PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR - MATRIZ

FACULTAD DE CIENCIAS ADMINISTRATIVAS Y CONTABLES

PROYECTO DE INVESTIGACIÓN Y GESTIÓN EMPRESARIAL
PREVIO A LA OBTENCIÓN DEL TÍTULO DE
INGENIERÍA EN CONTABILIDAD Y AUDITORÍA - C.P.A.

DISEÑO DE FORMATOS PARA IMPLEMENTAR UN SISTEMA DE GESTIÓN DE RIESGOS DENTRO DE UNA EMPRESA SIGUIENDO LOS LINEAMIENTOS DE COSO – ERM EN LA CIUDAD DE QUITO

DENNISSE STEPHANIE VACA AGUILAR

DIRECTOR: WILSON SILVA MANTILLA, C.P.A.

LÍNEA DE INVESTIGACIÓN: GESTIÓN DE RIESGOS

QUITO, ENERO 2017

DIRECTOR:

Wilson Silva Mantilla, C.P.A.

INFORMANTES:

Mgtr. Carlos Sierra

Mgtr. Edmundo Maldonado

DEDICATORIA

Dedico este trabajo y todos mis años de estudio a mis padres, Mercy y Nelson, quienes han sido mi gran apoyo e inspiración a lo largo de toda mi vida. Sin sus consejos, palabras y comprensión no sería la persona que soy ahora.

A mi hermano Ariel, mi pequeño ángel, que alegra mis días y me hace querer ser una mejor persona y profesional para ayudarlo y guiarlo por un buen camino.

A mi familia, amigas y amigos quienes también forman otra importante parte de mi vida y me ayudan siempre a seguir adelante en todo sentido.

Dennisse

AGRADECIMIENTO

Quiero agradecer infinitamente a Dios por permitirme cumplir todos mis sueños en el tiempo que él ha decidido y ha determinado justo para mi, por darme sabiduría y fuerzas para seguir todos los días sin importar qué tan difícil yo pueda creer que todo es.

A mis padres, por tanto apoyo y confianza, por sus consejos, su paciencia y su infinito amor, no sé qué sería de mí sin ustedes, son mi inspiración y todo lo que hago y soy es por y para ustedes.

A mi familia, amigas y amigos, por su incondicional apoyo y confianza depositada en mí.

Al Ing. Wilson Silva por su comprensión, paciencia y su excelente guía para culminar una de las etapas más importantes de mi vida.

Dennisse

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN EJECUTIVO

El manejo de riesgos es un tema muy importante dentro de las empresas e influye significativamente en su correcto desempeño dentro del mundo comercial globalizado y altamente competitivo.

Su correcto manejo y desarrollo sitúa como necesidad la implementación de un sistema para poder gestionar los riesgos que se puedan presentar dentro de las operaciones diarias de una organización.

Esta investigación propone un modelo de gestión de riesgos empresariales basándose en los lineamientos que propone el Committee of Sponsoring Organizations of the Treadway Commission en su publicación Enterprise Risk Management (por sus siglas en ingles COSO-ERM); diseñando y dando a conocer tanto formatos como políticas de elaboración propia de cada uno de los ocho componentes que constan dentro del documento antes mencionado, que cualquier empresa dentro de la ciudad de Quito puede hacer uso para implementar su propio sistema de gestión de riesgos.

INTRODUCCIÓN

En todo momento las empresas, sin importar su naturaleza, buscan una gestión eficiente y eficaz de sus operaciones, la misma que casi siempre llega a ser uno de los objetivos primordiales dentro de una organización. En un marco de análisis empresarial se puede determinar que todas enfrentan riesgos ya sean de tipo interno o externo. Para poder lograr enfrentar riesgos presentes, las empresas se basan en estudios realizados, los cuales determinarán las debilidades, los riesgos y sus posibles impactos; luego de esto toman decisiones en base a los resultados obtenidos.

Actualmente todas las empresas deben contar con un sistema de gestión de riesgos, el cual debe ser capaz de identificar, procesar y monitorear los riesgos que posiblemente pueden presentarse en su entorno, tanto interno como externo a la organización. Sin embargo existen organizaciones que desconocen este tipo de sistemas y su importancia dentro de sus operaciones diarias, los cuales ayudarán a detectar situaciones desfavorables que afectarán al correcto desempeño y funcionalidad de las empresas. A la vez que se pueden detectar situaciones desfavorables, también se pueden determinar situaciones favorables que surgen como oportunidades para las empresas y que no han sido tomadas en cuenta para elevar el rendimiento de las mismas, las cuales tienen como resultado crear una empresa más competitiva y mejor establecida para salir al mercado.

La implementación de un sistema de gestión de riesgos empresariales dentro de una organización utilizando teorías y fundamentos básicos aceptados internacionalmente, es

muy importante ya que la organización se vuelve más competitiva dentro del mercado no solo nacional sino también internacional, adoptando políticas y metodologías que llama la atención de inversionistas, grupos de interés y clientes. Esta es una ventaja muy grande que una empresa puede tener frente a su competencia ya que además de poder identificar situaciones a tiempo, se destaca en el mercado por la adopción de prácticas que no muchas empresas dentro de nuestro mercado nacional lo hacen.

El conocimiento de teorías y metodologías de riesgos para aplicarlos a una empresa es bien visto dentro de un mercado competitivo, ya que se está a la vanguardia de lo que está pasando en la actualidad de las empresas. La oportunidad de tener un sistema bien implementado y con pasos efectivos, solo lo logran organizaciones que ponen en marcha prácticas que han sido aprobadas y elegidas por organismos reguladores mundiales.

Dentro de esta investigación se toma como base el documento elaborado por el Committee of Sponsoring Organizations of the Tradeway Commission llamado Gestión de Riesgos Empresariales (por sus siglas en inglés COSO-ERM) tanto su marco teórico como sus técnicas de aplicación. Esta es una de las metodologías más famosas y aceptadas dentro de las organizaciones alrededor del mundo en tema de gestión de riesgos y la implementación de un correcto sistema para gestionar, identificar y responder sobre los riesgos encontrados dentro de las actividades normales de una empresa. La utilización de esta metodología asegura a las organizaciones que sus operaciones y labores diarias se realizarán en función de identificación oportuna de eventos, una correcta evaluación y un acertado proceso de responder a sus riesgos, supervisar, controlar e informar sobre sucesos posteriores.

1 CONCEPTUALIZACIONES, IMPORTANCIA Y TEORÍAS APLICADAS PARA LA GESTIÓN DE RIESGOS EMPRESARIALES

1.1 DEFINICIONES

Al momento de hablar sobre la administración de riesgos empresariales, es indispensable enfatizar en la importancia que tiene la misma dentro de las organizaciones, para ello en primer lugar se definirán los principales conceptos a ser utilizados a lo largo de este proyecto.

1.1.1 Debilidad

La palabra debilidad hace referencia a todo lo que la organización posee dentro de ella y que es desfavorable para su desenvolvimiento en el mercado, ya sean actividades que no pueda realizar, recursos que no posea, entre otras cosas que hace que la empresa tenga una posición menos atractiva frente a los usuarios y su competencia.

Las debilidades son una parte de un conjunto de elementos que se analizan dentro de una organización para ver si esta se encuentra operando de la mejor manera y se puedan tomar decisiones acertadas y oportunas para el futuro desenvolvimiento de la empresa. A su vez se puede decir que las debilidades también son un tema que hace que las organizaciones puedan o no sufrir ciertas

situaciones que afecten a su labor diaria y deben ser analizadas y corregidas oportunamente para evitar posibles situaciones desfavorables.

1.1.2 Riesgo

En torno a lo que riesgo se refiere, existen diversas definiciones, de las cuales se puede decir que al riesgo se lo define como la probabilidad de ocurrencia de un hecho, el cual puede ser por motivo internos o ajenos a la empresa que se está analizando, son de fuente interna los que provienen de los controles y procedimientos efectuados dentro de la misma organización y son de fuente externa aquellos que se refieren al entorno en el cual la empresa opera y se relaciona.

Al riesgo también se lo conoce como: “Amenazas que se originan por circunstancias, que pueden afectar adversamente la habilidad de la organización para lograr sus objetivos y ejecutar sus estrategias”; otros lo consideran como una “medida de incertidumbre”. (Mantilla B., 2003)

Existen diversos tipos de riesgos en los que se pueden destacar los Riesgos del entorno, Riesgo operativo, Riesgo de mercado, Riesgo precio de insumos y productos, Riesgos de crédito, Riesgo legal, Riesgos laborales, Riesgos empresariales.

Riesgos del entorno: Se refiere a elementos como el país donde está ubicada la empresa, su naturaleza, la región y ciudad, además del sector, la industria y condiciones económicas, políticas, sociales y culturales. (Mejía Quijano, 2006)

Riesgos generados en la empresa: dentro de esta clasificación se pueden resaltar el riesgo puro y riesgo de mercado:

Riesgo puro: este riesgo al materializarse origina perdida, como un incendio, un accidente, una inundación. (Mejía Quijano, 2006)

Riesgo operativo: es la posibilidad de pérdidas ocasionadas en la ejecución de los procesos y funciones de la empresa por fallas en procesos, sistemas, procedimientos, modelos o personas que participan en dichos procesos. (Mejía Quijano, 2006)

Riesgo de mercado: puede generar ganancias o pérdidas a la empresa al invertir en bolsa, debido a la diferencia en los precios que se registran en el mercado. (Mejía Quijano, 2006)

Riesgo precio de insumos y productos: se refiere a la incertidumbre sobre la magnitud de los flujos de caja debido a posibles cambios en los precios que una empresa puede pagar por la mano de obra, materiales y otros insumos de su proceso de producción, y por los precios que puede demandar por sus bienes o servicios. (Mejía Quijano, 2006)

Riesgo de crédito: consiste en que los clientes y las partes a las cuales se les ha prestado dinero, fallen en el pago. La mayoría de las empresas se enfrentan ante este riesgo por cuentas por cobrar, pero esta exposición es más alta en las instituciones financieras. (Mejía Quijano, 2006)

Riesgo legal: se refiere a la pérdida en caso de incumplimiento de la contraparte en un negocio y la imposibilidad de exigirle jurídicamente el cumplimiento de los compromisos adquiridos. También se puede presentar al cometer algún error de interpretación jurídica u omisión en la documentación, y en el incumplimiento de normas legales y disposiciones reglamentarias que pueden conducir a demandas o sanciones. (Mejía Quijano, 2006)

Riesgos laborales: pueden ser accidentes de trabajo y enfermedades profesionales, pueden ocasionar daños tanto a la persona como a la misma empresa. (Mejía Quijano, 2006)

Riesgos empresariales: estos son los riesgos en los que esta investigación tendrá un punto de partida, en donde al riesgos empresarial se le puede definir como "fenómeno subjetivo-objetivo del proceso de toma de decisión entre diferentes alternativas en situación de incertidumbre, con la probabilidad de ocasionar efectos negativos en los objetivos de la empresa, produciendo después de realizarse la acción decidida un resultado peor del previsto". (Mejía Quijano, 2006)

1.1.3 Medición del Riesgo

Una vez identificados y clasificados los riesgos que una empresa puede llegar a tener, estos deben ser medidos y analizados para evaluar su probabilidad de ocurrencia y el impacto que estos pueden tener en las actividades de la empresa, para posteriormente tomar decisiones acerca de qué hacer con estos riesgos.

Para medir la probabilidad de ocurrencia de un riesgo, se lo puede clasificar de la siguiente manera:

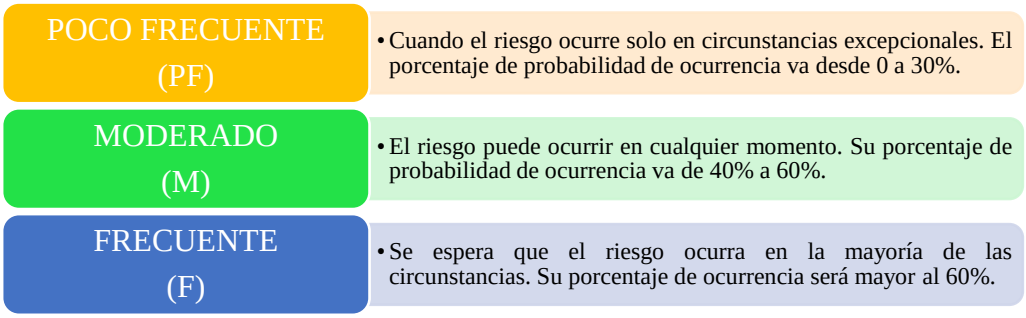


Figura 1: Probabilidad de ocurrencia del riesgo

Fuente: (Hernández Meléndez, 2006)

Después de analizada la probabilidad de ocurrencia, se debe proceder a analizar el impacto ante la ocurrencia de los riesgos, como se muestra en la siguiente tabla:

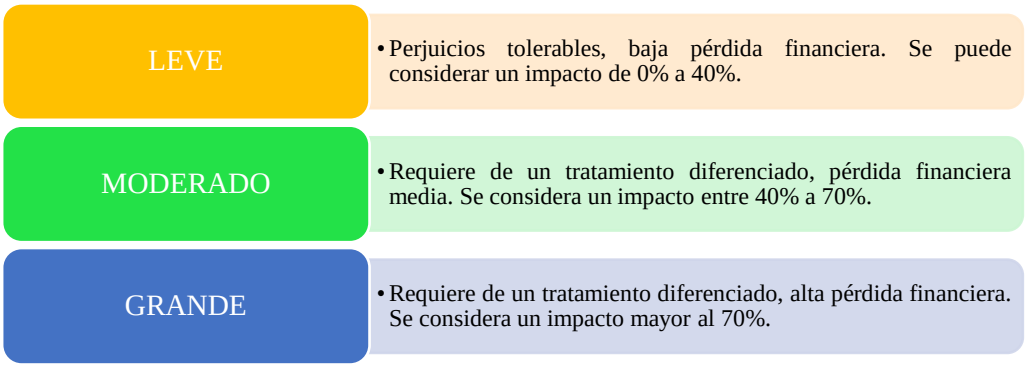


Figura 2: Impacto ante la ocurrencia del riesgo

Fuente: (Hernández Meléndez, 2006)

La evaluación de los riesgos después de analizado el impacto sería:

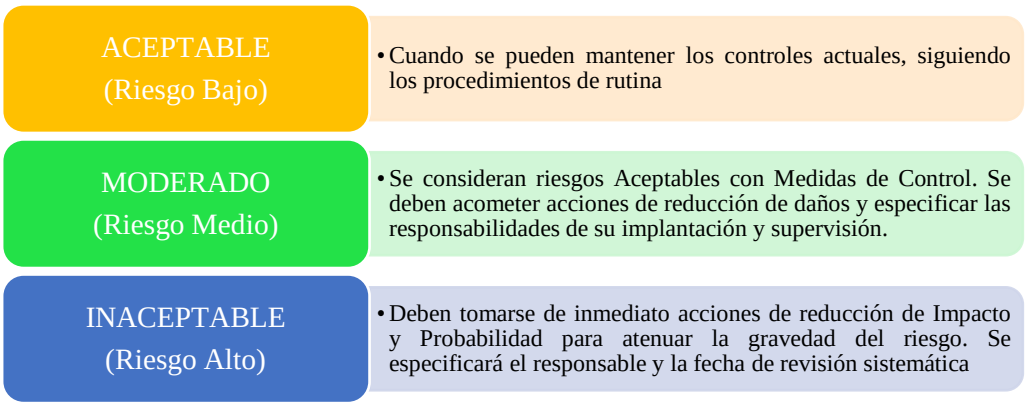


Figura 3: Evaluación del riesgo

Fuente: (Hernández Meléndez, 2006)

1.1.4 Respuesta al Riesgo

Después de determinados los riesgos potenciales que la empresa pueda llegar a tener, se evalúa la respuesta a esos riesgos, en donde a esta última se la define como las posibles respuestas que tenga la administración para aceptar, evitar, reducir o compartir los riesgos, utilizando diferentes acciones para que estos se

alineen con las estrategias de la empresa en cuanto a un riesgo aceptado y la tolerancia al riesgo establecida. (Mora, s.f.)

En esta respuesta al riesgo se deben encontrar actividades de control, las cuales aseguran que las respuestas a los riesgos se estén llevando a cabo eficazmente. A su vez se necesita de información y comunicación en donde se recibe información oportunamente para ser transmitida a los empleados para que asuman responsabilidades. Y por último la supervisión es importante para realizar modificaciones oportunas cuando sea necesario. (Mora, s.f.)

En respuesta a los riesgos encontrados se pueden, como se dijo en un inicio, evitar, aceptar, compartir y mitigar el riesgo, para lo que cual deben existir ciertas estrategias que acompañen con la acción tomada por la empresa. (Mora, s.f.)

1.2 IMPORTANCIA

Como se pudo observar en la definición de conceptos importantes, varios autores de obras acerca de la gestión de riesgos empresariales, coinciden en que existe una importancia muy grande dentro de lo que significa tener un sistema bien desarrollado para identificar y evaluar riesgos dentro de una organización.

Esta importancia radica en que las empresas siempre están y estarán expuestas a varias situaciones en que tanto los directivos de la empresa como los colaboradores, no tendrán una certidumbre de lo que pueda o no ocurrir, por lo que es necesario que estas

contemplen la necesidad de tener implementado un sistema que les permita identificar oportunamente situaciones de peligro para la empresa, es decir, riesgos, y como se ha dicho anteriormente estos pueden venir tanto de situaciones internas como externas a la compañía.

En primer lugar se debe entender la ventaja que una empresa puede llegar a tener al implementar un sistema bien estructurado de gestión de riesgos, debido a que dicha empresa está en constante cambio así como el entorno que la rodea, y el hecho de poder predecir ciertas circunstancias que puedan afectar el desempeño de la compañía hace que esta se ponga un paso más adelante que su competencia ya que no sufrirá por las mismas situaciones desfavorables o de peligro que puede que sufran el resto de empresas. Al momento de decir un sistema de gestión de riesgos, este se refiere a la capacidad de poder identificar riesgos, evaluar su ocurrencia e impacto dentro de la empresa y por ultimo saber qué tipo de decisiones tomar frente a lo que se ve que está ocurriendo dentro o fuera de ella.

1.3 GESTIÓN DE RIESGOS EMPRESARIALES

Los riesgos empresariales necesitan una gestión eficiente y eficaz para que puedan ser tratados de la mejor manera y a su vez se puedan tomar las mejores decisiones o planes de acción en torno a ellos. El informe (Committee of Sponsoring Organizations of the Treadway Commission, 2004) citado en (Ambrosone, 2007) define a la gestión de riesgos empresariales como:

> Un proceso efectuado por el consejo de administración de una entidad, su dirección y restante personal, aplicable a la definición de estrategias en toda la empresa y

diseñado para identificar eventos potenciales que puedan afectar a la organización, gestionar sus riesgos dentro del riesgo aceptado y proporcionar una seguridad razonable sobre el logro de los objetivos.

En base a múltiples definiciones existentes acerca de la gestión de riesgos empresariales y a diferentes teorías que han surgido acerca de cómo se debe llevar a cabo esta gestión, lineamientos y conceptos; a continuación se detallan los marcos de referencia más importantes y aceptados internacionalmente por las organizaciones.

1.3.1 ISO: International Organization For Standardization

En el año 2009 la Organización Internacional de Estandarización (por sus siglas en inglés ISO) crea un documento llamado ISO 31000 versión 2009: Gestión de Riesgos, Principios y Guías. Este documento pretende ser utilizado para la armonización de los procesos de gestión de riesgos, entre lo existente actualmente y lo fututo, proporcionar guías y lineamientos para la gestión de riesgos y su proceso implementado en un nivel operativo y estratégico de una organización. Esta norma no busca ser una certificación para las empresas ni tampoco instaurar una uniformidad de gestión de riesgos dentro de las mismas.

Junto con la norma ISO 31000:2009 coexisten dos normas más que hablan acerca de la gestión de riesgos dentro de las empresas, las cuales son:

ISO 31010- Gestión de Riesgos- Técnicas de Valoración del Riesgo.

ISO Guía 73 Gestión de Riesgos- Vocabulario.

La norma internacional, ISO 31000, puede ser aplicada a cualquier tipo de organización o institución, no es específica para ningún tipo de sector o industria. A su vez, esta norma puede ser aplicada para cualquier proceso o actividad que desarrolle la empresa y también ayuda para la aplicación a todo tipo de riesgo ya sea de hecho positivo o negativo dentro de la organización.

La implementación de esta norma establece que el sistema de gestión de riesgos cumpla con once principios elementales los cuales son:

- Crea valor
- Está integrada en los procesos de una organización
- Forma parte de la toma de decisiones
- Trata explícitamente la incertidumbre
- Es sistemática, estructurada y oportuna
- Está basada en la mejor información disponible
- Hecha a la medida
- Toma en cuenta factores humanos y culturales
- Es transparente e inclusiva
- Es dinámica, iterativa y sensible al cambio
- Facilita el realce y mejora continua de la organización

Además de los once principios ya mencionados, la ISO 31000 propone una estructura para la gestión del riesgo la cual debe ser dinámica y debe estar en constante movimiento, la estructura es la siguiente:

Figura 4: Estructura de gestión de riesgos

Fuente: (International Organization for Standardization, 2009)

Todo el proceso que ISO propone, al final del mismo, debe poder ser monitoreado y debe arrojar resultados para una buena toma de decisiones y mejora continua del proceso. Las decisiones relativas a la creación de registros deben tener en cuenta:

- Necesidades de la organización para el aprendizaje continuo;
- Los beneficios de la reutilización de la información a efectos de gestión;
- Costes y esfuerzos involucrados en la creación y el mantenimiento de registros;

- Necesidades legales, reglamentarios y operativos de los registros;

- Método de acceso, la facilidad de recuperabilidad y medios de almacenamiento;

- Período de retención, y

- La sensibilidad de la información. (International Organization for Standardization, 2009)

1.3.2 OCEG "Red Book" 2.0:2009

El Grupo Abierto de Cumplimiento y Ética (Open Compliance and Ethics Group por sus siglas en inglés) es una organización creada en el año 2002 a raíz de los fracasos económicos y de negocios como fueron Enron, Worldcom, y Healthsouth.

En un inicio la misión inicial del grupo fue mejorar el cumplimiento y la ética de las organizaciones, de ahí su nombre. Sin embargo con el tiempo los miembros de la organización se expandieron un poco más a lo que es la gestión del rendimiento, gestión de riesgos, gobierno y seguridad de las empresas.

Después de algunos meses, el primer estándar de OCEG surgió. En un inicio el libro se llamaba OCEG Modelo de las Capacidades. La portada del libro tenía un color rojo intenso, por lo que rápidamente fue conocido como OCEG Red Book (Libro Rojo).

En el año 2009 se saca al mercado una segunda versión del libro llamado GRC Modelo de Gobierno, Riesgo y Capacidad de Cumplimiento, el cual refleja un punto de vista más amplio, el del deseo de auditar al gobierno corporativo, gestión de riesgos y cumplimientos potenciales.

Este libro provee a las empresas una guía de alto nivel y detallada de las prácticas que ayudan a las organizaciones a direccionarse hacia temas del cumplimiento y la ética, sin embargo, también habla sobre la integración del gobierno corporativo, aseguramiento y administración del desenvolvimiento de la empresa, riesgos, cumplimiento y ética. (OCEG, 2009)

El libro dentro de sus páginas propone ocho componentes para una mejor gestión de riesgos junto con la participación del gobierno corporativo y el cumplimiento y la ética que una organización debe tener. Los componentes son los siguientes:

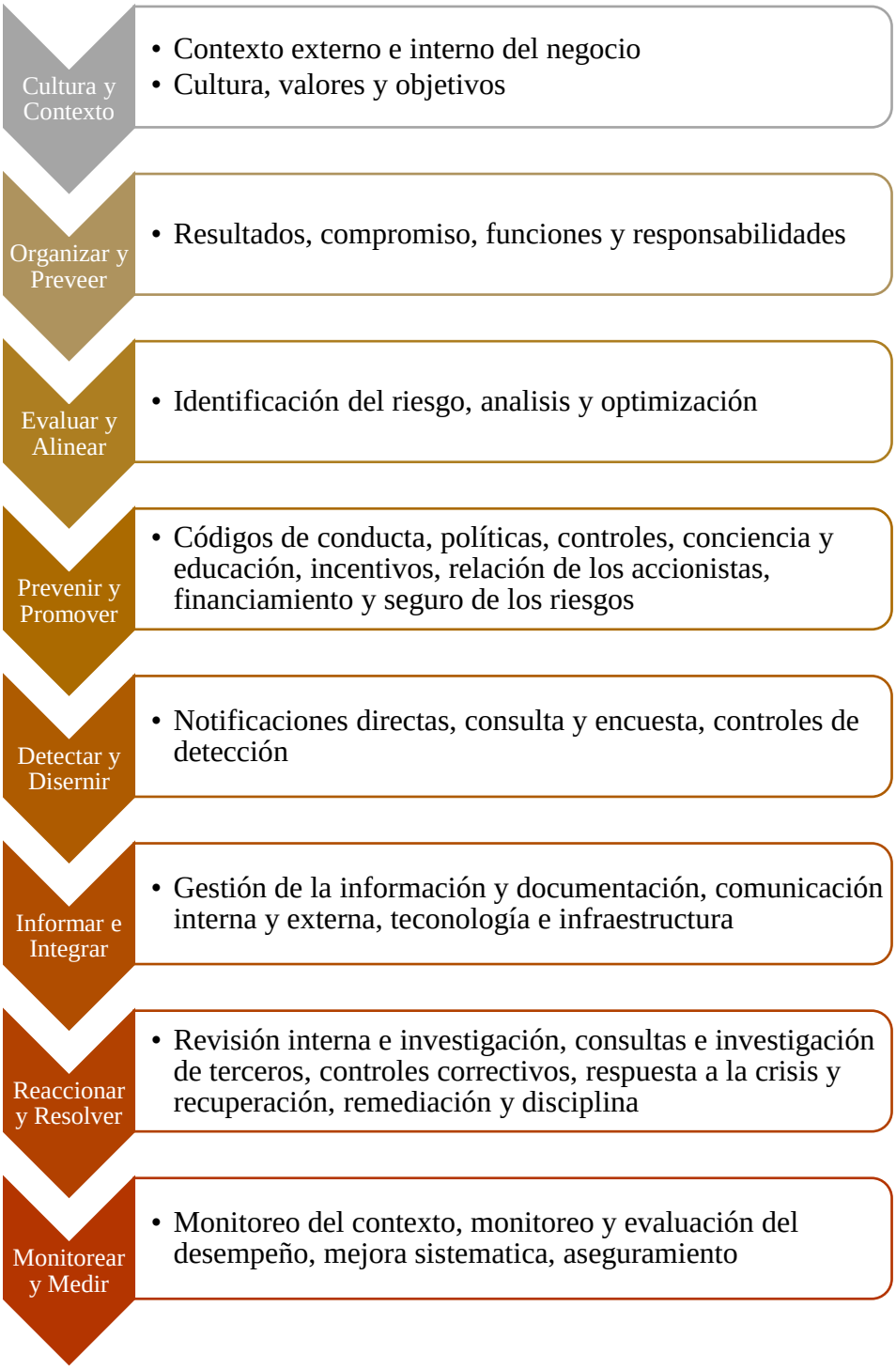


Figura 5: Componentes de GRC Modelo de Capacidades

Fuente: (OCEG, 2009) citado en (Fox, 2011)

Los componentes se relacionan como se puede observar en la siguiente figura:

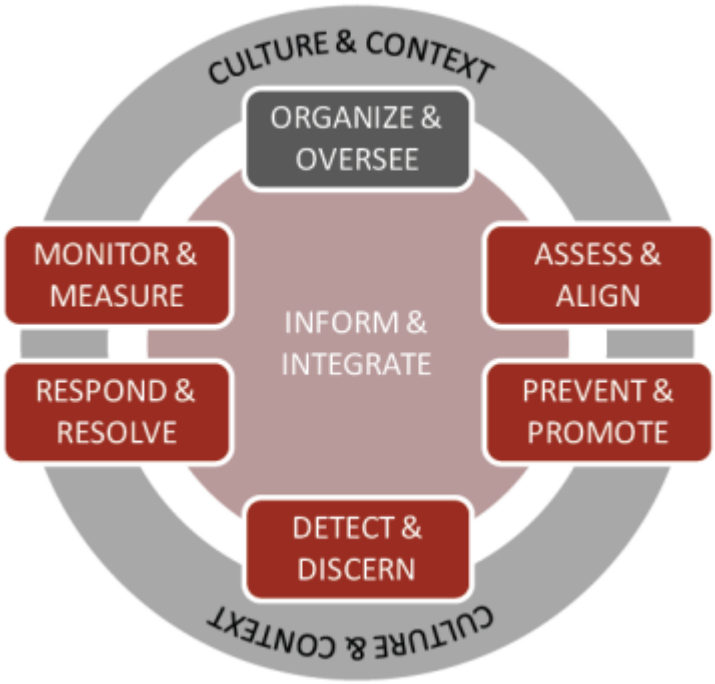


Figura 6: Relación de componentes

Fuente: (OCEG, 2009) citado en (Fox, 2011)

1.3.3 A Risk Management Standard

El estándar de gestión de riesgos fue publicado por el Instituto de Gestión de Riesgos (IRM por sus siglas en inglés) en el año 2002; junto con ellos también participaron de la creación de este documento organizaciones como la Asociación de Seguros y Gestión de Riesgos (The Association of Insurance and Risk Manager (AIRMIC)) y la Asociación Pública de Gestión de Riesgos (The Public Risk Management Association (Alarm)), para después ser adoptada por la Federación Europea de Asociaciones de Gestión de Riesgo (Federation of European Risk Management Association (FERMA)).

Este documento es una simple guía que da lineamientos prácticos y sistemáticos para la gestión de riesgos empresariales y brinda todo su apoyo a lo que la ISO 31000 imparte, por lo que comparten definiciones y ciertas guías para que una organización pueda llevar a cabo su sistema de gestión de riesgos.

Este estándar de gestión de riesgos propone un proceso general que las empresas deben seguir para gestionar sus riesgos, el cual consta de ocho pasos que están alineados también con lo que ISO propone. A continuación se presenta una figura con los pasos:

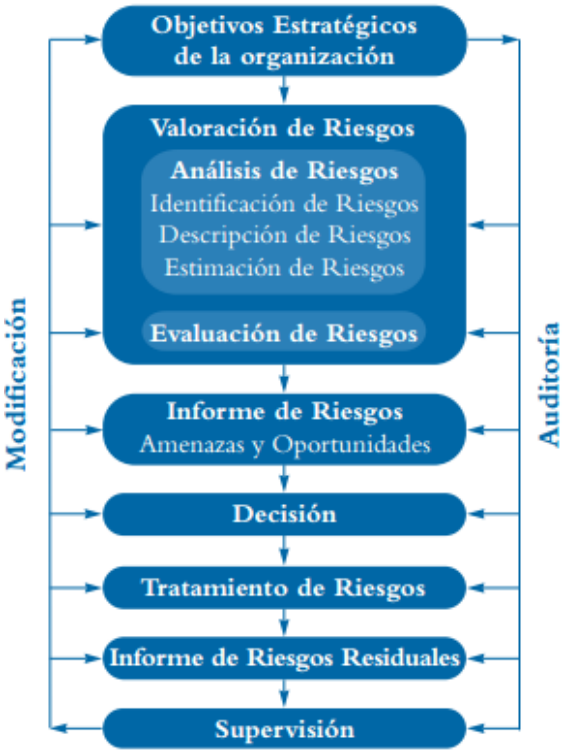


Figura 7: Proceso de gestión de riesgos según FERMA

Fuente: (The Institute of Risk Management , 2002) citado en (Federation of European Risk Management Associations, 2002)
Elaborado por: (Federation of European Risk Management Associations, 2002)

Es así como el IRM propone que con estos pocos pasos del proceso de gestión de riesgos, este último debe agregar valor tanto a la organización como a todos

sus grupos de interés mediante el apoyo de los objetivos de la empresa ya establecidos previamente.

1.3.4 Ley Sarbanes- Oxley

La Ley Sarbanes- Oxley o también llamada SOX, Sarbox o SOA, es una ley de Estados Unidos que es conocida como un Acta de Reforma de la Contabilidad Pública de Empresas y de Protección al Inversionista. Nació en el año 2002 con el propósito de controlar a todas las empresas que cotizan en bolsa de valores para evitar que el valor de sus acciones fuera fácilmente manipulado. Su objetivo principal es el de evitar fraudes, bancarrotas y proteger al inversionista en todo momento.

Esta ley se creó a raíz de los escándalos económicos y financieros de grandes corporaciones como fueron Enron, Tyco International, WorldCom y Peregrine Systems. Debido a la caída de estas grandes compañías, la reputación de las firmas auditoras fue puesta en duda alrededor del mundo.

Una de las partes más importantes de esta Ley, es la que establece una agencia privada llamada Public Company Accounting Oversight Board (PCAOB), la cual es la encargada de controlar a las firmas auditoras, establecer parámetros para medir controles internos y regular la independencia de las mismas; a su vez también impone sanciones a las empresas que incumplan que lo estipulado.

Entre los otros puntos que establece la Ley se encuentran (Ley de Sarbanes-Oxley, 2002):

- El requerimiento de que las compañías que cotizan en bolsa garanticen la veracidad de las evaluaciones de sus controles internos en el informe financiero, así como que los auditores independientes de estas compañías constaten esta transparencia y veracidad.

- Certificación de los informes financieros, por parte del comité ejecutivo y financiero de la empresa.

- Independencia de la empresa auditora.

- El requerimiento de que las compañías que cotizan en bolsa tengan un comité de auditoría, con consejeros completamente independientes, que supervisen la relación entre la compañía y sus auditores externos. Este comité de auditoría pertenece al consejo de administración, y los miembros que lo forman son completamente independientes a la misma.

- Prohibición de préstamos personales a directores y ejecutivos.

- Transparencia de la información de acciones y opciones, de la compañía en cuestión, que puedan tener los directivos, ejecutivos y empleados claves de la compañía y consorcios, en el caso de que posean más de un 10 % de acciones de la compañía. Asimismo estos datos deben estar reflejados en los informes de las compañías.

- Endurecimiento de la responsabilidad civil, así como las penas, ante el incumplimiento de la Ley. Se alargan las penas de prisión, así como las multas a los altos ejecutivos que incumplen y/o permiten el incumplimiento de las exigencias en lo referente al informe financiero.

- Protecciones a los empleados en el caso de fraude corporativo. La OSHA (Oficina de Empleo y Salud) se encargará en menos de 90 días de reinsertar al trabajador, se establece una indemnización por daños, la devolución del dinero defraudado, los gastos en pleitos legales y otros costes.

1.3.5 Comité de Basilea

En el año 1974 debido a la crisis financiera internacional presentada, se formó el Comité de Basilea, el cual estaba conformado por los países pertenecientes al G-10 y su sede de formación fue la ciudad de Basilea en Suiza. Este comité se instauró con el propósito de restaurar la confianza y estabilidad del sistema financiero internacional. Además de emitir un comunicado en el cual transmitían su apoyo al sistema de pagos internacionales, se formó un comité supervisor para desarrollar principios para las prácticas de regulación y supervisión de los mercados bancarios internaciones. (Baquero Herrera, s.f.)

Existen tres publicaciones del Comité de Basilea las cuales se denominan Basilea I, Basilea II y Basilea III. Basilea I hace referencia al capital regulatorio, el cual los bancos deben tener un capital mínimo, se dijo que era el 8% de sus activos de riesgo inicialmente, para poder cubrir sus riesgos de crédito, tipo de cambio

y mercado. Basilea II por su lado, fue creada debido a las limitaciones que poseía Basilea I, por lo que esta versión cuenta con tres pilares que explican de mejor manera la medición de los riesgos. A continuación se resumen los tres pilares:

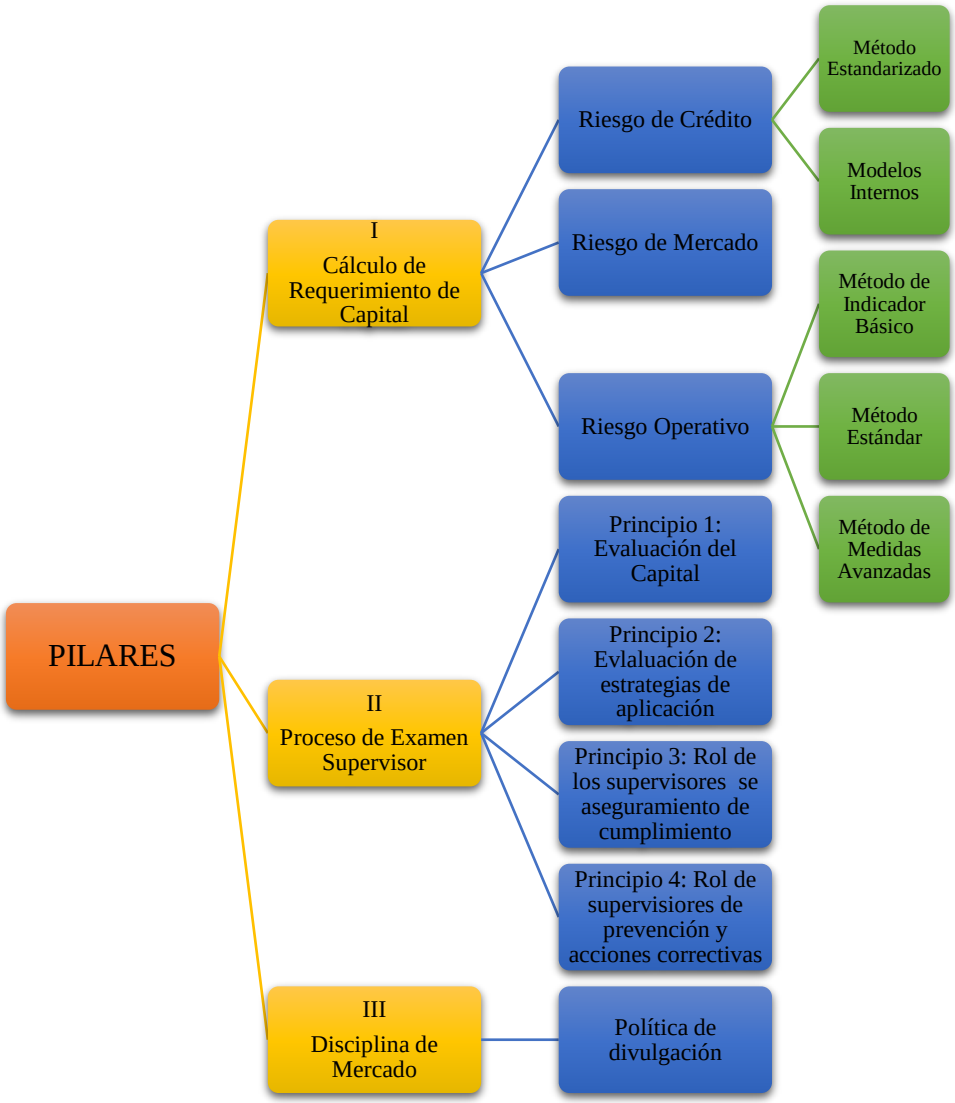


Figura 8: Pilares de Basilea II

Fuente: (Superintendencia de Banca y Seguros y AFP , 2006)

Los documentos del Comité de Basilea cuentan además con 25 principios que regulan toda la aplicación de esta norma:

Tabla 1: 25 Principios del Comité de Basilea

Condiciones previas para una efectiva Supervisión Bancaria: **Principio 1:** Proporcionar un sistema de gestión bancaria efectivo.
Autorizaciones y Estructura: **Principio 2:** Actividades de instituciones bancarias definidas y regulación de la palabra Banco. **Principio 3:** Proceso de autorización bancaria y la autoridad reguladora. **Principio 4:** Autoridad de los supervisores bancarios de rechazar propuestas de transferencia de propiedades y controlar interés de bancos. **Principio 5:** Autoridad de los supervisores bancarios para analizar adquisiciones o inversiones de un banco.
Regulaciones prudenciales y requerimientos: **Principio 6:** Establecimiento de requerimientos de mínimos de capital de los bancos reflejando el riesgo y la capacidad de absorber pérdidas. **Principio 7:** Evaluación de las políticas, prácticas y procedimientos para la administración de las carteras de préstamos e inversiones. **Principio 8:** Las políticas, prácticas y procedimientos deben evaluar la calidad de los activos, provisiones y reservas. **Principio 9:** Satisfacción de los sistemas de información gerencial de los bancos para identificar concentraciones dentro de la cartera. **Principio 10:** Establecimiento y aseguramiento de requerimientos básicos para préstamos relacionados. **Principio 11:** Satisfacción con las políticas y procedimientos para identificar, monitorear y controlar los riesgos del país. **Principio 12:** Satisfacción con el sistema de los bancos para medir, monitorear y controlar los riesgos de mercado para garantizar el capital activo del banco. **Principio 13:** Proceso integral del manejo de riesgos administrativos, identificación, medición, monitoreo y control de demás objetos de riesgo y retención de capital en contra de riesgos. **Principio 14:** Control interno de los bancos. **Principio 15:** Políticas, prácticas y procedimientos de la regla “conoce a tu cliente”, para promover estándares de ética y profesionalismo.

Métodos de supervisión bancaria progresiva: **Principio 16:** Supervisión del sistema de gestión bancaria. **Principio 17:** Contacto regular de los supervisores bancarios con la gerencia de los bancos. **Principio 18:** Métodos para recolectar, examinar y analizar reportes y datos estadísticos bancarios. **Principio 19:** Medios para determinar que la información obtenida de la supervisión es válida mediante exámenes directos o auditoria externa. **Principio 20:** Capacidad para supervisar un grupo bancario.
Requisitos de información: **Principio 21:** Aseguramiento del mantenimiento de registros adecuados y diseñados de acuerdo a la política contable.
Poderes formales de los Supervisores: **Principio 22:** Facultad de realizar acciones correctivas.
Bancos Extra-Fronterizos: **Principio 23:** Supervisión global en organizaciones bancarias internacionalmente activas primordialmente sus sucursales externas, co-inversiones y subsidiarias. **Principio 24:** Intercambios de información entre supervisores bancarios involucrados con las autoridades supervisoras del país anfitrión. **Principio 25:** Llevar a cabo una supervisión bancaria consolidada.

Fuente: (Superintendencia de Bancos y Seguros del Ecuador)

2 MARCO REGULATORIO DE LA GESTIÓN DE RIESGOS EMPRESARIALES ACEPTADO INTERNACIONALMENTE

2.1 COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

2.1.1 Historia

La organización COSO o también conocido como The Committee of Sponsoring Organizations, fue establecida en el año 1985 con el fin de promover una iniciativa del sector privado llamada the National Commission on Fraudulent Financial Reporting, la cual estudiaba las causas que podían dirigir información financiera fraudulenta, a su vez también desarrolló recomendaciones para compañías públicas y sus auditores externos.

La Comisión Nacional también estaba patrocinada por cinco asociaciones más establecidas en los Estados Unidos: The American Accounting Association (AAA), the American Institute of Certified Public Accountants (AICPA), Financial Executives International (FEI), The Institute of Internal Auditors (IIA), y the National Association of Accountants (la que ahora es the Institute of Management Accountants [IMA]). Todas estas organizaciones eran independientes y se incluyó representantes de las industrias, contabilidad pública, firmas inversoras y la bolsa de valores de Nueva York.

El objetivo de COSO es proporcionar el pensamiento de liderazgo relacionadas con tres materias relacionadas: gestión de riesgos empresariales (ERM), control interno y disuasión del fraude. (Committee of Sponsoring Organizations)

2.1.2 COSO Enterprise Risk Management

En el año 2004, COSO emite el Marco Integrado de gestión de riesgos empresariales (Enterprise Risk Management- Integrated Framework), en respuesta a la necesidad de las organizaciones de tener una guía que ayude a las entidades a diseñar e implementar enfoques efectivos y amplios sobre riesgos empresariales.

Este marco integrado es usado por organizaciones de todo el mundo para diseñar e implementar procesos efectivos de ERM, debido a que este contiene definiciones esenciales de los componentes de la gestión de riesgos, principios y conceptos, sugiere un lenguaje común de ERM y provee una clara dirección y guía para la gestión de riesgos empresariales. (Committee of Sponsoring Organizations)

La aplicación del documento en la vida de las organizaciones trae consigo varias ventajas que hacen que una empresa se destaque en el mercado, como son:

- Identificar y gestionar la diversidad de riesgos para toda la entidad.
- Reducir las sorpresas y pérdidas operativas.
- Mejorar las decisiones de respuesta a los riesgos.

- Alinear el riesgo aceptado y la estrategia.
- Aprovechar las oportunidades.
- Mejorar la dotación de capital. (Committee of Sponsoring Organizations of the Treadway Commission, 2004)

2.1.2.1 Definición de Gestión de Riesgos Empresariales

El (Committee of Sponsoring Organizations of the Treadway Commission, 2004) en su Marco Integrado define a la gestión de riesgos empresariales como:

> Un proceso efectuado por el consejo de administración de una entidad, su dirección y restante personal, aplicado en la definición de la estrategia y en toda la entidad y diseñado para identificar eventos potenciales que puedan afectar a la organización y administrar sus riesgos dentro del riesgo aceptado proporcionando una seguridad razonable sobre la consecución de los objetivos de la entidad.

Esta definición abarca varios aspectos como son que dicha gestión puede ser aplicada a toda la organización y a todo tipo de organizaciones; esta gestión es llevada a cabo por todo el personal de la compañía, pero principalmente por la alta dirección, y se centra principalmente en la consecución de objetivos que fueron previamente establecidos por la empresa para crear estrategias que establezcan la efectiva administración de la misma.

2.1.2.2 Objetivos de COSO-ERM

Todas las organizaciones tienen definidos sus objetivos estratégicos desde el inicio de sus operaciones, es de vital importancia que estos se encuentren bien definidos y entendidos por los diferentes niveles de la empresa ya que la consecución efectiva de los objetivos es lo que hace que la compañía se desenvuelva de mejor manera.

Cada organización es libre de tener el número de objetivos que determine conveniente para llevar a cabo sus operaciones, sin embargo, el (Committee of Sponsoring Organizations of the Treadway Commission, 2004) en su marco integrado establece que existen cuatro objetivos que las organizaciones tienen en común o que deberían tenerlos como básicos dentro de sus objetivos estratégicos, estos son:

- **Estratégicos:** Relativos a los objetivos de alto nivel, alineados con la misión de la entidad y prestándole apoyo.

- **Operativos:** Relativos al uso efectivos y eficiente de los recursos de la entidad.

- **Reporte:** Relativos a la confiabilidad de los informes de la entidad.

- **Cumplimiento:** Relativos al cumplimiento por la entidad de las leyes y regulaciones aplicables.

Como se puede observar los objetivos estratégicos COSO-ERM los separa por categorías, debido a que organizados de esta manera se puede tener un control efectivo de la consecución de los objetivos, de los responsables de su puesta en marcha y de las actividades que se realizan para llegar a ellos.

La administración de riesgos empresariales no asegura el cumplimiento ni efectividad de los objetivos solo por el hecho de organizarlos por categorías, todo eso es responsabilidad de la gerencia de la compañía. La administración lo que pretende es que la gerencia pueda tomar mejores decisiones, más acertadas y que la información de reporte de actividades, de consecución de objetivos, llegue a ellos oportunamente.

2.1.2.3 Componentes COSO-ERM

El marco integrado de COSO-ERM establece que existen ocho componentes relacionados entre sí para la aplicación de la administración de riesgos dentro de una organización. Se dice que estos componentes se relacionan entre sí debido a que la ejecución de los mismos se la puede realizar multidireccionalmente, esto no implican que uno se realice después de otro sino que cada componente puede influir en otro significativamente. A continuación se enlistan los ocho componentes, los cuales serán explicados a profundidad a lo largo de este capítulo:

- Ambiente interno
- Establecimiento de objetivos
- Identificación de eventos

- Evaluación de riesgos
- Respuesta a los riesgos
- Actividades de control
- Información y comunicación
- Monitoreo

Se ha establecido que tanto los componentes como los objetivos estratégicos de la empresa, antes mencionados, tienen una relación directa. Para representar esta relación COSO-ERM presenta una matriz tridimensional en forma de cubo que muestra dicha relación:

Figura 9: Relación entre objetivos y componentes de COSO-ERM

Fuente: (Committee of Sponsoring Organizations of the Treadway Commission, 2004)

Se puede observar en el figura que los objetivos de la organización se encuentran representados por las columnas verticales; los ocho

componentes se encuentran en las filas horizontales; mientras que en la tercera dimensión de la matriz se encuentran la entidad y sus unidades, la cual representa subsidiarias, divisiones y cualquier otra unidad de negocio. (Committee of Sponsoring Organizations of the Treadway Commission, 2004).

Los ocho componentes antes enlistados, forman una parte esencial de todo lo que COSO-ERM trata acerca de la gestión de riesgos empresariales, a continuación se explica cada uno de ellos:

- **Ambiente Interno**

  El ambiente interno expuesto en (Committee of Sponsoring Organizations of the Treadway Commission, 2004) abarca el tono de una organización, que influye en la conciencia de sus empleados sobre el riesgo y forma base de los otros componentes de la administración de riesgos corporativos, proporcionando disciplina y estructura.

  Los factores del ambiente interno incluyen la filosofía de administración de riesgos de una entidad, su apetito de riesgo, el monitoreo ejercido por la dirección, la integridad, valores éticos y competencia de sus colaboradores y la forma en que la dirección asigna la autoridad, responsabilidad, organiza y desarrolla a sus empleados. La base de una empresa esta constituida por su personal.

En el componente de ambiente interno es la dirección quien fija una filosofía respecto al riesgo y determina el riesgo aceptado, a su vez establece la base de cómo el personal de la empresa debe percibir y afrontar el control y el riesgo.

- **Establecimiento de objetivos**

Los objetivos deben existir antes de que la dirección pueda identificar los eventos potenciales que afectan a su consecución. Debe existir un proceso establecido para fijar objetivos y que los objetivos seleccionados apoyan la misión de la entidad y se alinean con ella, además deben ser consistentes con el riesgo aceptado. (Committee of Sponsoring Organizations of the Treadway Commission, 2004)

Los objetivos se establecen a nivel estratégico, estableciendo con ellos una base para los objetivos operativos, de reporte y de cumplimiento. Cada entidad se enfrenta a una variedad de riesgos procedentes de fuentes externas e internas, y una condición previa para la identificación efectiva de eventos, la evaluación de sus riesgos y la respuesta a ellos es fijar los objetivos, que tienen que estar alineados con el riesgo aceptado por la entidad, que orienta a su vez los niveles de tolerancia al riesgo de la entidad.

El establecimiento de objetivos es condición previa para la identificación de eventos, la evaluación de riesgos y la respuesta a

ellos. Tienen que existir primero los objetivos para que la dirección pueda identificar y evaluar los riesgos que impiden su consecución y adoptar las medidas necesarias para administrar dichos riesgos.

- **Identificación de Eventos**

En este componente se especifica que deben identificarse los eventos potenciales que pueden tener un impacto en la entidad. La identificación de eventos involucra la identificación de eventos potenciales de fuentes internas o externas que afectan el logro de los objetivos. Incluye la distinción entre eventos que representan riesgos, oportunidades y las dos.

La dirección identifica los eventos potenciales que si ocurren, afectarán a la entidad y determina si representan oportunidades o si pueden afectar negativamente a la capacidad de la empresa para implantar la estrategia y lograr los objetivos con éxito.

Los eventos con impacto positivo representan oportunidades que la dirección reconduce hacia la estrategia y el proceso de fijación de objetivos. Cuando se identifican los eventos, la dirección contempla una serie de factores internos y externos que pueden dar lugar a riesgos y oportunidades en el contexto del ámbito global de la organización.

- **Evaluación de Riesgos**

Los riesgos que hayan sido identificados previamente, son analizados para establecer una base y determinar como deben ser administrados. Los riesgos se asocian con los objetivos que pueden afectar. Los riesgos son evaluados sobre una doble perspectiva, inherente y residual, considerando su probabilidad e impacto.

La evaluación de riesgos permite a una entidad considerar la amplitud con que los eventos potenciales impactan en la consecución de objetivos. La dirección evalúa estos acontecimientos desde una doble perspectiva, probabilidad e impacto, y normalmente usa una combinación de métodos cualitativos y cuantitativos.

Los impactos positivos y negativos de los eventos potenciales deben examinarse, individualmente o por categoría, en toda la entidad. Los riesgos se evalúan con un doble enfoque de riesgo inherente y riesgo residual. El riesgo inherente es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto. El riesgo residual es el que permanece después de que la dirección desarrolle sus respuestas a los riesgos. La evaluación de riesgos es aplicada primero a los riesgos inherentes, una vez la respuesta a los riesgos ha sido incorporada, la dirección considerada el residual. (Committee of Sponsoring Organizations of the Treadway Commission, 2004).

- **Respuesta a los Riesgos**

El personal identifica y evalúa las posibles respuestas a los riesgos, las cuales incluyen evitar, aceptar, reducir y compartir. La dirección selecciona un conjunto de acciones para poner en línea los riesgos con sus tolerancias respectivas y el riesgo aceptado por la entidad.

Una vez evaluados los riesgos relevantes, la dirección determina cómo responder a ellos. Existen cuatro respuestas definidas dentro de (Committee of Sponsoring Organizations of the Treadway Commission, 2004) como son:

- Evitar: supone salir de las actividades que generen riesgos. Evitar el riesgo puede implicar el cese de una línea de producto, frenar la expansión hacia un nuevo mercado geográfico o la venta de una división.

- Reducir: implica llevar a cabo acciones para reducir la probabilidad o el impacto del riesgo o ambos conceptos a la vez. Esto implica típicamente a algunas de las miles de decisiones empresariales cotidianas.

- Compartir: la probabilidad o el impacto del riesgo se reducen trasladando o de otro modo, compartiendo una parte del riesgo. Las técnicas comunes incluyen la contratación de seguros, la

realización de operaciones de cobertura o la tercerización de una actividad.

- Aceptar: no se emprende ninguna acción que afecte a la probabilidad o el impacto del riesgo.

Al considerar su respuesta, la dirección evalúa su efecto sobre la probabilidad e impacto del riesgo, así como los costos y beneficios, y selecciona aquella que sitúe el riesgo residual dentro de las tolerancias al riesgo deseado. La dirección identifica cualquier oportunidad que puede existir y asume una perspectiva de portafolio de riesgos, determinando si el riesgo residual global concuerda con el riesgo aceptado por la entidad.

- **Actividades de Control**

Las políticas y procedimientos se establecen y ejecutan para ayudar a que se llevan a cabo efectivamente las respuestas a los riesgos seleccionados por la dirección.

Las actividades de control son las políticas y procedimientos que ayudan a asegurar que se llevan a cabo las repuestas de la dirección a los riesgos. Estas actividades de control tienen lugar a través de la organización, a todos los niveles y en todas las funciones. Incluyen una variedad de actividades como aprobaciones, autorizaciones,

verificaciones, conciliaciones, revisiones del funcionamiento operativo, seguridad de los activos y segregación de funciones.

Las actividades de control puede ser clasificadas por la naturaleza de los objetivos de la entidad con la que están relacionadas: estratégicos, operativos, de reporte y cumplimiento. Aunque algunas actividades de control corresponden exclusivamente a una sola categoría, a veces pueden utilizarse en varias. }

- **Información y Comunicación**

La información relevante se identifica, captura y comunica de un modo y en un plazo que permita a las personas desarrollar sus responsabilidades. Es necesaria información a todos los niveles de una entidad para identificar, evaluar y responder a los riesgos. También puede darse una comunicación eficaz en sentido amplio, cuando fluye hacia abajo y hacia arriba de la entidad. El personal debe recibir comunicaciones claras sobre su rol y responsabilidades.

La información pertinente se identifica, captura y comunica de una forma y en un marco de tiempo que permiten a las personas llevar a cabo sus responsabilidades. Los sistemas de información usan datos generados internamente y fuentes externas de información para la administración de riesgos y la toma de decisiones relativas a los objetivos.

Todo el personal recibe un mensaje claro desde la alta dirección que deben considerar seriamente las responsabilidades de administración de los riesgos empresariales. Las personas entienden su rol en la administración de riesgos corporativos y cómo las actividades individuales se relacionan con el trabajo de otros. Así mismo, deben tener unos medios para comunicar hacia arriba la información significativa. Por otro lado debe haber una comunicación efectiva con terceros, tales como los clientes, proveedores, reguladores y accionistas.

Cada empresa identifica y captura una variedad amplia de información relativa a actividades tanto internas como externas, relevantes para dirigir a la organización. Esta información facilita al personal de una forma y en un marco de tiempo que le permitan llevar a cabo su administración de riesgos empresariales y demás responsabilidades.

- **Monitoreo**

Toda la administración de riesgos empresariales se monitorea, realizando en ella las modificaciones que sean necesarias. De este modo, se puede reaccionar dinámicamente y cambiar si varían las circunstancias. Este monitoreo se lleva a cabo a través de actividades permanentes de la dirección, evaluaciones independientes de la administración de riesgos empresariales o una combinación de ambas situaciones.

El monitoreo de los riesgos se lleva a cabo revisando la presencia y funcionamiento de sus componentes a los largo del tiempo, lo que se lleva a cabo mediante actividades permanentes de monitoreo, evaluaciones independientes o una combinación de ambas técnicas.

Durante el transcurso normal de las actividades de gestión, el monitoreo permanente se lleva a cabo. El alcance y frecuencia de las evaluaciones dependerá de la evaluación de riesgos y la eficacia de los procedimientos de monitoreo permanente. Las deficiencias en la administración de riesgos empresariales se comunican de forma ascendente, reportando los temas más importantes a la alta dirección y al consejo de administración.

Todo el personal de la compañía tiene responsabilidad en la administración de riesgos empresariales. Sin embargo, existe una distinción entre aquellos que forman parte del proceso de la administración de riesgos de una entidad y los que no, cuyas acciones pueden afectar al proceso o ayudar a la entidad a conseguir sus objetivos.

2.1.2.4 Limitaciones de COSO-ERM

Una administración efectiva de riesgos empresariales únicamente proporciona una seguridad razonable a la dirección respecto a la consecución de objetivos de la entidad. Esta consecución esta afectada por

las limitaciones inherentes a cualquier proceso de administración. Esto incluye los factores como el juicio humano que en la toma de decisiones puede ser defectuoso y pueden ocurrir problemas por causa de fallas humanas como simples errores o equivocaciones.

Adicionalmente, cabe considerar que los controles pueden evadirse con la colusión de dos o más personas y la dirección tiene la capacidad para obviar el proceso de administración de riesgos empresariales, incluyendo las decisiones de respuesta a los riesgos y las actividades de control. Otro factor limitante es la necesidad de considerar los costos y beneficios relativos a las respuestas a los riesgos.

3 DISEÑO DE FORMATOS PARA IMPLEMENTAR UN SISTEMA DE GESTIÓN DE RIESGOS SIGUIENDO LOS LINEAMIENTOS DE COSO-ERM

3.1 ESTRUCTURA DE UN SISTEMA DE GESTIÓN DE RIESGOS

Dentro de este capítulo se pretende dar lineamientos a las empresas que deseen implementar un sistema de gestión de riesgos que les ayude a sus operaciones normales para evitar cualquier tipo de contratiempo y poder estar preparados ante situaciones desfavorables y a su vez aprovechar información que puede ser valiosa para mejoras dentro de sus actividades mientras se realiza esta implementación.

El documento que será utilizado como base para analizar los pasos a segiuir para la implementación de un sistema de gestión de riesgos es el elaborado por el Committee of Sponsoring Organizations of the Treadway Commission en su publicación acerca de la Gestión de Riesgos Empresariales (COSO-ERM por sus siglas en inglés). Se ha analizado anteriormente el marco integrado en donde se explica los conceptos que COSO-ERM considera importantes para aplicación de su modelo, sin embargo en este capítulo se tomará como punto de partida las Técnicas de Aplicación de COSO-ERM, las cuales basándose en los ocho componentes de la gestión de riesgos empresariales, dan a conocer al usuario técnicas aplicables a los elementos específicos del marco de gestión de riesgos empresariales.

El documento de técnicas de aplicación posee varios ejemplos y enfoques debido a que todas las empresas son diferentes y tienen formas diferentes de llevar a cabo sus operaciones, por lo que el propósito del documento es dar a conocer principios que puedan ser utilizados por las empresas de manera general ya que su tamaño, objeto, sector, valores, cultura y otras características podrán variar de empresa a empresa en su implementación. Lo que se pretende en este capítulo de esta investigación es mediante un ejemplo sencillo elaborar formatos y principios para que una empresa pueda seguir y entender la esencia de la implementación de este sistema de gestión de riesgos dentro de su organización.

3.1.1 Componente N°1: Ambiente Interno

Dentro de este componente se analiza la importancia que tiene una organización bien estructurada desde el ambiente y filosofía que maneja para realizar sus operaciones diarias, para una correcta implementación de un sistema de gestión de riesgos.

El documento COSO-ERM divide al ambiente interno en dos etapas que serán explicadas brevemente para tener una mejor comprensión de ellas y de lo que cada una contiene. Las dos etapas son las siguientes:

- Filosofía de la gestión de riesgos.
- Integridad y valores éticos.

3.1.1.1 Filosofía de la gestión de riesgos

El (Committee of Sponsoring Organizations of the Treadway Commission, 2004) define a la filosofía de la gestión de riesgos como:

"El conjunto de creencias y actitudes compartidas que caracterizan el modo en que la entidad contempla el riesgo en todas sus actuaciones, desde el desarrollo e implantación de la estrategia hasta sus actividades cotidianas".

Esta filosofía anteriormente definida es el punto de partida para la implementación del sistema de gestión de riesgos, en donde las creencias, conocimientos y valores de la empresa con relación a los riesgos va a afectar significativamente a un nuevo proceso que se intenta implementar, es necesario que toda la organización en su conjunto tenga conocimiento de la cultura de riesgos que posee la empresa para sus actividades, es decir, la forma específica de cómo se deben tratar los riesgos que se encuentran dentro de las diferentes actividades.

Muchas empresas realizan por escrito una declaración de la filosofía que mantiene la misma para tratar a los riesgos asociados con las actividades regulares de la organización, esta declaración contiene principalmente la forma en que se identifican riesgos, cómo se los trata y quiénes son los responsables de esta labor.

Estas declaraciones deben ser de conocimiento de todos los empleados de la organización para que estos puedan trabajar bajo las normas y filosofía de riesgos que la empresa pretende implantar. Sin embargo, existen casos en los que los empleados no tienen conocimiento acerca de este documento o esta filosofía, por lo que se suele realizar una encuesta cada cierto tiempo para comprobar que la filosofía de gestión de riesgos es de conocimiento de todos los empleados.

Esta encuesta mide la integración que tiene la filosofía de gestión de riesgos con la cultura de la organización y para ellos utiliza cuatro atributos que el (Committee of Sponsoring Organizations of the Treadway Commission, 2004) define que son los siguientes presentados en la figura a continuación:

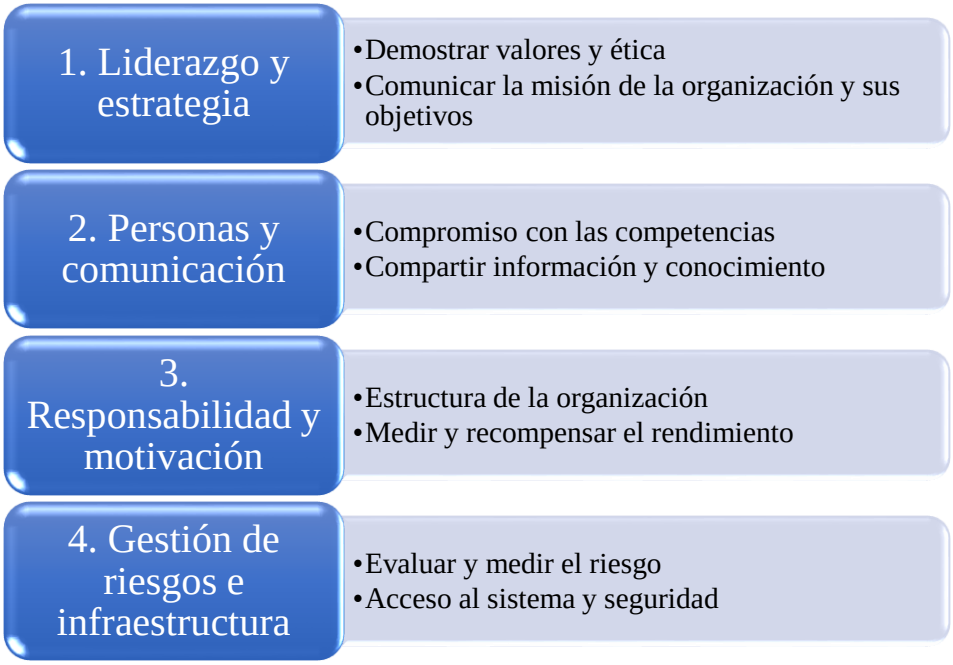


Figura 10: Atributos medidos en una encuesta sobre cultura de riesgos

Fuente: (Committee of Sponsoring Organizations of the Treadway Commission, 2004)

La frecuencia con la que se debe realizar las encuestas dependerá de cada organización. Los resultados que arroje la encuesta serán de mucha ayuda ya que proporcionan indicadores positivos que pueden ser tomados como fortalezas y a su vez indicadores negativos que vienen ser debilidades que la empresa tiene dentro de su cultura de riesgos.

Un modelo de encuesta sencilla que puede ser llevado a cabo por cualquier tipo de organización se presenta a continuación, en la cual se toma en cuenta preguntas que serán hechas al personal y los atributos que cada una de ellas representan.

Tabla 2: Encuesta sobre la cultura de riesgos

COMPAÑÍA ABC
ENCUESTA SOBRE LA CULTURA DE RIESGOS

Nombre del departamento:	
Fecha de elaboración:	

Objetivo de la encuesta:

Obtener conocimiento acerca de la cultura de riesgos, para identificar atributos que la compañía debe mejorar para una eficaz implementación de un sistema de gestión de riesgos.

N°	PREGUNTA	ATRIBUTO	CALIFICACIÓN MEDIA		DESV. EST.	CANTIDAD	MD	D	N	A	MA
1	Los lideres de mi unidad siguen positivamente los lineamientos de un comportamiento de conducta ética	Liderazgo y estrategia									
2	Comprendo la misión y estrategia general de la organización.	Liderazgo y estrategia									
3	En mi unidad se llevan a cabo acciones disciplinarias contra aquellos que muestran una conducta profesional inapropiada.	Responsabilidad y motivación									
4	La rotación del personal no afecta a nuestra capacidad de alcanzar los objetivos.	Personas y comunicación									
5	Los líderes de mi unidad de negocio son receptivos a cualquier tipo de comunicación acerca del riesgo, incluyendo noticias negativas.	Gestión de riesgos e infraestructura									

La interpretación para esta encuesta está dada por las respuestas que se obtengan de los empleados encuestados donde ellos deberán responder a interpretaciones cualitativas según su apreciación propia y cada una de estas respuestas tiene una valoración que va desde -2 a +2 según corresponda, por lo tanto Muy en desacuerdo (MD) equivale a -2, Desacuerdo (D) equivale a -1, Neutral (N) 0, De acuerdo (A) +1, Muy de acuerdo (MA) +2.

En esta encuesta también se puede aplicar un código de colores en donde dichos colores demostraran que si se debe o no tomar acciones para mejorar los diferentes atributos que se están calificando. Por último, el cálculo de la desviación estándar permitirá observar la concordancia que tienen las respuestas dadas frente al atributo evaluado.

3.1.1.2 Integridad y valores éticos

En esta etapa del ambiente interno de una organización trata acerca de todos los valores con los cuales debe contar cada uno de los empleados que formen parte de la organización. Si bien es cierto cada individuo es dueño de sus valores y creencias, las organizaciones deben contar con valores primordiales que los empleados deben seguir para que todas las actividades se realicen en armonía y con el mejor entendimiento posible.

Que una organización cuente con valores y principios bien establecidos y que sus colaboradores los sigan, establece una base sólida en la cual un

nuevo sistema de gestión de riesgos puede ser implementado sin ninguna dificultad.

Como se dijo anteriormente cada individuo es dueño de sus actos y valores, sin embargo dentro de las organizaciones deben existir personas con niveles de autoridad superiores, quienes serán los encargados de velar y ser un líder frente a los empleados demostrando siempre valores éticos y conductas apropiadas ya que serán los guías de sus seguidores. En la actualidad la mayoría de las organizaciones, además de contar con líderes de altos niveles, proponen por escrito todos los valores y principios con los que se trabaja y los que se espera que los empleados sigan durante su desempeño dentro de la misma, a estos documentos se los conoce como códigos de conducta.

El (Committee of Sponsoring Organizations of the Treadway Commission, 2004) define al código de conducta como:

> Una declaración proactiva de las posiciones de la entidad frente a las cuestiones éticas y de cumplimiento. Sin ser una guía exhaustiva de conducta, ni un documento legal, estos códigos pueden ser útiles como guías de fácil utilización acerca de las políticas relativas a la conducta de los empleados y de la propia organización.

En la tabla que se presenta a continuación se resume brevemente los temas claves de los que se debe tratar dentro de un código de conducta normal, consta de ocho secciones básicas que un código de conducta debe poseer y al lado derecho de cada sección se encuentra un breve contenido de cada

una de ellas, sin embargo cada organización es libre de incluir los puntos que mejor se acoplen a sus actividades y objetivos organizacionales.

Tabla 3: Estructura de un código de ética o conducta

SECCIONES	CONTENIDOS DE CADA SECCIÓN
1. Carta de la dirección general	- Mensaje de la alta dirección sobre la importancia de la integridad y los valores éticos para la organización. - Código de conducta, su propósito y manera de utilizarlo.
2. Objetivos y filosofía	- Se considera dentro de la organización: Su cultura Su negocio y sector Su ubicación geográfica, tanto nacional como internacionalmente Su compromiso con el liderazgo ético
3. Incompatibilidades	- Aborda las incompatibilidades y las formas de actuar en provecho propio. - Incompatibilidades en relación con el personal y otros agentes corporativos, así como aquellas actividades, inversiones o intereses que podrían afectar a la reputación o integridad de la organización.
4. Regalos y gratificaciones	- Penaliza el empleo de regalos y gratificaciones, estableciendo la propia política de la organización al respecto. - Establece normas y proporciona pautas con respecto a los regalos y gastos de representación, así como su adecuada comunicación.
5. Transparencia	- Incluye disposiciones/normas acerca del compromiso de la empresa con la generación de informes completos y comprensibles sobre impacto económico, social y medioambiental.
6. Recursos corporativos	- Incluye disposiciones/normas acerca de los recursos corporativos, incluyendo la propiedad intelectual y la información de activos propios, a quién pertenecen y cómo se protegen

SECCIONES	CONTENIDOS DE CADA SECCIÓN
7. Responsabilidad social	- Incluye el papel de la entidad como parte de la sociedad, incluyendo su compromiso con los derechos humanos, la preservación medioambiental, la implicación en el desarrollo de su comunidad y otras cuestiones económicas.
8. Otras cuestiones relativas a la conducta	- Incluye disposiciones/normas acerca de la fidelidad a las políticas establecidas en áreas específicas de actividad de la empresa, tales como: -Cuestiones relativas al empleo: prácticas laborales justas y lucha contra la discriminación. - Tratos con las autoridades, contrataciones, influencias y actividad política. - Seguridad y calidad del producto. - Prácticas antimonopolio y otras relacionadas con la competencia. - Buena fe y trato justo con clientes, competidores y proveedores. - Confidencialidad y seguridad de la información.

Fuente: (Committee of Sponsoring Organizations of the Treadway Commission, 2004)

A un código de conducta establecido se le puede dar cierto tipo de seguimiento en donde se realicen reuniones espontáneas con empleados tomados al azar y conversar acerca del conocimiento y acogida que tiene el código de conducta dentro de la organización, cómo se lo pone en práctica y si existe algún tipo de desvío o mala interpretación del mismo.

En la actualidad el uso de la tecnología no es una elección sino más bien una necesidad, algunas empresas utilizan este medio para difundir y siempre tener presente en los empleados cosas importantes acerca del código de conducta que debe ser seguido. Un ejemplo de estas acciones usando la tecnología es protectores de pantalla en las computadoras en

donde se resalten los valores más importantes que como compañía se tiene dentro de la misma. Existen también cursos de capacitación online que las empresas llevan a cabo para dar una certificación a los empleados en este tema.

3.1.2 Componente N° 2: Establecimiento de Objetivos

El establecimiento de objetivos es una de las fases más importantes de la implementación de un sistema de gestión de riesgos dentro de una organización, ya que se convierte en la base de una buena implementación para la consecución del resto de componentes y pasos que COSO-ERM plantea.

A continuación se presenta una figura que resume la relación que el componente de establecimiento de objetivos propone:

Figura 11: Relación del establecimiento de objetivos

Fuente: (Committee of Sponsoring Organizations of the Treadway Commission, 2004)

El componente de establecimiento de objetivos determina que debe existir un vinculo entre la misión/visión de la empresa con sus objetivos estratégicos y a su vez estos deben tener una relación con los objetivos relacionados. Estos dos últimos juntos deben alinearse con el nivel de riesgo aceptado y por último con la tolerancia al riesgo. (Committee of Sponsoring Organizations of the Treadway Commission, 2004). De esta manera este componente se divide en las cuatro secciones anteriormente mencionadas que serán explicadas brevemente.

3.1.2.1 Objetivos Estratégicos

Como ya se mencionó anteriormente, el establecimiento de objetivos estratégicos va estrechamente de la mano con el cumplimiento de la misión/visión de la organización. Los directivos de una empresa deben siempre tener presente que todos los objetivos que se planteen como negocio deben estar relacionados con el giro fundamental del mismo y de esta manera cumplir con lo ofrecido tanto a clientes, como a proveedores y empleados.

Todos los objetivos que se establezcan deben ser analizados junto con el riesgo que cada uno de estos presenta, para identificar los riesgos asociados a cada uno de los objetivos planteados se debe recurrir al uso de técnicas para identificar riesgos, estas técnicas utilizadas para identificación de riesgos serán expuestas en los componentes siguientes.

A la par de establecer objetivos estratégicos, las organizaciones deben presentar las estrategias que seguirán para alcanzar dichos objetivos, las cuales representan las acciones a ser tomadas para cumplir con los objetivos generales que como empresa se tienen.

3.1.2.2 Otros objetivos relacionados

Estos objetivos hacen relación a los objetivos específicos que cada organización tiene para cada uno de los departamentos o áreas con las que opera para desarrollar las actividades que son de su negocio propio.

Los objetivos relacionados van de la mano con los objetivos estratégicos y las estrategias que se utilizarán para llegar a ellos, es decir que son los objetivos que se espera lograr por áreas de trabajo que contribuyan al cumplimiento de un objetivo principal.

3.1.2.3 Riesgo Aceptado

El riesgo aceptado se refiere a la cantidad de riesgo que una organización está dispuesta a aceptar para cumplir sus objetivos, esta cantidad puede ser medida de manera cuantitativa como cualitativa. El riesgo aceptado se lo puede medir partiendo del ambiente interno de la empresa como puede ser dependiendo de la actuación de la empresa en el mercado, su cultura de riesgos, los valores y conducta que tengan los empleados, su desempeño laboral y capacidades técnicas que tengan sus colaboradores; y a su vez

por su ambiente externo a la empresa como leyes políticas, económicas o geográficas que no se encuentren bajo el control de la compañía.

El documento emitido por (Committee of Sponsoring Organizations of the Treadway Commission, 2004) establece que una vez que la organización haya establecido el riesgo aceptado está en capacidad de realizarse ciertas preguntas para evaluar su riesgo aceptado. Algunas de las preguntas se enlistan a continuación:

- ¿Qué riesgos relativos al negocio está dispuesta a asumir la empresa y cuáles no?

- ¿Se encuentra cómoda la empresa con la cantidad de riesgos aceptado actual o con la que acepte en el futuro en cada uno de sus negocios?

- ¿Se encuentra la empresa preparada para aceptar más riesgo del que actualmente admite? Y, en tal caso, ¿qué nivel de rendimiento se requiere?

- ¿Existen riesgos que específicos que la entidad no este preparada a acepta, tales como los que podría implicar el incumplimiento de leyes de privacidad de la información?

- ¿Se encuentra la organización más cómoda con un indicador cualitativo o cuantitativo?

Con el ejemplo de algunas de las preguntas que pueden existir, la compañía puede realizar una entrevista los niveles más altos de la organización o con mayor poder de decisión para analizar la coherencia del riesgo aceptado y a su vez poder comprobar que las personas responsables tienen total conocimiento de lo que la empresa está dispuesta a aceptar en circunstancias de incertidumbre.

Junto con esta entrevista, las organizaciones deben tener por escrito las políticas de riesgo aceptado que se van a mantener dentro de las mismas y estos documentos deben ser de conocimiento de todos los departamentos dentro de la empresa, claro está que cada departamento debe tener sus objetivos y su riesgo aceptado respectivamente para que las labores entre departamentos no se confundan. Todos los empleados deben tener conocimiento específico de lo que su área de desempeño pretende realizar y cómo se lo va a realizar.

Algunas organizaciones también se identifican con un mapa de riesgo, el cual muestra los límites que son y no son aceptados dentro del tema de riesgos. Dentro de esta mapa interactúan las variables probabilidad (ubicada en eje horizontal) y la variable impacto (ubicada en el eje vertical) las cuales medirán la probabilidad de ocurrencia de un evento frente al impacto que este causaría dentro de la empresa, si esta análisis se encuentra fuera de lo establecido se deben tomar acciones al respecto. El mapa de riesgo de muestra en la siguiente figura:

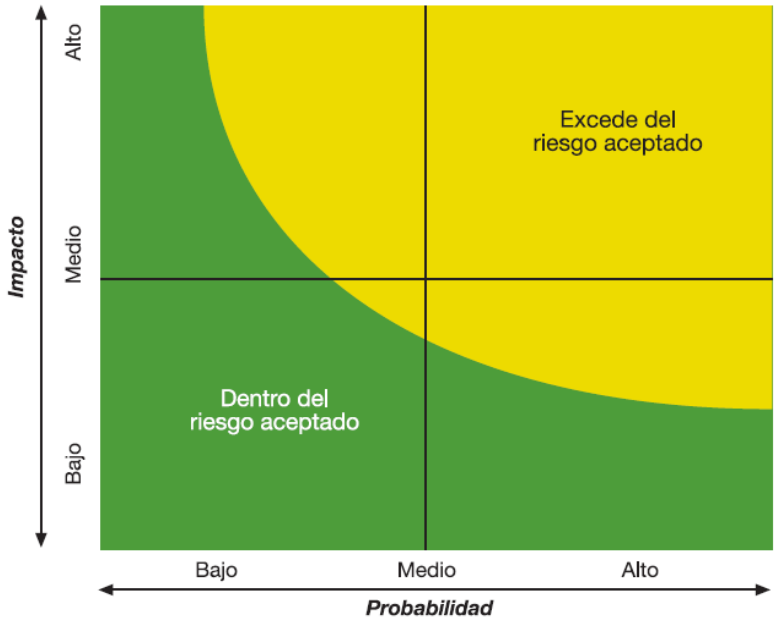


Figura 12: Mapa de Riesgo

Fuente: (Committee of Sponsoring Organizations of the Treadway Commission, 2004)

3.1.2.4 Tolerancia al riesgo

> La tolerancia al riesgo son los niveles aceptables de desviación relativa a la consecución de objetivos. Operar dentro de la tolerancia al riesgo proporciona a la dirección una mayor confianza en que la entidad permanece dentro de su riesgo aceptado, que, a su vez proporciona seguridad más elevada de que la entidad alcanzará sus objetivos. (Committee of Sponsoring Organizations of the Treadway Commission, 2004).

En otras palabras la tolerancia al riesgo representa a la variación que se obtenga después de establecer el riesgo aceptado que la empresa está dispuesta a aceptar para el cumplimiento de sus objetivos. Muchas veces la tolerancia al riesgo se establece a nivel general de organización y después se asigna a cada área de trabajo un porcentaje de este nivel de tolerancia.

3.1.2.5 Ejemplo de la relación que debe existir en el componente de establecimiento de objetivos

A continuación se realizará un ejemplo de una matriz en la que se relaciona la misión/visión de la compañía con sus objetivos estratégicos, estrategias, riesgo aceptado y tolerancia al riesgo, que las empresas pueden utilizar a manera de formato para evaluar que las etapas anteriormente mencionadas se relacionen entre sí y que todas estén cumpliendo una secuencia lógica.

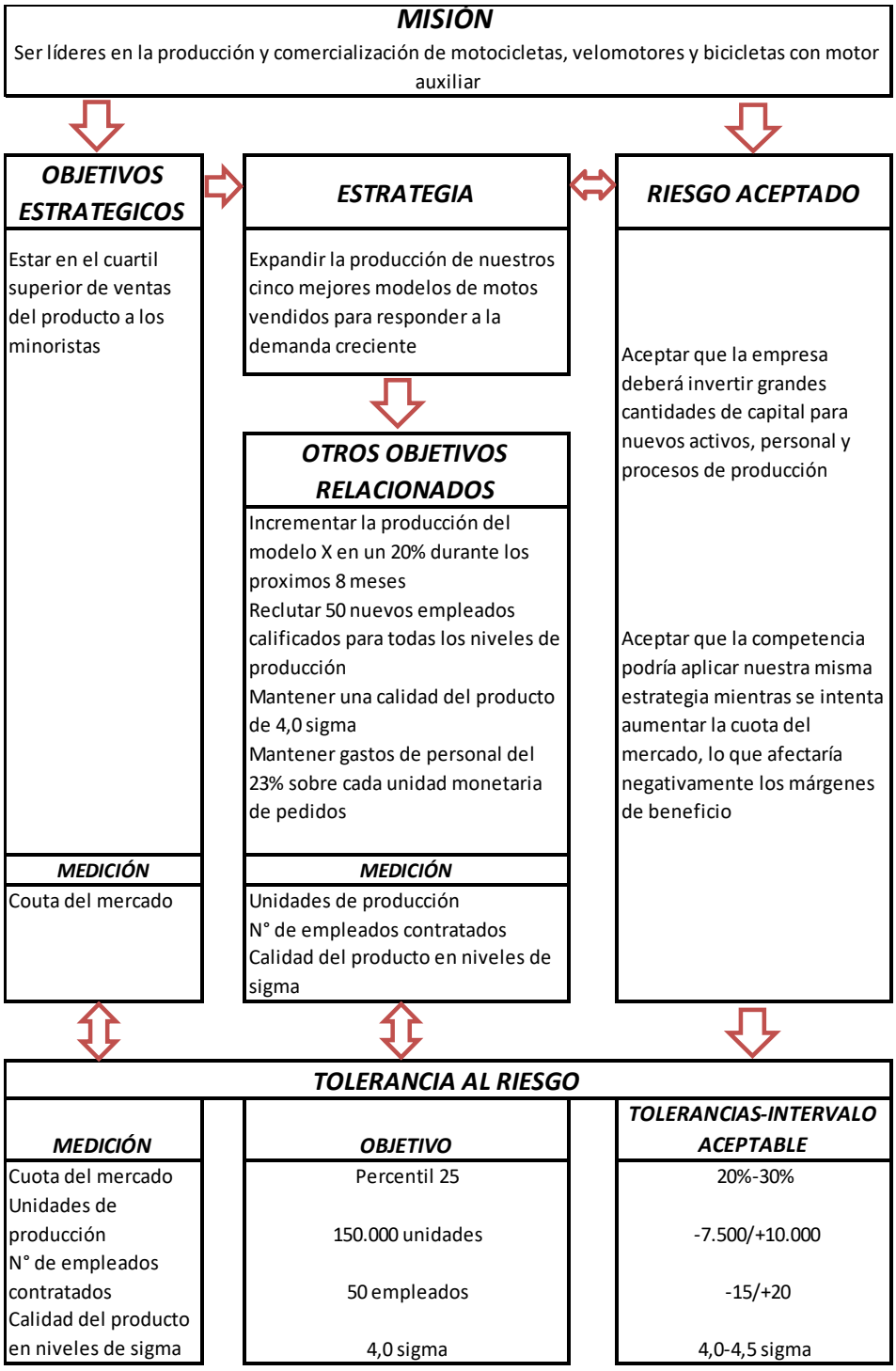


Figura 13: Matriz relación entre misión, objetivos riesgo aceptado y tolerancia

Fuente: (Committee of Sponsoring Organizations of the Treadway Commission, 2004)

3.1.3 Componente N° 3: Identificación de Eventos

Dentro de este componente se intenta determinar la naturaleza de los eventos a los que la compañía esta expuesta dentro de todas sus actividades de operación. Los eventos pueden ser de dos tipos positivos o negativos, los eventos positivos suelen representar oportunidades o fortalezas con las que la empresa cuenta y que serán beneficiosos al momento de combinarlos juntos con los objetivos generales y las estrategias que ya se encuentran planteadas; por otro lado, los eventos negativos suelen representar riesgos para la entidad, los cuales deben ser evaluados y necesitan un plan de acción frente a ellos por parte de los altos mandos de la organización.

En muchas organizaciones la relación que se tiene entre identificación de eventos dentro de los objetivos organizacionales es muy sencilla ya que a simple vista se pueden identificar los eventos, tanto positivos como negativos, su impacto dentro de los objetivos, su nivel de tolerancia y su unidad de medición. Sin embargo no en todas las organizaciones existe esta simplicidad, por lo que existen diversas técnicas de identificación de eventos en donde la dirección pretende identificar posibles acontecimientos que afecten al logro de sus objetivos, estas pueden ser riesgos u oportunidades. (Committee of Sponsoring Organizations of the Treadway Commission, 2004).

A continuación se enlistarán las técnicas de identificación de eventos que constan dentro del documento COSO-ERM:

- Inventario de eventos.

- Talleres y grupos de trabajo dirigidos.

- Entrevistas.

- Cuestionarios.

- Encuestas.

- Análisis del flujo de procesos.

- Técnicas de principales indicadores de riesgos y alarma.

- Seguimiento de datos de eventos con pérdidas asociadas usando información interna o externa.

- Identificación continua de eventos.

- Interrelación de eventos que pueden afectar a los objetivos.

- Clasificación de eventos por categorías.

En esta investigación se definirá y tomará como ejemplo la técnica de talleres y grupos de trabajos dirigidos y la técnica de Análisis de flujo de procesos, para dar a conocer a las empresas como la combinación de dos técnicas sencillas puede ayudar a la misma a la identificación de eventos dentro de sus actividades.

3.1.3.1 Talleres de trabajo o grupos de trabajo dirigidos

Esta es un técnica de identificación de eventos en donde se reúne a personal de las diferentes áreas de trabajo de la empresa o dependiendo del objetivo que se vaya a analizar, personal que tenga que ver con el desarrollo de cierta actividad en particular para que todos juntos colaboren en el desarrollo de identificación de acontecimientos que pueden afectar o no al cumplimiento de los objetivos que la empresa tiene planteado. El éxito y los resultados que arroje el taller, dependerá de la información que los participantes pueden contribuir al ejercicio.

La ventaja que tiene esta técnica es de tipo motivacional, en donde los empleados tienen la oportunidad de ser parte de un proceso importante para la compañía y podrán aportar con sus ideas en la búsqueda de oportunidades o riesgos para el mejoramiento de la entidad en dónde laboran.

En el punto 3.1.3.3. Ejemplo de técnicas de identificación de eventos, se podrá observar cómo se debe realizar el desarrollo de esta técnica y un pequeño formato que la compañía puede adaptar en sus procesos.

3.1.3.2 Análisis de flujo de procesos

Esta técnica de análisis de flujo de procesos se refiere a la representación gráfica de procesos generales dentro de la empresa o de un proceso en

particular que la entidad desee analizar. Mediante esta representación gráfica se pretende comprender la relación de las entradas, tareas, salidas y responsables de las actividades que se realizan diariamente dentro de la organización, con el fin de analizar paso a paso donde se puede presentar un problema.

En el punto 3.1.3.3. Ejemplo de técnicas de identificación de eventos, se podrá observar cómo se debe realizar el desarrollo de esta técnica y un pequeño formato que la compañía puede adaptar en sus procesos.

3.1.3.3 Ejemplo de técnicas de identificación de eventos

Dentro de este punto se realizará una combinación de las dos técnicas anteriormente descritas, talleres de trabajo y análisis de flujo de procesos, para ayudar a las empresas a tener una herramienta sencilla para la identificación de eventos. En este caso se realizará la identificación de eventos de un proceso en particular, cobros de cuentas.

A continuación se presenta el flujo de actividades del proceso de cobros de la Compañía ABC:

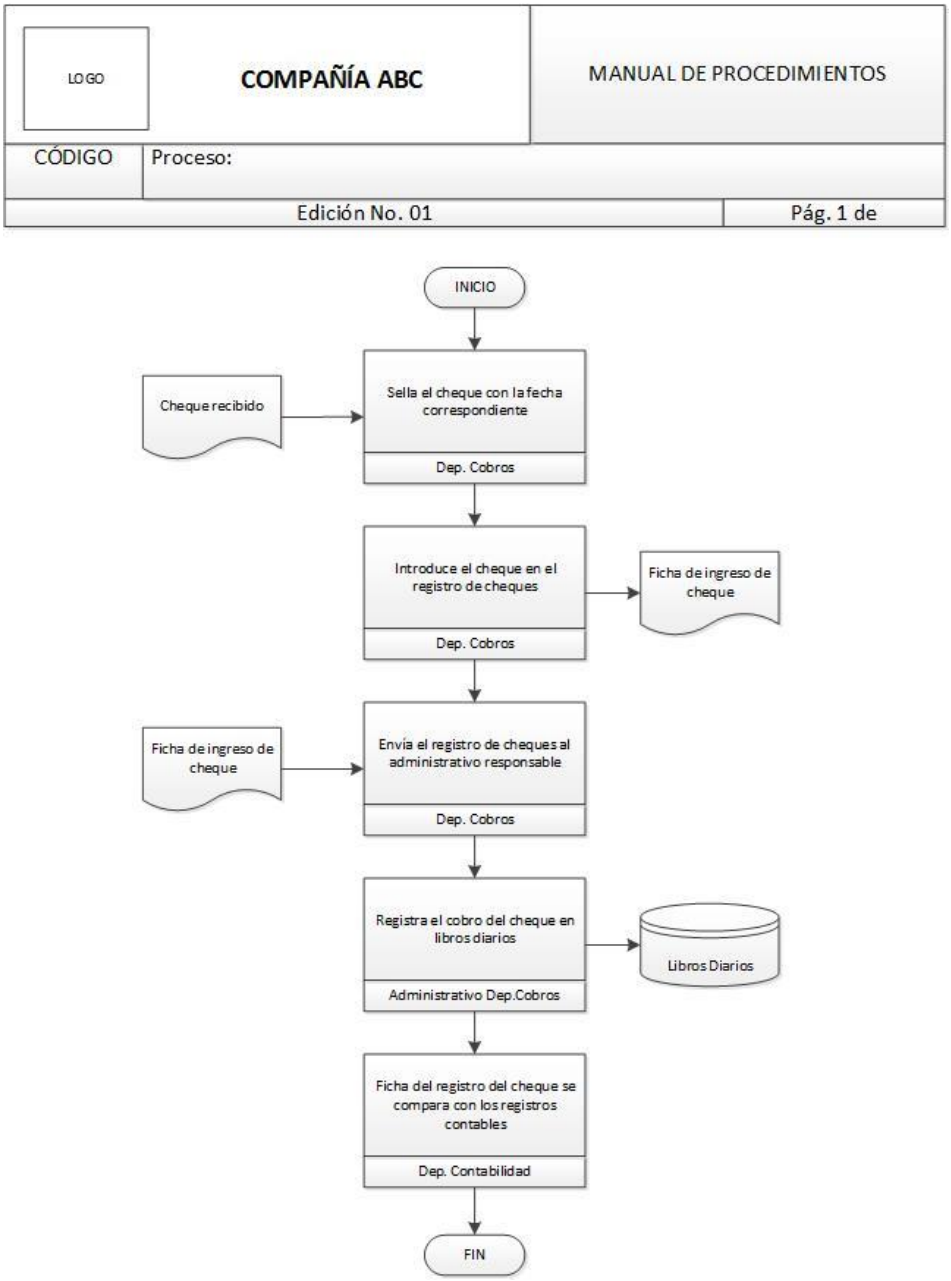


Figura 14: Flujo de actividades del proceso de Cobros

Fuente: (Committee of Sponsoring Organizations of the Treadway Commission, 2004)

Como se puede observar dentro del Figura 14, se encuentran las actividades que esta empresa realiza para el proceso de cobros. Dentro de los flujos de actividades se deben detallar todas las tareas por más simples que sean, de cómo se llevan a cabo los procesos seleccionados, sus responsables y todos los documentos que se generan después de realizada

la tarea, de esta manera será más fácil poder identificar eventos desfavorables dentro del proceso.

Una vez identificadas todas las tareas que se llevan a cabo dentro del proceso, a continuación se combinará la técnica de talleres de trabajo en donde se ejemplificará cómo se debe llevar a cabo este proceso.

Como se ha explicado anteriormente, los talleres de trabajo se realizan con un grupo de especialistas en el área a tratarse, en este caso el área de cobros. Debe existir una persona que sea el moderador del taller y que prepare un documento escrito en donde se especifique todos pasos a desarrollarse.

En un inicio el taller debe considerar los siguientes aspectos:

- Identificar un moderador experimentado y que puede ser de un alto nivel jerárquico para que dirija el taller, gestione la dinámica del grupo y planifique el mejor modo de captar las ideas.

- Establecer normas básicas y llegar a un acuerdo antes de que el taller tome inicio.

- Identificar los objetivos, categorías de objetivos y acontecimientos a donde se espera llegar con el taller.

- Invitar a un número apropiado de participantes al taller.

- Determinar las expectativas que se espera se cumplan con la realización del taller.

Durante el desarrollo del taller se debe tener en consideración que todo lo que se lleve a cabo dentro del mismo debe ser documentado por escrito por lo que se puede tener en consideración el siguiente formato para llevar a cabo el taller.

Tabla 4: Atributos medidos en una encuesta sobre cultura de riesgos

COMPAÑÍA ABC

TALLER DE GRUPO

Nombre del moderador:

Fecha del taller:

Departamento:

Objetivo o proceso a ser evaluado:

1. ***Introducción:***

   Dentro de este punto se debe explicar los antecedentes del taller y los motivos por los cuáles se está realizando el mismo. A su vez se deben explicar las normas básicas que se tomarán a consideración dentro del desarrollo del taller.

2. ***Procedimientos:***

   - Partiendo desde el flujo de actividades previamente realizado, elaborar una lista con todas las tareas primordiales dentro del proceso seleccionado para evaluación.
   - Para cada una de las tareas listadas, se estimulará a los participantes a que se discutan acontecimientos que puedan surgir y se elaborará un cuadro comparativo.

Tareas	Posibles acontecimientos
1. 2. 3. 4.	1. 2. 3. 4.

   - Para cada posible acontecimiento se determinará si representa una oportunidad o un riesgo para la entidad o para el departamento.
   - Si se determinó que el acontecimiento puede representar un riesgo para la compañía, de deberá determinar y llegar a un consenso sobre el nivel de riesgo aceptado y su respectiva tolerancia al riesgo.
   - Considerar de qué modo se relacionan entre sí los riesgos encontrados y en medida afectan a los objetivos planteados.

3. ***Cierre:***

   Obtener los resultados del taller y distribuir a los responsables de cada unidad para poder preparar un plan de respuesta para los siguientes pasos del componente.

Fuente: (Committee of Sponsoring Organizations of the Treadway Commission, 2004)

3.1.4 Componente N° 4: Evaluación de Riesgos

En este componente de evaluación de riesgos se intenta determinar en un nivel más amplio, cómo los posibles eventos impactan en los objetivos de la entidad, para ello COSO-ERM plantea que se deben evaluar mediante dos perspectivas, su probabilidad e impacto. Todos los eventos ya sean positivos o negativos se deben evaluar individualmente y conjuntamente con ello los eventos considerados como riesgos se evalúan mediante dos enfoques; como riesgo inherente y riesgo residual. (Committee of Sponsoring Organizations of the Treadway Commission, 2004)

El documento realizado por el (Committee of Sponsoring Organizations of the Treadway Commission, 2004) define al riesgo inherente como aquél al que la entidad se enfrenta en ausencia de acciones de la dirección para modificar su probabilidad o impacto; y a su vez define al riesgo residual como aquel que refleja el riesgo remanente una vez se han implantado de manera eficaz las acciones planificadas por la dirección para mitigar el riesgo inherente. Las posibles acciones para mitigar riesgos serán abordadas en los siguientes componentes que se explicarán después.

Existen diferentes técnicas cualitativas y cuantitativas para determinar los riesgos inherentes y residuales que presentan los objetivos de una organización. Existen empresas que aplican la combinación de los dos tipos de técnicas para determinar los riesgos asociados a los objetivos, sin embargo se puede decir que se utiliza una técnica cualitativa cuando los riesgos no presentan datos cuantificables o no se posee la información completa para realizarlo; y se utiliza

la técnica cuantitativa para complementar las técnicas cualitativas con datos más precisos o cuando se necesita evaluaciones mas sofisticadas.

Para evaluar los riesgos y estimar su probabilidad e impacto se necesita utilizar escalas de medición. El (Committee of Sponsoring Organizations of the Treadway Commission, 2004) establece que son existen cuatro escalas de medición y las define de la siguiente manera:

- **Medición Nominal:** implica el agrupamiento de eventos por categorías, estas categorías no deben ser ordenadas por grado de importancia, ni agregados, ni clasificados.

- **Medición Ordinal:** los eventos son clasificados por nivel de importancia y esta puede ser etiquetada como alta, media o baja y puede ser organizados mediante una escala.

- **Medición de intervalo:** utiliza una escala de distancias numéricas iguales. Si un evento es medido con un número determinado y otro evento con otro número superior no significa que el evento dos sea más importante que el evento uno.

- **Medición por ratios:** se utiliza escalas numéricas de la misma manera que la medición de intervalo, sin embargo en esta medición incluye el concepto del cero verdadero, en donde si al evento uno se le asigna un número menor al evento dos, quiere decir que el evento dos es de mayor importancia que el evento uno.

Dentro de estas definiciones se considera a las mediciones nominal y ordinal como técnicas cualitativas mientras que a las mediciones de intervalo y ratios se las considera como técnicas cuantitativas.

3.1.4.1 Técnicas de evaluación de riesgos

Dentro de las técnicas de evaluación de riesgos ya se ha dicho que existen de dos tipos, cualitativas y cuantitativas y lo que cada una de ellas representa.

Técnicas Cualitativas

Al hablar de la técnica de evaluación de riesgos cualitativas podemos destacar que estas pueden ser de tipo subjetivo y objetivo en donde se emplea el juicio del profesional que realice esta evaluación quién deberá también tener un amplio conocimiento del área del cual se realiza dicha evaluación, posibles eventos y todo lo que pueda afectarlos.

La evaluación cualitativa suele ser presentada mediante cuadros comparativos en donde se evalúan los riesgos clasificando las probabilidades de ocurrencia de un riesgo como alta, media o baja y que afectarán al cumplimiento de objetivos; o a su vez también se puede evaluar presentando listados de los posibles impactos que podría tener la compañía en el caso de que el evento desfavorable ocurra. Con estas clasificaciones se intenta resaltar los riesgos que tienen mayor

probabilidad de ocurrencia y que su impacto en la entidad sea muy desfavorable y que necesiten acciones inmediatas.

Técnicas Cuantitativas

Este tipo de técnica se lleva a cabo cuando el evaluador cuenta con toda la información y datos necesarios para poder estimar la probabilidad de ocurrencia y el impacto de los riesgos dentro de la organización. Dentro de esta técnica se incluyen de tipo probabilístico y no probabilístico. El (Committee of Sponsoring Organizations of the Treadway Commission, 2004) sugiere algunas técnicas las cuales se enlistan en la siguiente figura.

Tabla 5: Técnicas cuantitativas de evaluación de riesgos

Probabilísticas	***No Probabilísticas***
• Valor en riesgo • Flujo de caja en riesgo • Beneficio en riesgo • Distribuciones de pérdidas • Análisis retrospectivo (Back-Testing)	• Análisis de sensibilidad • Análisis de escenarios • Pruebas de tolerancia a situaciones límite • Benchmarking

Fuente: (Committee of Sponsoring Organizations of the Treadway Commission, 2004)

3.1.4.2 Presentaciones de evaluaciones de riesgo y ejemplo de aplicación

Después de escoger la técnica ideal para evaluar los riesgos, su probabilidad de ocurrencia y su impacto, la entidad debe escoger el método más adecuado para presentar los resultados encontrados.

Existen varios métodos de cómo se puede presentar los resultados de las evaluaciones, sin embargo los más usuales suelen ser los mapas de riesgo o de calor. Los mapas de calor trazan estimaciones cualitativas y cuantitativas de la probabilidad y el impacto de los riesgos. Los riesgos se representan de manera en que los más significativos resalten de los menos significativos, los cuales suelen diferenciarse por colores que el evaluador utiliza, normalmente el color rojo representa un nivel de riesgo alto, color amarillo nivel de riesgo medio y el color verde representa un nivel de riesgo bajo. (Committee of Sponsoring Organizations of the Treadway Commission, 2004).

A continuación se presenta un formato de un mapa de calor con sus respectivas interpretaciones para que las empresas puedan tomar como modelo en su aplicación de un sistema de gestión de riesgos.

Tabla 6: Mapa de calor

COMPAÑÍA ABC

MAPA DE CALOR

(1) PROCESO	(2) OBJETIVO	(3) ACTIVIDADES	(4) FACTORES DE RIESGO	(5) ORIGEN DEL RIESGO	(6) POTENCIAL CONSECUENCIA	(7) IMPACTO (A)	(8) PROBABILIDAD DE OCURRENCIA (A)	(9) NIVEL DE RIESGO INHERENTE (A)	(10) CONTROL DE RIESGO	(11) EFECTIVIDAD (B)	(12) OBSERVACIONES
Especificar el nombre del proceso evaluado	Describir el objetivo del proceso evaluado	Enlistar las actividades y tareas que forman parte del proceso	Describir el riesgo encontrado dentro de las actividades descritas en (3)	Identificar si el riesgo encontrado es interno o externo	Describir la consecuencia encontrada en caso de que el riesgo sea desfavorable y atente al cumplimiento del objetivo	Escoger si el impacto del riesgo es alto, medio o bajo	Escoger si la probabilidad de ocurrencia del riesgo es alta, media o baja	Identificar el número que le corresponde según el impacto y probabilidad escogido basándose en la tabla de nivel de riesgo inherente	Detallar el control que se posee para el riesgo determinado en (4)	Determinar el número que le corresponde según la tabla (B) dependiendo el control que se tenga para el riesgo	Anotar cualquier observación que pueda surgir en la evaluación

(A) Nivel de riesgo inherente

El nivel de riesgo inherente que debe ser calculado en el mapa de calor anteriormente explicado, viene siendo parte del producto entre el impacto y probabilidad de ocurrencia del riesgo examinado, para determinar este cálculo partiremos de la explicación del impacto y probabilidad de ocurrencia.

El impacto y probabilidad de ocurrencia de forma cualitativa, deben ser determinadas por un grupo de especialistas en el tema de riesgos dentro de la organización, ellos serán los responsables y entendidos en el tema para poder dar su criterio y su evaluación a riesgos escogidos. A continuación se detalla una política para determinar el impacto y probabilidad de ocurrencia de un riesgo dentro de las actividades de la compañía, esta última deberá tomar en cuenta los siguientes aspectos.

Tabla 7: Atributos medidos en una encuesta sobre cultura de riesgos

COMPAÑÍA ABC

POLÍTICA DE DETERMINACIÓN DE IMPACTO Y PROBABILIDAD DE OCURRENCIA DE RIESGOS

Impacto:

Al impacto que puede tener un riesgo dentro de la organización se lo considerará dentro de los siguientes rangos o niveles:

- Insignificante: aquel riesgo de impacto no percibido por la organización dando como resultado consecuencias muy bajas.
- Bajo: riesgo de impacto mínimo, donde sus consecuencias amenazarían un elemento de una función.
- Medio: riesgo de impacto moderado, sus consecuencias requieren ajustes significativos.
- Alto: riesgo de impacto importante, sus consecuencias amenazarían objetivos funcionales.
- Muy Alto: riesgo de impacto grave, sus consecuencias impiden el logro de objetivos funcionales.

Probabilidad de ocurrencia:

La probabilidad de ocurrencia de un riesgo deberá ser ubicada dentro de los siguientes cinco niveles:

- Insignificante: riesgo que no es probable que ocurra en un tiempo determinado.
- Bajo: riesgo improbable o con una mínima probabilidad de que ocurra.
- Medio: riesgo posible, probable de que ocurra.
- Alto: riesgo muy probable de que ocurra.
- Muy Alto: riesgo seguro y casi un hecho de que ocurra.

Elaborado por: Dennisse Vaca

A cada uno de los niveles, tanto de impacto como de probabilidad de ocurrencia, se les asigna un número de identificación en donde en cada uno de los casos se parte desde 1=Insignificante, 2=Bajo, 3=Medio, 4=Alto, 5=Muy Alto. A estos niveles se los combina dentro de una tabla de doble entrada para que el producto de cada rango de como resultado el nivel de riesgo inherente, como se puede ver a continuación.

Tabla 8: nivel de riesgo inherente

Impacto						
	MUY ALTO	5	10	15	20	25
	ALTO	4	8	12	16	20
	MEDIO	3	6	9	12	15
	BAJO	2	4	6	8	10
	INSIGNIFICANTE	1	2	3	4	5
		INSIGNIFICANTE	BAJO	MEDIO	ALTO	MUY ALTO

Frecuencia o Probabilidad de ocurrencia

Como se puede observar dentro de la Tabla 8, existen colores dependiendo del resultado generado de la combinación del impacto y la probabilidad de ocurrencia de un riesgo, su interpretación es la siguiente.

Se considera riesgos bajos al color verde, los cuales constan dentro de un rango de 1-6 puntos, dentro de este se encuentra el rango insignificante, el cual no se considera como amenaza dentro de la evaluación. Seguido se encuentran los riesgos medios representados por el color amarillo dentro de un rango de 8-10 puntos. Finalmente se encuentran los riesgos altos, que generan peligro dentro de la organización y que a su vez necesitan una

mayor atención y planes de acción inmediatos, resaltados con color rojo, los cuales se encuentran dentro del rango de 12-25 puntos.

Los resultados obtenidos dentro de este procedimiento, deben ser ubicados dentro de los casilleros (7), (8) y (9) del mapa de calor antes expuesto.

(B) Efectividad de control del riesgo

Dentro del casillero (10) del mapa de calor, se deben especificar los controles que posee la compañía para manejar el riesgo determinado y que son usados en el momento de la evaluación. La efectividad de los mismos viene a ser la determinación de las características cualitativas del control, las cuales son identificadas por los expertos que estén realizando la evaluación según la siguiente tabla.

Tabla 9: Efectividad de los controles

CONTROL	EFECTIVIDAD
Ninguno	1
Bajo	2
Medio	3
Alto	4
Destacado	5

Los controles pueden ser calificados según los rangos especificados en la tabla y cada uno de ellos se les asigna un número, el cual demostrará en general que tan efectivos serán los controles que posee la organización.

A manera de ejemplo, a continuación se adjunta un mapa de calor en donde se presentan varias situaciones que una empresa de vigilancia puede enfrentar, los riesgos que ocasiona y su respectivo análisis.

Tabla 10: Ejemplo de mapa de calor

COMPAÑÍA DE SEGURIDAD XYZ
MAPA DE CALOR

(1) PROCESO	(2) OBJETIVO	(3) ACTIVIDADES	(4) FACTORES DE RIESGO	(5) ORIGEN DEL RIESGO	(6) POTENCIAL CONSECUENCIA	(7) IMPACTO	(8) PROBABILIDAD DE OCURRENCIA	(9) NIVEL DE RIESGO INHERENTE (A)	(10) CONTROL DE RIESGO	(11) EFECTIVIDAD (B)	(12) OBSERVACIONES
SEGURIDAD Y VIGILANCIA	Proteger y resguardar los bienes y personas puestos a cuidado del servicio de seguridad con la mayor eficiencia	Registro de bienes encontrados por las personas del servicio de guardianía	Falta de un proceso que regule el registro de bienes encontrados por el personal para que estos puedan ser posteriormente devueltos a su dueño	ENDÓGENO	Robo de pertenencias olvidadas o perdidas, seguido de excesivos reclamos por parte de los dueños de los bienes	Medio	Alta	12	Ninguno	1	
	Generar una percepción de seguridad y confianza que favorezca la actividad productiva, comercial, de servicios o el bienestar de la Universidad	Registro en formatos específicos de los recorrido del personal de seguridad por las instalaciones de la Universidad	Mal manejo en los registros de actividades de recorridos por las instalaciones diarios que debe llevar el personal de seguridad. No existe evidencia de los recorridos diarios, ni se	EXÓGENO	Ambiente de inseguridad dentro de la Universidad que provoca que cualquier incidente pueda ocurrir	Alto	Medio	12	Hojas de registro de los recorridos en los que se evidencian fechas, turnos, responsables y actividad	1	

(1) PROCESO	(2) OBJETIVO	(3) ACTIVIDADES	(4) FACTORES DE RIESGO	(5) ORIGEN DEL RIESGO	(6) POTENCIAL CONSECUENCIA	(7) IMPACTO	(8) PROBABILIDAD DE OCURRENCIA	(9) NIVEL DE RIESGO INHERENTE (A)	(10) CONTROL DE RIESGO	(11) EFECTIVIDAD (B)	(12) OBSERVACIONES
			observa personal alrededor de las instalaciones								
		Intervalos de los recorridos del personal por las instalaciones	Los recorridos del personal por las instalaciones de la Universidad son muy grandes unos con otros, por lo que existe un tiempo amplio en el que las instalaciones dejan de ser vigiladas hasta que otro guardia en turno haga su recorrido	EXÓGENO	Posibles siniestros en intervalos de recorridos	Medio	Medio	9	Ninguno	1	
	Adoptar medidas preventivas para evitar hechos que puedan	Plan de contingencia elaborado para cualquier situación de emergencia	No existe un plan de contingencia que deba ser seguido por el personal de	EXÓGENO	Posibles accidentes que pongan en riesgo las instalaciones de la	Medio	Medio	9	Ninguno	1	

(1) PROCESO	(2) OBJETIVO	(3) ACTIVIDADES	(4) FACTORES DE RIESGO	(5) ORIGEN DEL RIESGO	(6) POTENCIAL CONSECUENCIA	(7) IMPACTO	(8) PROBABILIDAD DE OCURRENCIA	(9) NIVEL DE RIESGO INHERENTE (A)	(10) CONTROL DE RIESGO	(11) EFECTIVIDAD (B)	(12) OBSERVACIONES
	afectar la seguridad de nuestros clientes, o reducir sus efectos negativos.		seguridad que contenga medidas preventivas para cualquier situación de riesgo dentro de la Universidad		Universidad y que no se tenga un plan para disminuir su impacto						

Después de realizado el mapa de calor, la compañía también puede presentar el nivel de impacto y de probabilidad de sus riesgos mediante un mapa de riesgo matricial, en donde se podrá visualizar a cada uno de los riesgos identificados en un plano cartesiano e identificar cuáles son los más importantes y que requieren una acción inmediata. A continuación se presenta un ejemplo:

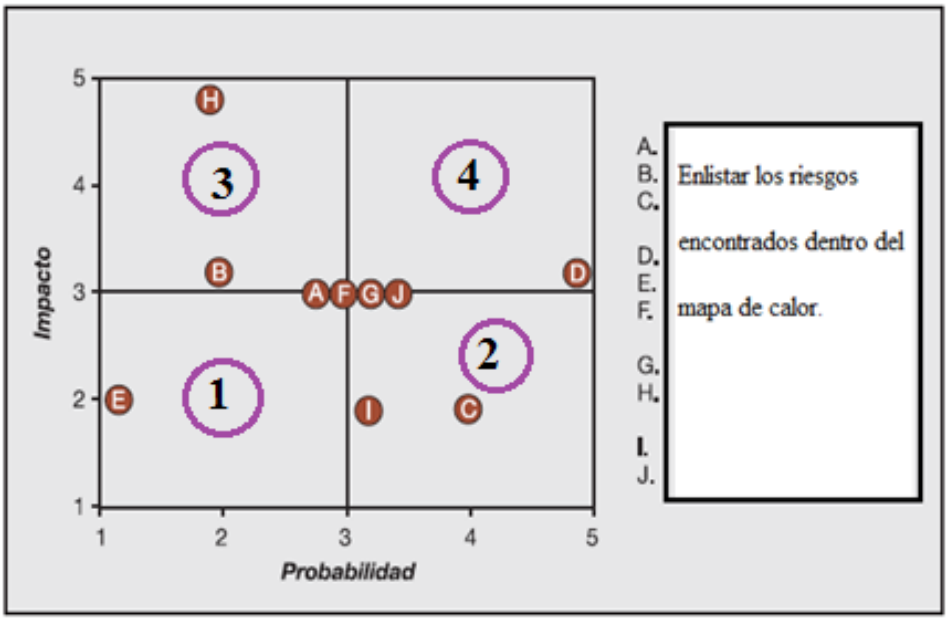


Figura 15: Mapa de riesgos matricial

Fuente: (Committee of Sponsoring Organizations of the Treadway Commission, 2004)

Como se puede observar en la figura existen escenarios en donde pueden estar ubicados los riesgos y según la calificación dada en el mapa de calor estos pueden ser ubicados. Los riesgos que se encuentran en el escenario 1 son los menos probables de que ocurran y su impacto será mínimo mientras que los que se encuentren en el escenario 4 son muy desfavorables para la compañía ya que su probabilidad de ocurrencia y su impacto será muy alto por lo que necesitan tener un plan de acción

inmediato. Los otros dos escenarios, los número 2 y 3 deben ser tratados según el criterio del evaluador ya que pueden ser interpretados de distintas maneras y dependerán del objetivo evaluado.

3.1.5 Componente N° 5: Respuesta a los riesgos

Una vez identificados los riesgos, su impacto y probabilidad de ocurrencia, el siguiente paso para la organización es encontrar planes de acción frente a los riesgos encontrados, a esto se lo conoce más comúnmente como respuesta a los riesgos.

En el documento COSO-ERM se dan a conocer cuatro alternativas de respuesta al riesgo que una empresa puede tener a momento de escoger un plan de acción. Estas cuatro alternativas son:

- Evitar el riesgo
- Reducir el riesgo
- Compartir el riesgo
- Aceptar el riesgo

El (Committee of Sponsoring Organizations of the Treadway Commission, 2004) define dentro de su marco integrado, a las cuatro alternativas de respuesta al riesgo las cuales serán presentadas junto con ejemplos de las mismas en la siguiente figura.

Figura 16: Alternativas de respuesta al riesgo

Fuente: (Committee of Sponsoring Organizations of the Treadway Commission, 2004)

Además de encontrar una respuesta al riesgo dentro de una de las alternativas explicadas en el Figura 16, las organizaciones también se ven en la obligación de determinar cuáles serán los costos y beneficios asociados con las alternativas escogidas para responder a los riesgos. Toda alternativa escogida sin importar su naturaleza acarreará costos de aplicación y puesta en marcha; y, los beneficios de cada una de ellas serán variados.

Las mediciones de costos y beneficios son realizadas por personal especializado de la empresa, quienes conozcan todo el movimiento y lo que significará para la empresa escoger entre varias alternativas. Después de plantear los diferentes escenarios, los directivos de las empresas son los responsables de tomar las decisiones correspondientes según la alternativa que más le convenga a la empresa y que todos estén dispuestos a desarrollarla.

Las empresas pueden aplicar un sistema de elección de alternativas y distintos escenarios en donde se elabore un cuadro comparativo y se detallen las alternativas junto con los costos y beneficios que cada una de ellas implique tener. A continuación se presenta una tabla que ayudará a las empresas a tener una visión más clara para escoger la alternativa idónea.

Tabla 11: Comparación de respuestas al riesgo incluyendo costo y beneficio

COMPAÑÍA ABC

COMPARACIÓN DE RESPUESTAS AL RIESGO INCLUYENDO COSTO Y BENEFICIO

(1) PROCESO	(2) OBJETIVO	(3) ACTIVIDADES	(4) FACTORES DE RIESGO	(5) RESPUESTA AL RIESGO	(6) COSTO	(7) DESCRIPCIÓN DE LA RESPUESTA AL RIESGO	(8) BENEFICIOS	(9) OBSERVACIONES
Especificar el nombre del proceso evaluado	Describir el objetivo del proceso evaluado	Enlistar las actividades y tareas que forman parte del proceso	Describir el riesgo encontrado dentro de las actividades descritas en (3)	Escoger entre las cuatro alternativas (Aceptar, Evitar, Compartir, Reducir) del riesgo descrito en (4)	Determinar el costo en unidades monetarias de la acción tomada	Describir la acción a ser emprendida considerando (5) y (6)	Describir los beneficios encontrados para la entidad al tomar la acción seleccionada	Anotar cualquier observación que surja de la evaluación

Fuente: (Committee of Sponsoring Organizations of the Treadway Commission, 2004)

Dentro del casillero número 5, respuesta al riesgo, la compañía debe tomar en cuenta que debido a que esta es una tabla comparativa, cada uno de los riesgos pueden tener distintas respuestas al riesgo, es decir, se puede tener las cuatro alternativas de respuesta al riesgo con sus respectivos costos y beneficios para un mismo riesgo y de esta manera la dirección tendrá más claro cuál de las posibles alternativas es la que más le conviene adoptar a la organización para un mejor desempeño en cuanto a riesgos se refiere.

Para poder llevar a cabo de una manera eficaz el componente de respuesta al riesgo, la organización debe considerar que deben existir pasos a seguir para conseguir una adecuada realización de dicho componente, ya que este representa las acciones que serán tomadas y su mala determinación y ejecución será evidenciada en pérdidas de dinero y tiempo, fraudes y pondrá en peligro las operaciones y la estabilidad de la empresa.

A continuación se presenta un formato de políticas para llevar a cabo el componente de respuesta a los riesgos, en donde se especifica los pasos a seguir para su ejecución.

Tabla 12: Atributos medidos en una encuesta sobre cultura de riesgos

COMPAÑÍA ABC

POLÍTICA DE RESPUESTA A LOS RIESGOS

Realizado por:

Departamento:

1. Introducción:

- El Comité de Riesgos será el encargado de realizar la evaluación de las respuestas a los riesgos.
- Determinar los objetivos que se esperan cumplir al desarrollar esta actividad.
- Determinar el alcance que tendrá el taller.
- Informar a todos los especialistas participantes los pasos a seguir.

2. Desarrollo:

- Identificación y clasificación de los riesgos encontrados para cada actividad.
- Analizar las posibles respuestas a cada uno de los riesgos considerando lo siguiente:
  - ✓ Puntos críticos de control
  - ✓ Causas de los riesgos
  - ✓ Límites de control
- Determinar si cada una de las alternativas de respuesta al riesgo se alinea con el riesgo previamente aceptado y la tolerancia al riesgo correspondiente.
- Detallar cada una de las alternativas de respuesta en el cuadro de comparación.

3. Cierre:

- Obtener conclusiones acerca de lo elaborado.
- Realizar un informe de actividades del comité de riesgos.
- Informar los resultados a los directivos de la organización.

3.1.6 Componente N° 6: Actividades de Control

Las actividades de control surgen para asegurar que las acciones detalladas en la respuesta a los riesgos se cumplan y se lleven a cabo de la mejor manera según

los lineamientos de la dirección. Estas actividades de control usualmente vienen en forma de políticas, manuales y/o procedimientos.

Las actividades de control son impuestas por los altos mandos de la compañía para ser aplicados y acatados por todos los demás niveles de la organización. Muchas veces estas actividades forman parte del control interno de la compañía en donde se detallan los procedimientos a los diferentes procesos que tiene la compañía para realizar sus operaciones.

Las actividades de control deben tener una estrecha relación con las respuestas a los riesgos escogidas, ya que estas serán las reguladoras de que dichas respuestas se lleven realmente a cabo. Sin embargo, existen ocasiones en donde las actividades de control se convierten en las respuestas a los riesgos, esto dependerá de los objetivos y riesgos que están siendo evaluados. Este tipo de particular se presenta usualmente cuando los eventos que están siendo analizados tienen relación con el control interno de la compañía, ahí es donde los controles adecuados y pertinentes se convierten en respuesta a los riesgos, sin importar la alternativa que se haya tomado para tratar al riesgo.

Si bien es cierto que muchas de las actividades de control se traducen en políticas y manuales de procedimientos, estas pueden ser agregadas o modificadas dentro de los documentos de control pertinentes con los que la compañía cuente; existen otras actividades que surgen como nuevas dentro de este proceso las cuales deben ser documentadas físicamente y convertirse en una nueva manera de tratar los riesgos y actividades que realice la empresa, de esta manera esta última

tendrá respaldos de que el personal debe cumplir con los nuevos procedimientos establecidos.

Dentro del documento de COSO-ERM no se especifica ninguna herramienta o técnica que pueda ser utilizada para establecer actividades de control, por lo que este componente queda a criterio de las propias organizaciones al momento de la aplicación de un sistema de gestión de riesgos. A continuación se presentan algunas actividades de control que pueden ser acogidas por la organización:

Tabla 13: Política de actividades de control

COMPAÑÍA ABC
POLÍTICA DE ACTIVIDADES DE CONTROL
Realizado por:
Departamento:
Dentro de la política de actividades de control se detallan las actividades que deberán realizarse para controlar que los riesgos identificados y sus respectivas respuestas se estén llevando a cabo según lo establecido por el comité de riesgos. • Revisiones por parte de la alta dirección; en donde se examinan datos reales de la organización según los presupuestos mantenidos, datos históricos y se realiza la supervisión de las actividades propuestas como nuevas. • Revisión de informes de rendimiento. • Reprocesamiento de información y revisión de sistemas de información contable, en donde se revise la exactitud, claridad y oportunidad de la información que arrojan los sistemas utilizados y las transacciones correspondientes. • Controles físicos, en donde se comparen las existencias físicas reales de inventarios, equipos, maquinaria, entre otros con lo registrado en los sistemas de información. • Supervisión de indicadores de rendimiento. • Segregación de funciones, para reducir el riesgo de error y fraude. • Aseguramiento del cumplimiento de leyes y normas legales impuestas por organismos de control. • Revisión de autorizaciones para realizar actividades y transacciones.

3.1.7 Componente N° 7: Información y Comunicación

3.1.7.1 Comunicación

Cada empresa debe contar con un sistema eficaz de comunicación dentro de ella, debido a que la comunicación y entendimiento de la información es esencial para una buena implementación de un sistema de gestión de riesgos.

Un buen sistema de comunicación tanto interna como externa permite que todos los colaboradores de la empresa se encuentren informados y conozcan muy bien las actividades que deben realizar y cómo las deben realizar. La comunicación de una organización debe ser multidireccional, es decir, debe fluir por todos los niveles de la organización empezando por los altos mandos quienes son los responsables y más interesados en que el sistema de gestión de riesgos este funcionando a la perfección. La comunicación no solo debe ser interna, también debe ser clara, precisa y concisa para los terceros como clientes, proveedores y accionistas. (Committee of Sponsoring Organizations of the Treadway Commission, 2004)

Una buena comunicación dentro de la organización se traduce en que la dirección de la misma puede transmitir específicamente a sus colaboradores las intenciones que se tienen con la implementación de un sistema de gestión de riesgos, las nuevas políticas que se van a adoptar y

la nueva cultura de riesgos que deberá ser manejada desde la implementación del sistema en adelante. Desde el momento de la implementación todo el sistema de comunicaciones de la organización debe alinearse con la filosofía de riesgos que deba a adoptar para que todo concuerde y sea parte de un mismo sistema integrado de actividades.

Como se dijo al inicio del capítulo, la comunicación de la filosofía de la empresa y de su cultura de riesgos es imprescindible y es la base para el desarrollo de los demás componentes de un sistema de gestión de riesgos. Para que la comunicación del nuevo sistema de gestión de riesgos funcione adecuadamente, las empresas pueden adoptar nuevas políticas en donde se incluya este nuevo tipo de comunicación. Dentro de dichas políticas debe constar la manera en cómo la entidad va a lograr comunicar todo el tema de riesgos y los planes de acción que se tomarán para que esta sea asimilada por todos los colaboradores. A continuación se presenta un modelo de políticas que una empresa puede adoptar para comunicar la nueva cultura y filosofía de riesgos.

Tabla 14: Políticas de comunicación de la filosofía de riesgos

COMPAÑÍA ABC

POLÍTICAS DE COMUNICACIÓN DE LA CULTURA DE RIESGOS

1. Filosofía de gestión de riesgos

- La dirección comentará los riesgos y las respuestas al riesgo asociadas en reuniones informativas con los empleados de manera periódica.
- Las políticas, estándares y procedimientos de gestión de riesgos se facilitan a los empleados junto con declaraciones firmes de su cumplimiento.
- Las capacitaciones para nuevos empleados incluyen información y documentación sobre la filosofía de gestión de riesgos de la empresa y su programa de gestión de riesgos.
- Los empleados que desempeñen cargos antiguos son obligados asistir a capacitaciones sobre iniciativas de gestión de riesgos.
- La nueva filosofía de gestión de riesgos es reforzada a través de programas continuos de comunicación interna y externa.

2. Tipo de comunicación a ser utilizada

- Correos electrónicos
- Correos de voz
- Boletines corporativos
- Bases de datos
- Páginas de intranet donde se muestra información de interés
- Comunicaciones corporativas continuas
- Conferencias
- Carteles, letreros
- Capacitaciones
- Foros abiertos

3. Uso del internet para la comunicación de gestión de riesgos

- Foros de discusión
- Políticas y procedimientos ubicados en la intranet de la empresa
- Preguntas más frecuentes
- Informes de gestión de riesgos y actividades relevantes
- Enlaces en sitios web a políticas y procesos claves
- Listado de información de contacto de los responsables y personal de apoyo del programa de gestión de riesgos.

Fuente: (Committee of Sponsoring Organizations of the Treadway Commission, 2004)

3.1.7.2 Información

En el aspecto de la divulgación de la información también es muy importante al momento de implementar un nuevo sistema de gestión de riesgos dentro de una organización. Se establece que toda la información que vaya ser utilizada para analizar los distintos objetivos, actividades y riesgos debe ser exacta, clara, precisa y concisa.

El flujo de la información con la que la empresa va a contar para llevar a cabo su sistema de gestión de riesgos debe estar bien estructurado y comprendido por todos los niveles pertenecientes a la organización debido a que esta recopila toda la información de las bases de datos de las empresas para establecer objetivos, estrategias, identificar eventos, evaluar riesgos, determinar respuestas a ellos, es decir, llevar a cabo todo el proceso de gestión de riesgos y para que este se desarrolle y fluya de manera adecuada la información debe ser exacta.

El flujo de la información no solo debe ser interno, también existe información procedente de terceros que son externos a la empresa. Todas las actividades que se realicen dentro y fuera de la empresa deben ser consideradas como procesos, en donde se establezca que cada proceso tendrá información de entrada, las tareas respectivas e información de salida; de esta manera el flujo de la información será tomado en cuenta con la importancia que requiere.

Dentro del documento COSO-ERM se presenta una figura en donde se muestra como debería ser el flujo de información de una organización de manera general.

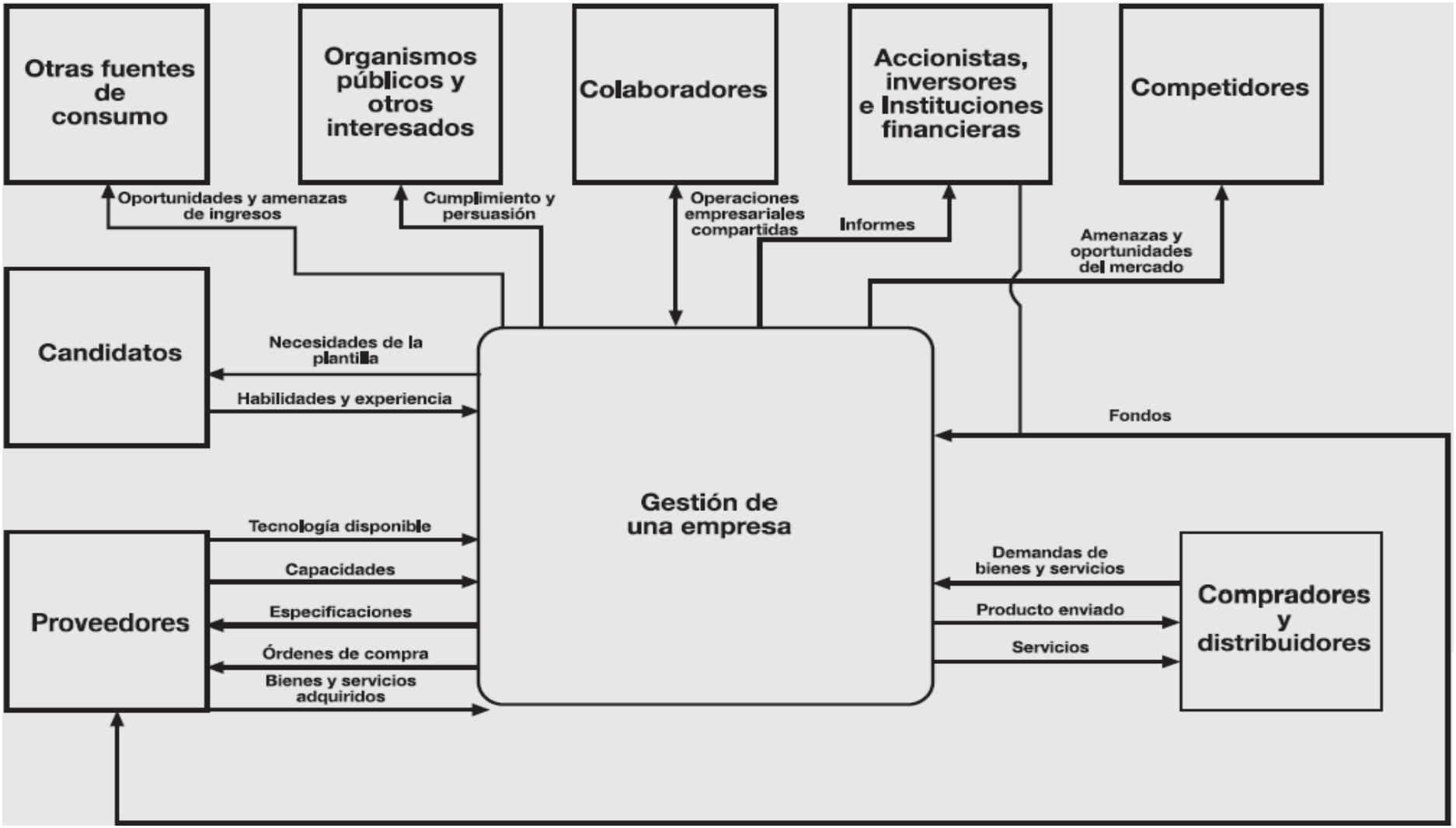


Figura 17: Flujo de información genérico

Fuente: (Committee of Sponsoring Organizations of the Treadway Commission, 2004)

Además de existir una relación entre la información dentro de la compañía en general, dentro de todo el proceso de la implementación del sistema de gestión de riesgos también debe existir coherencia y relación entre todos los componentes que forman parte del sistema. Así mismo el documento COSO-ERM presenta una figura en donde se evidencias las relaciones de información que cada componente del sistema de gestión de riesgos debe tener.

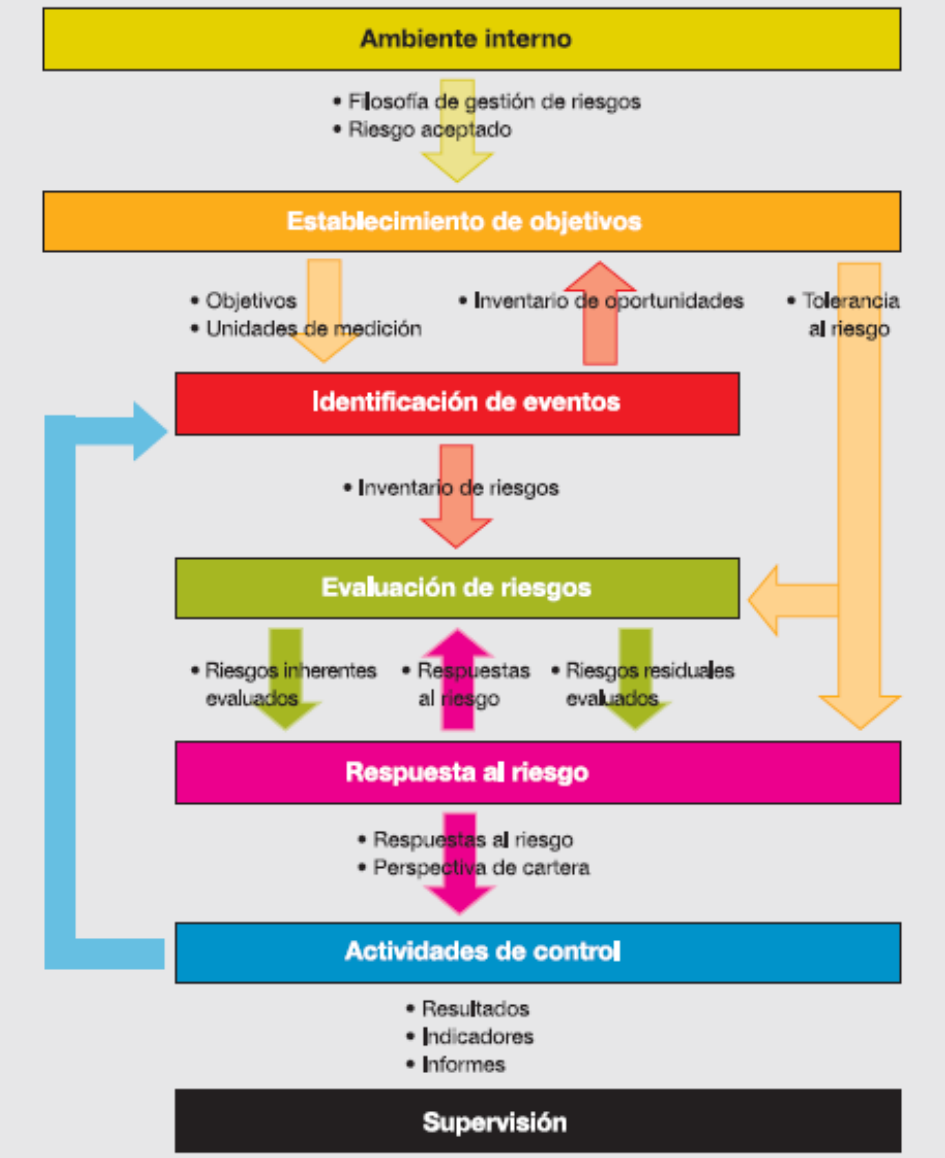


Figura 18: Flujo de información en la gestión de riesgos

Fuente: (Committee of Sponsoring Organizations of the Treadway Commission, 2004)

En la actualidad, las empresas se ven en la obligación de utilizar la tecnología para llevar a cabo todas las actividades que tengan relación con su negocio, sin embargo existen empresas que debido a su gran tamaño, tienen todos sus sistemas automatizados y por otro lado existen empresas pequeñas que tienen ciertas cosas bajo el uso de la tecnología.

Dentro del documento COSO-ERM se realizan ciertas recomendaciones a las empresas que cuentan con todos sus procesos y actividades automatizadas. Las recomendaciones se centran principalmente en que la información de todos los departamentos y unidades de la empresa debe estar vinculada y tener relación entre sí ya que está información servirá de base para realizar todo el análisis que se ha expuesto a lo largo de este capítulo.

Muchas corporaciones grandes hacen uso de un sistema de gestión de riesgos para su empresa también automatizado en el cual toda la información necesaria para llevar a cabo la evaluación se encuentra dentro del sistema y los cálculos, estimaciones y probabilidades se realizan por sí solas con solo ingresar una pequeña cantidad de información. El uso de estos sistemas en empresas grandes representa una ayuda significativa ya que este tipo de organizaciones cuenta con muchos procesos y actividades que llevando a cabo la implementación manualmente no resulta factible ni comprensible.

Finalmente pero no menos importante la correcta información que maneje la compañía se refiere también acerca de los informes que la

implementación del sistema de gestión de riesgos arroje. Estos informes deben ser claros y de ayuda para la toma de decisiones de la compañía. Estos informes pueden ser muy elaborados y formales para dar a conocer resultados importantes o simplemente un respaldo del proceso que se llevó a cabo. En las empresas grandes que cuentan con herramientas informáticas que realizan estos informes estos deberían ser arrojados en tiempo real e inmediatamente para ser informados a la dirección.

Existen informes de la gestión de riesgos llamados cuadro de mando los cuales son definidos por el (Committee of Sponsoring Organizations of the Treadway Commission, 2004) como:

> Informes que permiten a la dirección determinar con rapidez en qué medida se encuentra alineado el perfil de riesgo de la entidad con las tolerancias al riesgo, si estos no se encuentran en línea, quiere decir que los controles no funcionan de la manera esperada y la dirección debe emprender acciones necesarias.

Un ejemplo de un informe de cuadro de mando se presenta a continuación en la siguiente figura.

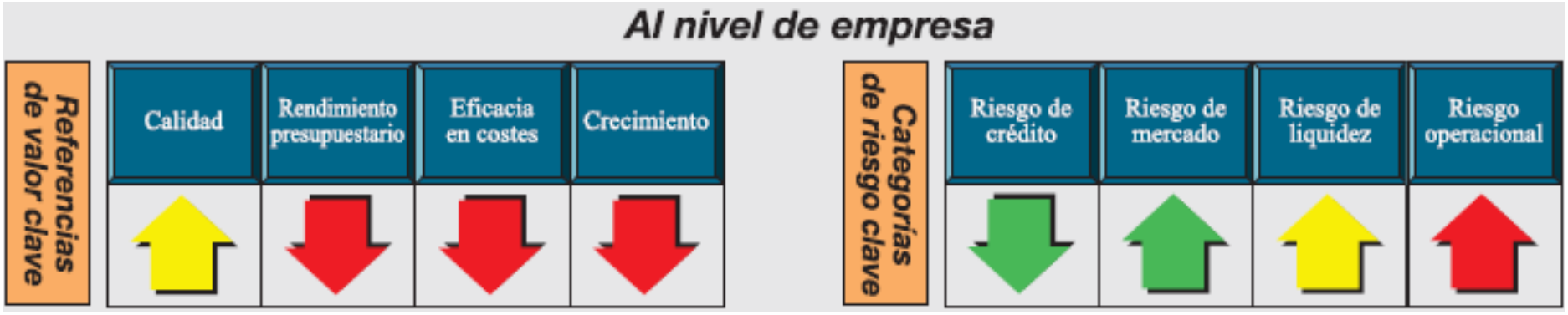


Figura 19: Informe de cuadro de mando

Fuente: (Committee of Sponsoring Organizations of the Treadway Commission, 2004)

Dentro de cada categoría analizada se encuentran flechas de colores las cuales tiene dos interpretaciones:

- La posición de la flecha indica la tendencia entre un periodo evaluado y otro, en este caso de las pérdidas generadas por los riesgos evaluados; si una flecha descendente indica una reducción de las pérdidas esperadas y viceversa. (Committee of Sponsoring Organizations of the Treadway Commission, 2004)

- El color de las flechas compara el riesgo residual con la tolerancia al riesgo. Una flecha color verde indica que las pérdidas se encuentran dentro del rango de la tolerancia al riesgo, la flecha color amarillo indica que la pérdida se encuentra en el límite de tolerancia y la flecha roja indica que la pérdida se encuentra fuera del nivel de tolerancia al riesgo. (Committee of Sponsoring Organizations of the Treadway Commission, 2004).

3.1.8 Componente N° 8: Monitoreo

Siendo la supervisión el último componente del sistema de gestión de riesgos, este se refiere a que todo el proceso de la implementación del sistema debe ser supervisado y monitoreado tanto a lo largo de su desarrollo como durante todo el tiempo que se encuentra en vigencia, es decir, la supervisión es constante.

Existen diferentes herramientas para supervisar este sistema, en donde se pueden realizar actividades de supervisión permanente o evaluaciones independientes,

las cuales ayudarán a comprobar que el sistema se esté realizando de la mejor manera y con los controles adecuados.

Las evaluaciones permanentes son aquellas realizadas diariamente dentro de la organización, donde la dirección será la responsable de revisar que las actividades se estén desarrollando adecuadamente. El (Committee of Sponsoring Organizations of the Treadway Commission, 2004) en lista algunos ejemplos de evaluaciones permanentes y son los que se presentan a continuación:

- La dirección revisa informes de indicadores claves de actividad del negocio.

- La dirección operativa compara la producción, inventario, medidas de calidad, ventas y otra información obtenida en el curso de las actividades diarias con información generada en el sistema, así como con el presupuesto y planificación.

- La dirección revisa el rendimiento, comparándolo con los límites establecidos para los índices de riesgo.

- La dirección revisa transacciones comunicadas a través de indicadores de alerta.

- La dirección revisa indicadores clave de rendimiento, como se describe en el capítulo de Identificación de eventos.

Por su lado, las evaluaciones independientes, se llevan a cabo dentro de periodos determinados para la organización en donde se realiza una inspección general a todo el proceso de sistema de gestión de riesgos que una entidad esta llevando a cabo. Este proceso se lo realiza para tener una doble opinión acerca del desarrollo del sistema de gestión de riesgos. Usualmente las evaluaciones independientes son realizadas por la dirección de la organización, el departamento de auditoria interna, auditores externos o la combinación de las tres partes.

Usualmente el monitoreo del sistema de gestión de riesgos lo realiza el departamento de auditoria interna, esta responsabilidad es designada por la alta dirección de la compañía.

Dentro de las evaluaciones independientes, se establece que existen varios métodos y herramientas que pueden ser utilizados para que la dirección supervise y verifique que el sistema de gestión de riesgos está dando resultados positivos y se esta llevando a cabo de acuerdo a lo planificado. Las herramientas que pueden ser utilizadas varían entre realizar entrevistas, cuestionarios, cuadros de mando y también diagramas de flujo.

A continuación se presentarán unos pasos que pueden ser seguidos por la dirección para evaluar de manera independiente el sistema de gestión de riesgos.

Tabla 15: Evaluación independiente del sistema de gestión de riesgos

COMPAÑÍA ABC

EVALUACIÓN INDEPENDIENTE DEL SISTEMA DE GESTIÓN DE RIESGOS

Realizado por:

Departamento:

1. Planificación:

- Definir los objetivos y alcance de la evaluación
- Identificar el responsable de la evaluación
- Determinar el equipo con el que se contará para la evaluación
- Definir metodologías y los pasos a seguir para la evaluación

2. Ejecución:

- Obtener conocimiento de las actividades de la unidad de negocio o departamento
- Comprender el proceso del sistema de gestión de riesgos
- Aplicar la metodología acordada para la evaluación
- Analizar resultados
- Documentar problemas encontrados y las soluciones según el caso
- Informar sobre los resultados encontrados a quien corresponda

3. Informes y plan de acción:

- Comentar los resultados con la dirección general y la de negocio
- Determinar planes de acción adecuados
- Incorporar retroalimentación de la dirección al informe final de la evaluación

Como se mencionó anteriormente, el departamento de auditoria interna, también puede ser el responsable del monitoreo de la adecuada implementación, puesta en marcha y desarrollo del sistema de gestión de riesgos. A continuación se presenta una política que resume algunas actividades que el departamento de auditoria interna puede realizar en la etapa de monitoreo.

Tabla 16: Política de monitoreo del departamento de auditoria interna

COMPAÑÍA ABC

POLÍTICA DE MONITOREO DEL DEPARTAMENTO DE AUDITORIA INTERNA

Realizado por:

Actividades antes de revisar el sistema de gestión de riesgos:

1. Investigar y revisar desarrollos, tendencias e información actualizada del entorno organizacional de la compañía.

2. Revisar las políticas corporativas, informes de la administración para determinar estrategias de negocio.

3. Revisar informes realizados previamente de evaluación de riesgos.

Actividades durante la revisión el sistema de gestión de riesgos:

1. Entrevistar a la gerencia general y por departamentos para conocer los objetivos del negocio

2. Revisar información para dar una opinión independiente acerca del proceso de evaluación de riesgos.

3. Revisar la oportunidad e integridad de la información obtenida.

4. Determinar la eficacia de los procesos de evaluación y gestión de riesgos implementado.

Actividades para finalizar la revisión del sistema y prevenir riesgos de fallos de control:

1. Crear un programa de aseguramiento y mejora de la calidad.

2. Análisis en determinados períodos de la metodología y plan sostenido para realizar las auditorias.

3. Realizar una planificación de auditoria efectiva.

4. Diseño de una auditoria efectiva.

5. Revisiones constantes de informes de riesgos y gestión de riesgos emitidos.

6. Asignación de recursos apropiados para realizar las revisiones.

Fuente: (Silva M., 2014)

Finalmente dentro del componente de supervisión cabe destacar que la documentación de todo el proceso de implementación de un sistema de gestión

de riesgos es sumamente importante, debido a que esta documentación del proceso ayuda a la organización a tener respaldos de todo el trabajo realizado y a su vez, ayuda a la dirección a que la tarea de supervisar sea más fácil y rápida.

Cuando una organización tiene respaldos físicos y la documentación adecuada y organizada de manera precisa, permite que las revisiones identifiquen si todas las actividades, procesos y políticas que se hayan establecido son los adecuados para que la compañía pueda enfrentarse de la mejor manera a los riesgos.

La documentación que debe existir durante una evaluación del sistema de gestión de riesgos puede incluir lo siguiente: (Committee of Sponsoring Organizations of the Treadway Commission, 2004)

- Organigramas
- Manuales de políticas
- Procedimientos operativos
- Flujos de procesos
- Controles relevantes
- Indicadores clave de rendimiento
- Riesgos claves identificados
- Mediciones claves del riesgo

3.2 RESUMEN DE FORMATOS Y POLÍTICAS ESTABLECIDOS POR COMPONENTE, SEGÚN LINEAMIENTOS DE COSO-ERM

A continuación se resumen mediante una tabla, todos los formatos y políticas que se han dado a conocer por cada componente establecido por COSO-ERM para que una empresa pueda llevar a cabo de manera exitosa, la implementación de un sistema de gestión de riesgos basado en los lineamientos de COSO-ERM.

Tabla 17: Resumen de formatos y políticas para cada uno de los componentes establecidos por COSO-ERM

COMPONENTE	***NOMBRE DEL FORMATO O POLÍTICA***
1. Ambiente Interno	• Encuesta sobre la cultura de riesgos • Estructura de un código de ética o conducta
2. Establecimiento de objetivos	• Mapa de riesgos • Matriz de relación entre misión, objetivos, riesgo aceptado y tolerancia al riesgo
3. Identificación de eventos	• Flujo de actividades de un proceso • Política de taller de grupo
4. Evaluación de riesgos	• Mapa de calor • Política de determinación de impacto y de probabilidad de ocurrencia de riesgos • Tabla de nivel de riesgo inherente • Tabla de efectividad del control interno • Ejemplo de mapa de calor • Mapa de riesgo matricial
5. Respuesta al riesgo	• Mapa de comparación de respuestas a los riesgos incluyendo su costo y beneficio • Política de respuesta al riesgo
6. Actividades de control	• Política de actividades de control
7. Información y comunicación	• Política de comunicación de la cultura de riesgos • Flujo de información genérico • Flujo de información de la gestión de riesgos • Informe de cuadro de mando
8. Monitoreo	• Evaluación independiente del sistema de gestión de riesgos • Política de monitoreo del departamento de auditoria interna

4 CONCLUSIONES Y RECOMENDACIONES

4.1 CONCLUSIONES

De acuerdo con el objetivo general: Elaborar formatos basados en la metodología COSO-ERM para que las empresas de la ciudad de Quito puedan implementar un sistema de gestión de riesgos; durante la investigación realizada al documento COSO-ERM se pudo apreciar que es una de las metodologías más famosas y apreciadas dentro del tema de riesgos empresariales. Se han propuesto varios formatos de cada uno de los componentes que forman parte de esta teoría, los cuales sirven como base y lineamientos para que las empresas de la ciudad de Quito, sin importar su tamaño ni características específicas, puedan adoptar este sistema de manera sencilla y práctica; asegurando que cumplen con normativas mundialmente aceptadas.

Para el objetivo específico: Investigar los diferentes tipos de metodologías de gestión de riesgos empresariales mundialmente aceptadas; según la investigación realizada, se ha podido determinar que existen varias metodologías y teorías mundialmente aceptadas en el mercado con respecto a sistemas ERM, las cuales son todas muy efectivas al momento de aplicarlas a las empresas para gestionar sus riesgos y actividades diarias. La importancia radica en que las empresas acojan cualquier teoría y lleven a la práctica dentro de ellas, ya que son herramientas muy útiles que ayudan a prevenir muchos acontecimientos desfavorables como son los fraudes, pérdidas de

cantidades de dinero considerables, ineficiencias, incumplimientos de normativas, entre otros.

Para el siguiente objetivo específico: Determinar las características y beneficios que ofrecen las distintas metodologías de gestión de riesgos empresariales; se realizaron las investigaciones pertinentes acerca del tema de los sistemas de gestión de riesgos empresariales, al respecto se puede decir que estos, sin importar su metodología, son muy importantes dentro de las organizaciones debido a que ayudan en todo aspecto a mejorar las operaciones de las entidades. Así mismo se ha podido determinar que el objetivo principal de la aplicación de un sistema de gestión de riesgos dentro de una empresa, se centra en brindar apoyo en las gestiones diarias, atraer inversiones, reducir riesgos y pérdidas, mejorar las prácticas y procedimientos establecidos, optimizar las estrategias propuestas y obtener mejores rendimientos económicos.

Para el último objetivo específico: Elaborar formatos de un sistema de gestión de riesgos, resaltando los beneficios que una empresa puede llegar a tener aplicando lo propuesto; se determinó que la aplicación de un sistema de gestión de riesgos empresariales basado en los lineamientos de COSO-ERM contribuye a las organizaciones a en primer lugar reafirmar la cultura organizacional en lo que a riesgos se refiere y a evaluar el conocimientos que los empleados tienen acerca de este tema para que puedan contribuir de mejor manera a las labores diarias; ayuda también a formular mejores objetivos y estrategias alineándolos a la misión de la empresa; identificar eventos que representen riesgos dentro de las actividades normales de la entidad; identificar, monitorear y responder a los riesgos encontrados, optimizar los procesos de comunicación e información que se llevan a cabo y emprender nuevas

técnicas de supervisión y retroalimentación por parte de los directivos para hacer de este proceso el idóneo al momento de mejorar las prácticas que históricamente se vienen realizando.

Finalmente después de la investigación se pudo determinar además que la fijación de roles y responsabilidades es de suma importancia dentro de la aplicación de un sistema de gestión de riesgos para que este sea tratado con la importancia requerida. El rol de los directivos y altos mandos de la compañía es el más importante dentro de este sistema ya que ellos serán los responsables y expertos de impartir la nueva filosofía y ejemplo a seguir a todos los colaboradores que se encuentran laborando dentro de la organización.

4.2 RECOMENDACIONES

Se recomienda a las empresas de la ciudad de Quito adoptar los formatos y políticas propuestos dentro de esta investigación para implementar un sistema de gestión de riesgos adecuado a sus necesidades organizacionales. La aplicación de este sistema se debe realizar a todos los departamentos de la organización, los mismos que deben implementarse de a poco, observando las reacciones de los colaboradores y la acogida que vayan teniendo hacia el mismo ya que la implementación de nuevos procesos puede generar malestares laborales y de inconformidades si los empleados no son informados con el debido cuidado y atención, por lo que cabe destacar que la buena implementación del componente interno en primer lugar es de vital importancia para el éxito del sistema ERM.

Se recomienda a las organizaciones generar un ambiente interno de trabajo lleno de confianza y a su vez de compromiso por parte de todos los colaboradores de la empresa sin importar su cargo o rango dentro de la misma, ya que ellos serán los encargados de la implementación práctica del sistema de gestión de riesgos y el éxito del mismo dependerá del compromiso y entrega que ellos pongan.

La aplicación del sistema de gestión de riesgos, como ya se ha dicho, debe ser aplicado en la organización por partes, es decir siguiendo los lineamientos de COSO-ERM que divide la aplicación en ocho componente que fueron explicados y en cada uno de ellos propuesto un formato. A su vez, debe ser aplicado a todos los departamentos y niveles de la organización, sin embargo se debe tomar en consideración que todos los componentes del sistema de gestión de riesgos deben estar interrelacionados y conectados entre si, deben tener una secuencia lógica y deben ser aplicados una vez que el componente anterior haya sido desarrollado y terminado con éxito. Se debe tener muy en cuenta que el logro exitoso de la implementación depende de cómo los ocho componentes fueron aplicados con éxito y deben arrojar ciertos conocimientos importantes y aprendizaje oportuno a los directivos de la organización para que ellos puedan tomar las mejores decisiones.

REFERENCIAS

1. Ambrosone, M. (Mayo de 2007). *La Administración del Riesgo Empresarial: Una responsabilidad de todos-Enfoque COSO.* Obtenido de http://ayhconsultores.com/img/COSO.pdf

2. Audisec. (s.f.). *El software perfecto para integrar en su organización*. Obtenido de GlobalSuite Risk Management: http://www.globalsuite.es/es/risk-management-iso-31000/?gclid=CP_whYio7MsCFUIfhgod_hgO2Q

3. Audisec. (s.f.). *Gestione los riesgos de su organización de manera integrada utilizando sus propias metodologías configurables en Globalsuite® - Risk Management*. Obtenido de GlobalSuite Risk Management: http://www.globalsuite.es/wp-content/uploads/2015/12/GlobalSUITE-Risk-Management.pdf

4. Baquero Herrera, M. (s.f.). *Estándares de Supervisión Bancaria*. Obtenido de http://www.eumed.net/libros-gratis/2006b/mbh/1b.htm

5. Committee of Sponsoring Organizations . (s.f.). *COSO Committee of Sponsoring Organizations of the Treadway Commission*. Obtenido de http://www.coso.org/aboutus.htm

6. Committee of Sponsoring Organizations of the Treadway Commission. (2004). *Enterprise Risk Management – Integrated Framework.* (PricewaterhouseCoopers LLP, Trad.)

7. Committee of Sponsoring Organizations of the Treadway Commission. (2004). *Gestión de Riesgos Corporativos- Técnicas de Aplicación.*

8. Federation of European Risk Management Associations. (2002). *Estándares de Gerencia de Riesgos.* Obtenido de https://www.theirm.org/media/886346/rm_standard_spanish_15_11_04-1-.pdf

9. Fox, C. (15 de Marzo de 2011). *ERM Standards of Practice and Shared Risk Principles.* Obtenido de http://www.ermsymposium.org/2011/pdf/gs3_fox.pdf

10. Hernández Meléndez, E. (3 de Mayo de 2006). *Riesgos en Auditoría.* Obtenido de http://www.gestiopolis.com/riesgos-en-auditoria/

11. Hernández S., R. (1997). *Metodología de la Investigación.* McGraw-Hill.

12. IBM. (s.f.). *Analítica de Riesgos*. Obtenido de http://www-03.ibm.com/software/products/es/category/risk-management#products

13. International Organization for Standardization. (2009). *ISO 31000:2009 Gestión de Riesgos- Principios y Guías.*

14. López N., F. (2002). *El análisis de contenido como método de investigación* . Obtenido de http://rabida.uhu.es/dspace/bitstream/handle/10272/1912/b15150434.pdf?sequence=1

15. Mantilla B., S. A. (2003). *Control Interno: Informe COSO.* Bogotá: ECOE Ediciones.

16. Mejía Quijano, R. C. (2006). *Administración del Riesgo un enfoque empresarial.* Medellín, Colombia: Fondo editorial Universidad EAFIT. Obtenido de Consultorio Contable: http://www.eafit.edu.co/escuelas/administracion/consultorio-contable/Documents/notas-clase/nota2-auditoria.pdf

17. Mora, C. (s.f.). *Gestión de Riesgos Corporativos, Marco Integrado COSO 2*. Obtenido de http://www.econ.unicen.edu.ar/attachments/2009_MaterialERM.pdf

18. OCEG. (2009). *OCEG "Red Book" 2.0: 2009 - a Governance, Risk and Compliance Capability Model.*

19. Olaya, J. (6 de Julio de 2006). *Riesgo Operativo en Ecuador*. Obtenido de http://riesgooperativo.blogspot.com/

20. Palisade Corporation. (s.f.). *El futuro en una hoja de trabajo* . Obtenido de http://www.palisade-lta.com/risk/?gclid=CNSx9teMlMsCFdAWHwoduagK2g

21. Risk Consulting Colombia. (s.f.). *Sherlock.* Obtenido de http://www.software-sherlock.com/inicio/

22. Silva M., W. (2014). *Apuntes de Auditoria Operativa.* Quito.

23. Superintendencia de Banca y Seguros y AFP . (Octubre de 2006). *Basilea II: El nuevo acuerdo de capital*. Obtenido de http://www.sbs.gob.pe/repositorioaps/0/0/jer/REGUL_PROYIMP_BASIL_FUNSBS/BasileaII-Introduccion-JPoggi-MLuy.pdf

24. Superintendencia de Bancos y Seguros del Ecuador. (s.f.). *25 principios de Basilea*. Obtenido de http://www.sbs.gob.ec/practg/sbs_index?vp_art_id=7&vp_tip=2#UP

25. The Institute of Risk Management . (2002). *A Risk Management Standard.* Obtenido de https://www.theirm.org/media/886059/ARMS_2002_IRM.pdf

26. Universidad de Alcalá. (s.f.). *Fuentes de Información*. Obtenido de http://www3.uah.es/bibliotecaformacion/BPOL/FUENTESDEINFORMACION/tipos_de_fuentes_de_informacin.html

27. Wikipedia. (30 de Julio de 2002). *Ley de Sarbanes- Oxley*. Obtenido de https://es.wikipedia.org/wiki/Ley_Sarbanes-Oxley

ANEXOS

Anexo 1: Encuesta sobre la cultura de riesgos

COMPAÑÍA ABC
ENCUESTA SOBRE LA CULTURA DE RIESGOS

Nombre del departamento:
Fecha de elaboración:

Objetivo de la encuesta:

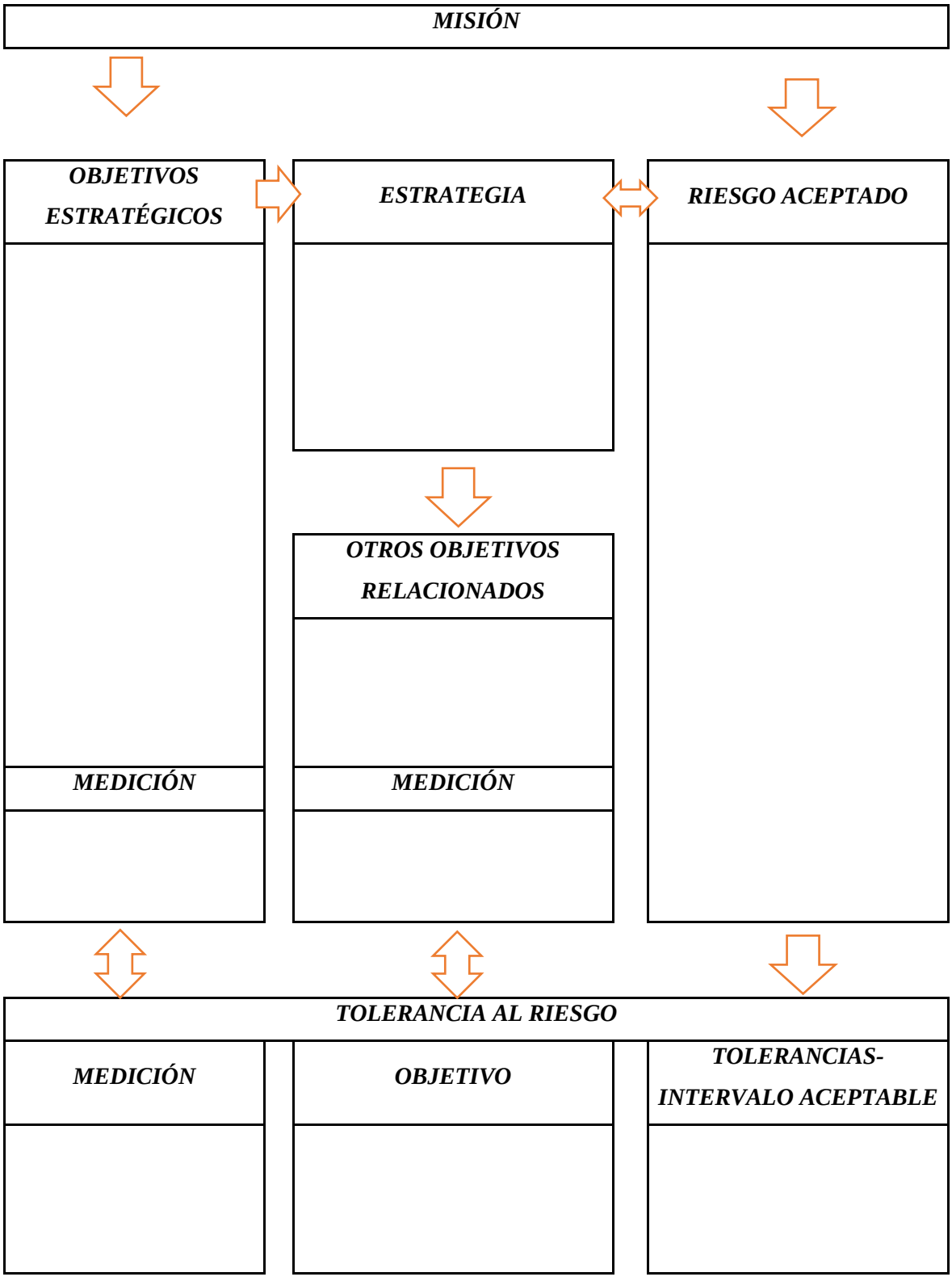
Obtener conocimiento acerca de la cultura de riesgos, para identificar atributos que la compañía debe mejorar para una eficaz implementación de un sistema de gestión de riesgos.

N°	PREGUNTA	ATRIBUTO	CALIFICACIÓN MEDIA		DESV. EST.	CANTIDAD	MD	D	N	A	MA
1	Los líderes de mi unidad siguen positivamente los lineamientos de un comportamiento de conducta ética	Liderazgo y estrategia									
2	Comprendo la misión y estrategia general de la organización.	Liderazgo y estrategia									
3	En mi unidad se llevan a cabo acciones disciplinarias contra aquellos que muestran una conducta profesional inapropiada.	Responsabilidad y motivación									
4	La rotación del personal no afecta a nuestra capacidad de alcanzar los objetivos.	Personas y comunicación									
5	Los líderes de mi unidad de negocio son receptivos a cualquier tipo de comunicación acerca del riesgo, incluyendo noticias negativas.	Gestión de riesgos e infraestructura									

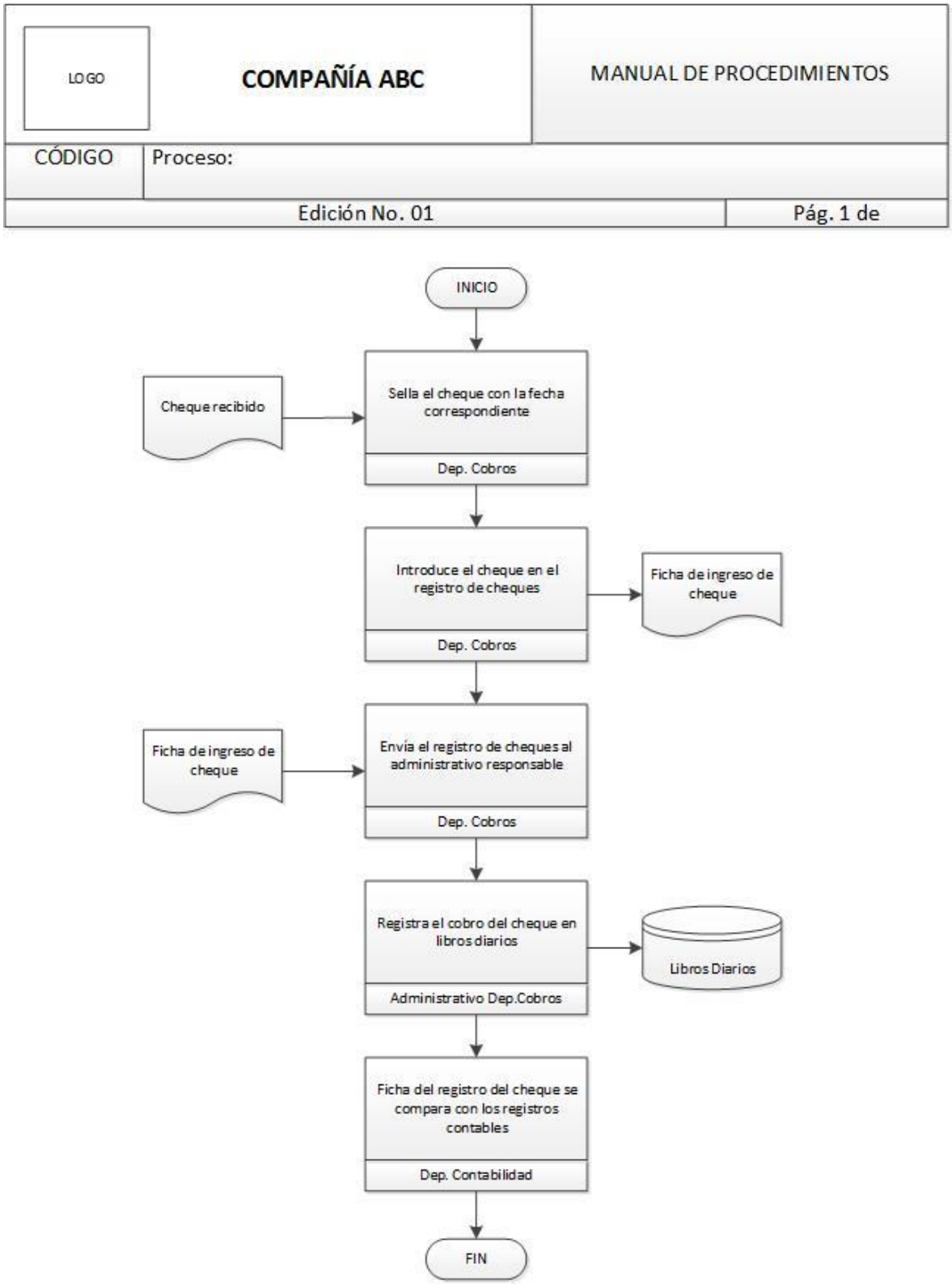
Anexo 2: Estructura de un código de ética o conducta

SECCIONES	CONTENIDOS DE CADA SECCIÓN
1. Carta de la dirección general	- Mensaje de la alta dirección sobre la importancia de la integridad y los valores éticos para la organización. - Código de conducta, su propósito y manera de utilizarlo.
2. Objetivos y filosofía	- Se considera dentro de la organización: Su cultura Su negocio y sector Su ubicación geográfica, tanto nacional como internacionalmente Su compromiso con el liderazgo ético
3. Incompatibilidades	- Aborda las incompatibilidades y las formas de actuar en provecho propio. - Incompatibilidades en relación con el personal y otros agentes corporativos, así como aquellas actividades, inversiones o intereses que podrían afectar a la reputación o integridad de la organización.
4. Regalos y gratificaciones	- Penaliza el empleo de regalos y gratificaciones, estableciendo la propia política de la organización al respecto. - Establece normas y proporciona pautas con respecto a los regalos y gastos de representación, así como su adecuada comunicación.
5. Transparencia	- Incluye disposiciones/normas acerca del compromiso de la empresa con la generación de informes completos y comprensibles sobre impacto económico, social y medioambiental.
6. Recursos corporativos	- Incluye disposiciones/normas acerca de los recursos corporativos, incluyendo la propiedad intelectual y la información de activos propios, a quién pertenecen y cómo se protegen
7. Responsabilidad social	- Incluye el papel de la entidad como parte de la sociedad, incluyendo su compromiso con los derechos humanos, la preservación medioambiental, la implicación en el desarrollo de su comunidad y otras cuestiones económicas.
8. Otras cuestiones relativas a la conducta	- Incluye disposiciones/normas acerca de la fidelidad a las políticas establecidas en áreas específicas de actividad de la empresa, tales como: -Cuestiones relativas al empleo: prácticas laborales justas y lucha contra la discriminación. - Tratos con las autoridades, contrataciones, influencias y actividad política. - Seguridad y calidad del producto. - Prácticas antimonopolio y otras relacionadas con la competencia. - Buena fe y trato justo con clientes, competidores y proveedores. - Confidencialidad y seguridad de la información.

Anexo 3: Matriz de relación entre misión, objetivos, riesgo aceptado y tolerancia al riesgo



Anexo 4: Flujo de actividades de un proceso especifico



Anexo 5: Modelo taller de grupo para identificación de eventos

COMPAÑÍA ABC

TALLER DE GRUPO

Nombre del moderador:

Fecha del taller:

Departamento:

Objetivo o proceso a ser evaluado:

1. Introducción:

Dentro de este punto se debe explicar los antecedentes del taller y los motivos por los cuáles se está realizando el mismo. A su vez se deben explicar las normas básicas que se tomarán a consideración dentro del desarrollo del taller.

2. Procedimientos:

- Partiendo desde el flujo de actividades previamente realizado, elaborar una lista con todas las tareas primordiales dentro del proceso seleccionado para evaluación.
- Para cada una de las tareas listadas, se estimulará a los participantes a que se discutan acontecimientos que puedan surgir y se elaborará un cuadro comparativo.

Tareas	Posibles acontecimientos
5.	5.
6.	6.
7.	7.
8.	8.

- Para cada posible acontecimiento se determinará si representa una oportunidad o un riesgo para la entidad o para el departamento.
- Si se determinó que el acontecimiento puede representar un riesgo para la compañía, de deberá determinar y llegar a un consenso sobre el nivel de riesgo aceptado y su respectiva tolerancia al riesgo.
- Considerar de qué modo se relacionan entre sí los riesgos encontrados y en medida afectan a los objetivos planteados.

3. Cierre:

Obtener los resultados del taller y distribuir a los responsables de cada unidad para poder preparar un plan de respuesta para los siguientes pasos del componente.

Anexo 6: Formato Mapa de Calor

COMPAÑÍA ABC

MAPA DE CALOR

(1) PROCESO	(2) OBJETIVO	(3) ACTIVIDADES	(4) FACTORES DE RIESGO	(5) ORIGEN DEL RIESGO	(6) POTENCIAL CONSECUENCIA	(7) IMPACTO	(8) PROBABILIDAD DE OCURRENCIA	(9) NIVEL DE RIESGO INHERENTE (A)	(10) CONTROL DE RIESGO	(11) EFECTIVIDAD (B)	(12) OBSERVACIONES

Anexo 7: Política de determinación de impacto y probabilidad de ocurrencia de riesgos

COMPAÑÍA ABC

POLÍTICA DE DETERMINACIÓN DE IMPACTO Y PROBABILIDAD DE OCURRENCIA DE RIESGOS

Impacto:

Al impacto que puede tener un riesgo dentro de la organización se lo considerará dentro de los siguientes rangos o niveles:

- Insignificante: aquel riesgo de impacto no percibido por la organización dando como resultado consecuencias muy bajas.
- Bajo: riesgo de impacto mínimo, donde sus consecuencias amenazarían un elemento de una función.
- Medio: riesgo de impacto moderado, sus consecuencias requieren ajustes significativos.
- Alto: riesgo de impacto importante, sus consecuencias amenazarían objetivos funcionales.
- Muy Alto: riesgo de impacto grave, sus consecuencias impiden el logro de objetivos funcionales.

Probabilidad de ocurrencia:

La probabilidad de ocurrencia de un riesgo deberá ser ubicada dentro de los siguientes cinco niveles:

- Insignificante: riesgo que no es probable que ocurra en un tiempo determinado.
- Bajo: riesgo improbable o con una mínima probabilidad de que ocurra.
- Medio: riesgo posible, probable de que ocurra.
- Alto: riesgo muy probable de que ocurra.
- Muy Alto: riesgo seguro y casi un hecho de que ocurra.

Anexo 8: Tabla de nivel de riesgo inherente

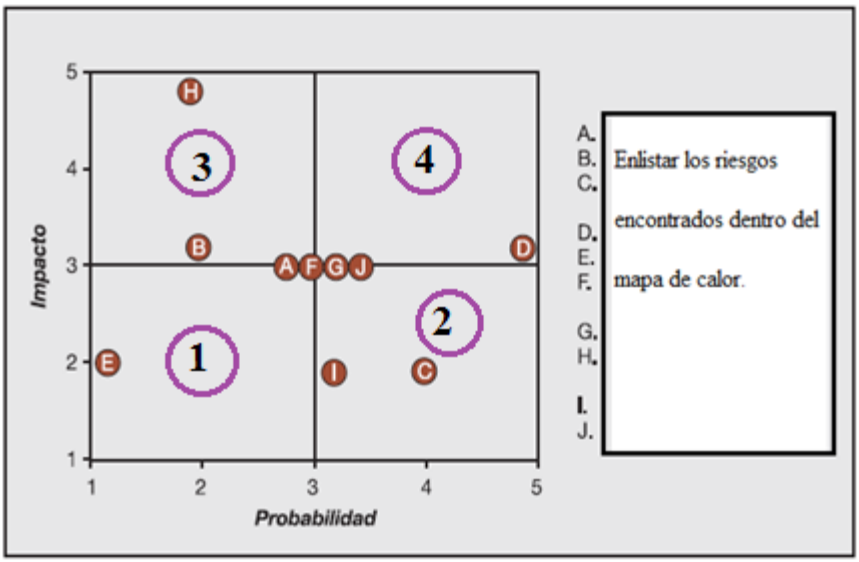
Impacto						
	MUY ALTO	5	10	15	20	25
	ALTO	4	8	12	16	20
	MEDIO	3	6	9	12	15
	BAJO	2	4	6	8	10
	INSIGNIFICANTE	1	2	3	4	5
		INSIGNIFICANTE	BAJO	MEDIO	ALTO	MUY ALTO

Frecuencia o Probabilidad de ocurrencia

Anexo 9: Tabla de efectividad de control interno

CONTROL	EFECTIVIDAD
Ninguno	1
Bajo	2
Medio	3
Alto	4
Destacado	5

Anexo 10: Mapa de riesgo matricial



Anexo 11: Formato de respuesta al riesgo y su comparación incluyendo costo y beneficio

COMPAÑÍA ABC

COMPARACIÓN COSTO/BENEFICIO DE RESPUESTAS AL RIESGO

(1) PROCESO	(2) OBJETIVO	(3) ACTIVIDADES	(4) FACTORES DE RIESGO	(5) RESPUESTA AL RIESGO	(6) COSTO	(7) DESCRIPCIÓN DE LA RESPUESTA AL RIESGO	(8) BENEFICIOS	(9) OBSERVACIONES

Anexo 12: Política de respuesta a los riesgos

COMPAÑÍA ABC

POLÍTICA DE RESPUESTA A LOS RIESGOS

Realizado por:

Departamento:

1. Introducción:

- El Comité de Riesgos será el encargado de realizar la evaluación de las respuestas a los riesgos.
- Determinar los objetivos que se esperan cumplir al desarrollar esta actividad.
- Determinar el alcance que tendrá el taller.
- Informar a todos los especialistas participantes los pasos a seguir.

2. Desarrollo:

- Identificación y clasificación de los riesgos encontrados para cada actividad.
- Analizar las posibles respuestas a cada uno de los riesgos considerando lo siguiente:
  - ✓ Puntos críticos de control
  - ✓ Causas de los riesgos
  - ✓ Límites de control
- Determinar si cada una de las alternativas de respuesta al riesgo se alinea con el riesgo previamente aceptado y la tolerancia al riesgo correspondiente.
- Detallar cada una de las alternativas de respuesta en el cuadro de comparación.

3. Cierre:

- Obtener conclusiones acerca de lo elaborado.
- Realizar un informe de actividades del comité de riesgos.
- Informar los resultados a los directivos de la organización.

Anexo 13: Política de actividades de control

COMPAÑÍA ABC

POLÍTICA DE ACTIVIDADES DE CONTROL

Realizado por:

Departamento:

Dentro de la política de actividades de control se detallan las actividades que deberán realizarse para controlar que los riesgos identificados y sus respectivas respuestas se estén llevando a cabo según lo establecido por el comité de riesgos.

- Revisiones por parte de la alta dirección; en donde se examinan datos reales de la organización según los presupuestos mantenidos, datos históricos y se realiza la supervisión de las actividades propuestas como nuevas.
- Revisión de informes de rendimiento.
- Reprocesamiento de información y revisión de sistemas de información contable, en donde se revise la exactitud, claridad y oportunidad de la información que arrojan los sistemas utilizados y las transacciones correspondientes.
- Controles físicos, en donde se comparen las existencias físicas reales de inventarios, equipos, maquinaria, entre otros con lo registrado en los sistemas de información.
- Supervisión de indicadores de rendimiento.
- Segregación de funciones, para reducir el riesgo de error y fraude.
- Aseguramiento del cumplimiento de leyes y normas legales impuestas por organismos de control.
- Revisión de autorizaciones para realizar actividades y transacciones.

Anexo 14: Política de comunicación

COMPAÑÍA ABC

POLÍTICAS DE COMUNICACIÓN DE LA CULTURA DE RIESGOS

1. Filosofía de gestión de riesgos

- La dirección comentará los riesgos y las respuestas al riesgo asociadas en reuniones informativas con los empleados de manera periódica.
- Las políticas, estándares y procedimientos de gestión de riesgos se facilitan a los empleados junto con declaraciones firmes de su cumplimiento.
- Las capacitaciones para nuevos empleados incluyen información y documentación sobre la filosofía de gestión de riesgos de la empresa y su programa de gestión de riesgos.
- Los empleados que desempeñen cargos antiguos son obligados asistir a capacitaciones sobre iniciativas de gestión de riesgos.
- La nueva filosofía de gestión de riesgos es reforzada a través de programas continuos de comunicación interna y externa.

2. Tipo de comunicación a ser utilizada

- Correos electrónicos
- Correos de voz
- Boletines corporativos
- Bases de datos
- Páginas de intranet donde se muestra información de interés
- Comunicaciones corporativas continuas
- Conferencias
- Carteles, letreros
- Capacitaciones
- Foros abiertos

3. Uso del internet para la comunicación de gestión de riesgos

- Foros de discusión
- Políticas y procedimientos ubicados en la intranet de la empresa
- Preguntas más frecuentes
- Informes de gestión de riesgos y actividades relevantes
- Enlaces en sitios web a políticas y procesos claves
- Listado de información de contacto de los responsables y personal de apoyo del programa de gestión de riesgos

Anexo 15: Evaluación del sistema de gestión de riesgos de forma independiente

COMPAÑÍA ABC

EVALUACIÓN INDEPENDIENTE DEL SISTEMA DE GESTIÓN DE RIESGOS

Realizado por:

Departamento:

1. Planificación:

- Definir los objetivos y alcance de la evaluación
- Identificar el responsable de la evaluación
- Determinar el equipo con el que se contará para la evaluación
- Definir metodologías y los pasos a seguir para la evaluación

2. Ejecución:

- Obtener conocimiento de las actividades de la unidad de negocio o departamento
- Comprender el proceso del sistema de gestión de riesgos
- Aplicar la metodología acordada para la evaluación
- Analizar resultados
- Documentar problemas encontrados y las soluciones según el caso
- Informar sobre los resultados encontrados a quien corresponda

3. Informes y plan de acción:

- Comentar los resultados con la dirección general y la de negocio
- Determinar planes de acción adecuados
- Incorporar retroalimentación de la dirección al informe final de la evaluación

Anexo 16: Política de monitoreo del departamento de auditoria interna

COMPAÑÍA ABC

POLÍTICA DE MONITOREO DEL DEPARTAMENTO DE AUDITORIA INTERNA

Realizado por:

Actividades antes de revisar el sistema de gestión de riesgos:

1. Investigar y revisar desarrollos, tendencias e información actualizada del entorno organizacional de la compañía.

2. Revisar las políticas corporativas, informes de la administración para determinar estrategias de negocio.

3. Revisar informes realizados previamente de evaluación de riesgos.

Actividades durante la revisión el sistema de gestión de riesgos:

1. Entrevistar a la gerencia general y por departamentos para conocer los objetivos del negocio

2. Revisar información para dar una opinión independiente acerca del proceso de evaluación de riesgos.

3. Revisar la oportunidad e integridad de la información obtenida.

4. Determinar la eficacia de los procesos de evaluación y gestión de riesgos implementado.

Actividades para finalizar la revisión del sistema y prevenir riesgos de fallos de control:

1. Crear un programa de aseguramiento y mejora de la calidad.

2. Análisis en determinados períodos de la metodología y plan sostenido para realizar las auditorias.

3. Realizar una planificación de auditoria efectiva.

4. Diseño de una auditoria efectiva.

5. Revisiones constantes de informes de riesgos y gestión de riesgos emitidos.

6. Asignación de recursos apropiados para realizar las revisiones.