanzas y gestión de créditos y cobranzas. Ha publicado diversos artículos académicos y casos de estudio en revistas indexadas en Scopus e ISI - Emerging. Se ha desempeñado como asesora y consultora del Organismo Nacional de Sanidad Pesquera, SANIPES.
Correo electrónico: gabriela.barriga.a@gmail.com

*** Doctor en Administración y Dirección de empresas, Universidad Ramón Llull de Barcelona. Magíster en Economía por la Pontificia Universidad Católica del Perú. Economista. Profesor Principal de Pontificia Universidad Católica del Perú, CENTRUM Católica (Perú). Acreditado por Concytec (DINA – REGINA). Correo electrónico: kburneo@pucp.edu.pe

**** Candidato a Doctor en Finanzas de la Empresa - Universidad Autónoma de Madrid y Universidad Complutense de Madrid. Maestría en Banca y Finanzas - Universidad de Lima (Perú), Ingeniero Metalúrgico y Siderúrgico. Profesor de la UCV Sede Chimbote (Perú). Correo electrónico: lalonoriega@msn.com

Los autores agradecen la colaboración de Celeste Gaspar y Miguel Alegre, estudiantes de Administración y Finanzas de la Universidad ESAN.

Resumen

El presente artículo busca explicar de qué manera las empresas pueden aplicar la gestión de riesgos desde un enfoque operacional y los lineamientos necesarios para llevar a cabo una eficiente gestión de los mismos (Bromiley et al., 2015). En primer lugar, se analiza el riesgo en las operaciones y se explican los tipos de pérdidas y los factores que las puede originar; además, se detallan herramientas de medición como la severidad. Luego, se revisa la teoría de los estándares de gestión relacionados a los riesgos, tales como el ISO 37001, ISO 31000 y COSO, en sus últimas versiones. El documento de investigación propone una aplicación en el área de riesgos, mediante una propuesta de esquema general de riesgos y una estructura de gestión de riesgos para las organizaciones. Finalmente, se desarrollan nuevos aspectos a considerar como el caso del riesgo cibernético.

Palabras clave: riesgo operacional, matriz de riesgo, ISO 31000, ISO 37001, gestión de riesgos.

Risk Management and Anti-Bribery: An Operational Approach from the Perspective of iso 31000 and iso 37001

Abstract

This paper seeks to explain how companies can apply risk management from an operational approach and the necessary guidelines to carry out an efficient management of it (Bromiley et al., 2015). Therefore, we first work out the risk in operations and explain the types of events, the factors that cause it, and details measurement tools such as severity. Then, the theory about management standards related to risk management, such as ISO 37001, ISO 31000 and COSO, in their latest versions, is reviewed. The research paper proposes an application in the area of risks, through a proposal of a general risk scheme and a structure of risk management for organizations. Finally, new aspects are developed to consider the case of cybernetic risk.

Keywords: Operational risk, risk matrix, ISO 31000, ISO 37001, risk management.

Gestão Integral de Riscos e Anti suborno: Um enfoque operacional desde a perspetiva ISO 31000 e ISO 37001

Resumo

O presente artigo busca explicar de que maneira as empresas possam aplicar a gestão de riscos desde um enfoque operacional e os lineamentos necessários para levar a cabo uma eficiente gestão dos mesmos (Bromiley et al., 2015). Por conseguinte, em primeiro lugar, se analisa o risco nas operações e explica os tipos de eventos de perdas, os fatores que o pode originar, e detalha ferramentas de medição como a severidade. Logo, se revisa a teoria acerca dos standards de gestão relacionados aos riscos, tais como o ISO 37001, ISO 31000 e COSO, em suas últimas versões. O documento de pesquisa propõe uma aplicação na área de riscos, mediante uma proposta de esquema geral de riscos e uma estrutura de gestão de riscos para as organizações. Finalmente, se desenvolvem novos aspetos a considerar como o caso do risco cibernético.

Palavras-chave: risco operacional, matriz de risco, ISO 31000, ISO 37001, gestão de riscos.

Introducción

En la actualidad, las empresas están comenzando a dar mayor énfasis a la gestión de riesgos, producto de diversos eventos que se presentan de manera interna y externa. Dichos riesgos siempre han estado presentes dentro las empresas, aunque abordados desde un enfoque financiero (Croitoru, 2014); sin embargo, se tiene más consciencia de ellos a partir de los últimos años.

Una de las razones de que se le esté otorgando mayor relevancia no fue solo la crisis financiera del 2008, sino eventos previos como el caso Enron a principios de 2000 y el caso del Banco Barings a finales de los noventa (Stein, 2000). La crisis finaciera de 2008, que fue originada en el sector financiero y bancario de Estados Unidos, tuvo como una de sus principales causas el aumento del índice de morosidad de las hipotecas *subprime* (hipotecas de menor valor), suceso que se veía desde 2006 y que generó cuantiosas pérdidas a entidades financieras de nivel internacional. Producto de ello, el banco de inversión Lehman Brothers se tuvo que declarar en quiebra, lo que originó, entre otras cosas, que el gobierno de los Estados Unidos anunciara la intervención de las agencias Fannie Mae y Freddie Mac (Wallison & Calomiris, 2009), lo que derivó en diversos estímulos que tuvo que realizar para evitar que el sistema en su totalidad cayera en crisis y en riesgo sistémico.

Estos casos y las grandes pérdidas que generaron evidencian los problemas que puede causar la ausencia de una gestión integral de riesgos, llegando a afectar incluso a las más grandes compañías financieras. Como resultado, según Pacheco (2009), instrumentos más especializados para monitorear, mitigar y controlar las gestiones del sector financiero fueron adoptados por parte de las entidades públicas a cargo de velar por los intereses del público y del buen desempeño de dicho sector.

Debido a ello, incluso las organizaciones mundiales, como el Comité de Basilea (BCBS), enfocado en la supervisión bancaria, se encontraron en la necesidad de establecer políticas, procedimientos y metodologías para gestionar los diferentes tipos riesgos (Lizarzaburu, 2013), que pueden ser de varios tipos, como crédito, mercado, liquidez, operativo, reputacional y legal, entre otros. Así mismo, se busca mejorar la operatividad de la empresa

mediante herramientas que hagan posible identificar, evaluar, mitigar y monitorear los diferentes riesgos a los que se encuentran expuestos.

Para los directivos puede resultar difícil realizar esta tarea debido a que no cuentan con un banco o base de datos que registre los eventos y las pérdidas, cuestión necesaria para realizar el modelo que permita la medición de los riesgos (Patterson & Neailey, 2002). Por esta razón, se recomienda realizar dicha base de datos con una temporalidad de tres a cinco años, pudiendo llegar en algunos casos a ocho, incluyendo en ella los eventos críticos; en caso de no tenerla, lo importante es que la empresa pueda ir elaborándola (Bromiley et al., 2015). No obstante, si no se poseen datos históricos, se puede utilizar diversos escenarios para la medición del riesgo, para los cuales se utilizan variables cualitativas en la elaboración de la matriz de riesgo operacional. Además, Baltov (2016) concluye que las dificultades y excesos de costos están relacionadas a los riesgos mal identificados y a una ausencia de estrategias de gestión de ellos, producto de una mala información, lo que hace importante contar con la misma.

Por otro lado, en el estudio de Fong-Woon y Shad (2017) se tiene resultados empíricos en los cuales se evidencia que la gestión de riesgos genera valor económico agregado a las empresas mediante la reducción del costo medio ponderado de capital y el incremento del retorno sobre el capital invertido, ratios financieros utilizados para valorar los proyectos de inversión.

En el presente documento de investigación se tiene como objetivo revisar y analizar la literatura existente acerca de la gestión del riesgo, su impacto operacional de manera principal y su relación con la ISO 31000 y la ISO 37001. Dicha literatura permitirá realizar una propuesta de esquema general de riesgos y una estructura de gestión de riesgos que podrá ser empleada por las empresas con la finalidad de gestionarlos mejor.

1. Definición de riesgo desde un enfoque operacional

El Banco de España (2012) define al riesgo operacional como "la posibilidad de sufrir pérdidas como consecuencia de la inadecuación de procesos, sistemas, equipos técnicos y humanos, o por fallos en los mismos, así como por hechos externos, incluido el riesgo

legal" (p. 26). Además, según Chernobai, Rachev y Menn (2006) este riesgo incluye también el fraude de tarjeta de crédito, las actividades de comercio no autorizadas, el incumplimiento de pago de impuestos o los fallos deliberados en la contabilidad.

Este tipo de riesgo es considerado como el más antiguo y se presenta en todos los tipos de negocio y en casi todas las actividades existentes. Es complejo por los distintos factores que lo causan y las grandes consecuencias ocasionadas en la industria financiera demuestran la falta de herramientas para gestionarlo de manera adecuada (Núñez & Chávez, 2010). Así mismo, Carillo-Menéndez y Suárez (2012) especifican que, además de resultar de procesos internos inapropiados, el modelamiento de este riesgo conlleva aún muchas incertidumbres; por otro lado, el riesgo operacional es también derivado de problemas en los sistemas de información y en los controles internos (Cruz, Coleman & Salkin, 1998).

1.1. Tipos de eventos de pérdidas

Un evento de pérdida es aquel acontecimiento que puede ser originado por factores externos o internos. Este afecta negativamente las estrategias y los objetivos de la empresa, provocando daños que pueden ser medidos en la organización (Pacheco, 2009). En la tabla 1 se encuentran los tipos de evento y su definición:

Tabla 1. Tipos de eventos de pérdidas

Tipo de evento	Definición
Fraude Interno	Pérdidas causadas por actos de intento de fraude, apropiación indebida de bienes o evitar las regulaciones, la ley de la empresa y la política empresarial, sin incluir discriminación o eventos de diversidad, en la que al menos una parte de la empresa se encuentra implicada.
Fraude Externo	Pérdidas derivadas de una actuación por parte de un tercero encaminada a cometer fraude, apropiarse de bienes indebidamente o evadir la ley.
Vínculos laborales y seguridad en el puesto de trabajo	Pérdidas derivadas de actuaciones incompatibles con la legislación o los acuerdos laborales sobre higiene o seguridad en el trabajo, el pago de reclamaciones por daños personales, o casos relacionados con discriminación.
Incidencias en el negocio y fallos en el sistema	Pérdidas derivadas de la interrupción en el negocio y los fallos en el sistema.
Daños a activos materiales	Pérdidas por desastres naturales y otros eventos que generan daños en los activos materiales de la empresa.
Clientes, productos y prácticas comerciales	Pérdidas derivadas del incumplimiento involuntario o negligente de una obligación con clientes o de la naturaleza o diseño de un producto.
Ejecución, entrega y gestión de procesos	Pérdidas que se derivan de errores de procesamiento de operaciones o gestión de procesos, al igual que de las relaciones con contrapartes comerciales y proveedores.

Fuente: elaboración propia con base en Pacheco (2009).

1.2. Factores del riesgo operacional

Según Basilea, el riesgo operacional es aquel que genera pérdidas monetarias como resultado de fallos o de la falta de adecuación de factores como los procesos internos, las personas, los sistemas, o por eventos externos. Respecto a las aportaciones de los acuerdos de Basilea, Power (2005) indica que la especificación de las causas publicada en el año 2001 es más amplia que la de año 1994, y establece mejor la diferenciación entre riesgo reputacional y estratégico. Por otra parte, de acuerdo con Cruz et al. (1998), la manera de evaluar dichos factores se había centrado más en el ámbito cualitativo que en el cuantitativo. Siendo así, dichos factores se encuentran detallados a continuación:

- Personas: riesgo de los recursos humanos de la empresa, relacionado a la inadecuada capacitación, negligencia, error humano, sabotaje, fraude, robo, paralizaciones y apropiación de información sensible, entre otros (Burneo, et al., 2013). Además, dentro de este grupo existe también la posibilidad de un riesgo de corrupción por parte de los individuos; en este caso, los consumidores no pueden mantener una relación estable con las empresas por tres razones (Lin & Chuang, 2016): primero, porque los consumidores tienen menos poder de negociación en cuanto a las leyes, debido a que las compañías tienen el capital para pagar sobornos; segundo, las empresas son más favorecidas en los juzgados, y tercero, los consumidores son uno de los grupos de interés principales para la empresa, la cual desvía su atención de ellos al haber corrupción, puesto que se torna más oportunista al momento de poder sacar ventaja de cualquier situación de manera ilegal.
- Tecnologías de Información: estos riesgos están relacionados con fallas en la seguridad y continuidad operativa de los sistemas informáticos, así como con problemas en su implementación o una inadecuada inversión en tecnología. (Burneo, et. al., 2013); estos fallos pueden generar pérdidas financieras y de este modo perjudicar los servicios de la empresa (Palma, 2011). También se incluyen las fallas o interrupciones de los sistemas y la recuperación inadecuada de desastres y cualquier evento que atente contra la confidencialidad, integridad, accesibilidad y conveniencia de la información de la empresa (Rodríguez-Wyler, 2010).

- Procesos: se asocia a los errores en los procesos internos de la empresa. Según Jiménez (2010), estos pueden ser de tres tipos:
  - Riesgo con los modelos: se deben a errores metodológicos de dirección o en el modelo de mercado elaborado.
  - Riesgo de transacciones: errores en la realización de las operaciones, riesgo contractual y el nivel de complejidad de los productos, entre otros, y podría estar relacionado con el cumplimiento.
  - Riesgo de control: relacionado al volumen de las operaciones y el riesgo de seguridad, entre otros.

- Eventos externos: son los riesgos asociados a agentes humanos o físicos no relacionados a la empresa y a su control sobre ellas (terceros). Se relaciona a los desastres naturales, los atentados terroristas y los actos delictivos, entre otros. Según Martínez y Venegas (2013), para poder estudiar estas variables se tiene que recurrir a un experto y así determinar las probabilidades de que ocurran. Son riesgos que no pueden preverse con facilidad ni administrarse, y por lo general, no se cuenta con información histórica de ellas.

1.3. Herramientas de medición: la severidad

La matriz de riesgo, usualmente empleada para la identificación de las actividades (proceso y producto) más significativas de las empresa, así como el nivel de riesgo y el tipo de riesgo relacionado a esta, es considerada como una herramienta de control y de gestión (Lehar 2005), que, además, permite identificar los agentes exógenos y endógenos relacionados con los riesgos mencionados anteriormente. Por otro lado, uno de sus objetivos es medir los efectos de la concretización de los riesgos e idear un plan de contingencia (Palma, 2011). Una matriz de riesgo también permite evaluar la efectividad de una gestión y administración adecuada de los riesgos financieros que puedan impactar negativamente en los resultados de una organización. Así, la función principal de la matriz es permitir la elaboración de un plan de acción y luego de contingencia, y realizar controles y acciones que permitan que la gestión se realice de forma adecuada, a través de la identificación y el tratamiento de los riesgos.

El realizar el mapa de riesgos aporta ventajas a la organización, como menciona Rodriguez-Wyler (2010):

> – Favorece la cultura inteligente de riesgos y de control dentro de la organización, de manera que incentiva el entendimiento de los empleados sobre la importancia de los riesgos propios del giro del negocio y su participación en el proceso de reducción de los mismos a través del control interno.
> – Estimula a las distintas áreas del negocio a un mejoramiento en la efectividad de la gestión de los sistemas de control, mediante el incentivo de una reflexión crítica.
> – Permite el incremento en cantidad y calidad de la información fiables acerca del control de los existentes riesgos.
> – Aporta solidez al sistema de control interno, y en consecuencia reduce la desconfianza de auditorías posteriores.
> – Posibilita un mayor énfasis en los riesgos más relevantes para el negocio y así, reducir o mitigar los costos de revisiones (2010, p. 9).

- Identificación de riesgos: para elaborar la matriz, lo primero que se debe hacer es desarrollar un proceso para la identificación de las actividades principales y los riesgos a los que se están expuestas. Según Palma (2011) existen cuatro categorías para las fuentes de estos riesgos: personas, procesos internos, tecnología de información y eventos externos. Así mismo, Castillo y Mendoza (2004), plantean que es imprescindible que este proceso conlleve a un cálculo de las medidas que deben ser tomadas en cuenta para mitigar cualquier evento de pérdida asociada a los riesgos identificados.
- Probabilidad: el primer paso será determinar la frecuencia o probabilidad de que ocurra el riesgo. La frecuencia que se puede dar y la puntuación que recibe cada una se presenta en la tabla 2.

Tabla 2. Parámetros de frecuencia o probabilidad de ocurrencia[1]

Frecuencia	Puntuación	Frecuencia
Muy alta	5	Suele ocurrir en varias circunstancias.
Alta	4	Puede ocurrir una vez.
Moderada	3	Ocurre algunas veces.
Baja	2	Puede que ocurra alguna vez.
Muy baja	1	Muy rara vez sucede.

Fuente: elaboración propia con base en Gutteling (2015).

- Impacto: el impacto de los eventos puede ser positivo, negativo o ambos. Aquellos eventos que podrían tener un impacto negativo se denominan riesgos y los que podrían tener un impacto positivo se denominan oportunidades.

Siguiendo con la matriz, se detalla el impacto que causa cada uno de estos riesgos, los cuales pueden ser en los clientes, los proveedores, los accionistas y otras partes involucradas dentro y/o fuera de la empresa. En la tabla 3 se enumera el tipo de impacto que causaría un evento y la puntuación que se le aplica. Así mismo, se muestra un ejemplo de cómo sería el impacto para el caso de los clientes de una empresa X ante el riesgo operacional que se presenta:

Tabla 3. Parámetros de impacto[2]

Impacto	Puntuación	Repercusión sobre clientes
Alto	5	Afecta a muchos clientes.
Mayor	4	Suspensión prolongada del servicio.
Moderado	3	Repercusión sobre los clientes significativa.
Bajo	2	Probabilidad de suspensión de servicio, pero impacto insignificante sobre los clientes.
Muy Bajo	1	No impacta.

Fuente: con base en Gutteling (2015).

1 La probabilidad también puede ser medida como porcentaje de 0 a 100%.

2 El impacto también puede ser medido como porcentaje de 0 a 100%.

- Severidad, Probabilidad * Impacto: según Martínez, Martínez y Venegas (2016), se define como el producto de la probabilidad con el impacto de que ocurra dicho riesgo; así mismo, señalan que se requiere una cantidad adecuada de distribuciones de probabilidad para cada punto. Por otro lado, resulta importante tener en cuenta la severidad del riesgo al momento de gestionar los riesgos operacionales.
- Priorización o lista de riesgos: en este punto se procede a ordenar los riesgos identificados según su nivel de impacto, dando prioridad a los que puedan presentar un mayor efecto negativo respecto a la estrategia y objetivos de la empresa en cuestión. La priorización es un proceso que se obtiene de clasificar los riesgos según las posibilidades de cruce de las variables impacto y frecuencia (Crouhy, Galai & Mark, 2005).

De esta manera, como muestra la figura 1, se procede a construir una primera matriz para identificar el nivel de riesgo que tiene el evento, según la frecuencia e impacto del mismo, comenzando por los de color verde, que son aquellos que tienen un nivel bajo de efectos sobre la empresa al tener una frecuencia moderada con bajo impacto e impacto moderado con baja frecuencia.

Por otra parte, los de color rojo son aquellos que tienen de baja a muy alta frecuencia de ocurrir, con un impacto que va desde moderado hasta catastrófico, siendo estos las que más ocurren y más daño causan en la empresa; por lo tanto, son los que requieren mayor control y un plan que permita eliminarlos o mitigarlos.

En la figura 1 se evidencia una matriz 5 x 5, con colores que representan las categorías de riesgos de muy alto (rojo, alta severidad) hasta bajo (verde, baja severidad).

Frecuencia						
Muy alta	5	Alto	Alto	Muy Alto	Muy Alto	Muy Alto
Alta	4	Moderado	Alto	Alto	Muy Alto	Muy Alto
Moderada	3	Bajo	Moderado	Alto	Muy Alto	Muy Alto
Baja	2	Bajo	Bajo	Moderado	Alto	Muy Alto
Muy baja	1	Bajo	Bajo	Moderado	Alto	Alto
		1	2	3	4	5
		Insignificante	Bajo	Moderado	Alto	Catastrófico
				Impacto		

Figura 1. Propuesta de matriz de frecuencia-impacto o Matriz de Severidad
Fuente: Crouhy, Galai y Mark (2005).

- Tratamiento de los riesgos: proceso o etapa en la que se opta por aceptar el riesgo, disminuir la probabilidad de ocurrencia y su impacto, transfiriéndolo total o parcialmente, o evitándolo. También puede darse una combinación de las medidas anteriores, de acuerdo con el nivel de tolerancia al riesgo definido (Palma, 2011).

Según el Estándar Australiano (1999), las respuestas de las organizaciones que se tomen, respecto a los riesgos calificados, considerarán las siguientes actividades:

  - Evitar: no se debe llevar cabo la actividad que podría generar el riesgo, incluso cuando sea viable. La aversión al riesgo, que es un comportamiento usualmente influenciado por el sistema interno de una entidad, podría ser contraproducente, debido a que evitar riesgos sin ningún criterio objetivo puede aumentar la significación de otros.
  - Reducir o mitigar: realizar acciones que reduzcan la severidad del riesgo, su probabilidad e impacto.
  - Transferir: compartir el riesgo con otra parte dentro de la entidad para reducir la frecuencia o el impacto. Las técnicas comunes incluyen la contratación de seguros, operaciones de cobertura y estructuras organizacionales, como los Joint Venture o tercerización de actividades.
  - Aceptar o retener: preservar el riesgo sin efectuar medidas distintas a su eficiente monitoreo, lo cual permite que los riesgos puedan ser retenidos estratégicamente (Blackburn, Brennan & Ruggiero, 2014).

- Monitoreo y control de los riesgos: según Samano (2013), el monitoreo es el proceso que consiste en la evaluación del diseño y operación de los controles por parte del personal indicado y la implementación de las acciones necesarias, las cuales deben ser realizadas en el tiempo adecuado. Es aplicable a todas las actividades incluidas dentro de una organización y, según sea el caso, a contratistas externos. Su objetivo es asegurar el correcto funcionamiento del sistema y adaptarse a las necesidades y cambios en las circunstancias. Si bien algunos autores consideran que la comunicación puede ser realizada en cada etapa de manera transversal, es importante indicar que una adecuada comunicación en la gestión de riesgos puede contribuir a que esta sea más eficiente y puede ser considerada como una actividad independiente dentro de la misma gestión (Gutteling, 2015).

2. Estándares de Gestión

Existe una variedad de estándares para la gestión del riesgo. Actualmente, entre los más importantes están la ISO 37001:2016 y la Guía de Gestión de Riesgo del Fraude, así como el marco de control interno COSO y el riesgo cibernético.

2.1. ISO 37001:2016[3]

Uno de los riesgos más comunes que se pueden identificar dentro de las organizaciones es el soborno, y esto se debe a que este "método" ayuda a conseguir grandes negocios de manera rápida, supuestamente segura y sin realizar muchos esfuerzos. Estos pueden ser directos o indirectos y ser llevados a cabo por socios o colaboradores.

La Real Academia Española define al acto de sobornar como "dar dinero o regalos a alguien para conseguir algo de forma ilícita". Así, existen autores como Kafel (2016) quienes explican que estos regalos ilícitos significan costos para la empresa y, en el mediano plazo, costos para toda la sociedad y la industria. En consecuencia, el autor concluye que los costos de los sobornos influencian significativamente en la calidad de vida. "La corrupción puede definirse como el abuso de una posición de confianza para la obtención de un beneficio deshonesto" (Argandoña, 2007, citado por Frías-Aceituno, Rodríguez-Domínguez & García-Sánchez, 2014, p. 32).

El soborno y la corrupción, en general, distorsionan las inversiones y afectan la libre competencia, haciendo que se pierda el bienestar de los grupos de interés, además de elevar costos y ser una barrera de entrada para nuevas empresas o mercados. Según Malgwi (2016), su impacto cambia en magnitud y localización de acuerdo con la naturaleza del negocio, y por esto es importante y esencial comprender su heterogeneidad al momento de señalar sus factores de mitigación.

Así mismo, Lin y Chuang (2016) señalan que cuando las empresas multinacionales, que tienen controlado los sobornos de mejor manera dentro de su organización, ingresan a un país con un nivel alto de corrupción, son menos propensas a pagar sobornos en dicho país en comparación con las compañías locales. En consecuencia, los consumidores preferirán y confiarán en las multinacionales más que en las empresas nacionales.

3 Para consultar la norma, visitar https://www.iso.org/iso-37001-anti-bribery-management.html

Siendo así, se considera beneficioso aproximarse a la evaluación del riesgo de corrupción a través del enfoque del ciclo del proyecto (Manuhwa & Stansbury, 2016), debido a que el riesgo cambia de acuerdo con la etapa del negocio en la que se encuentre y porque es mejor identificarlo en los periodos iniciales para poder planificarlo de manera adecuada. Por otro lado, es importante resaltar que la literatura presenta estudios en los cuales se analiza la percepción de la corrupción y el soborno en instituciones de 107 países representativos de cada continente y los resultados se encuentran por encima de la media de corrupción, es decir, las personas sienten que el soborno en su país ocurre más de lo que debería. Este grupo de instituciones abarcan a la policía, parlamento y empresas del sector privado. Debido a esto, se aprecia la necesidad de un estándar como la ISO 37001 que permita a los organismos mitigar estos efectos negativos; por ello, la Organización Internacional de Normalización publicó, el 15 de octubre de 2016, la primera versión de este estándar, luego de iniciar el proceso de elaboración en noviembre de 2013.

2.1.1.Definición

La ISO 37001 es un nuevo estándar (publicado por ISO en el 2016) de sistemas de gestión antisoborno. Comenzó a gestarse en 2014 con la participación de profesionales de más de 30 países y más de 20 en calidad de observadores. Esto debido a que el soborno constituye un riesgo comercial y es común en muchas empresas alrededor del mundo, en todos los sectores. Además, Kafel (2016) indica que la corrupción ocurre en todos los niveles de desarrollo económico y social y por ende se encuentra presente en todos los países.

En este estándar se especifican una serie de medidas y requisitos a implementar por la organización, lo que ayudará tanto a prevenir como a detectar y abordar el soborno, además de brindar información para orientar acerca de su aplicación.

La ISO 37001 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.

En el ecosistema actual de las empresas, se encuentran relaciones entre el directorio, la gerencia general y la alta administración, que tienen como objetivo el mejoramiento continuo y la mitigación de los riesgos como los sobornos. Para ello, se debe recurrir a auditorías tanto internas como externas y gestionar un sistema de denuncias que vele

por el cumplimiento de la gestión de crisis y riesgos por la administración; además, estas relaciones y controles necesitan siempre llegar y ser del conocimiento del directorio.

En la actualidad, las empresas están siendo siempre evaluadas tanto internamente como externamente por terceros y grupos de interés o *stakeholders* en un ambiente de mayor diversidad. Son estos desafíos los que hacen necesarias las aplicaciones de sistemas de control interno, como lo son el COSO, UK Bribery Act o la ISO 37001 que se estudia en esta investigación.

Este estándar es importante porque permite un mejor accionar del negocio en nuevos mercados. Esto se explica porque cuando una empresa está involucrada en sobornos, le es indiferente actuar tanto en entornos corruptos como en entornos trasparentes, es decir, tiene más campo de maniobra; sin embargo, una empresa que siempre ha estado ligada a la legalidad, le será muy difícil actuar en ambientes en donde prime la corrupción y el soborno porque no está adecuada a ella ni a un ambiente alineado con sus valores (Malgwi, 2016).

Por otra parte, el accionar de este estándar otorga ventajas a la organización dado que facilita la sistematización del sistema de gestión contra el soborno, provee confianza a los accionistas, clientes y otros grupos de interés o *stakeholders* en general, y es una herramienta de mucha ayuda en la defensa ante tribunales en caso de alguna pesquisa, ya que brinda evidencia de que la empresa toma medidas para la prevención del soborno.

Por otro lado, brinda menores riesgos para los clientes cuando operan en mercados internacionales y permite que identifiquen a las organizaciones comprometidas con la lucha contra el soborno. De este modo, pueden contar con mejores proveedores y así tener una imagen de marca más transparente. Según Lin y Chuang (2016), se afecta también el valor de marca cuando las empresas están localizadas en países con un alto nivel de sobornos, ya que este ambiente de corrupción aminora las capacidades del *marketing*, las cuales son necesarias para generar valor de marca. Por ello, muchas empresas incurren en costos de reformas, algunas veces altos, para evitar y eliminar la corrupción y el soborno de su entorno. Normas como la ISO 37001 resultan cruciales para mitigar los efectos dañinos en el valor de marca, el cual tiene un efecto positivo en los ingresos de las empresas.

Finalmente, el estándar ayuda al mercado de manera íntegra y general, porque reduce la incertidumbre y genera confianza, la cual es clave para el desarrollo de la economía y de las empresas.

2.1.2.Alcances de la norma

Los requisitos establecidos para poder estar en línea con este estándar son el compromiso, la responsabilidad y el liderazgo de la alta gerencia, designar a un encargado de *compliance*, capacitar al personal, contar con una política antisobornos, tener controles (tanto comerciales como financieros) de los contratos, y llevar a cabo procedimientos para recabar la información del riesgo.

Respecto al ámbito del contexto de la organización, es importante conocer y comprender a la empresa y al sistema anticorrupción. Por ello, el estándar indica los puntos importantes a tomar en cuenta dentro de este contexto, que están expresados en la tabla 4.

Tabla 4. Contexto de la organización

Entender la organización y su contexto	• Tamaño y estructura corporativa. • Diagrama de delegación de las decisiones. • Entorno geográfico presente y futuro. • Modelo de negocios. • Organizaciones que controla la empresa y que la controlan a ella. • Socios. • Ámbito legal, regulatorio y contractual de las obligaciones de la empresa.
***Entender las necesidades y expectativas de* stakeholders**	• Han de ser relevantes para los posibles efectos del soborno. • Verificar los requerimientos que son irrelevantes, así como su fuente de procedencia.
Determinar el alcance del sistema anticorrupción	• Se diagnostica si el sistema es independiente o integrado. • Considera los resultados de la evaluación de riesgo.
Evaluación periódica del riesgo	• Se identifican riesgos que se pueden anticipar. • Se procede a analizar y priorizar estos riesgos. • Establecer criterios para evaluar los riesgos. • Esta evaluación se hace continuamente y también cuando ocurren cambios significativos en las actividades o estructura del negocio. • Finalmente, se documenta el uso de las evaluaciones para una posterior mejora o diseño del programa.

Fuente: Deloitte (2017).

Con respecto a las operaciones de la empresa, ella abarca cláusulas clave para que el sistema sea implementado de manera eficaz y su gestión sea más sencilla. Por ellos es necesario planificar, ejecutar, supervisar y controlar los procesos que llevan a cabo. Se distinguen principalmente dos tipos de controles en este ámbito, los cuales pueden ser financieros o no financieros (tabla 5).

Tabla 5. Controles en la operación

Controles Financieros	Controles No Financieros
• Esquema con niveles de autoridad para la aprobación de pagos. • Contar con descripciones y categorizaciones de cuentas contables claras. • Uso restringido del efectivo. • Delegación de funciones en la aprobación de pagos. • Verificar la prestación del servicio.	• Los procesos de licitación deben contar con al menos tres competidores. • Por lo menos deben ser dos las personas encargadas de evaluar y adjudicar las ofertas. • Se debe evaluar la verdadera necesidad de los servicios. • Es recomendable tener una tasa de contingencia y contar con pagos razonables. • Controlar la efectividad del servicio prestado.

Fuente: Deloitte (2017).

En cuanto al monitoreo, es importante saber quién es la persona que está a cargo de esta función para saber a quién y de qué manera se reportan los resultados. Por otro lado, si no existen métodos que permitan monitorear analizar o evaluar los riesgos, no se podrá tener certeza de qué deberá ser cuantificado y monitoreado.

2.1.3. Factores que definen el acierto del sistema antisobornos

Existen conceptos clave que influyen en la efectividad de este modelo integral. Entre los factores negativos se tiene que dicho modelo sea percibido por las distintas unidades de negocio como una amenaza que dificulta la fluidez de la empresa; por otro lado, el nivel de corrupción de un país afectará negativamente la efectividad de este sistema (Kafel, 2016). De otro modo, la literatura señala que puede existir una descoordinación entre unidades horizontales de apoyo y control, obtener informes o reportes insatisfactorios que no logren monitorear confiablemente las acciones de la empresa y no gestar una cultura corporativa comprometida a cumplir los lineamientos.

Según Manuhwa y Stansbury (2016), el hecho de que existan monopolios, como en el caso de los servicios públicos, las privatizaciones o los grandes proyectos de construcción, aumenta la posibilidad de corrupción y por ende puede mermar la capacidad efectiva del sistema antisobornos. Estos autores identifican tres niveles de prevención para disuadirlo: proyectual, corporativo y profesional.

Según Kafel (2016) la efectividad de este modelo está directamente relacionada con el compromiso real de la alta gerencia. Por consiguiente, si se tiene el esfuerzo coordinado en todos los niveles del negocio en cuanto a los controles, podrán estar más enfocados en los riesgos. Así mismo, si se respalda un enfoque estratégico que vaya desde la alta gerencia y que tenga más en cuenta cómo estos riesgos afectan la creación de valor y los activos de la empresa, los esfuerzos serán más certeros y no se gastarán recursos en vano.

2.2. Guía de Gestión del Riesgo de Fraude

Según el el convenio de la comisión europea, se puede definir al "fraude" como cualquier acción u omisión intencionada que está relacionada a la utilización o presentación de declaraciones o documentos falsos, inexactos o incompletos. El objetivo de estas acciones sería la percepción o la retención indebida de fondos. También es considerado fraude, el incumplimiento de la obligación expresa de comunicar información, que tenga como propósito y efecto el desvío de fondos hacia otros fines distintos de los que fueron concebidos en un principio (Comisión Europea, 2014).

La Guía de Gestión del Riesgo de Fraude pretende ser un apoyo para el Marco 2013 y sirve como guía de mejores prácticas en las organizaciones. El Marco 2013 es la revisión del marco original, Internal Control-Integrated Framework, publicado en el año 1992 por el Comité de Organizaciones Patrocinadoras de la Comisión Treadway, también conocido como COSO. Así, el Marco 2013 integra principios que proporcionan claridad sobre el diseño e implementación de sistemas de control interno, los cuales ayudan en la comprensión de los requisitos para que este sea efectivo. (Committee of Sponsoring Organizations of the Treadway Commission, 2016). Cabe resaltar que el mercado se ve beneficiado con la implementación del Riesgo de Fraude, debido a que genera una mejor imagen, mayor seguridad y se identifican a las organizaciones que optan por un ambiente sin sobornos.

La Guía de Gestión del Riesgo de Fraude (2016) orienta sobre el establecimiento de un programa general de gestión del riesgo de fraude que incluya:

- Establecimiento de políticas de gobernanza de este tipo de riesgo.
- Realización de una evaluación de riesgo de fraude.
- Diseñar y desplegar actividades de control preventivo y de detección de fraude.
- Realizar investigaciones.
- Seguimiento y evaluación del programa total de gestión del riesgo de fraude.

2.3. ISO 31000:2009[4]

La ISO 31000:2009 es una herramienta que proporciona los principios, el marco y un proceso para una adecuada gestión de riesgos (Choo & Goh, 2015). Puede ser utilizado por cualquier organización, independientemente de su tamaño, actividad o sector (Frigo & Anderson, 2011).

El uso de la ISO 31000 puede ayudar a las organizaciones a incrementar la probabilidad de alcanzar los objetivos, mejorar la identificación de oportunidades y amenazas, y asignar y utilizar recursos efectivamente para el tratamiento del riesgo. Sin embargo, la ISO 31000 no puede utilizarse con fines de certificación, solo proporciona una orientación para programas de auditoría interna o externa, por ello sus lineamientos deberían ser adaptados en las empresas en lugar de adoptados (Frigo & Andreson, 2014). Las organizaciones que lo utilizan pueden comparar sus prácticas de gestión de riesgos con un punto de referencia internacionalmente reconocido, proporcionando principios sólidos para una gestión y un gobierno corporativo eficaces. (International Organization for Standarization, 2009).

Algunos estándares relacionados a la ISO 31000 son:

- ISO Guide 73:2009, la cual proporciona una serie de términos y definiciones relacionados con la gestión de riesgo.
- ISO/IEC 31010:2009, que provee asesoramiento en temas de riesgo.

4 Para consultar la norma, visitar https://www.iso.org/iso-31000-risk-management.html

Para 2017 se realizó una nueva revisión de la ISO 31000. Por otro lado, según Choo y Goh (2015), al momento de adaptar la ISO 31000 en una compañía, la metodología más apropiada para lograrlo es el Six Sigma. Con ella se obtiene un enfoque orientado al cliente y los utiliza en conjunto con la información del negocio para identificar las necesidades de la gestión de riesgo. Por otro lado, indican que deberían existir nuevas metodologías que sean distintas al típico modelo de reducción de la varianza, debido a que existen empresas que tienen ventaja frente a los riesgos operacionales pues cuentan con mejor acceso a la información que poseen. Aunque, en algunos casos, este hecho puede dar lugar a especulaciones, es utilizado para manejar los fondos de mejor manera, dependiendo del grado de aversión al riesgo de la compañía.

Según Power (2005) la relación entre la gestión de riesgos que plantea la ISO 31000 con la gestión de riesgos operacionales parte de la reforma de regulación bancaria Basilea 2, la cual se encuentra actualmente en la versión tres y con miras a una cuarta versión para 2019. A partir de esta reforma, se tratan diversos elementos de la práctica de gestión de riesgos en materia regulatoria, que dan lugar a la gestión de riesgos operacionales. Además, el potencial de esta categoría radica en que tiene implicancias en el fraude, el procesamiento de errores, la administración de recursos humanos y los compromisos legales.

Resulta importante destacar quiénes son los actores que interactúan en la gestión de riesgos. Como lo proponen López et al. (2017), se puede elaborar un modelo de *partes interesadas* para tener un análisis más preciso de la norma, de acuerdo con las distintas áreas de la empresa. Esto permite observar tres sectores principales: los que gobiernan, los que son gobernados y los recursos que se utilizan en los procesos; estos requisitos pueden ser aplicados tanto para organizaciones del sector público como del privado y se presentan en el siguiente figura:

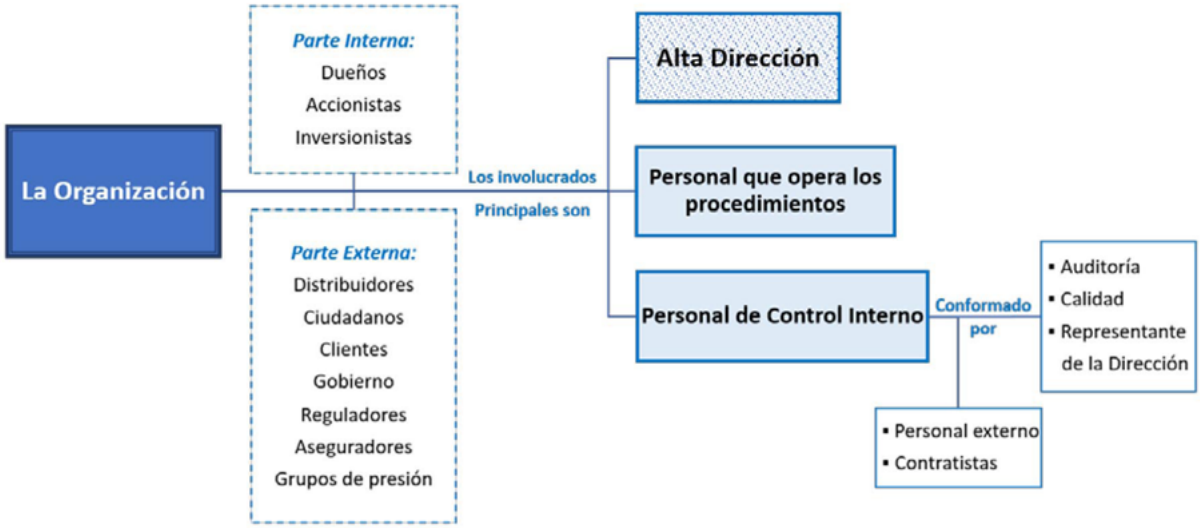

Figura 2. Contexto de la organización: modelo de partes interesadas
Fuente: elaboración propia con base en López, Garduño, Romero y Alvarado (2017).

2.3.1. Ciclo planificar, hacer, verificar y actuar o PHVA

Por otro lado, de acuerdo con Ramírez y Ortiz (2011), es posible utilizar el modelo PHVA para diseñar la metodología de la gestión de riesgos, además de ser beneficioso, ya que busca establecer un enfoque orientado a la mejora. El ciclo PHVA se define como una herramienta para lograr la mejora continua que consta de cuatro pasos: planificar, hacer, verificar y actuar.

De este modo, al momento de analizar la ISO 31000, se puede aplicar dicho ciclo y sus pasos. En primer lugar, en ***planificar*** se busca declarar los objetivos y los lineamientos para poder gestionar el riesgo (Montes & Garzón, 2013). Esto se realiza con la finalidad de obtener resultados que cumplan las expectativas de las políticas de la empresa y de su misión y visión. Diversos planes son hechos en esta etapa y pueden abarcar todos los tipos de riesgos

Hacer está ligado a todas las operaciones que se ponen en práctica para cumplir con los objetivos mediante los controles y procedimientos. En esta etapa se realiza la valoración y tratamiento de riesgos de acuerdo a la recopilación de datos (García, Quispe & Ráez, 2003).

Luego, se procede a ***verificar***, que según Yáñez (2012) significa revisar si los resultados de las evaluaciones fueron satisfactorios según la política y los objetivos de la empresa planteados durante la planificación. Esto es posible gracias a la medición de los riesgos y los impactos generados.

Finalmente, corresponde ***actuar***. En este momento, luego de haber verificado los indicadores, se implementan los cambios requeridos de acuerdo con los resultados y se puede establecer una política de gestión de riesgos a futuro. De este modo, se sigue con la mejora continua y el monitoreo constante de los riesgos (Ramirez & Ortiz, 2011). Esta metodología puede ser resumida señalando los factores claves en la figura 3:

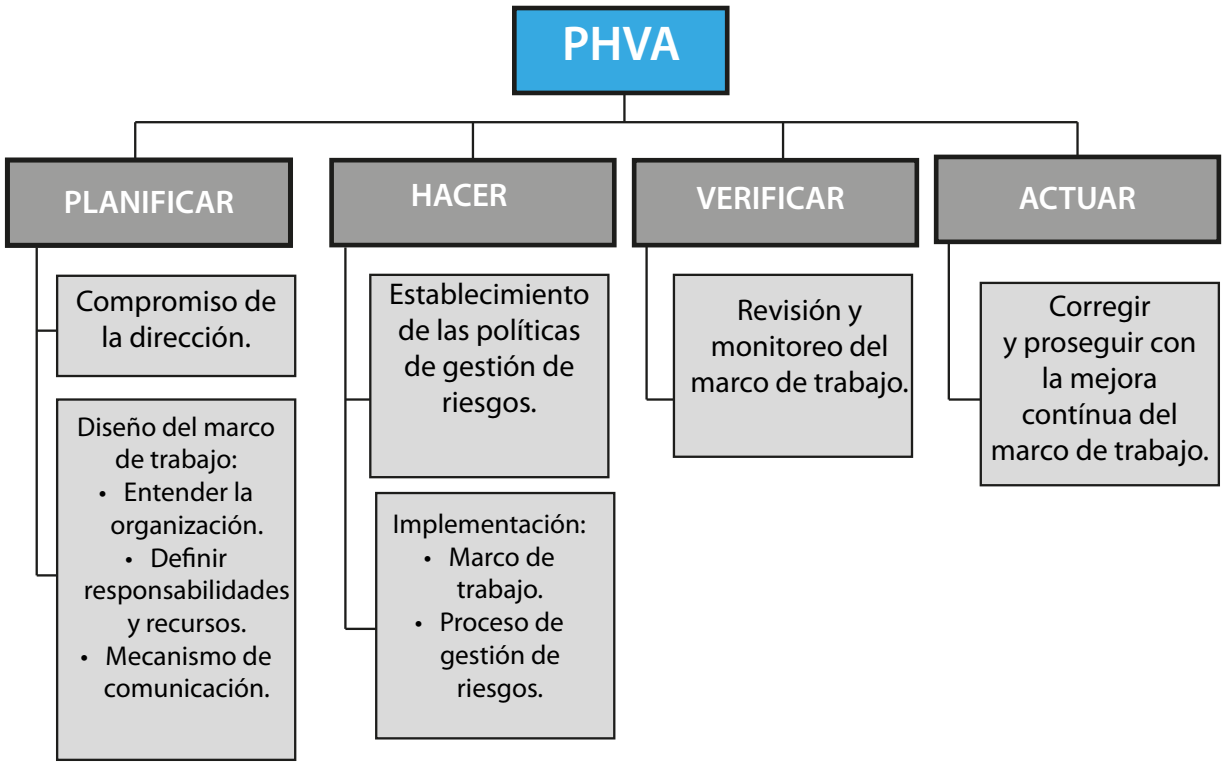

Figura 3. ISO 31000 en el ciclo PHVA
Fuente: elaboración propia con base en Ramírez y Ortiz (2011).

2.3.2. Requisitos

En su contenido, la ISO 31000 incluye puntos necesarios para cumplir con los lineamientos de la gestión de riesgos, llamados clausulas. Entre ellas se destacan, en primer lugar, el alcance de la norma, una definición de ella, en qué lugares aplicarla o cuándo aplicarla, es decir, propone los límites de su aplicabilidad dentro de las operaciones de la compañía:

estrategias, decisiones, procesos, funciones, proyectos, productos, servicios y activos. Así mismo, deja claro que no es específica para algún sector o industria y, más importante aún, para ningún tipo especial de riesgo.

En segundo lugar, están los términos y definiciones de lo que son los conceptos a tratar en la norma. Entre ellos se encuentran el riesgo, el poseedor del riesgo, el contexto externo, la identificación de las fuentes que generan el riesgo, la evaluación, el tratamiento y control de los riesgos, entre otros. En tercer lugar, se encuentran los términos y definiciones a adoptar por la empresa y los principios que constituyen directrices de carácter genérico para llevar a cabo dicha tarea. Según la norma, estos **principios** son los siguientes (tabla 6):

Tabla 6. Principios ISO 31000

Principios de la ISO 31000	
• Crear y proteger el valor.	• Ser hecha a la medida de sus valores organizacionales.
• Ser parte integral de los procesos organizacionales.	• Tomar en cuenta factores culturales y humanos.
• Ser parte de la toma de decisiones.	• Ser transparente e inclusiva.
• Abordar la incertidumbre.	• Ser dinámica, iterativa y receptiva al cambio.
• Ser sistemática, estructurada y precisa.	• Ser capaz de aplicar la mejora continua.
• Basada en la mejor información disponible.	

Fuente: elaboración propia con base en la norma ISO 31000.

De la tabla anterior, se puede indicar que el disponer de la mejor información representa una de las principales herramientas para poder realizar la implementación de la norma, ya que esta serviría como elemento de entrada para construir adecuadamente el sistema de gestión de riesgos.

Como cuarta clausula, se tiene el marco de trabajo. En él, la norma señala que el éxito de la gestión de riesgos llevada a cabo dependerá del manejo de este marco, que atraviesa todos los niveles de la empresa. Por otro lado, utilizarlo asegura que la información sea adecuadamente reportada y que sea usada para el proceso de toma de decisiones y demás responsabilidades en todos los niveles de la organización. Así mismo, cabe resaltar que la eficacia de esta cláusula radica en gestionar adecuadamente los riesgos según el marco de trabajo que propone la norma, el cual consta de consta de cuatro componentes (figura 4):

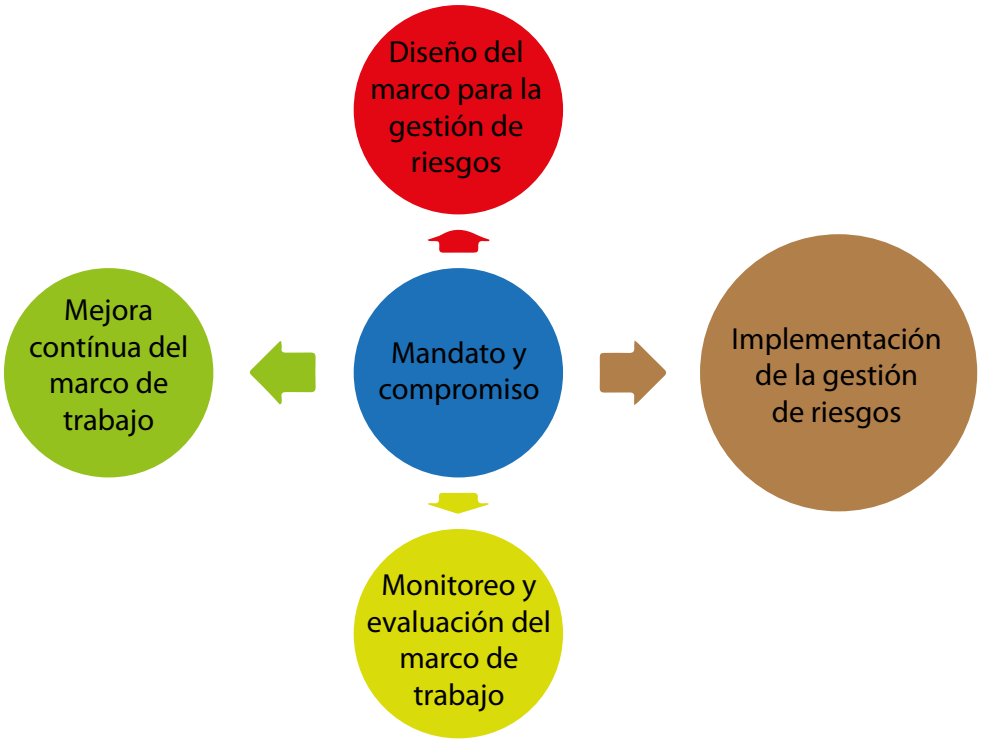

Figura 4. Marco de trabajo de la ISO 31000
Fuente: Elaboración propia con base en ISO 3100.

Por último, se tiene la quinta clausula, la cual explica el proceso de gestión del riesgo. Éste indica pasos como identificar el contexto de la organización, reconocer el riesgo y sus fuentes, analizar de qué manera el riesgo afectaría a la empresa, proceder a cuantificarlo, y finalmente realizar un plan para mitigar el riesgo. Así mismo, la norma señala que estas etapas deben estar enmarcadas en un ambiente de comunicación, consulta y manteniendo siempre el monitoreo y evaluación. Para ello, es necesario registrar el proceso de gestión de riesgos.

2.3.3. Metodología

Para poder ayudar al proceso de gestión, autores como Beasley, Branson y Hancock (2010), señalan la trascendencia de establecer indicadores de apoyo con el fin de servir como alertas y así poder anticiparse a las consecuencias. Según lo explicado acerca del riesgo operacional, se puede aplicar una primera metodología según la ISO 31000 para la gestión de riesgos operacionales. Es necesario determinar el nivel al que está expuesta la empresa luego de categorizar el riesgo según las áreas, como recursos humanos, clientes, información, tecnología de la Información, uso y administración de los recursos financieros. Luego se procede con la primera metodología:

- Identificar categorías generales y específicas del riesgo.
- Ponderar la probabilidad y gravedad de la ocurrencia del riesgo.
- Determinar el estado de cada foco de riesgos, mediante encuestas y entrevistas en la empresa.
- Crear mapas de situación para cada uno de los riesgos operacionales, buscando también mapas de acción alternativos.

Por otro lado, de acuerdo con Ramírez y Ortiz (2011) se propone una metodología un tanto distinta, pero bajo el enfoque de la mejora continua, esencial en la ISO 31000 y en cada proceso operacional de la empresa (figura 5).

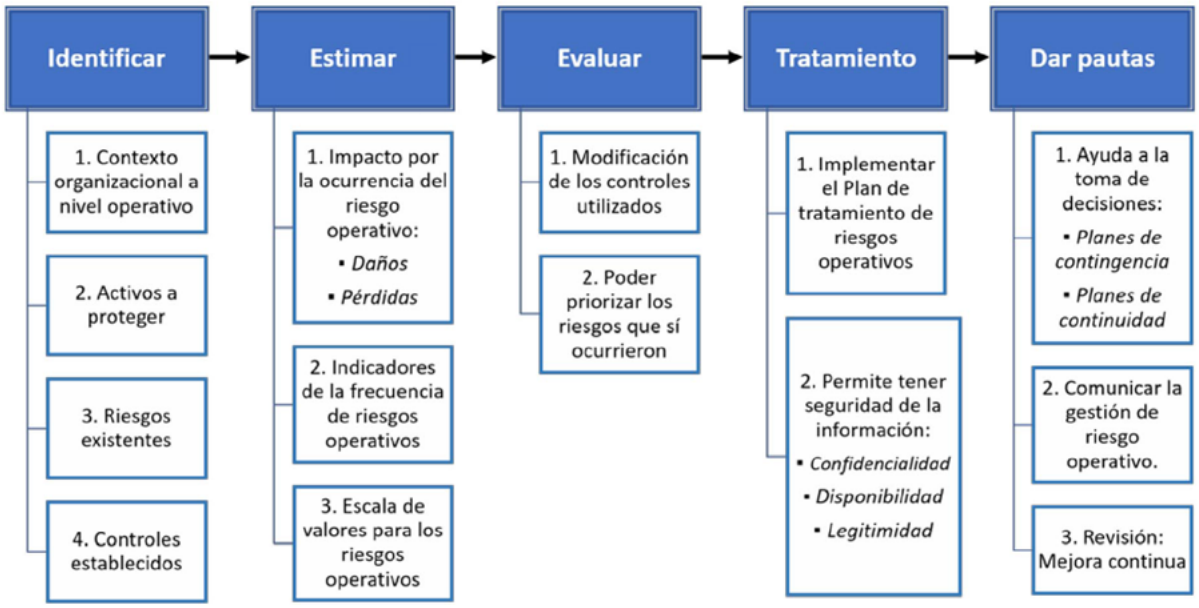

Figura 5. Pasos de la metodología de la gestión de riesgos
Fuente: elaboración propia.

Se resalta que los incidentes o riesgos respondidos de manera efectiva son parte de una gestión de riesgo operacional de calidad. Del mismo modo, el control de cambios para lograr una constante actualización de la gestión conlleva a una posterior mejora continua del negocio, la cual es citada ampliamente por la literatura como uno de los resultados de la ISO 31000.

Frigo y Anderson (2011), analizando la gestión estratégica de riesgos y el alcance de la norma, indican pasos necesarios para dar un valor agregado a la gestión de riesgos, entre los que se encuentra comunicar y compartir información externamente entre negocios, la cual es considerada una de las mejores prácticas a realizar en esta gestión. Así mismo, es posible señalar que la incertidumbre juega un papel importante en este sistema, ya que surgir por información que no está disponible, no es precisa o abarca cambios de probabilidades durante el tiempo.

Así, una manera de tratar estos riesgos operacionales es decidiendo si se continúa con la actividad operativa que lo genera o compartir el riesgo con otros niveles de la organización en el caso de un riesgo negativo.

2.3.4. Beneficios

Resulta importante resaltar la importancia de los sistemas de información de la empresa, de los cuales depende la eficacia de un sistema de gestión de riesgo basado en este estándar. Por ello, contar con indicadores como KPI's ayuda a poder prever fuentes de riesgo, por lo que poder adaptar las tecnologías de la información a las necesidad y objetivos de la empresa es la tarea complicada en este ámbito (López et al., 2017).

Luego de ello, gracias a la norma, es posible mejorar tres aspectos clave de la empresa: la gobernabilidad, la información financiera y la confianza de los grupos de interés o *stakeholders*. Así mismo, ser consistentes de la necesidad de identificar y mitigar el riesgo en el negocio genera una base para tomar decisiones y planificar.

Por otro lado, Stulz (1996) concluye que gestionar los riesgos también contribuye a que las empresas logren alcanzar el uso óptimo de su capital y de su estructura organizacional, debido a que se reducen los costos asociados a problemas financieros.

Por último, se cuenta con el beneficio de cumplir los reglamentos y requerimientos legales, con los cuales será posible cumplir con otras normas internacionales. Así, si se gestionan adecuadamente los riesgos operacionales, también se mejora la seguridad y la protección del medio ambiente de ser el caso. De acuerdo con González, Moreno y Henao (2017), el llevar una gestión de riesgos significa estar en la vanguardia de la planeación estratégica y asegurar la permanencia en el mercado gracias a la mejora continua. Finalmente,

podríamos afirmar que esta norma es beneficiosa porque consolida el conocimiento de los riesgos, lo cual se traduce en mayor competitividad de la empresa.

2.4. COSO 2013[5]

Es importante señalar que esta organización emitió una nueva estructura conceptual para COSO, luego de más de diez años de ejecución del marco de control interno emitido por el Committee of Sponsoring Organizations of the Tradeway Comission (COSO) en 1992 y su revisión en 2004, que se adecua eficientemente a los cambios importantes del entorno de negocios y operaciones actuales.

Power (2005) indica que la estructura del COSO ha sido usada como marco de referencia para bancos como Chase Manhattan en los procesos de riesgo operacional. Además, Dorsey y Brinkley (2015) plantean que el COSO 2013 significa un medio para lograr un objetivo y no un objetivo en sí mismo.

COSO 2013 (estructura 2013) ha mantenido los puntos clave del modelo de 1992:

- La definición del control interno como "un proceso efectuado por la Junta Directiva, las gerencias y otro personal de la organización, diseñado para proveer seguridad razonable en relación con el cumplimiento de los objetivos en las siguientes categorías: efectividad y eficiencia de las operaciones, confiabilidad de reportes, cumplimiento con leyes y regulaciones aplicables" (COSO, [en línea]).
- Las tres categorías de objetivos y los cinco componentes del sistema.
- El rol clave del juicio en el diseño, implementación y evaluación de la efectividad del sistema de control interno.

Sin embargo, los principios y puntos de atención si han introducido cambios en cada uno de los componentes, todo ellos con el objetivo de mejorar y facilitar la implementación y el mantenimiento del sistema de control interno. En ese sentido, como indica Rittenberg (2013), los cambios más resaltantes se centraron en:

5 Para consultar, visite https://www.coso.org/

- Un enfoque basado en 17 principios.
- Aclara la necesidad de establecer los objetivos estratégicos como condición previa a la fijación de los objetivos de control interno.
- Refleja la importancia del uso de tecnología de la información.
- Fortalece los conceptos de gobierno corporativo.
- Amplía el objetivo del reporte financiero.
- Fortalece la importancia de asumir que existe expectativa de fraude en cualquier evaluación.
- Considera los diferentes modeles de negocio y estructuras empresariales.

La nueva estructura actualizada considera el uso de principios para describir los componentes del control interno. COSO 2013 contiene 17 principios que explican los conceptos asociados con los cinco componentes de la estructura de COSO. Una muy buena ayuda que ofrece esta actualización para el gestor es el uso de puntos de atención que describen de manera adicional cada principio. Crear una manera más formal para diseñar y evaluar el control interno de acuerdo con los principios COSO 2013 amplía las discusiones sobre cada componente y principio, por ejemplo, la evaluación del riesgo incluye discusiones sobre riesgo inherente, tolerancia al riesgo, relación entre actividades de control y el riesgo, etc. Además de lo descrito líneas arriba, se incluye en forma explícita que toda evaluación de riesgos debe considerar el riesgo de fraude. En la tabla 8 se muestran los principios de la Estructura de COSO 2013.

Tabla 7. Estructura de Control Interno COSO 2013

ESTRUCTURA DEL CONTROL INTERNO – COSO 2013				
AMBIENTE DE CONTROL	**EVALUACIÓN DE RIESGOS**	**ACTIVIDADES DE CONTROL**	**INFORMACIÓN Y COMUNICACIÓN**	**SUPERVISIÓN**
Principio 1. Demostrar responsabilidad frente la integridad y los valores éticos. **Principio 2.** Poseer responsabilidad por la vigilancia. **Principio 3.** La empresa debe desarrollar su estructura con autoridad y responsabilidad. **Principio 4.** Se muestra el compromiso para reclutar, capacitar y retener personas competentes y comprometidas. **Principio 5.** Mantener en la organización a los empleados de confianza comprometidos con las responsabilidades de control interno.	**Principio 6.** Se detallan acciones claras para identificar y evaluar riesgos, los cuales ayudan con el logro de los objetivos. **Principio 7.** Identificar y analizar los riesgos para determinar cómo se deben ser mitigados. **Principio 8.** Tener en consideración sobre posibles casos de fraude en la evaluación de riesgos. **Principio 9.** Reconocer y valorar modificaciones que podrían afectar de manera importante el sistema de control interno.	**Principio 10.** Elegir el tratamiento de actividades de control que aporten a la disminución de los riesgos a niveles aceptables. **Principio 11.** La organización debe seleccionar y desarrollar actividades de controles generales de tecnología para apoyar el logro de los objetivos. **Principio 12.** Implementar diferentes actividades de control gracias a las políticas y procedimientos.	**Principio 13.** Crear y usar información de calidad para el soporte en el funcionamiento del control interno. **Principio 14.** Comunicación interna de los objetivos y las responsabilidades de control interno. **Principio 15.** Comunicación externa de los asuntos que afectan el funcionamiento de los controles internos.	**Principio 16.** Con el propósito de resolver si los componentes del control interno están presentes y funcionando, se realizan evaluaciones sobre la marcha y por separado. **Principio 17.** Evaluar y comunicar de manera oportuna sobre las deficiencias en el control interno, principalmente a los responsables de tomar acciones correctivas, lo cual incluye a la alta dirección y al consejo de administración.

Fuente: COSO 2013.

2.5. ISO 9001:2015

La norma ISO 9001 es sobre gestión de la calidad, perteneciente a la familia de las ISO's 9000 de normas de sistemas de gestión de la calidad (junto con ISO 9004). La norma ayuda a las organizaciones a cumplir con las expectativas y necesidades de sus clientes, y entre otros beneficios, complementa la gestión y control al enfocarse en la calidad de todos los procesos. Por otro lado, es la que tiene mayor reconocimiento en el mundo en cuanto a gestión de la calidad, y además es considerada un estándar de referencia, debido a que detalla cómo lograr un *performance* y servicio consistentes

(British Estándar Institution, 2016). La ISO 9001 no es un estándar obligatorio para las empresas, sin embargo les sirve para compararse con otras, por tanto podría ser considerada como un estándar certificable base en la actualidad.

La ISO 9001 versión 2015 trae consigo cambios importantes, como la incorporación de la gestión del riesgo o el enfoque basado en riesgos dentro de los Sistemas de Gestión de la Calidad; además, existe un periodo de transición de tres años por el cual, a partir de 2018, los certificados de la versión del 2008 no tendrán validez (Escuela Europea de Excelencia, 2015).

Así mismo, este estándar presenta cambios en su estructura los cuales buscan ser de alto nivel y lograr que el tiempo y recursos invertidos en la gestión sean reducidos considerablemente.

Según Torres et al. (2015), los requisitos de esta norma tienen una relación directa o indirecta con la gestión de riesgos, es decir, de cumplirla se estaría acercando de cierto modo a los lineamientos de dicha gestión. Esto puede inferirse debido a que una gestión de calidad debería tomar en cuenta el riesgo, en menor o mayor medida. Así mismo, uno de los objetivos de la norma es asegurar la consistencia de la calidad que ofrece.

La ISO 9001:2015 está compuesta por diez capítulos que puede ser divididos en dos partes. La primera abarca las generalidades: alcance, referencias normativas, términos y definiciones. La segunda está conformada por los requisitos que deben ser implementados para lograr un sistema de gestión de calidad, en ella encontramos: contexto de la organización, liderazgo, planificación, soporte, operación, evaluación del desempeño y mejora. Esta norma, al igual que la ISO 3100, tiene a mejora continua como objetivo.

De acuerdo con Medic, Karlovic y Cindric (2016), esta norma, que incorpora el pensamiento basado en riesgos, trata de lograr el sistema de gestión preventivo mediante sus requerimientos. Así mismo, señala al riesgo expresado como el resultado de la probabilidad y la consecuencia del evento potencial que lo genera; sin embargo, en la ISO 31000 el riesgo está mejor definido como el efecto de la incertidumbre en los objetivos. Por otro lado, el estándar incorpora en su nueva versión una sección de operaciones, la cual conlleva a una gestión basada en procesos que deben operar de manera unificada e integrada.

En ese sentido, una de las ventajas del enfoque en procesos de la norma es que toma en cuenta las interacciones entre los niveles jerárquicos y operacionales de la empresa. Morelos, Fontalvo y Vergara (2013) sostienen, con base en los resultados obtenidos en su estudio, que con una certificación como la ISO 9001 la empresa obtiene un mayor margen operacional (ratio entre la utilidad operacional y las ventas). Además, una mejor gestión administrativa, ocasionada por esta norma, ayuda a generar estos beneficios financieros tangibles para la empresa (Lizarzaburu, 2015). En consecuencia, se puede deducir que su relación con la gestión del riesgo operacional se origina a partir del cumplimiento de los lineamientos de esta norma para controlar las operaciones y así, contar con un plan operacional que tome en cuenta los riesgos en pos de la búsqueda de la calidad.

Finalmente, entre los beneficios de esta norma se encuentra una mayor satisfacción del cliente, una empresa más productiva y un mejor enfoque en los procesos y sus relaciones, lo cual conlleva a una mejora continua en la calidad que puede convertirse en ventaja competitiva (Lizarzaburu, 2015). De este modo, de acuerdo con la literatura, se puede inferir que su efecto positivo para la gestión de los riesgos operacionales se origina a través de identificar los procesos y sus consiguientes riesgos de manera más estructurada.

3. Aspectos nuevos a considerar: riesgo cibernético (*cyber risk*)

Uno de los ejemplos de riesgo en el caso de tecnologías o sistemas de información es el riesgo el riesgo cibernético (*cyber risk*).

El riesgo cibernético es definido como la exposición a daños o pérdidas, que resultan de infracciones o ataques a los sistemas de información. Una mejor definición podría ser el potencial de pérdida o daño relacionado con la infraestructura o el uso de la tecnología dentro de una organización. (RSA, s.f.).

Olsen (2013) menciona los tipos de riesgo cibernético:

- Ataque de hacker.
- Violación de datos.

- Transmisión de un virus.
- Extorsión cibernética.
- Saboteo de empleados.
- Tiempo de inactividad de la red.
- Responsabilidad multimedia.
- Error humano.

Olsen (2013) también afirma que cualquier empresa u organización que almacene información personal identificable que dependa de páginas web, información digital, internet, redes y computadoras, está expuesta a este tipo de riesgo.

De acuerdo con Fox y Antonucci (2017), la ISO 31000:2009 se integra con la gestión de las tecnologías de información de una empresa, porque provee de guías deseables que están en línea con dicha área, y señalan que, aunque el término *cyber* se suele utilizar para referirse a un sector en específico de las TI, la gestión debe abarcar todos los niveles de la organización y actividades relacionadas con esas tecnologías. Según el Allianz Global Corporate y Specialty (2015), el aumento de la interconectividad, la globalización y la «comercialización» de la ciberdelincuencia generan una mayor frecuencia y gravedad de los incidentes cibernéticos, incluidas las violaciones de datos. Uno de los principales riesgos de este tipo es la privacidad y protección de los datos; sin embargo, la legislación se ha vuelto dura en algunos países como Estados Unidos, Hong Kong y Australia, y en algunos países de la Unión Europea.

Por otro lado, entre los principios para manejar el riesgo cibernético se encuentran los COBIT 5 (Control Objectives for Information and related Technology), los cuales proporcionan un marco de trabajo que se centra en cinco fundamentos: conocer las necesidades de los accionistas, proporcionar una perspectiva holística, considerar la empresa a fondo, aplicar un modelo único e integrado y, finalmente, separar la gestión del gobierno de las tecnologías de la información (Fox, 2017).

Finalmente, Ramirez y Ortiz (2011) sustentan que, debido a las grandes pérdidas a las que están expuestas las empresas por el riesgo tecnológico, es imperativo contar con planes de seguridad que se enfoquen en la creación de conciencia en seguridad informática y así tener una efectiva cultura preventiva.

4. Propuesta de aplicación: área de riesgos

4.1. Propuesta de esquema general de riesgos

El esquema de riesgo a plantear no busca ser una camisa de fuerza, sino que bien manejado se convierte en un mecanismo que no sólo evita pérdidas, sino que aumenta las posibilidades de ganancia. A fin de alcanzar este objetivo, es necesario que la totalidad de la estructura de la firma esté identificada y aplique el esquema de riesgos.

El proceso de Planeación de la gestión de riesgos planteado se dará a través de las siguientes fases:

4.1.1. Niveles para la gestión de riesgos

- Nivel A. Desarrollo de algunos programas para la gestión de riesgos.
- Nivel B. Desarrollo de una conciencia sobre el riesgo en áreas independientes, sin una concepción centralizada ni políticas claras establecidas.
- Nivel C. Desarrollo de una conciencia de riesgo, con controles diarios.
- Nivel D. Desarrollo de personal encargado de analizar las fuentes de riesgo en las diferentes áreas, las cuales se basan en los juicios de dicho personal para la toma de decisiones.
- Nivel E. Desarrollo de una conciencia a nivel global y de la Junta Directiva, la cual patrocina departamentos independientes de riesgo que se interrelaciona con las diferentes áreas, en capacitación, procesos, controles, monitoreo y toma de decisiones, bajo un entorno estratégico.

4.1.2. Identificación del riesgo en una empresa

Se debe tener en cuenta que el ente que controle el riesgo no debe ser parte del área comercial, es decir, es importante que no se presenten conflictos de intereses. Siendo así, para identificar el riesgo en una empresa, se propone clasificarlos en riesgos de crédito, de mercado y operacionales.

Luego, es posible identificar tres etapas mediante un enfoque sistémico que permita lograr la meta de la gestión global del riesgo. Dicha metodología se presenta en la tabla 8.

Tabla 8. Etapas en la Gestión de Riesgos de acuerdo al tipo de riesgo

		ETAPA I	ETAPA II	ETAPA III	
Enfoque sistemático para la toma de decisiones en un entorno en incertidumbre	**[1] Riesgo de Crédito y Emisor**	Establecer políticas para la gestión del riesgo de crédito y emisor.	• Desarrollo de modelos y sistemas. • Reporte automálastico. • Inversión según LSD oportunidades.	Iniciar una gestión activa del portafolio Crear alertas de prevención.	META: Gestión Global del Riesgo
	[2] Riesgo de mercado	Creación de metodologías para el control del riesgo de mercado.	• Tener un marco y política definida. • diseñar la estrategia y controles del riesgo de mercado. • Alinear la estrategia de riesgos con las políticas de la empresa.	Se desarrolla el *stresstesting* a la empresa.	
	[3] Riesgo Operacional	Implementación del plan de gestión operativa.	• Tener un marco y política definida. • Contar con modelos de contingencia. • Demarcación de funciones y responsabilidades.	Adquirir seguros para cubrir riesgos.	
	[4] Introducción del concepto de gestión global del riesgo	Apoyo de la Junta Directiva y de las áreas de Gestión.	• Nombramiento de los gerentes de riesgo. • Marco y política definida con los niveles de tolerancia. • Desarrollo de reportes de riesgo global.	Desarrollo de stress-testing y sus planes de respuesta.	

Fuente: elaboración propia.

4.2. Propuesta de Estructura en la Gestión de Riesgos

La estructura básica en la gestión de riesgos consta de tres niveles:

I. Junta directiva.
II. Área de administración riesgos.
III. Comité de de riesgos.

El área a definir debe ser independiente; dentro de las funciones a evaluar de cada una de ellas se mencionan las siguientes (tabla 9):

Tabla 9. Funciones de la junta directiva y el área de riesgos

Junta Directiva	Área de riesgos
Aprobación estructura de riesgos.	Montar la estructura de riesgos de acuerdo con las líneas de negocio de la firma.
Aprobación mecanismos para administrar riesgos.	Evaluar límites para enfrentar el riesgo.
Aprobar límites de exposición al riesgo.	Velar porque las políticas de cubrimiento de riesgo se cumplan.
Velar porque la estructura de riesgos esté actualizada.	Hacer seguimiento a las estructuras de riesgo.
Velar por una mayor "cultura de riesgo".	Informar a la junta directiva, a la presidencia y, en general, a la parte comercial los límites que se tienen en riesgo.
Establecer programas de capacitación para los miembros de la administración de riesgo.	

Fuente: elaboración propia.

4.3. Comité de riesgos

Las actividades que el comité de riesgos debe realizar en una gestión de riesgo operativa son:

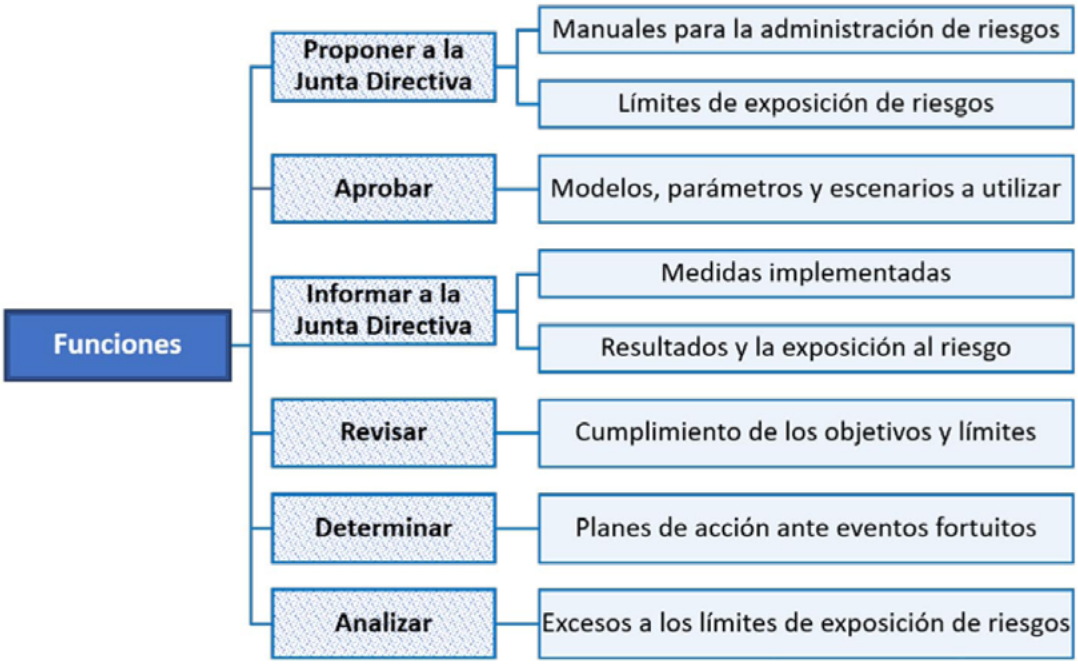

Figura 6. Funciones del comité de riesgos
Fuente: elaboración propia.

Conclusiones

En la presente investigación, se han señalado, analizado e identificado los beneficios y las implicancias de las normas ISO 31000, ISO 37001 y complementariamente la ISO 9001 con la gestión de riesgos desde el enfoque operacional. Esto se realizó revisando la literatura y los documentos fuente que explicaban un claro proceso en la tarea de mitigar los riesgos por parte de las empresas.

Como hemos visto a lo largo de este artículo, es importante reconocer el entorno o el contexto de la organización, porque de esa manera se puede tener un mejor entendimiento del campo de trabajo en el que se aplicará la gestión de riesgos, debido a que se consideran los diversos grupos de interés. Conocer los recursos y la cultura organizacional de la empresa es vital para poder adaptar las normas y hacerlas a la medida de dicha estructura, con el objetivo de que sean ampliamente aceptadas por la organización.

Así mismo, de la revisión de literatura se evidencia la necesidad de contar con un equipo de liderazgo comprometido, que pueda transmitir los lineamientos para poder llevar a cabo una gestión de riesgos exitosa, la cual se debe traducir en reducir la severidad de los riesgos identificados. Como se ha analizado, las operaciones son fuente de riesgo en parte porque son operadas por personas, las cuales son susceptibles a cometer errores o incurrir en fraudes en busca de su propio beneficio; esto se ilustra claramente con el problema del agente-principal. Siendo así, la ISO 37001 es una herramienta que reduce la incertidumbre y puede contribuir a aumentar la confianza de los diversos grupos de interés.

Una gestión del riesgo deberá llevar a cabo los pasos que propone la ISO 31000. Estos indican identificar el riesgo, evaluarlo, analizarlo, mitigarlo, comunicarlo, monitorearlo y controlarlo, a treavñes de un proceso que cuente con retroalimentación (dinámica) para que puedan ser efectuados los cambios necesarios luego de ver los resultados de aquellos riesgos que no pudieron ser controlados, teniendo claro además los responsables de los planes de acciones y la segregación de funciones.

Por otro lado, resulta de suma importancia contar con un sistema de información que pueda proveer una base de datos con la cual trabajar una matriz de riesgo y gestionar las

políticas antisoborno que las empresas puedan implementar. Las organizaciones no suelen tener este tipo de data y, además, supone también la existencia de un riesgo cibernético que debe ser controlado, producto de potenciales "fugas de información".

El uso de las herramientas de gestión podría mejorar la reputación de las empresas tomando en consideración que este riesgo debe ser gestionado en ambas normas ISO y se presenta en todo tipo de empresas, incluida las bancarias (Lizarzaburu & Del Brio, 2016).

Siguiendo los estándares explicados, entre los principales beneficios de aplicar una gestión de riesgos y antisoborno se puede obtener una mejora en la gobernabilidad y la confianza tanto de los colaboradores como de los grupos de interés, ya que supone un valor agregado para la organización. De acuerdo con la literatura consultada, existe evidencia empírica que señala una reducción de costos al aplicar la gestión de riesgos.

Finalmente, se desarrolla el concepto de la mejora continua, el cual ilustra el establecimiento de planes estratégicos a futuros, basados en los resultados evaluados en la gestión de riesgos. Esto se relaciona con la ISO 9001 que tiene incidencia en la mejora de indicadores clave en las organizaciones. Se recomienda desarrollar capacidades de comunicación para lograr el compromiso de la empresa con las normas establecidas.

Referencias

Allianz Global Corporate y Specialty. (2015). *A Guide to Cyber Risk: Managing the Impact of Increasing Interconnectivity*. Recuperado de http://www.agcs.allianz.com/assets/PDFs/risk%20bulletins/CyberRiskGuide.pdf

Argandoña A. (2007). La Corrupción y las Empresas. Ocasional Paper, ISE Business School. Universidad de Navarra.

Baltov, M. (2016). Risk Management in the Business Projects. *Journal Business Directions/ Journal Biznes Posoki*, (2). 3-8.

Beasley, M., Branson, B., & Hancock, B. (2010). *Current State of Enterprise Risk Oversight and Market Percetions of COSO's ERM framework*. Recuperado de https://www.coso.org/Documents/COSO-Survey-Report-FULL-Web-R6-FINAL-for-WEB-POSTING-111710.pdf

British Estándar Institution. (2016). *Norma ISO 9001. Gestión de la Calidad.* Recuperado de http://www.bsigroup.com/es-ES/Gestion-de-Calidad-ISO-9001/

Bromiley, P., McShane, M., Nair, A., & Rustambekov, E. (2015). Enterprise Risk Management: Review, Critique, and Research Directions. *Long range planning, 48*(4), 265-276.

Burneo, K., Berggrun, L., & Lizarzaburu, E. (2013). El riesgo operacional, SAE16 y as5: herramientas de control y mejora. *Strategy y Management Business Review, 4*(1), 43-63.

Carillo-Menéndez, S., & Suárez, A. (2012). Robust Quantification of the Exposure to Operational Risk, Bringing Economic Sense to Economic Capital. *Computers y Operations Research, 39*(4), 792-804.

Castillo, M., & Mendoza, A. (2004). Diseño de una metodología para la identificación y la medición del riesgo operativo en instituciones financieras. *Revista de Ingeniería*, *19*, 45-52.

Chernobai, A., Rachev, S., & Menn, C. (2006). Empirical Examination of Operational Loss Distributions. En *Perspectives on Operations Research* (pp. 379-401). DOI: https://doi.org/10.1007/978-3-8350-9064-4_21

Choo, B., & Goh, J. (2015). Pragmatic Adaptation of the ISO 31000:2009 Enterprise Risk Management Framework in a High-Tech Organization Using Six Sigma. *International Journal of Accounting y Information Management, 23*(4), 364-382. Doi: 10.1108/IJAIM-12-2014-0079

Comisión Europea. (2014). *Evaluación del riesgo de fraude y medidas efectivas y proporcionadas contra el fraude.* Recuperado de http://www.mapama.gob.es/es/pesca/temas/fondos-europeos/guiaevaluacionriesgofraudeymedidascontraelfraude_tcm7-384121.pdf

Committee of Sponsoring Organizations of the Treadway Commission. (2016). *Fraud Risk Management Guide.* Recuperado de http://www.coso.org/documents/COSO-Fraud-Risk-Management-Guide-Executive-Summary.pdf

Croitoru, I. (2014). Operational Risk Management and Monitoring. *Internal Auditing y Risk Management, 9*(4), 21-31.

Crouhy, M., Galai, D., & Mark, R. (2005). The Essentials of Risk Management. Estados Unidos: McGraw Hill.

Cruz, M., Coleman, R., & Salkin, G. (1998). Modeling and Measuring Operational Risk. *Journal of Risk, 1*(1), 63-72.

Deloitte (2017). *Compliance 2.0. Sistema de Gestión Anticorrupción. Estándar ISO 37001:2016.* Recuperado de https://www2.deloitte.com/content/dam/Deloitte/cl/Documents/financial-services/cl-compliance.pdf

Dorsey, A., & Brinkley, M. (2015). COSO 2013: The path forward. *Internal Auditor, 72*(4), 71-73.

Escuela Europea de Excelencia. (2015). *Nuevas normas ISO*. Recuperado de http://www.nueva-iso-9001-2015.com/

Estándar Australiano. (1999). *Administración de riesgos*. Recuperado de http://www.bcu.gub.uy/Acerca-de-BCU/Marzo2016/Bibliograf%C3%ADa%20PGE/Administracion_de_riesgo_Estandar_Australiano.pdf

Fong-Wong, L., & Shad, M. (2017). Economic Valued Added Analysis for Enterprise Risk Management. *Global Business & Management Research*, (9), 338-347.

Fox, C., & Antonucci, D. (2017). Principles Behind Cyber Risk Management. En *The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities* (23-33). Wiley.

Frigo, M., & Anderson, R. (2011). Strategic Risk Management: a Foundation for Improving Enterprise Risk Management and Governance. *The Journal of Corporate Accounting y Finance, 22*(3), 81-88.

Frigo, M., & Anderson, R. (2014). Risk Management Frameworks: Adapt, Don't Adopt. *Strategic Finance. 96*(1), 47-52.

García, M., Quispe, C., & Ráez, L. (2003). Mejora continua de la calidad en los procesos. *Industrial Data, 6*(1), 89-94.

González, E. M. R., Moreno, J. C. A., & Henao, G. J. C. (2017). Evolución de la cultura de la gestión de riesgos en el entorno empresarial colombiano. *Journal of Engineering and Technology, 6*(1), 22-45.

Gutteling, J. M. (2015). *Risk communication*. DOI: https://doi.org/10.1002/9781118541555.wbiepc143

International Organization for Standarization. (2009). *ISO 31000 - Risk management*. Recuperado de http://www.iso.org/iso/home/standards/iso31000.htm

UNE-ISO 31000:2018, Gestión del riesgo. Directrices. Asociación Española de Normalización [AENOR]. Madrid, España. 28 de marzo de 2018.

Jiménez, E. (2010). *El riesgo operacional: metodologías para su medición y control*. España: Delta Publicaciones.

Kafel, P. (2016). *Anti-Bribery Management System as a Tool to Increase Quality of Live*. Papel presentado en la 1st International Conference on Quality of Life, Kragujevac, Serbia: Center for Quality.

Lehar, A. (2005). Measuring Systemic Risk: A Risk Management Approach. *Journal of Banking & Finance, 29*(10), 2577-2603.

Lin, C., & Chuang, C. (2016). Corruption and Brand Value. *International Marketing Review, 33*(6), 758-780.

Lizarzaburu, E. (2015). La gestión de la calidad en Perú: un estudio de la norma ISO 9001, sus beneficios y los principales cambios en la versión 2015. *Universidad y Empresa*, *18*(30), 33-54.

Lizarzaburu, E. R., Berggrun, L., & Quispe, J. (2012). Gestión de riesgos financieros. Experiencia en un banco latinoamericano. *Estudios Gerenciales, 28*(125), 96-103.

Lizarzaburu, E., & Del Brio, J. (2016). Responsabilidad Social Corporativa y Reputación Corporativa en el sector financiero de países en desarrollo. *Revista de Globalización, Competitividad y Gobernabilidad*, *10*(1), 42-65.

López, F., Garduño, E., Romero, A., Alvarado, V., & Caballero, M. (2017). Propuesta de un sistema de gobierno, riesgos y cumplimiento para ser alineado a distintas normativas y regulaciones en pequeñas y medianas empresas. *Revista electrónica sobre tecnología, educación y sociedad*, 4(7), 1-25.

Malgwi, C. (2016). Corollaries of Corruption and Bribery on International Business. *Journal of Financial Crime*. *23*(4). 948-964.

Manuhwa, M., & Stansbury, N. (2016). *Anti-Bribery Standards, Systems and Strategies for Optimising Engineering Projects Delivery*. Recuperado de http://www.academia.edu/19513530/Anti-Corruption_Strategies_and_Anti Bribery_Standards_in_Engineering

Martínez, J., & Venegas, F. (2013). Riesgo operacional en la banca transnacional: un enfoque bayesiano. *Revista de Economía*, *32*(1), 31-72.

Martínez, J., Martínez, M., & Venegas, F. (2016). An Analysis on Operational Risk in International Banking: a Bayesian Approach (2007-2011). *Estudios Gerenciales*, *32*(140), 208-220.

Medic, S., Karlovic, B., & Cindric, Z. (2016). New Standard ISO 9001:2015 and its Effect on Organisations. *Interdisciplinary Description of Complex Systems*, *14*(2), 188-193.

Montes, D., & Garzón, G. (2013). Desarrollo e implementación de un modelo de sistema de gestión de la calidad y plan de mejoramiento continuo, ajustado a la norma NTC-ISO 13485:2003, en una empresa manufacturera de dispositivos médicos. *Ingenium*, *8*(19), 47-54.

Morelos, J., Fontalvo, T., & Vergara, J. (2013). Incidencia de la certificación ISO 9001 en los indicadores de productividad y utilidad financiera de empresas de la zona industrial de Mamonal en Cartagena. *Estudios Gerenciales*, *29*(126), 99-109.

Núñez Mora, J. A., & Chávez Gudiño, J. J. (2010). Riesgo operativo: esquema de gestión y modelado del riesgo. *Análisis Económico, XXV,* 123-157. Recuperado de http://www.redalyc.org/articulo.oa?id=41313083007

Olsen, T. (2013). *Insurance Cyber Risk*. Recuperado de http://www.pwc.dk/da/arrangementer/assets/cyber-tineolsen.pdf

Pacheco, D. (2009). *Riesgo operacional: conceptos y mediciones*. Recuperado de https://www.sbif.cl/sbifweb/internet/archivos/publicacion_8511.pdf

Palma Rodríguez, C. (2011) ¿Cómo construir una matriz de riesgo operativo? *Ciencias económicas*. 29(1), 629-635.

Patterson, F. D., & Neailey, K. (2002). A Risk Register Database System to Aid the Management of Project Risk. *International Journal of Project Management*, *20*(5), 365-374.

Power, M. (2005). The Invention of Operational Risk. *Review of International Political Economy*, *12*(4), 577-599.

Real Academia Española. Recuperado de http://dle.rae.es/?id=Y5DSzSr

Ramirez, A., & Ortiz, Z. (2001). Gestión de riesgos tecnológicos basada en ISO 310000 e ISO 27005 y su aporte a la continuidad de negocios. *Ingeniería*, *16*(2), 56-66.

Rittenberg, L. (2013). COSO 2013. *Internal Auditor*, *70*(4), 60-65.

Rodriguez-Wyler, F. (2010). Riesgo Operativo. *Veritas IMCP,* 3-16. Recuperado de http://www.ccpm.org.mx/veritas/diciembre2010/images/Riesgo_Operativo.pdf

RSA (s.f). *Cyber Risk Appetite: Defining and Understanding Risk in the Modern Enterprise*. Recuperado de https://www.rsa.com/content/dam/rsa/PDF/2016/05/h15150-cyber-risk-appetite-wp.pdf

Samano, O. (2013). *Modelo de riesgo operacional. Maestro en administración. Instituto Politécnico Nacional.* Recuperado de http://148.204.210.201/tesis/1377536285920TESISMODELODE.pdf

Sigweb. (s.f.). *Matriz de Riesgo, Evaluación y Gestión de Riesgos*. Recuperado de http://www.sigweb.cl/biblioteca/MatrizdeRiesgo.pdf

Stein, M. (2000). The Risk Taker as Shadow: A Psychoanlytic View of the Collapse of Barings Bank. *Journal of Management Studies*, *37*(8), 1215-1230.

Stulz, R. M. (1996). Rethinking Risk Management. *Journal of applied Corporate Finance*, *9*(3), 8-25.

Torres, C., Malta, N., Zapata, C., & Aburto, V. (2015). Metodología de gestión de riesgo para procesos en una institución de salud previsional. *Universidad, Ciencia y Tecnología*, *19*(75), 91-102.

Wallison, P. J., & Calomiris, C. W. (2009). The Last Trillion-Dollar Commitment: the Destruction of Fannie Mae and Freddie Mac. *The Journal of Structured Finance*, *15*(1), 71-80.

Yánez, J., & Yánez, R. (2012). Auditorías, Mejora Continua y Normas ISO: factores clave para la evolución de las organizaciones. Ingeniería Industrial. *Actualidad y Nuevas Tendencias*, *3*(9), 83-92.