PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE CIENCIAS ADMINISTRATIVAS Y CONTABLES

SISTEMA DE GESTIÓN DE RIESGOS EN UNA EMPRESA MULTINACIONAL COMERCIALIZADORA DE PRODUCTOS FARMACÉUTICOS UBICADA EN QUITO

TRABAJO DE TITULACIÓN DE GRADO PREVIA LA OBTENCIÓN DEL TÍTULO DE INGENIERÍA EN CONTABILIDAD Y AUDITORÍA CPA

LEONARDO RAMIRO BAJAÑA MOLINA

DIRECTOR: ING. WILSON SILVA

QUITO, DICIEMBRE 2014

DIRECTOR DE TRABAJO DE TITULACIÓN: ING. WILSON SILVA

LECTOR 1: ING. NANCY PÉREZ

LECTOR 2: ING. VÍCTOR RUIZ

AGRADECIMIENTOS Y DEDICATORIA

Un agradecimiento especial al Ing. Wilson Silva - Director del Trabajo de Titulación y Experto Senior en Auditoría Interna y Externa por su valioso apoyo y guía para el desarrollo de este trabajo, Ing. Víctor Ruíz – Lector del Trabajo de Titulación y Experto Senior en Auditoría Interna y Externa, Ing. Nancy Pérez – Lectora del Trabajo de Titulación y Experta Senior en Auditoría Interna y Externa. A MM S.A. por incluir dentro de sus controles algunas de las herramientas mencionadas en este trabajo, especialmente al Director Financiero y al Contralor de la compañía mencionada quienes apoyaron esta iniciativa en un 100% siempre con apertura para escuchar y considerar nuevas prácticas que se utilizan en el mercado internacional.

Dedico este trabajo a mi esposa y a mi hija por su gran soporte y comprensión, siempre han sido mi inspiración para seguir adelante en la vida y para no rendirme nunca a pesar de las largas jornadas laborales y de estudio. A mis padres que siempre estuvieron apoyándome durante todo este tiempo, a mis amigos y conocidos que de cierta manera formaron parte de la investigación.

ÍNDICE

RESUMEN EJECUTIVO

El tema tratado en este trabajo surge de una necesidad importante que en el Ecuador se ha tornado cada vez más evidente y clave para el éxito en las organizaciones. Sus conceptos son simples y básicos de los fundamentos administrativos y se fusionan de manera trascendental con los procesos financieros y no financieros, es decir, funcionan de manera horizontal en toda la organización y necesitan de toda su participación. Esto es la Gestión de Riesgos Corporativos (ERM por sus siglas en inglés) como un elemento de control indispensable para el cumplimiento de los objetivos organizacionales.

El contenido de este trabajo está basado en el libro Enterprise Risk Management Integrated Framework (denominado COSO II), elaborado por The Committee of Sponsoring Organizations of the Treadway Commission en el año 2004 y que abarca los puntos principales que deberían ser manejados en una organización para administrar y reducir los riesgos corporativos de manera correcta con el fin de mejorar sus procesos y lograr la consecución de sus objetivos en general. Este documento no intenta describir todas las técnicas o estrategias existentes en la materia, sino dar a conocer una guía práctica para la implementación del sistema basado en fundamentos teóricos de gran reconocimiento a nivel mundial.

A lo largo del desarrollo se realiza una revisión superficial del Marco Integrado para el Control Interno que fue el primer documento emitido por COSO en el año 1992, el Marco Integrado para la Gestión de Riesgos Empresariales, los conceptos principales del GRC y algunas prácticas que según COSO se han utilizado en algunas empresas en el mundo para la administración de riesgos. Adicionalmente, se mencionan aspectos principales del funcionamiento de MM S.A., compañía que es el objeto de investigación.

El núcleo del presente documento está compuesto por el capítulo II y III en donde se realiza un análisis comparativo de los pasos y componentes que menciona el COSO II para la implementación de un Sistema de Gestión de Riesgos integral para los procesos de MM S.A de manera general. Además, se proponen acciones en base a las condiciones actuales de la compañía para la aplicación del sistema de manera práctica y que genere eficiencias en las condiciones actuales del negocio.

Finalmente el capítulo IV hace un compendio de todos los aspectos revisados en los capítulo II y III, se mencionan algunas conclusiones de lo aprendido durante el estudio de la materia teórica del trabajo y se realizan recomendaciones para la aplicación general del Sistema de Gestión de Riesgos propuesto por COSO en la vida cotidiana de la empresa multinacional MM S.A.

INTRODUCCIÓN

La vida, tanto de los seres humanos como de las organizaciones, presenta a lo largo de su existencia varios riesgos y oportunidades de diferentes tipos, fuentes, magnitudes, naturalezas, propósitos, impactos, etc. Para optar por el camino más conveniente, es necesario tomar decisiones acertadas que permitan mitigar riesgos y aprovechar oportunidades con el fin de acercarnos más al éxito; este hecho diferencia a un ser humano de otro y a una organización de otra.

El riesgo es una constante de la vida, dependerá de la estrategia y habilidad de cada ente para transformarlo en un reto con el fin de obtener los resultados deseados. Sin embargo, la cuestión que surge de este planteamiento es el **¿cómo?,** y es ahí donde inicia el tratamiento del tema propuesto en este trabajo de titulación de grado para la carrera de Ingeniería en Contabilidad y Auditoría CPA de la Facultad de Ciencias Administrativas y Contables de la Pontificia Universidad Católica del Ecuador.

Retomando la cuestión del anterior párrafo, el ¿cómo?, estará definido por la metodología que utilizará la organización para administrar sus riesgos y mitigarlos de manera que su ocurrencia tenga la menor afectación en su vida y primordialmente, para que todas las estrategias direccionen a la misma hacia el alcance de los objetivos organizacionales propuestos.

La empresa farmacéutica multinacional MM S.A. con domicilio en la ciudad de Quito será el objeto de investigación del presente trabajo. Su actividad principal es la importación y comercialización al por mayor de productos farmacéuticos en muchas especialidades como ya se mostrará más adelante.

La organización con sucursal en Ecuador no presenta un sistema integral para administración de riesgos como se muestra en el contenido de este trabajo. Esto implica que de cierta manera, la identificación de debilidades, riesgos e impactos podría no estar correctamente estructurada, lo que en ocasiones conlleva a las organizaciones a (Marco Internacional para la Práctica Profesional de la Auditoría Interna, 2012: 127):

- Falta de lineamiento de los objetivos organizacionales con la misión de la organización.

- Carencia de evaluación de los riesgos

- Dificultad en el establecimiento de controles que mitiguen los riesgos adecuadamente

- Procesos sin indicadores de gestión y no alineados con los objetivos corporativos

- Escaso conocimiento del impacto que ocasionan los riesgos en cada proceso

- Poco conocimiento de los niveles aceptables de los riesgos en la organización

- Otras consecuencias relacionadas con la operación del negocio

En base a estos antecedentes, la corporación tiene la necesidad de implementar un sistema de gestión de riesgos para evaluar cada proceso e identificar posibles brechas de control interno que no se estén considerando; de esta manera, mantener un proceso de mejoramiento que agregue valor a la operación.

La importancia primordial de este documento dentro de la organización es buscar maneras más eficientes de trabajo, con procesos de calidad que brinden seguridad al negocio y se ubiquen dentro de los estándares administrativos más altos del medio. Por la experiencia obtenida en esta investigación, se podría decir que el nivel profesional de los empleados de MM S.A. es bastante alto, lo que implica una excelente predisposición para el cambio positivo y apoyo en la implementación que se piensan realizar con esta investigación.

La organización busca gestionar de mejor manera sus actividades para generar más recursos, armonizar sus procesos y objetivos, eliminar las ineficiencias, controlar sus riesgos, establecer políticas y lineamientos que lleven los resultados a la consecución de su misión y visión organizacional, en fin, establecer un sistema de mejora continua en base al análisis de los riesgos y lo que esto conlleva para todas sus áreas.

El contenido que se mostrará en la investigación tiene fines estrictamente académicos y sus datos han sido cambiados para preservar la identidad de la organización, sin que esto afecte a la objetividad del desarrollo e implementación del Sistema de Gestión de Riesgos.

Cabe recalcar que la metodología propuesta se fundamenta en aspectos teóricos de gran relevancia a nivel mundial en la actualidad, desarrollados por organizaciones emisoras de estándares de control con certificación y reconocimiento internacional.

A continuación se detallarán todos los puntos principales que una organización debe considerar para la implementación de un Sistema de Gestión de Riesgos y se hará hincapié en las condiciones que mantiene al momento la empresa MM S.A. con las recomendaciones respectivas para que este sistema pueda funcionar bajo su estructura y de manera general en la industria farmacéutica.

1. CAPÍTULO I : MM S.A, FUNDAMENTOS PRINCIPALES DEL COSO I Y II Y GRC

1.1 MM S.A.

MM S.A. es una compañía multinacional dedicada al desarrollo, investigación, fabricación y comercialización de productos farmacéuticos. Su matriz se encuentra establecida en los Estados Unidos y tiene sucursales en aproximadamente 40 países alrededor del mundo incluyendo Ecuador. De la misma manera tiene centralizadas sus actividades principales de investigación, fabricación, distribución y otras operativas para reducir costos y estandarizar prácticas.

La compañía empezó sus actividades farmacéuticas en 1851 y llegó al Ecuador en el año 1973. A partir de este año su estructura ha ido cambiando con el tiempo de manera considerable y en la actualidad tiene una sola sucursal en Ecuador ubicada en la ciudad de Quito. Sin embargo, los productos de MM S.A. son vendidos a todas las regiones del país y son promocionados por representantes médicos de la compañía, actividad que es considerada el motor de las ventas de la organización.

Los clientes principales de la compañía son distribuidores dueños de las más grandes cadenas de farmacias del país, como Fybeca, Sana Sana, Pharmacys, Cruz Azul,

Económicas, entre otras que generan aproximadamente el 75% de las ventas de la empresa. Por otro lado se encuentran las instituciones gubernamentales que de manera general se interesan por productos estratégicos del país y para los cuáles las empresas multinacionales han desarrollado medicamentos para combatir enfermedades crónicas y de impactos fuertes en los pacientes. Estos productos son vendidos a las instituciones a través de adjudicaciones y ofertas públicas y de manera general se enfocan en áreas oncológicas, vacunas, salud femenina, diabetes, entre otros.

Las principales áreas de enfoque de vacunas, medicamentos y productos de consumo en los que se enfoca MM S.A. son: Salud humana, anticoncepción, anestesia, cardiología, dermatología, diabetes, dolor, endocrinología, enfermedades infecciosas, enfermedades respiratorias, fertilidad, hipertensión arterial, inmunología, oftalmología, oncología, osteoporosis, menopausia, neurociencias, reumatología y virología.

Debido al tamaño y áreas de enfoque de la organización, MM S.A. ha dividido sus operaciones en diferentes departamentos y estructuras entre las cuales se encuentran: Área comercial compuesta por unidades de negocio respiratoria, cuidado primario, cardiología, especialidades, vacunas y salud femenina todas estas para ventas y marketing, servicios de soporte, eventos, compliance, planificación de demanda, entre otras. Existen otras áreas de soporte al negocio, distribución e investigación que son: Gerencia general, dirección médica, asuntos legales, finanzas, compras, recursos humanos, sistemas informáticos, facilidades, logística, calidad, pruebas clínicas, asuntos regulatorios, seguridad salud y ambiente, entre otras.

Por otro lado, estas áreas están interconectadas por procesos que fluyen por toda la organización a través de sus actividades operativas que son: Order to Cash que se compone de las operaciones para las ventas, PtP que se refiere a compras no inventariables, Payroll relacionado a los procesos de nómina, Inventory en relación al manejo y costeo de los inventarios, Meals and Entertainment que trata sobre los reportes de gastos de viaje y gestión de los empleados y otros.

MM S.A. es la empresa para la cual se ha diseñado la propuesta y diagnóstico de los puntos relacionados a la Gestión de Riesgos Empresariales en base a los fundamentos teóricos de dos marcos que se han emitido por The Committee of Sponsoring Organizations of the Treadway Commission que se detalla más adelante, enfocándose primordialmente en el Enterprise Risk Management Integrated Framework.

La misión de MM S.A. es:

> Brindar productos y servicios innovadores y diferenciados que salven y mejoren vidas, y que satisfagan las necesidades de nuestros clientes, ser reconocidos como un excelente lugar para trabajar, y darles a nuestros inversionistas una tasa de rendimientos superior (MM S.A., 2014).

La visión de MM S.A. es:

> Hacemos una diferencia en la vida de las personas en todo el mundo, a través de nuestros medicamentos innovadores, vacunas y productos para el cuidado de la salud del consumidor y de la salud animal. Aspiramos a ser la mejor compañía en el cuidado de la salud en el mundo y estamos dedicados a brindar innovaciones y soluciones de primer nivel para el futuro (MM S.A., 2014).

A continuación los aspectos principales de los marcos mencionados.

1.2 MARCO INTEGRADO DE CONTROL INTERNO SEGÚN C.O.S.O & MARCO INTEGRADO PARA LA GESTIÓN DE RIESGOS EMPRESARIALES

C.O.S.O. (Committee of Sponsoring Organizations of the Treadway Commission por sus siglas en inglés), es un comité conformado por las siguientes entidades: American Institute of Certified Public Accountants (AICPA), American Accounting Association (AAA), The Institute of Internal Auditors (IIA), Institute of Management Accountants (IMA) y el Financial Executives International (FEI). Este comité ha emitido varios informes acerca del control interno, guías prácticas y otros documentos fundamentales para la actividad de auditoría interna y administración de riesgos.

El documento más importante emitido por C.O.S.O es el Internal Control - Integrated Framework en el año 1992, al cual también se lo denomina COSO I. Este describe un marco integrado de las actividades de control interno en las corporaciones proponiendo algunas prácticas e importantes consejos para la salud organizacional adoptadas por entidades muy importantes alrededor del mundo como el Banco Mundial, el BID y muchas organizaciones del sector público y privado de los Estados Unidos. De esta manera, se fue propagando por todo el mundo y especialmente por Latinoamérica. Sin embargo, durante los próximos años ocurren una serie de acontecimientos en todo el mundo relacionados a riesgos empresariales los que generaron una necesidad en las corporaciones y empresas a nivel global para un mejor manejo y administración de riesgos. Es por este motivo que más adelante, C.O.S.O emite el ERM Integrated Framework (Enterprise Risk Management Integrated

Framework) conocido también como COSO II en el año 2004, que define la Gestión de Riesgos Empresariales como sigue:

> Un proceso ejecutado por el consejo directivo, la administración y otro personal de una entidad, aplicado en el establecimiento de estrategias en toda la empresa, designado para identificar eventos potenciales que pudieran afectar a la entidad, y administrar los riesgos para mantenerlos dentro de su propensión al riesgo para proporcionar seguridad razonable referente al logro de objetivos de la entidad". (MacLeod, y otros, 2012, pág. 4), basado en la definición dada por The Committee of Sponsoring Organizations of the Treadway Commission.

1.2.1 Marco Integrado de Control Interno

A pesar de que el Control Interno (C.I.) no es el objetivo principal de este trabajo, es muy relevante abarcarlo suficientemente para introducir el enfoque del texto: COSO II (Enterprise Risk Management Integrated Framework) y otros conceptos de control interno.

El Internal Control - Integrated Framework es un marco que tiene como propósito ayudar a la administración de una organización a mejorar sus mecanismos de control, así como también proveer a la directiva de una perspectiva de C.I. necesaria para el cumplimiento de objetivos operacionales y financieros. A su vez, apoya a una organización en el cumplimiento de leyes y regulaciones que permiten a la misma lidiar eficientemente con los cambios económicos y competitivos del mercado; así como también, acceso a mejores maneras de liderazgo, concentrando los esfuerzos en actividades prioritarias y desarrollando nuevos modelos de negocio.

Como parte de este trabajo se hará una pequeño resumen de todos los componentes principales del COSO I con un estudio más específico en la administración de riesgos corporativos que será la base para el Capítulo II y III, fundamentado en tres componentes del COSO II.

El COSO I tiene como uno de sus propósitos "Proveer claridad en control interno usando una definición común e integrando varios conceptos de control interno en un marco que define los componentes del control interno" (Committee of Sponsoring Organizations of the Treadway Commission, 2011, pág. 1)

Para entender adecuadamente esta sección del trabajo es necesario definir en una primera instancia lo que es Control Interno. El C.I. se ubica dentro de todos los niveles de la organización y en ocasiones podría pasar desapercibido. Dentro del texto antes mencionado se define al C.I. como:

> Un proceso que es efectuado por Directores, Gerentes y otro Personal de la compañía. Su finalidad básicamente es asegurar, a través de varias actividades, que todos los procesos de la compañía cumplan con los objetivos propuestos, principalmente en los siguientes puntos: (Committee of Sponsoring Organizations of the Treadway Commission, 2011, pág. 13):
>
> - Efectividad y eficiencia de las operaciones.
> - Confiabilidad de los reportes.
> - Cumplimiento de las leyes aplicables y regulaciones.

De esta manera el C.I. es un compendio de cinco puntos principales que son: los procesos, la gente que maneja esos procesos y establece los controles, la seguridad razonable que proporciona el control interno, la orientación del control

interno al cumplimiento de objetivos y su capacidad de adaptación a cualquier estructura de una organización.

A continuación se analizarán uno por uno cada uno de los aspectos antes mencionados para entender mejor el propósito y existencia del control interno.

El control interno (C.I.) es un **proceso** constante y reiterativo que se encuentra o debería encontrarse dentro de todas las actividades operativas y no operativas de una compañía. Además, en muchas de las ocasiones el C.I. es inherente a la manera en la que una directiva maneja una organización. Ahora bien, los procesos de una compañía no son nada más que el reflejo de sus políticas y procedimientos. "Las políticas reflejan lo que la Directiva de una organización establece como acciones permitidas y no permitidas, mientras que los procedimientos reflejan los actos a través de los cuáles las políticas son implementadas" (Committee of Sponsoring Organizations of the Treadway Commission, 2012, pág. 3).

Los procesos de organizaciones grandes pasan a través de varias áreas de manera horizontal y están sujetos a las actividades de planeación, ejecución y monitoreo. El C.I. básicamente está compuesto por estas tres actividades y debe llevarse a cabo a través de las arterias de toda la compañía, de manera horizontal y a través de las actividades más importantes de la misma, de manera que tenga un efecto positivo en la consecución de los objetivos empresariales.

Por otro lado, el C.I. es llevado a cabo por parte del **consejo de administración, la gerencia y otro personal** a través de las distintas actividades que la compañía establece para el alcance de objetivos específicos y que a su vez llevarán al cumplimiento de objetivos generales. Asimismo, la función de la directiva de una compañía es de gran importancia para el C.I. ya que debe dirigir las acciones de la gerencia y auspiciar la aprobación de políticas y procedimientos, cada nivel gerencial o jerárquico debe contar con un nivel adecuado de aprobación o autoridad (Committee of Sponsoring Organizations of the Treadway Commission, 2012).

En cuanto a la **seguridad razonable** es importante recalcar que el C.I. no puede asegurar el cumplimiento de los objetivos. Siempre existen factores que no pueden ser controlados en su totalidad dentro de las actividades de una compañía, como son los riesgos inherentes, errores humanos, factores externos o los actos fraudulentos por parte de los integrantes de una organización. Por lo tanto, no se puede hablar de una seguridad absoluta y es preciso crear flexibilidad en los procesos para situaciones cambiantes, tanto en el medio como dentro de la misma organización. Debido a los factores antes mencionados es posible que un sistema de control interno no cumpla con su objetivo, por lo que es vital para una compañía que sea revisado constantemente.

El control interno se **adapta** a una organización en todos sus niveles, puede ser aplicado basado en las decisiones gerenciales, requerimientos legales y regulatorios y de acuerdo al modelo operativo de una organización.

Como último elemento del control interno, se presenta la capacidad del mismo para contribuir al **cumplimiento de objetivos.** Existen tres tipos de objetivos para los cuales el C.I. se enfoca principalmente (Committee of Sponsoring Organizations of the Treadway Commission, 2012, pág. 2):

- **Objetivos Operativos:** Referido a las operaciones de la entidad, las metas financieras y a la protección de los activos vs las ganancias.

- **Objetivos de Reportaje:** Mismos que se refieren a la manera en que la compañía reporta sus cifras y condición tanto externa como internamente, de manera transparente y en tiempo, conforme a sus obligaciones corporativas.

- **Objetivos de Cumplimiento (Compliance):** Enfocados en el cumplimiento de regulaciones y leyes del entorno en el que una entidad se desenvuelve.

Un objetivo puede pertenecer a más de una de las tres categorías y puede ser llevado a cabo bajo la responsabilidad de distintos departamentos y personas. El cumplimiento de los objetivos antes mencionados dependerá en gran parte de cómo una empresa lleva su control interno. Cuando una compañía se maneja en base a estándares externos puede presentar una seguridad razonable acerca del cumplimiento efectivo de sus objetivos operacionales. Sin embargo, el control

interno no puede asegurar que las decisiones u otros factores externos afecten el cumplimiento de objetivos; simplemente es una herramienta que permite minimizar riesgos y apoyar a las operaciones a que cumplan con su propósito.

Una vez analizado el propósito y significado del control interno es posible ver más a fondo cómo se establecen los objetivos, los componentes del control interno y sus principios.

El COSO I propone los siguientes componentes como indispensables para un buen manejo del C.I. (Committee of Sponsoring Organizations of the Treadway Commission, 2012, pág. 5):

a) Ambiente de Control

b) Administración del Riesgo

c) Actividades de Control

d) Información y Comunicación

e) Monitoreo

Estos componentes son de gran importancia para toda la estructura de la compañía, sucursales y cualquiera de sus unidades operativas. Es decir, sus conceptos se pueden adaptar y estandarizar para diferentes tamaños estructurales.

Asimismo, los objetivos de una organización tienen una relación estrecha con los componentes de control interno y las operaciones de una entidad; ésta puede ser representada por la siguiente **Figura 1.1** ((tomado del Internal Control Integrated Framework (Committee of Sponsoring Organizations of the Treadway Commission, 2012, pág. 5)):

Figura 1.1: Cubo de Componentes del COSO I

Sin embargo, como se verá más adelante el Enterprise Risk Management Integrated Framework (COSO II) detalla 8 componentes. Esto no quiere decir de ninguna manera que estos 8 componentes reemplazan a los 5 del COSO I; es

preciso tomar en cuenta que el COSO II se enfoca más en riesgos, sin embargo, en algunos componentes se guarda una evidente similitud.

En la **Figura 1.1** se puede observar el cubo que propone el Internal Control Integrated Framework (COSO I) en donde los componentes se encuentran de manera horizontal como filas (5 componentes), los diferentes objetivos se encuentran en la cara superior del cubo (Operaciones, Reportaje y Cumplimiento) y la estructura de la organización es representada por las columnas verticales que se encuentran en la cara derecha del cubo (Entidad Global, Divisiones o Subsidiarias, Unidades Operativas y Funciones).

Los componentes del C.I. están interrelacionados entre sí, por lo que es importante que cada uno sea considerado dentro del sistema de control interno en una organización.

Además, es muy relevante mencionar que a pesar de que el control interno es realizado de manera estándar y global en todas las empresas grandes del mundo, siempre va a diferir en su manera de aplicación para cada entidad. Esto se debe a que dependiendo del giro del negocio y tipo de industria de una organización, sus procesos, políticas y procedimientos serán diferentes. Por este motivo se dice que nunca podrán existir dos entidades que compartan un mismo sistema de C.I., tampoco deberían.

Esta es la parte más interesante del control interno; se trata de creatividad, de pro actividad, de comunicación, de simplificación, en fin es un sistema libre y objetivo alineado con todos los procedimientos corporativos y si se lo lleva correctamente es un aliado fidedigno clave para el cumplimiento de objetivos empresariales.

Antes de revisar los 8 componentes de la Gestión de Riesgos Empresariales (ERM), es importante ahondar el conocimiento de cada una de las categorías de objetivos.

Los objetivos en las organizaciones son establecidos por la gerencia. El equipo de control interno debe estar al tanto de los mismos para determinar si los procedimientos son los adecuados para asegurar de manera razonable su cumplimiento y a su vez identificar niveles de riesgo que podrían disminuir la capacidad de la organización para cumplir estos objetivos.

De manera más específica los objetivos principalmente se dividen en tres categorías como se había mencionado anteriormente (Committee of Sponsoring Organizations of the Treadway Commission, 2012):

- **Objetivos Operativos:** Estos objetivos básicamente se enfocan en el cumplimiento de la misión y visión de la compañía, son muy básicos y

están directamente relacionados con el giro del negocio de la organización.

Deben estar enfocados principalmente en el mejoramiento de indicadores financieros, productividad, calidad, prácticas medioambientales, innovación y a la satisfacción de los clientes y empleados. Todo dependerá de la actividad principal que realiza la compañía.

Por otro lado, varios de los objetivos de una empresa deben estar alineados con las regulaciones legales del país, así como también con las políticas y procedimientos corporativos.

- **Objetivos de Reportaje:** Estos se refieren a la entrega de reportes financieros y no financieros, internos y externos de la organización dirigidos a los interesados de la compañía.

Los **Objetivos Financieros de Reportaje Externo** se refieren primordialmente a la necesidad que tiene una organización para entregar información fidedigna que será utilizada por ciertas partes interesadas como los stakeholders, el mercado de capitales, bancos, proveedores, clientes en general y el gobierno. El cumplimiento de estos objetivos permitirá a la empresa consolidar sus negociaciones de manera

fundamental para su supervivencia como negocio. Por ejemplo, en el Ecuador la presentación de estados financieros a la Superintendencia de Compañías es de suma importancia para que una sociedad pueda justificar su existencia y funcionamiento, así como también asegurar que está en concordancia con el cumplimiento de las regulaciones legales para el país.

Por otro lado, los **Objetivos no Financieros de Reportaje Externo** se refieren básicamente a la entrega de ciertos reportes relacionados con otras actividades relevantes del negocio.

- **Objetivos de Compliance:** Las entidades deben estructurar sus actividades basándose principalmente en las regulaciones legales de cada país, así como también, en concordancia con las políticas corporativas y locales.

  El marco de control interno incluye al cumplimiento de regulaciones externas dentro de los objetivos de compliance mientras que para el cumplimiento de políticas y normativas internas se refiere a objetivos operativos.

Los objetivos que se han descrito hasta esta parte del documento se describen como objetivos generales, sin embargo, para el cumplimiento de los mismos es

necesario que estén soportados por otros objetivos específicos de cada área, departamento, proceso o función. El C.I. cumple también un propósito importante en este aspecto ya que asegura de manera razonable que los objetivos específicos dirijan a la organización al cumplimiento de aquellos objetivos más generales.

1.2.2 Marco Integrado para la Gestión de Riesgos Empresariales

El Marco Integrado para la Gestión de Riesgos Empresariales es la base teórica principal de este documento ya que su enfoque primordialmente se dirige a la gestión de riesgos. Al igual que el COSO I, el COSO II tiene varios componentes; sin, embargo hace un enfoque más directo a los riesgos, por lo tanto, sus conceptos podrían variar en comparación con los del COSO I. Esta comparación no será realizada en este trabajo ya que no es el objetivo del mismo.

De manera similar al COSO I, el **COSO II** menciona al ERM como (The Comittee of Sponsoring Organizations of the Treadway Commission, 2004):

- **Un proceso, continuo y que fluye en toda la entidad:** Debe ser flexible y debe ser representado en varios pasos en los que un riesgo puede ser analizado y evaluado.

- **Realizado por personas de todos los niveles de la organización:** Las directrices de una compañía deben ser realizadas con la participación de aquellos trabajadores que se involucran directamente con el proceso.

- **Aplicado de una manera organizada:** Una empresa debe tener una serie de estrategias para enfrentar una situación en todas sus áreas, el ERM permite tomar decisiones complejas de una manera estratégica y organizada. Es aplicado en todos los niveles de la compañía e incluye el levantamiento del punto de vista del riesgo en la organización.

- **Diseñado para identificar eventos potenciales que afecten a la organización y manejar el riesgo dentro del apetito del riesgo definido por la gerencia:** Todos los gerentes y las organizaciones deben tener una idea del nivel del riesgo que se maneja para los procesos involucrados. En ciertas ocasiones una empresa o gerente prefiere tener un mayor riesgo en una inversión o procedimiento por un motivo o por un retorno prometedor, esto es definido como el apetito al riesgo.

- **Una herramienta que provee seguridad razonable a la administración de la empresa y a su Comité:** Esto quiere decir que el ERM no asegura que los objetivos serán cumplidos ya que dependerá de otros factores no asociados a la administración del riesgo, esto ya se explicó en secciones anteriores.

- **Orientado al cumplimiento de objetivos en sus diferentes categorías como un medio, más como un fin en sí.**

1.2.2.1 ¿Por qué implementar el ERM en una organización?

Para implementar un sistema de gestión de riesgos en una compañía, es necesario conocer las ventajas que este sistema traerá a la misma. Estos puntos principales serán analizados a continuación (Protiviti-Independent Risk Consulting, 2006, págs. 3,4):

En primera instancia un sistema de gestión de riesgos de acuerdo a COSO permite reducir ineficiencias a través de la identificación de eventos riesgosos y su impacto si ocurre; además, ayuda a la organización a desarrollar procedimientos de control para mitigar el impacto de los riesgos identificados o manejar una situación si los mismos ocurren.

Por otro lado, el ERM se enfoca en prevenir eventos adversos y evitar que los mismos se presenten de manera sorpresiva o por accidente, de esta manera una compañía se encontrará en mejores condiciones para lograr sus objetivos.

El ERM brinda una visión conjunta y global del riego empresarial, esto se debe a que el sistema de gestión de riesgos debe estar implementado en todos los procesos de la compañía. Así, la compañía tiene la posibilidad de unir las diferentes visiones del riesgo en cada nivel para entender de manera íntegra la relación que existe entre cada departamento, área o función y los riesgos más significativos que los involucran.

Las partes interesadas de una compañía constantemente están requiriendo información importante de la misma y el manejo del riesgo es un punto fundamental que refleja un correcto control interno y además brinda una exposición más confiable para la comunidad y otros terceros. Esto también permite a la organización determinar si los retornos de las inversiones son adecuados en base a los riesgos tomados y evaluar si dicha organización está en la capacidad de enfrentar los cambios que se presentan en su entorno (mercado).

La administración de riesgos está estrechamente relacionada con el gobierno corporativo ya que permite a las gerencias a tener una mejor visión de los procesos, establece de manera más efectiva el involucramiento del personal en la identificación de riesgos, delimita las responsabilidades y los roles en la administración de riesgos, establece los límites y las autoridades de riesgo y permite a la organización comunicar efectivamente los riesgos existentes que se

relacionan con los objetivos establecidos. Estas acciones ayudan a la administración a desarrollar de una manera más efectiva sus funciones en su carrera por alcanzar las metas corporativas.

Como es conocido, el mercado está constantemente cambiando por varios factores externos. Las compañías están obligadas a adaptar sus modelos de negocio para asegurar su existencia y rentabilidad. En este aspecto, el ERM soporta formidablemente a que las organizaciones puedan evaluar los diferentes escenarios futuros y las mejores alternativas que se deben considerar para que los cambios de modelos sean exitosos; lo que determinará el correcto uso de recursos y las probabilidades de que diferentes riesgos se presenten en estos nuevos modelos.

El ERM permite además alinear la estrategia y la cultura organizacional. Esto se da ya que a través de esta herramienta es posible generar una cultura de identificación de riesgos y su administración por todos los integrantes de un proceso como parte integral del mismo; con esta premisa, los individuos se encuentran seguros y en total libertad de reportar cualquier evento adverso que represente una debilidad ya que la filosofía del control de riesgos se encuentra dentro de su cultura. Asimismo, el ERM mejora la habilidad para establecer políticas, mejora la focalización y brinda un ambiente de disciplina y control.

A continuación se presentan en la **Figura 1.2** los componentes que están contenidos dentro del Enterprise Risk Management Integrated Framework (COSO II) y que difieren en su enfoque principal a los mencionados anteriormente en el Internal Control Integrated Framework:

Figura 1.2: Cubo de Componentes del COSO II

El Marco para la Gestión de Riesgos Empresariales presenta ocho componentes dentro de su fundamentación teórica, denominados también componentes de riesgo. Estos son (The Comittee of Sponsoring Organizations of the Treadway Commission, 2004):

a) Ambiente Interno

b) Establecimiento de Objetivos

c) Identificación de Eventos

d) Administración del Riesgo

e) Respuesta al Riesgo

f) Actividades de Control

g) Información y Comunicación

h) Monitoreo

Además de estos componentes, se muestra en la parte superior del cubo (**Figura 1.2**) los cuatro tipos de objetivos que son:

- Objetivos Estratégicos
- Objetivos Operacionales
- Objetivos de Reportaje

- Objetivos de Compliance

A diferencia del COSO I el primer objetivo es propuesto en el COSO II. Los Objetivos Estratégicos son de nivel superior, determinados por el Comité Ejecutivo de la organización en su nivel más alto.

Adicionalmente, en la cara derecha del cubo se muestran las diferentes divisiones que una corporación puede presentar dentro de su estructura, lo que ubica al ERM como una herramienta integral y universal (The Comittee of Sponsoring Organizations of the Treadway Commission, 2004):

- Subsidiarias

- Unidades de Negocios

- Divisiones

- Niveles Organizacionales

1.3 G.R.C.

Para entender a cabalidad los componentes del ERM mencionados en el COSO II, es importante revisar ciertos conceptos y fundamentos que las corporaciones han desarrollado durante décadas a partir de errores que en su momento desembocaron en problemas financieros, administrativos y legales. Muchos de estos casos son conocidos públicamente a nivel mundial y han marcado un nuevo punto de enfoque importante a ser considerado para la administración de futuras generaciones de empresas y para un mejor desempeño en búsqueda de objetivos organizacionales.

El GRC (Governance, Risk and Compliance) representa uno de los fundamentos principales del ERM. Cuando las empresas iniciaron su funcionamiento en la antigüedad, existía la práctica de que una o un grupo de personas establezca las reglas que enmarcan el procedimiento de todos los empleados y directivos de una organización. Esto funcionaba bien de manera general para las empresas grandes que hoy conocemos y que en ese entonces contaban con estructuras limitadas. Con el avance del tiempo, las empresas fueron adquiriendo cada vez más divisiones y unidades; esto a su vez creó la necesidad de contar con cuerpos multifuncionales que establezcan eficientes y eficaces procesos de **gobierno corporativo (G)** para establecer políticas y procedimientos**.**

El gobierno corporativo se refiere también a la manera en que los directivos de una organización se aseguran que las actividades de la misma sean realizadas en base a los procedimientos, regulaciones y decisiones tomadas por los mismos, así como también

que tengan el direccionamiento correcto en relación a los objetivos y metas propuestas. Entre otras de las actividades que debe realizar el gobierno corporativo está el aseguramiento de que los riesgos corporativos estén siendo manejados de una manera correcta, que los recursos de la compañía sean utilizados apropiadamente y el monitoreo en el cumplimiento de las normas establecidas, proporcionando recompensas y sanciones en relación al compliance.

A continuación se muestra la **Figura 1.3** que envuelve el gobierno corporativo, situándose en el medio el Comité Ejecutivo y sus puntos de enfoque alrededor (Robert R. Moeller- John Wiley & Sons - Citación de Enterprise Risk Management Integrated Framework 2004, 2011):

Figura 1.3: Características del Gobierno Corporativo

El mundo empresarial en la actualidad está enmarcado en una serie de normas que se sitúan en varios niveles y categorías. Estas normas van desde políticas locales y de seguridad pública hasta leyes nacionales e inclusive internacionales. En otro nivel se ubican también los estándares internacionales para prácticas profesionales de todo tipo que se encuentran en concordancia con las prácticas más rigurosas de calidad en todo contexto. En todos estos niveles, las compañías están obligadas a cumplir las normas y regulaciones para asegurar su éxito y evitar problemas legales, financieros, administrativos y otros resultantes de su incumplimiento (Robert R. Moeller- John Wiley & Sons - Citación de Enterprise Risk Management Integrated Framework 2004, 2011). A esto se le denomina **compliance (C)**.

El compliance puede ser una tarea muy difícil de ejecutar en una corporación, se requiere de una participación completa de todos los empleados. Las dificultades externas que se pueden presentar en este sentido surgen principalmente de la manera en que las entidades gubernamentales locales e internacionales establecen parámetros y regulaciones para el funcionamiento de las personas jurídicas.

Estos cambios o emisiones de nuevas regulaciones obligan a las organizaciones a estar siempre en constante actualización. Además, en ocasiones las leyes son escritas de formas no muy claras que exigen interpretaciones, en parte subjetivas y que representan un reto importante para el compliance. Adicionalmente, existen otro tipo de normativas que surgen por organizaciones que emiten estándares internacionales y otras que nacen de la misma organización. Para que una compañía pueda adaptarse a estos cambios rápidamente y sin costos excesivos, se recomienda que el departamento

de compliance tenga un alcance global que incluya a todas las estructuras de la misma y que funcione con la ayuda de las herramientas tecnológicas que hoy en día existen en el mundo.

El efectivo manejo del compliance también permite a una organización tener una mayor ventaja frente a sus competidores ya que facilita el entendimiento y control de los procesos, así como también a establecer respuestas más rápidas a presiones internas o externas.

El alcance del compliance en una compañía se divide en cuatro partes para un mejor entendimiento (Robert R. Moeller- John Wiley & Sons - Citación de Enterprise Risk Management Integrated Framework 2004, 2011):

- **Estrategia:** A medida que una organización define sus estrategias, es imperante que se reconozcan las regulaciones y reglamentos relevantes para su funcionamiento. Así, desarrollar ideas sustentables para estrategias de compliance.

- **Organización:** La estructura de la organización debe ser establecida de manera que permita el cumplimiento de leyes y normativas tanto internas como externas.

- **Procesos:** Los procesos más importantes de la compañía deben ser documentados y practicados de acuerdo a los lineamientos establecidos para los mismos. Las auditorías juegan un papel importante en este sentido, ayudando a la organización a determinar si la ejecución de los procesos se dan en cumplimiento de las leyes y regulaciones.

- **Aplicaciones e Información:** Las aplicaciones que utiliza la organización para su funcionamiento deben ser implementadas y monitoreadas constantemente para asegurar que soporta al compliance. De la misma manera, la información debe ser manejada con la debida precaución de acuerdo a los requerimientos legales y corporativos.

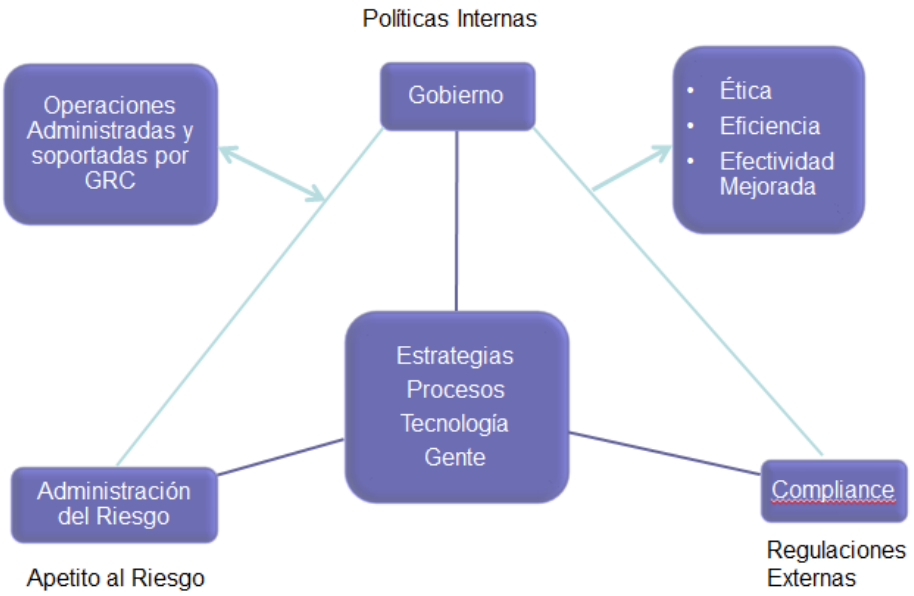
- **Facilidades:** Las facilidades deben ser diseñadas y disponibles en cumplimiento de regulaciones específicas.

El incumplimiento de las normas de gobierno corporativo y compliance trae consigo diferentes **riesgos (R)** empresariales que deben estar dentro de la mira del Comité Ejecutivo. Para esto, el Marco Integrado para la Gestión de Riesgos Empresariales nos muestra un conjunto de principios y prácticas relacionadas a la relación entre el gobierno, el compliance y el riesgo.

A continuación se detalla la **Figura 1.4** muy interesante acerca de la filosofía del GRC que se debe manejar dentro de la cultura organizacional como un mecanismo integral a

todo nivel (Robert R. Moeller- John Wiley & Sons - Citación de Enterprise Risk Management Integrated Framework 2004, 2011):

Figura 1.4: Concepto del G.R.C.



Como se puede observar los componentes principales del GRC son la estrategia, los procesos, la tecnología y las personas que llevan a cabo todas las actividades del negocio. Asimismo, el principio del Gobierno Corporativo es soportado por las Políticas Internas, el Compliance se direcciona en base a las Regulaciones Externas y el Manejo del Riesgo es soportado por el Apetito al Riesgo. Las operaciones de la compañía son manejadas y fundamentadas por este triángulo que representa el concepto del GRC y que su correcto manejo estará basado en la capacidad que tiene la organización en demostrar robustos procesos éticos, eficientes y de continuo mejoramiento.

2. CAPÍTULO II: DIAGNÓSTICO DEL SISTEMA DE GESTIÓN DE RIESGOS EN MM S.A.

Para éste capítulo y el siguiente, se extraen los aspectos más relevantes de los 8 componentes del COSO II ubicados en las 7 secciones de la Metodología de Gestión de Riesgos (**Figura 1.2)** propuesto por COSO y que fundamentan el **Diagnóstico del Sistema de Gestión de Riesgos** y la **Propuesta para MM S.A.** como sigue:

a) **Estructuración de la gestión de riesgos:** Que incluye aspectos del componente No. 1 (Ambiente Interno) y No. 2 (Establecimiento de Objetivos) del marco; además se da a conocer la **estrategia y organización** para la gestión de riesgos que tiene MM S.A., su composición **estructural**, las **políticas** relevantes y los **criterios** generales que utiliza la compañía para la gestión de riesgos.

b) **Identificación de los riesgos:** En esta parte se topa lo relacionado al componente No. 3 (Identificación de Eventos) y básicamente se analiza la capacidad actual que tiene MM S.A. para identificar los riesgos comparado con la metodología del ERM Integrated Framework.

c) **Evaluación de los Riesgos:** Incluye el componente No. 4 del marco (Administración del Riesgo) y se evalúan los procesos que mantiene MM S.A. para determinar la cuantificación de **probabilidades de ocurrencia**, **niveles de impactos**, **priorización** de riesgos y **análisis de brechas.** Se mostrarán los pasos que se utilizan en la compañía para priorizar los riesgos y todo lo concerniente a la cuantificación de eventos adversos.

d) **Respuesta al Riesgo:** Se refiere únicamente a lo que se menciona en el componente No. 5 (Respuesta al Riesgo), se analiza cómo MM S.A. reacciona ante riesgos identificados y de qué manera se establecen las acciones para mitigación, aceptación o rechazo de los mismos.

e) **Control de Riesgos:** Que está compuesto por el componente No. 6 (Actividades de Control) y es donde se revisan las actividades de identificación, evaluación e implementación de controles en MM S.A. para riesgos identificados.

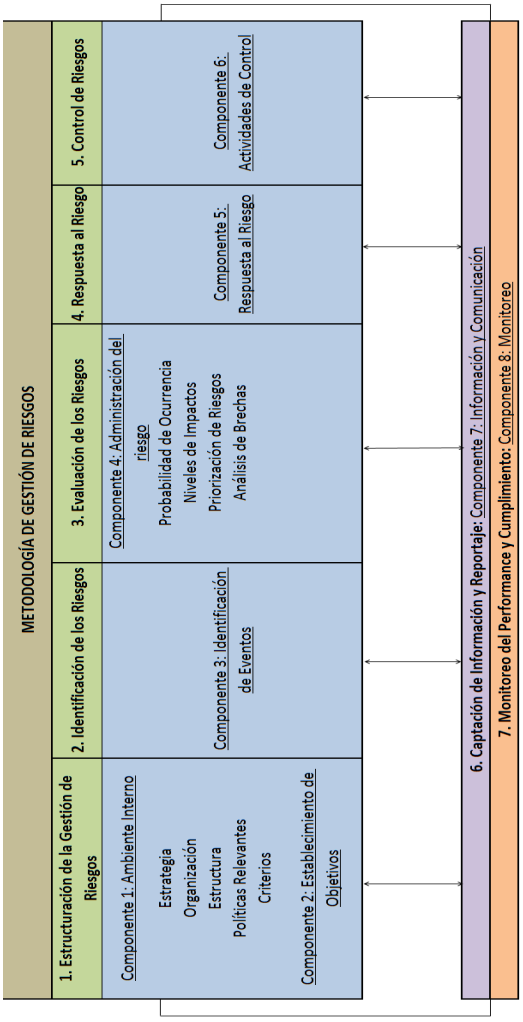
Además de estos, se proponen actividades para los siguientes componentes que también forman parte del Sistema de Gestión de Riesgos pero debido a que MM S.A. no presenta este sistema solo se mencionan en el capítulo III:

f) **Captación de Información y Reporte:** Aquí se incluye el componente No. 7 (Información y Comunicación).

g) **Monitoreo del Performance y Cumplimiento:** Que contiene el componente No. 8 (Monitoreo).

Cabe mencionar que los últimos dos componentes se llevan a cabo luego de la implementación de los planes de acción sugeridos en los pasos 1, 2, 3, 4 y 5 de la Metodología de Gestión de Riesgos. Sin embargo, se explicará lo que quieren decir estos dos componentes y cómo se pueden aplicar luego de haber realizado todo el proceso práctico y de levantamiento de riesgos.

Figura 2.1 Cuadro Resumido del Sistema de Gestión de Riesgos



2.1 PASO 1 - ESTRUCTURACIÓN DE LA GESTIÓN DE RIESGOS

2.1.1 Componente 1: Ambiente interno

En esta parte se analiza el primer componente del cubo del ERM Integrated Framework **(Ambiente Interno)** considerado como el pilar de los otros componentes por su alta influencia en los demás. Su alcance influye al establecimiento de objetivos y estrategias de una corporación, la estructura de las actividades del negocio relacionadas a los riesgos empresariales y la identificación de riesgos. Este primer componente está constituido por los siguientes elementos:

2.1.1.1 Filosofía del manejo de riesgos

Este elemento sin duda es uno de los más importantes para el eficiente manejo de los riesgos. Básicamente se basa en las creencias y actitudes a través de las cuales una organización toma en cuenta al riesgo y al control interno en todas las actividades que realiza. Es la manera en que todos los empleados de una compañía visualizan al riesgo en las grandes y pequeñas acciones; tanto en la toma de decisiones para incurrir en un proyecto que puede traer diferentes resultados (en ocasiones inciertos), como en los pasos que tomamos para realizar el día a día en el trabajo.

Una de las maneras en que la gerencia refleja su consideración del riesgo en las actividades que lleva a cabo es mencionándolo en los escritos que forman parte de los lineamientos de la compañía, como su código de conducta, comunicaciones internas, etc. Sin embargo, simplemente mencionarlo no es lo que creará una filosofía consciente de los riesgos asociados a las actividades diarias, se deben realizar talleres, encuestas, conversaciones personalizadas con todos los miembros y otro tipo de técnicas para hacer que la consideración del riesgo sea parte consciente de todo el personal que forma parte de la empresa (Robert R. Moeller- John Wiley & Sons - Citación de Enterprise Risk Management Integrated Framework 2004, 2011).

2.1.1.1.1 Situación actual de la filosofía del manejo de riesgos de MM S.A.

En MM S.A. las políticas y procedimientos a nivel corporativo mencionan al riesgo de diversas maneras pero los procedimientos y políticas locales no contienen consideraciones expresas del riesgo y en otros casos tampoco mencionan el motivo por el cual los controles se llevan a cabo (**Debilidad, ver numeral 2.6**). Este es un indicio de que la consideración del riesgo en las actividades diarias de los funcionarios de la compañía no está formalizada e inmersa en la cultura organizacional como tal. Existe una especie de

sexto sentido en relación al riesgo por la presencia de normativas formales.

Al realizar un levantamiento de varios de los procesos de la compañía, se identificó que los actores de los mismos no tienen una visión clara del control y se considera que ésta es una función única del área de Contraloría (**Debilidad, ver numeral 2.6**). Es decir, no existe un conocimiento claro de dónde existen los puntos de control fundamentales del proceso, ni tampoco cuál es su participación en este sentido. Sin ánimos de generalizar esta situación, se detectó en casos puntuales que las novedades de control saltan a la vista por un sentido común que poseen los integrantes del equipo.

Esto no quiere decir que la organización está zarpando a la deriva, por el contrario, la compañía mantiene varias **políticas** corporativas y locales que regulan las operaciones principales del negocio. MM S.A. tiene más de 80 políticas y procedimientos corporativos que rigen a todas las sucursales del mundo en la mayoría de casos y en otros regulan las actividades de mercados específicos. Dentro del grupo de políticas mencionadas se encuentran: Política de conflicto de interés; seguridad; lanzamiento de invenciones a empleados, seguridad salud y ambiente, prevención de soborno y

corrupción, manejo de riesgos informáticos, experiencias adversas de salud humana y animal y reporte de quejas de calidad de productos; política de calidad; manejo de productos devueltos; política de compras; política de reembolsos de gastos, viajes y uso de tarjetas de crédito corporativas; política de crédito y cobranzas; protección de secretos del negocio; política de precios de transferencia global; reportar y responder a violaciones potenciales de compliance, entre otras.

Como se puede evidenciar existen políticas para muchas de las actividades y eventos que resulten de las operaciones del negocio. Sin embargo, esto no necesariamente significa que todos los empleados conocen las políticas y procedimientos que se relacionan a los procesos en los que se involucran (**Debilidad, ver numeral 2.6**).

Además, existen diferentes maneras de realizar las actividades de la compañía para cada sucursal (no en esencia), lo que amerita que cada mercado desarrolle políticas adicionales a las corporativas que regulen estas "áreas grises" que se puedan producir. Estos lineamientos locales no deben de ninguna manera ser más permisivos que los corporativos,

punto que no ha sido demostrado en su totalidad por parte de la sucursal ubicada en Ecuador.

MM S.A. en Ecuador tiene muchas políticas y procedimientos locales; a pesar de este particular, no se tiene conocimiento exacto del número de políticas, ni su alcance. En muchos casos las políticas y procedimientos están desarrollados de diferentes maneras, es decir no hay un estándar definido, por ende, es posible que no cubran las necesidades del negocio para mitigar riesgos correctamente (**Debilidad, ver numeral 2.6**).

Por otro lado, MM S.A. tiene una Política de Auditoría Corporativa que define a grandes rasgos las responsabilidades del equipo global de manejo de riesgos; sin embargo, la misma no es tomada en cuenta en el mercado local, ni tampoco define claramente la estructura que debe tener un sistema integral de gestión de riesgos para cada sucursal. Es decir, localmente no se cuenta con un lineamiento definido para un equipo ERM que debe asumir las responsabilidades para una eficiente administración de riesgos como menciona la política corporativa antes mencionada (**Debilidad, ver numeral 2.6**).

Adicionalmente, al momento en que se diseñan los procesos para nuevos proyectos o metodologías no se identifican puntos de control claves de manera documentada; esto es evidente aún más en procesos antiguos cuyos procedimientos y políticas fueron desarrollados años atrás y para los cuales en algunos casos no se conoce su vigencia y en el peor de los casos ni siquiera es tomado en cuenta. En otras ocasiones los controles que se deben llevar a cabo en un proceso pueden ser obvios, sin embargo, es preciso identificar en los flujos gráficos todos los puntos claves de control y emitir normativas que regulen las situaciones que se presentan en esos puntos clave, actividad que no se lleva a cabo de manera general en los procesos de la compañía (**Debilidad, ver numeral 2.6**).

Si bien es cierto, la normativa corporativa evita la ocurrencia de hechos desfavorables en los procesos de MM S.A., el simple hecho de que no se maneje la filosofía del riesgo en la cultura organizacional podría significar la elaboración incompleta de procedimientos que mitiguen riesgos locales. Estos podrían tener impactos muy desfavorables en el negocio si no son identificados en cada área o unidad oportunamente.

2.1.1.2 Apetito al riesgo

Este término se refiere al nivel de riesgo que una organización está dispuesta a aceptar en la persecución del éxito. Es importante tomar en cuenta que para que una organización tenga éxito en la ejecución de sus estrategias, necesita tomar ciertos riesgos inherentes a la industria mercado, estrategias, competencia, etc. En ciertos casos el riesgo puede ser aceptable de acuerdo a los objetivos que se intentan alcanzar, en otros el riesgo podría ser muy desfavorable y por ende no aceptable. Por este motivo es necesario que los niveles de riesgo sean categorizados formalmente en forma cuantitativa y que la Gerencia desde el nivel más alto esté al tanto de los niveles máximos de riesgo que está aceptando en la realización de las distintas actividades que le permiten alcanzar los objetivos organizacionales. Los riesgos en la mayoría de ocasiones no pueden ser mitigados en su totalidad a través de los distintos controles y lineamientos. Dentro del ERM se menciona que es fundamental que este concepto esté inmerso en todos los niveles gerenciales y también en los empleados en general y define al apetito al riesgo como:

> La cantidad de riesgo, en un nivel amplio, que una entidad está dispuesta a aceptar en la búsqueda de valor. Refleja la filosofía del riesgo de una entidad y que a su vez influencia en la cultura y estilo operativo de la entidad….El apetito al riesgo guía la colocación de recursos….El apetito al riesgo (asiste a la organización) alineando la organización, su gente, y los procesos en (diseñando) la infraestructura necesaria para responder y monitorear a los riesgos efectivamente. (Committee of Sponsoring Organizations of the Treadway Commission, 2012, pág. 9)

2.1.1.2.1 Situación actual del apetito al riesgo de MM S.A.

MM S.A. no presenta un conocimiento escrito, documentado o formalizado de los niveles de riesgo que se aceptan en sus procesos (**Debilidad, ver numeral 2.6)**. Esto se observa en casi todos los procesos de la organización. De cierta manera esta situación se puede presentar a causa de una falta en la identificación de los riesgos locales que se encuentran inmersos en cada uno de los procesos de la compañía; a su vez, esto dificulta la correcta evaluación de la eficiencia de los procesos en relación a los objetivos propuestos.

Está claro que las políticas y procedimientos que se manejan en las corporaciones están diseñados para mitigar los riesgos, sin embargo, sin una definición formal de estos niveles aceptables o no aceptables no es posible determinar acciones prioritarias preventivas de eventos que podrían tener impactos desfavorables para la compañía y que en ocasiones podrían pasar desapercibidos.

Las políticas y procedimientos existentes en MM S.A. guían las acciones de los empleados y terceros para no incurrir en riesgos, a pesar de esto MM S.A. no cuenta con una declaración formal de los niveles de apetito al riesgo para sus

distintas áreas. Por lo antes expuesto se cree que la administración del riesgo y control interno no tiene un enfoque completo que pueda asegurar de manera razonable la eficacia de sus operaciones en apoyo al cumplimiento de objetivos estratégicos, operacionales, de reportaje y compliance.

2.1.1.3 Actitud de la Junta Directiva, estrategia y organización

La junta directiva de una compañía que maneja sus riesgos a través de un sistema formal, tiene un rol muy importante en la implementación de este modelo como ente de guía y control. Su misión como parte del ambiente interno es también la de realizar un análisis adecuado acerca de las acciones que se deben tomar para evitar situaciones que resultan muy riesgosas para la organización y definir planes de remediación en caso de que las mismas ocurran.

En este punto también se incluye el diagnóstico de la **estrategia** y **organización** de MM S.A. para llevar a cabo las actividades relacionadas a la administración de los riesgos, haciendo mención a lo que la compañía determina como actividades de control interno y que de cierta manera podría ser considerado como un sistema similar.

2.1.1.3.1 Situación actual de la actitud de la Junta Directiva de MM S.A., estrategia y organización

Relacionando este punto a MM S.A. es importante mencionar que la compañía tiene una junta directiva a nivel mundial ubicada en su casa matriz que se encarga supervisar muy desde arriba todas las características de los mercados en los cuales la compañía compite, así como también el funcionamiento de los procesos más importantes que se llevan a cabo de manera estandarizada para la región. Sin embargo y de manera adicional, cada sucursal cuenta con su propio Comité Ejecutivo que podría ser considerado como el Consejo de Administración, mismo que se reúne constantemente para revisar las condiciones del negocio dentro del país (**Fortaleza, ver numeral 2.6**).

En cada una de estas reuniones mensuales, se identifican eventos adversos asociados a procesos o estrategias nuevas o en formación, así como también planes de acción para reducir la probabilidad de ocurrencia de este tipo de eventos. Como se observará a través de algunos de los componentes del COSO II, es posible que la simple detección de un evento adverso dentro de un proceso o función, no sea suficiente para un correcto manejo de los riesgos potenciales

identificados en los mismos. De todas maneras, estas actitudes son las que se mencionan en este elemento del ambiente interno y que guían a una compañía de manera importante hacia la correcta administración de riesgos.

A pesar de que son necesarias más acciones para integrar todo un sistema de administración de riesgos, se puede considerar que MM S.A. cuenta con la necesaria actitud de la Junta Directiva para auspiciar de manera adecuada al sistema que se propone.

En cuanto a la **organización**, MM S.A. no cuenta con un Comité de Auditoría como tal dentro de la localidad a pesar de que si existe un Comité de Auditoría Interna Corporativa ubicado en casa matriz y localmente estas funciones las asume de manera parcial el Área de Contraloría. Se menciona que las funciones se realizan de manera parcial debido a que el Área de Contraloría no reporta ni cuestiona asuntos de control directamente con el Comité Ejecutivo mencionado anteriormente y en pocas ocasiones forma parte de la elaboración de nuevos modelos y estrategias de negocio que se proponen en la compañía (**Debilidad, ver numeral 2.6)**.

Se considera que el Departamento de Contraloría no hace las funciones de Comité de Auditoría de manera integral por no contar con una estructura organizacional adecuada como ya se verá más adelante; por otro lado, el área tampoco cuenta con apoyo externo en esta materia para que exista equilibrio en relación a la independencia y objetividad del trabajo de control interno necesario para una compañía tan grande como MM S.A (**Debilidad, ver numeral 2.6**).

Como **estrategia** para detectar riesgos, el Departamento de Auditoría Interna Corporativa realiza revisiones generales de los procesos más importantes en cada país (**Fortaleza, ver numeral 2.6**). Esta revisión se hace cada dos años aproximadamente y no incluye todos los procesos que se manejan localmente, además, se fundamenta en la detección de eventos en base a guías corporativas y que en algunos casos no se ajustan a las actividades locales que se realizan en la sucursal (**Debilidad, ver numeral 2.6**). El Departamento de Contraloría es el encargado de coordinar las actividades con el equipo de auditoría interna cuando se presentan las visitas de revisión.

Otras de las estrategias que utiliza el Departamento de Contraloría para detectar riesgos es un selfassessment

(traducido al español quiere decir una autoevaluación) de los procesos financieros más importantes como parte del control interno (**Fortaleza, ver numeral 2.6**). Esta revisión se basa en lineamientos corporativos diseñados para un sistema contable distinto al que utiliza la sucursal en Ecuador (**Debilidad, ver numeral 2.6**). Además, se toma como referencia una última revisión realizada hace aproximadamente 2 años, misma que no estandarizó la metodología en relación a los puntos más importantes que se deben revisar en cada proceso.

En resumen, MM S.A. cuenta con procedimientos corporativos no estandarizados para la localidad para revisiones de control interno; en las nuevas revisiones tampoco se determinan puntos de control para un seguimiento posterior (**Debilidad, ver numeral 2.6**), a pesar de que si se realiza un informe que es entregado a Dirección Financiera para que sea comunicado posteriormente al Comité Ejecutivo local (**Fortaleza, ver numeral 2.6)**.

2.1.1.4 Integridad y valores éticos

Como parte del ambiente interno, es estrictamente necesario que una corporación cuente con un código de conducta que permitirá enlazar las

políticas y procedimientos con la misión y visión de la compañía, así como también, valores éticos definidos para todas las actividades que realiza. Adicionalmente, es fundamental que una empresa presente normas que guíen el comportamiento de los empleados en la organización; una fuerte cultura interna es primordial para que los funcionarios en todos los niveles puedan optar por correctas decisiones basadas en riesgos. El éxito de un eficiente sistema de riesgos está basado en los **criterios** mencionados y debe estar arraigado en la actitud y cultura individual de todos los empleados. Una compañía no deberá estar dispuesta a incurrir en riesgos que atenten en contra de la integridad ética en cómo la organización intenta alcanzar sus objetivos (Robert R. Moeller- John Wiley & Sons - Citación de Enterprise Risk Management Integrated Framework 2004, 2011).

El equipo Directivo de una compañía debe ser el ejemplo infalible de conducta ética y su compromiso en este sentido es imperante para que la organización pueda (Robert R. Moeller- John Wiley & Sons - Citación de Enterprise Risk Management Integrated Framework 2004, 2011):

- Tener empleados que hagan las cosas de manera correcta en torno a lo legal y moral.

- Generar una cultura arraigada al compliance, como parte del GRC.

- Explorar áreas o situaciones en las que no se han definido normas específicas para su control.

- Promover una actitud proactiva para reportar eventos adversos antes de que se generen situaciones desfavorables para la compañía.

En el Marco Integrado para la Gestión de Riesgos Empresariales se presenta un ejemplo ilustrativo acerca de los puntos que debería abordar un código de conducta. Estos son (The Comittee of Sponsoring Organizations of the Treadway Commission, 2004):

- Carta del Presidente Ejecutivo de la Compañía con el propósito de dar a conocer la importancia de la ética e integridad en la corporación, así como también hacer una breve introducción del documento en cuanto a su propósito y formas de uso.

- Objetivo del código y su filosofía en donde se nombra la cultura, razón social e industria, locación local e internacional y compromiso en liderazgo ético.

- Conflicto de intereses en cuanto a su identificación, auto negociación y aborda las actividades, inversiones o intereses que se reflejan en la reputación de la compañía.

- Regalos y propinas en donde se definen normas para este tipo de entregas y la forma correcta de reportarlas.

- Transparencia que se muestra en las formas como la organización muestra sus actividades y cifras.

- Recursos corporativos que incluye propiedad intelectual y dominio de la información.

- Responsabilidad social en su compromiso con los derechos humanos, sustentabilidad, inclusión de la comunidad, problemas ambientales y financieros.

- Otros puntos relacionados a la conducta de los empleados en los que se incluyen temas específicos de las distintas áreas de la organización. En estos se pueden incluir asuntos relacionados a empleados como prácticas justas de trabajo y no discriminación; negociaciones gubernamentales; prácticas competitivas; buena voluntad y negociaciones justas; confidencialidad y seguridad de la información; prácticas medioambientales; seguridad y calidad de los productos; otras específicas.

Adicional a lo antes expuesto, las organizaciones deben utilizar las herramientas tecnológicas para asegurar que exista una correcta integridad y los valores éticos estén presentes en todas las actividades de la organización.

2.1.1.4.1 Situación actual de la integridad y valores éticos de MM S.A.

Realizando un breve recuento de lo que se menciona en el COSO II en relación a la integridad y valores éticos, es necesario verificar si MM S.A. está cumpliendo con estos **criterios** importantes de la estructura de riesgos.

La cultura organizacional de MM S.A. está fundamentada en una estructura llamada "Pirámide de Políticas" (**Fortaleza, ver numeral 2.6**) esta refleja en su base los comportamientos de liderazgo de la organización que son (MM S.A., 2014):

- Enfoque en los clientes y pacientes que básicamente se refiere a escuchar, comprender y colaborar con los clientes para proporcionarles lo que realmente necesitan. Asimismo, dirigir los esfuerzos de los empleados a la satisfacción de las necesidades de los pacientes/clientes relacionadas a los productos farmacéuticos que comercializa la compañía.

- Actuar con coraje y sinceridad que trata acerca de expresar la perspectiva de los miembros de la organización con sinceridad y convicción.

- Tomar decisiones rápidas y disciplinadas que se refiere a mantenerse seguro de las convicciones de cada uno, así como también de las decisiones tomadas.

- Fomentar la colaboración al momento de trabajar en equipo, como una sola compañía y escuchando al compañero, a pesar de contar con una estructura compleja y grande.

- Impulsar los resultados haciéndose responsable del rendimiento y cumplimiento de los objetivos de MM S.A.

- Desarrollar los talentos, fomentar el desarrollo de los empleados e inspirarlos a crecer.

- Demostrar ética e integridad que se refiere a que todos los empleados deben demostrar valores éticos en todas sus actividades y sentirse responsables del bienestar de miles de personas que utilizan los productos de MM S.A.

El segundo nivel base de la "Pirámide" son las divisiones, funciones y recursos regionales que establecen estándares de conducta para prácticas del negocio relevantes para las diferentes divisiones, funciones y funciones en las que opera MM S.A.

El tercer nivel muestra las políticas corporativas y procedimientos que de igual manera son estándares de conducta que todos los empleados deben cumplir.

Finalmente como un nivel 4 y final de la "Pirámide" (punta de la estructura) se encuentra el código de conducta que son los valores y estándares universales que todos los empleados deben saber para realizar sus actividades.

De manera general, el contenido del código de conducta de MM S.A. se divide de la siguiente manera en un documento compuesto de 43 hojas en su III edición:

- Recursos para los empleados, en donde se muestran los diferentes departamentos que atienden las dudas de todos los funcionarios de la compañía. Por ejemplo, en primera instancia el punto de contacto para cualquier duda es el Supervisor quien deriva al subordinado a los diferentes departamentos como Recursos Humanos, Departamento Legal, Director de Finanzas, Oficina de Ética y Compliance, Comité de Auditoría del Consejo de Administración, entre otras.

- Luego viene una sección que contiene la carta por parte del Presidente Ejecutivo de la Compañía dirigida a los empleados de MM S.A. en todo el mundo. Aquí el Presidente hace una introducción del documento en donde se menciona, de manera muy rápida, los cambios que se han dado en la industria a lo largo de 12 años desde que la compañía emitió por primera vez su código de conducta. Se resalta la persistencia de los valores éticos que guían las actividades de la compañía haciendo hincapié en la honestidad e integridad y también mencionan las actualizaciones a la anterior edición sobretodo relacionadas al manejo de la tecnología, la información y los medios sociales. Además, se hace una citación de la misión de MM S.A.

- A continuación se divide el documento en 6 secciones: Clientes, empleados, accionistas, proveedores, acción social y cómo plantear dudas acerca de las conductas y procedimientos que realizan los distintos funcionarios de la organización. Estas partes podrían ser entendidas como los estándares específicos de conducta de MM S.A.

A nivel general, el código de conducta de MM S.A. está completamente compuesto de todos los puntos necesarios tal y como lo menciona el COSO II y se podría decir que la compañía cuenta con un compendio de estándares necesarios que satisfacen el elemento de integridad y valores éticos del componente de ambiente interno (**Fortaleza, ver numeral 2.6**).

Cabe recalcar que aparte de este documento importante, MM S.A. cuenta con un robusto sistema tecnológico de entrenamientos online que permiten certificar a todos los empleados en el conocimiento de valores éticos y conductas de comportamiento necesarios para el cumplimiento de objetivos de manera ética. Por otro lado, existe un departamento que se enfoca específicamente en la recepción y procesamiento de quejas por prácticas incorrectas que se pueden presentar en la industria en sus múltiples áreas (**Fortaleza, ver numeral 2.6**).

Para el cumplimiento de los objetivos de este trabajo, no es practicable introducirse profundamente en el contenido del código de conducta de MM S.A. ya que sería necesario revisar cada uno de los puntos contenidos en el mismo y hacer un levantamiento de las diferentes aristas que tiene la

industria para determinar los riesgos relacionados. Para llegar a determinar estos riesgos es preciso llevar a cabo los componentes relacionados a la identificación y medición de los riesgos para todos los procesos de la compañía como ya se ha mencionado anteriormente en los anteriores capítulos de este documento. Sin embargo, se detallará más adelante cómo una organización debe mapear sus riesgos en base a su apetito.

2.1.1.5 Compromiso con la competencia

Competencia se refiere básicamente a los conocimientos y habilidades necesarias para el cumplimiento de una tarea asignada (Robert R. Moeller- John Wiley & Sons - Citación de Enterprise Risk Management Integrated Framework 2004, 2011). Los Directivos en este sentido tienen la responsabilidad de cumplir con las tareas asignadas u objetivos, utilizando las estrategias y los recursos necesarios y disponibles de la organización incluyendo el talento humano. La intención de este elemento es dar a conocer a la compañía que el simple hecho de asegurar el cumplimiento de un objetivo no tendrá ningún efecto si no se toman las acciones necesarias. Cuando una compañía no maneja de manera adecuada su compromiso con la competencia puede sufrir consecuencias lamentables al ver que el precio de sus acciones en la bolsa cae al no darse los resultados tan anunciados.

2.1.1.5.1 Situación actual del compromiso con la competencia de MM S.A.

MM S.A. presenta un flujo sistemático para materializar las estrategias corporativas a nivel mundial. Es decir, todas las estrategias para implementar proyectos nuevos o para aprovechar oportunidades identificadas en el mercado son revisadas minuciosamente antes de ser llevadas a cabo (**Fortaleza, ver numeral 2.6**). Este hecho demuestra una filosofía de administración de riesgos, sin embargo, no se puede asegurar que este análisis sea tan completo como se menciona en el ERM Integrated Framework.

Tan pronto el Comité Ejecutivo decide optar por un camino para la implementación de una estrategia, comunica este particular a todos sus empleados y sucursales alrededor del mundo; el cumplimiento de todas las condicionantes establecidas es monitoreado constantemente para asegurar que la estrategia será llevada a cabo con éxito y que de manera razonable es posible llegar a la meta establecida.

Internamente en cada sucursal, este mismo monitoreo se realiza para proyectos que son considerados “grandes”. Sin embargo, hay otros proyectos más pequeños que en ocasiones no se materializan y se podría considerar que se necesitan mayores acciones para que todos los proyectos independientemente de su tamaño puedan cumplir con su propósito (**Debilidad, ver numeral 2.6**).

Los proyectos que se realizan en MM S.A. a nivel local son parte de los objetivos que uno o varios empleados se proponen anualmente y los mismos ayudan a la dirección de su unidad en el cumplimiento de otros objetivos más generales que deberán estar ligados a la misión y visión de la compañía. A pesar de que se maneja una herramienta informática para el establecimiento de objetivos (**Fortaleza, ver numeral 2.6**), el seguimiento lo debe manejar cada persona con ayuda de su supervisor sin un cronograma establecido o indicadores específicos para monitoreo de objetivos. En ocasiones esto podría provocar el incumplimiento de algunos objetivos o que sean llevados a cabo a último momento, antes que finalice el año (**Debilidad, ver numeral 2.6**). Esto afecta a la competencia profesional que se maneja a nivel gerencial para el cumplimiento de objetivos más específicos, sin embargo y como ya se comentó anteriormente los proyectos grandes (objetivos

prioritarios) son monitoreados con mayor intensidad (**Fortaleza, ver numeral 2.6**).

A nivel de Recursos Humanos en MM S.A. se manejan descripciones específicas para cada puesto de trabajo, así como también, se han identificado los conocimientos y habilidades necesarias para ejercer una determinada función. Estas características son comunicadas detalladamente a una consultora externa que se encarga de la selección del personal avalada por diferentes estándares reconocidos a nivel nacional (**Fortaleza, ver numeral 2.6**).

2.1.1.6 Estructura organizacional

La **estructura** organizacional se refiere a que una compañía necesita tener correctamente definidos sus niveles jerárquicos que permitan establecer una excelente comunicación entre sus miembros, tanto para autoridad como para líneas de reportaje por parte de los subordinados (Robert R. Moeller- John Wiley & Sons - Citación de Enterprise Risk Management Integrated Framework 2004, 2011).

El equipo de control interno necesita una estructura organizacional adecuada para que el control como tal, fluya correctamente por todas las arterias de la compañía.

2.1.1.6.1 Situación actual de la estructura organizacional de MM S.A.

Volviendo la atención a MM S.A., su estructura organizacional tiene varios niveles. Por ejemplo, el área de Finanzas a nivel local cuenta con un Director Financiero, un Contralor, 5 Gerentes medios, un Contador General, un Coordinador de Contabilidad, un Coordinador de Costos y 4 Analistas. Más arriba, el Director Financiero reporta a un Director Regional de Finanzas. Asimismo el área comercial cuenta con una estructura similar con algunas otras áreas específicas en distintas ramas para el desarrollo de diversas estrategias en beneficio del negocio.

El Comité Ejecutivo está conformado por todos los Directores de la Sucursal en Ecuador: Director General, Directores de Unidades de Negocio, Director de Finanzas, Director Médico, Director de Recursos Humanos, Director de Asuntos Regulatorios, Gerente de IT, Gerente de Logística, Oficial de Compliance, Gerente de Comunicación

Organizacional, Gerente de Estrategias de Negocio, Gerente Comercial, entre otros.

El Departamento de Contraloría se encarga de velar por el cumplimiento de las políticas y procedimientos principalmente del Área de Finanzas reportando directamente al Director Financiero. Entre las responsabilidades asignadas al Departamento de Contraloría para control interno se encuentran:

- Asegurar que los procesos financieros cumplan con las políticas corporativas y requerimientos legales de la organización.

- Revisar las políticas y procedimientos existentes en todas las áreas de la compañía para verificar que se ajusten a las necesidades actuales del negocio y se encuentren en concordancia con los lineamientos corporativos y legales.

- Reportar novedades de control a través de la entrega de varios reportes al Departamento Regional de Contraloría y Dirección Financiera.

- Coordinar las actividades de auditores externos e internos con las diferentes áreas de la organización.

- Coordinar autoevaluaciones de control interno en las áreas financieras de la organización para la identificación de eventos adversos.

- Soportar al negocio con procedimientos eficientes para el desarrollo de nuevas estrategias.

- Otras actividades relacionadas a control interno como área de soporte de las actividades "core" del negocio.

Si bien es cierto, algunas de estas actividades forman parte de un sistema de riesgos, no se presenta una estructura sistemática específica para administrarlo de manera adecuada, el enfoque está más centrado en el control interno y no en riesgos. Es necesario establecer un Departamento de Riesgos dentro de la sucursal que permita una mejor coordinación de las actividades de control basada en riesgos (**Debilidad, ver numeral 2.6**).

Por otro lado, dentro del área Comercial se encuentra el Oficial de Compliance que de igual manera enfoca su trabajo en asegurar el cumplimiento de las políticas y procedimientos del área Comercial y reporta Directamente al Director General de MM S.A. en Ecuador, así como también participa en reuniones del Comité Ejecutivo para certificar que las nuevas actividades y proyectos que surjan en la organización estén dentro de los lineamientos de la compañía (**Fortaleza, ver numeral 2.6**). El Oficial de Compliance no realiza actividades relacionadas a gestión de riesgos, únicamente identifica asuntos de control en las estrategias comerciales, así como también asesora a los distintos departamentos de la compañía en temas relacionados a compliance (**Debilidad, ver numeral 2.6**).

Contraloría y Compliance trabajan de manera separada, ciertas revisiones de control que realiza Compliance son comunicadas a Contraloría pero esto no se da en sentido contrario. Además, se ha detectado que no existe una comunicación adecuada entre las dos áreas y hay una poca coordinación para las actividades de control en conjunto (**Debilidad, ver numeral 2.6**).

Asimismo, la compañía carece de un procedimiento de control definido para que las dos áreas utilicen sistemas estándar de revisión que estén certificadas por los Directivos de MM S.A. específicamente por el Director de Finanzas que en este caso tomaría las funciones del Director de Riesgos, de esta manera, las revisiones de control podrían no abarcar los puntos necesarios para mitigar riesgos que estén de acuerdo a las necesidades del negocio (**Debilidad, ver numeral 2.6**).

Para reportar hallazgos de control el Departamento de Contraloría emite informes de los procesos revisados durante todo el año que son entregados en primera instancia al Director Financiero para que los comunique al Comité Ejecutivo en sus reuniones mensuales (**Fortaleza, ver numeral 2.6**). Con estas novedades se establecen ciertas acciones de remediación que en ocasiones no son comunicadas al Departamento de Contraloría para el seguimiento (**Debilidad, ver numeral 2.6**). Otras novedades las toma el Oficial de Compliance y las comunica al Oficial de Compliance Regional para determinar acciones posteriores como memos, sanciones u otras dependiendo del caso. Para esto si existe una política corporativa en relación a las sanciones que se dan por comportamientos inadecuados, sin embargo, ninguno de los dos departamentos de control está correctamente capacitado para aplicar esta política

integralmente y tampoco se ha establecido una versión local de la política para las distintas circunstancias que se puedan presentar en la sucursal.

Por los puntos antes mencionados, se considera que MM S.A. cuenta con una estructura organizacional que divide los esfuerzos de control y que no permite al área de Contraloría tener un mayor peso en la gestión de riesgos tanto en procesos ya establecidos como también en la implementación de nuevas estrategias para el cumplimiento de objetivos organizacionales. El alcance de las revisiones que realiza Contraloría está limitado a procesos Financieros y los informes que surgen de los mismos son informados a Dirección Financiera para que posteriormente sean comunicados a las áreas respectivas en reuniones de Comité Comercial y Ejecutivo, lo que deja a un lado muchos otros procesos que tampoco son abarcados por Compliance y que posiblemente necesiten establecer mayores controles (**Debilidad, ver numeral 2.6**). Como parte del concepto GRC que se mencionó anteriormente, el Compliance debe darse a todo nivel de la estructura organizacional y debe estar alineado en todo sentido con el equipo ERM (Departamento de Contraloría en MM S.A.) que ejecuta la estrategia para una correcta gestión de riesgos.

2.1.1.7 Asignación de autoridad y responsabilidad

Este aspecto representa el grado de autoridad que es asignado a los empleados de una compañía con el propósito de autorizar distintas transacciones que surgen de las necesidades del negocio. En el COSO II se menciona que distintas compañías alrededor del mundo en la actualidad, permiten que los empleados de la organización tengan distintos niveles de autoridad para eliminar procedimientos burocráticos e ineficientes. Cabe recalcar que de cierta manera resulta un poco riesgoso otorgar autoridad a muchas personas dentro de una compañía en base a un monto determinado, ya sea de gasto, capital, activos fijos, ingresos, etc. Sin embargo, si la compañía tiene un robusto proceso de selección de personal, un código de conducta bien definido y controles en los flujos de aprobación se disminuye considerablemente este riesgo.

2.1.1.7.1 Situación actual de la designación de autoridad y responsabilidad de MM S.A.

MM S.A. tiene bien definidos sus niveles de autoridad y las maneras de delegarlos. Este nivel de autoridad es denominado Grant of Authority (GOA), el mismo que se encuentra detallado específicamente en un documento formalizado emitido por Casa Matriz en el cual constan las

firmas del Presidente y Vicepresidente Ejecutivo de la compañía.

Esta normativa cae como cascada en todas las sucursales de la compañía alrededor del mundo. Además, dentro del documento se mencionan las distintas clases de transacciones las cuales se dividen en acciones de rutina y de no rutina (**Fortaleza, ver numeral 2.6**). Las acciones de rutina tienen que ver con operaciones normales del negocio que se dan día a día, para las cuales se asignan distintos niveles de autoridad de acuerdo al nivel de la posición del empleado. Las acciones de no rutina son aquellas que no se dan normalmente en las operaciones regulares del negocio como por ejemplo capitalizaciones, compras de activos fijos, asuntos relacionados al personal, entre otras y para las cuales los niveles de autoridad son bastante específicos y generalmente se dan únicamente para posiciones Directivas.

De manera general, se entiende que un Supervisor inmediato directo siempre deberá tener un GOA superior al de su subordinado y que siempre exista el consentimiento del Supervisor para cualquier transacción.; esta es la misma esencia del C.I. aplicado a través de las personas dentro de una organización (**Fortaleza, ver numeral 2.6**).

2.1.1.8 Estándares de recursos humanos

La manera en que una compañía contrata, entrena, promueve, disciplina y realiza otras acciones relacionadas al manejo de los recursos humanos, envía un mensaje claro a sus empleados en el sentido de que es favorecido, tolerado y perdonado. De esta manera si la gerencia no realiza acciones de remediación inmediata en áreas que no están especificadas en ningún estándar, rápidamente este comportamiento es visto por otras áreas y demás empleados de la organización, por lo que se recomienda que siempre se tomen acciones estrictas por comportamientos inadecuados y se establezcan lineamientos en puntos frágiles de los procesos (Robert R. Moeller- John Wiley & Sons - Citación de Enterprise Risk Management Integrated Framework 2004, 2011).

2.1.1.8.1 Situación actual de los estándares de recursos humanos de MM S.A.

MM S.A. tiene una política corporativa para el Área de Recursos Humanos la cual determina que se deben realizar investigaciones previas de los empleados contratados, así como también revisiones posteriores en cuanto a las condiciones legales y éticas alrededor de mundo, utilizando un sistema que tiene una interface con la base de datos de

diferentes instituciones de control en los Estados Unidos de América y otros países de relevancia en el mundo (**Fortaleza, ver numeral 2.6**).

Existen otras políticas y procedimientos corporativos relacionados a la selección de personal y otras funciones de recursos humanos; en la localidad, MM S.A. no cuenta con procedimientos formalizados (**Debilidad, ver numeral 2.6**), pero utiliza a un tercero reconocido en el medio para la contratación garantizada de profesionales competentes para la función vacante (**Fortaleza, ver numeral 2.6**).

En relación a las actividades de entrenamiento para el conocimiento de políticas y procedimientos, MM S.A. tiene un sofisticado sistema de entrenamiento continuo a través de intranet (**Fortaleza, ver numeral 2.6**).

Los refuerzos de las políticas se dan para los aspectos más relevantes correspondientes al código de conducta; manejo de la información; reporte de eventos adversos de la calidad de los productos de la compañía; seguridad, salud y ambiente; respuesta a emergencias, entre otras. Sin embargo, no se realizan entrenamientos semestrales o anuales para refrescamiento de políticas y procedimientos de finanzas para

el Área Financiera por ejemplo u otras relacionadas a procesos que se presentan en el día a día (**Debilidad, ver numeral 2.6**). Cabe recalcar que cuando ingresan nuevos empleados a la compañía si se realizan entrenamientos para el conocimiento de procesos importantes de la corporación pero el Área de Recursos Humanos no conoce específicamente si todos los procesos fundamentales han sido tomados en cuenta (**Fortaleza, ver numeral 2.6**).

Las "áreas grises" en los procesos se definen como aquellas acciones que no están definidas específicamente en una política, procedimiento o estándar y que de manera indefinida podrían causar ambigüedades en los actos de los empleados.

Las políticas y procedimientos de MM S.A. localmente regulan muchas de las actividades de la compañía, sin embargo, en base a la experiencia obtenida en la realización de este trabajo, siempre existirán situaciones resultantes de dilemas, sin guías y para las cuales muchas veces se toman decisiones basadas en valores y conductas éticas. En este sentido se identificó la necesidad de realizar un mapeo de políticas y procedimientos de toda la compañía en todas sus áreas, iniciativa liderada por el departamento de Contraloría para justamente identificar estas denominadas áreas grises.

En relación a este punto, se ha detectado un aspecto débil para la corporación localmente, ya que muchas de las políticas actuales podrían estar desactualizadas y a su vez podrían no reflejar el entorno actual de la industria como ya se mencionó anteriormente. Además, es posible que existan estándares que no se estén tomando en cuenta por desconocimiento de las partes involucradas en los procesos.

2.1.2 Componente 2: Establecimiento de objetivos

Los objetivos en una organización son determinados a un nivel estratégico, es decir, en lo más alto de la estructura organizacional. A su vez, estos objetivos estratégicos funcionan como una base para los objetivos operativos, de reportaje y compliance que fluyen como una cascada a través de todas las sucursales de la compañía en el mundo. Los objetivos a todo nivel deben estar alineados con el apetito al riesgo, lo que permitirá el establecimiento de niveles de tolerancia para cada objetivo relacionado a la estrategia. En este sentido una compañía deberá establecer sus objetivos de acuerdo a lo que la entidad estará dispuesta a asumir con un enfoque en los riesgos asociados. Pueden existir un sinnúmero de consideraciones para determinar un objetivo de acuerdo a la industria en la que se ubica la compañía en cuestión (Committee of Sponsoring Organizations of the Treadway Commission, 2004).

2.1.2.1 Situación actual del establecimiento de objetivos de MM S.A.

Los objetivos de MM S.A. se establecen por departamento y son revisados de manera anual para mantener dentro de sus necesidades los cambios del mercado y la tecnología (**Fortaleza, ver numeral 2.6**).

En MM S.A. los objetivos de casa matriz son cascadeados a todas sus subsidiarias en todo el mundo y reflejan la misión y visión de la compañía global (**Fortaleza, ver numeral 2.6**). Las subsidiarias toman estos objetivos como los principales del negocio en la localidad y los adapta a su entorno, de manera que se generan nuevos objetivos más específicos para cada área, realizados por cada Director de Área y Unidad. Estos servirán de bases para los funcionarios operativos y no operativos que trabajan en cada área. Es por este motivo que de cierta manera todos los empleados de MM S.A. están alineados con las intenciones de la Directiva de la compañía.

Los objetivos operativos de MM S.A. se enfocan principalmente en: incrementar las ventas, disminuir los gastos promocionales, estar entre las primeras farmacéuticas de preferencia para los médicos, realizar nuevos lanzamientos en el mercado, mantener un stock adecuado de inventario en el mercado, mejorar la distribución de las ventas en el mes, simplificar los procesos financieros, ingresar al cuadro básico de

medicamentos del país, proteger los activos de la compañía, entre muchos otros.

Para los objetivos de reportaje, MM S.A. maneja una serie de informes que se utilizan para fines internos y otros para fines externos. Por ejemplo, se utilizan reportes internos relacionados con la actividad de control interno, índices financieros, demanda, producción, etc. Para fines externos principalmente se utilizan Estados Financieros bajo las normas americanas US GAAP, reportes de planificación (Budget y Forecast), entre otros.

Para MM S.A. la entrega de reportes financieros externos le permite demostrar su desempeño a nivel global, lo que es fundamental para el Comité Ejecutivo en la toma de decisiones. De igual manera, los reportes externos sirven para que la empresa destaque sus logros obtenidos dentro del mercado, la región y el mundo; sin esta información relevante MM S.A. a nivel global no estaría en las condiciones de consolidar su situación económica, ni tomar las decisiones adecuadas acerca de dónde debe invertir para obtener los mejores resultados financieros como uno de los objetivos financieros de reportaje externo. En general estos objetivos estarán definidos por estándares a nivel mundial, políticas financieras corporativas y/o requerimientos legales de presentación de Estados Financieros (**Fortaleza, ver numeral 2.6)**.

En MM S.A. el compliance es uno de los puntos más importantes a ser tomados en cuenta. Como base del compliance está el código de ética y conducta de MM S.A. el cual se debe cumplir de manera íntegra y estricta en todas las áreas. De esta manera, es preciso tomar en cuenta que los objetivos de compliance siempre estarán formando parte de todos los objetivos operativos y de reportaje (**Fortaleza, ver numeral 2.6**).

Debido a que la información acerca de los objetivos generales, estrategias de la compañía y otros objetivos relacionados (operacionales, de reportaje, compliance) a nivel corporativo (todo el mundo) son estrictamente confidenciales, se tomó como punto referencial la misión de MM S.A. a nivel local; como objetivos estratégicos y relacionados los propuestos por el Departamento de Finanzas y el Área de Cuentas por Cobrar para dar un diagnóstico acerca del procedimiento que se utiliza para el establecimiento de objetivos a nivel general. Se tomará únicamente 1 objetivo estratégico y 1 objetivo relacionado como ejemplo de esta sección.

La **misión** de MM S.A. se ha establecido como sigue:

> Brindar productos y servicios innovadores y diferenciados que salven y mejoren vidas, y que satisfagan las necesidades de nuestros clientes, ser reconocidos como un excelente lugar para trabajar, y darles a nuestros inversionistas una tasa de rendimientos superior. (MM S.A., 2014).

Objetivo Estratégico, Estrategia de Dirección Financiera, KPI's, Apetito al Riesgo, Niveles de Tolerancia de Riesgos:

- **Mejoramiento de Procesos y Tecnología:** Presentar una implementación exitosa de la facturación electrónica en MSD Ecuador. Además, mejorar considerablemente el apoyo que brinda Finanzas al área Comercial, automatizando los reportes del área con ayuda de las herramientas corporativas. **Estrategia:** No se mencionan estrategias específicas dentro del sistema de objetivos; sin embargo, se han llevado a cabo las siguientes actividades: El Director Financiero ha dado prioridad del proyecto de facturación electrónica como una de las principales acciones que debe tomar el departamento financiero en 2014. Se han evaluado diferentes alternativas para su implementación oportunamente de acuerdo a los requerimientos tributarios del país y destinando el presupuesto necesario para que se lleve a cabo. Además, se ha entregado todo el apoyo necesario interna y externamente para desarrollar mejores maneras de sintetizar información financiera para la toma acertada de decisiones, esto incluye, soporte externo de terceros especializados en herramientas informáticas de acuerdo al presupuesto destinado. **KPI:** No se menciona un indicador específico para evaluar el nivel de cumplimiento de este objetivo (ej. sobrepasa, cumple, dentro de lo aceptable, no cumplió).

A partir de la estrategia de Dirección Financiera, el área de Cuentas por Cobrar ha diseñado los siguientes objetivos relacionados:

- **Estrategia; Priorización & Simplificación:** Automatización de reportes de ventas para una mejor gestión por parte del área comercial ya sea internamente o con ayuda de terceros externos a la compañía. Fecha de evaluación: Diciembre 2014. **Estrategia:** Actualizar la Política de Crédito, verificar la posibilidad de que un externo asesore a la compañía en la realización de procesos más automatizados, entrega de mantenimiento de files de clientes al centro regional. **Target:** Reporte de estados de cuenta al mes de mayo 2014; reporte de días de cartera con información completa de clientes, facturas, productos y otros; reporte de antigüedad de cartera con datos completos a julio 2014; reporte de ventas institucionales con Nota de Pedido Valorada (ver glosario); reporte de notas de crédito emitidas por el cumplimiento de la política comercial. **KPI:** No se menciona un indicador específico para evaluar el nivel de cumplimiento de este objetivo (ej. sobrepasa, cumple, dentro de lo aceptable, no cumplió). El objetivo no ha sido clasificado como operacional, de reportaje o de compliance.

- **Mejoramiento de Procesos y Tecnología**: Desarrollar proyectos del área que soporten activamente las nuevas necesidades del

negocio con un mayor enfoque en el análisis. Fecha de evaluación: Diciembre 2014. **Target:** Control y recuperación de comprobantes de retención; manejo de files de clientes; implementación de facturación electrónica. **KPI:** No se menciona un indicador específico para evaluar el nivel de cumplimiento de este objetivo (ej. sobrepasa, cumple, dentro de lo aceptable, no cumplió). El objetivo no ha sido clasificado como operacional, de reportaje o de compliance.

De acuerdo a los objetivos y estrategias propuestas en los párrafos anteriores y los analizados en otras áreas se pueden identificar los siguientes factores (**Debilidad, ver numeral 2.6**):

- No se utiliza el mismo idioma de clasificación de objetivos.

- Los objetivos de Cuentas por Cobrar han sido determinados en base a las consideraciones del área, más no fundamentados en las estrategias de Dirección Financiera.

- Los objetivos de ambas partes no tienen KPI´s específicos que permitan establecer niveles de evaluación y cumplimiento de objetivos.

- Las fechas de cumplimiento son muy flexibles y podrían afectar en la planificación para los propósitos propuestos.

- El objetivo estratégico si permite que la compañía pueda alcanzar la misión.

- No se han determinado aspectos específicos en relación al apetito al riesgo aunque de cierta manera las políticas y procedimientos de la compañía si establecen lineamientos claros para determinadas situaciones.

- No es posible determinar niveles de flexibilidad de objetivos si las circunstancias del mercado cambian, es decir, los objetivos resultan ser muy rígidos al no mostrar niveles aceptables de cumplimiento.

- No hay un cuadro formato que una los objetivos de las diferentes áreas que soportan a un negocio para visualizar los diferentes aspectos mencionados.

A pesar de lo antes expuesto se podría decir que los objetivos de cierta manera están alineados unos con otros, es decir, se soportan para su

alcance pero podrían funcionar de mejor manera si se aplican las técnicas mencionadas en el Sistema de Gestión de Riesgos que se ha venido detallando y que se mencionarán en el siguiente capítulo.

2.2 PASO 2 - IDENTIFICACIÓN DE LOS RIESGOS

El componente No. 3, 4 y 5 conforman la sección más crítica del Sistema de Gestión de Riesgos. Para estos componentes existe una gran cantidad de propuestas teóricas ya que se trata de uno de los puntos más complejos e importantes en la administración de riesgos. Es primordial revisar la materia fundamental para entender el propósito de este punto, sin embargo, se va a realizar un muy reducido resumen de cada componente.

2.2.1 Componente 3: Identificación de eventos

La administración de riesgos en una corporación está enfocada en los principios del GRC, como se había mencionado anteriormente el GRC es un concepto que debe estar arraigado dentro de la cultura profesional de una compañía a todo nivel y en todos los procesos. Tomando en cuenta este precepto, existen algunos pasos importantes que se deben realizar para elaborar un Sistema de Gestión de Riesgos que permita a la administración manejarlos de manera favorable y que funcione como un apoyo incondicional en la toma decisiones. El paso 3 de esta sección se puede resumir de la siguiente manera:

Los eventos son incidentes internos o externos a una corporación que podrían afectar al cumplimiento de los objetivos de la misma y a su vez influir dramáticamente en el Sistema de Gestión de Riesgos como tal. Estos eventos pueden tener impactos negativos vistos como riesgos para los cuales la administración debe implementar acciones de mitigación; positivos vistos como oportunidades para los cuales se deben implementar estrategias e incluirlos dentro de objetivos; o ambos. De manera general, una empresa debe estar muy enfocada en monitorear eventos que ocurren en procesos operativos e identificar los factores que causan diferencias en los presupuestos versus el resultado real.

En esta primera sección se deben analizar los riesgos que podrían afectar al negocio en sus distintas funciones y procesos. Debido a que los posibles riesgos podrían ser innumerables es importante que cada proceso se vaya analizando de manera individual en todo su flujo. Esta fase también funciona para nuevos proyectos en los que se esté incursionando y también considera factores externos que podrían no estar controlados por la organización. Se incluye la identificación de factores de riesgo, priorización de factores de riesgo e identificación del perfil de oportunidades de riesgo.

La identificación de riesgos puede ser una tarea bastante compleja de realizar. Básicamente esto se da debido a que muchas de las ocasiones existe incertidumbre en relación a los niveles de ocurrencia e impacto de los riesgos, además, cuando una organización global intenta aplicar un sistema como este, se topa con el obstáculo de los diferentes puntos de vista de los gerentes en todas

las unidades y subunidades de cada sucursal. Para evitar esta complicación se recomienda que se haga un mapeo de todas las unidades y procesos que tiene una organización.

2.2.1.1 Situación actual de la identificación de eventos de MM S.A.

Las diferentes unidades de MM S.A. en Ecuador enfrentan separadas realidades de riesgos que podrían afectar o no a otras unidades. Por ejemplo, un gerente de IT podría estar enfocado a mitigar los riesgos relacionados a los controles de los sistemas con los que trabaja la compañía, mientras que, un gerente de impuestos estará enfocado en reducir los riesgos impositivos a través de los procesos financieros de la compañía. En un nivel más amplio, el Gerente General deberá estar al tanto de los riesgos que se presentan en todas las áreas de manera consolidada. De todas maneras, es importante que las unidades interdependientes de otras, estén informadas acerca de los diferentes riesgos que se presentan en sus procesos y los que se conectan con otras áreas.

La compañía en este sentido no presenta un procedimiento y flujo específico para la identificación de riesgos como tal (**Debilidad, ver numeral 2.6**). Por otro lado, si existe un requerimiento corporativo para que Contraloría reporte los riesgos de ciertas áreas sobre todo en lo relacionado a los procesos que pasan por el Departamento Financiero

pero no existe la metodología para identificarlos (**Fortaleza, ver numeral 2.6**). Además, este reporte entregado a Contraloría Regional es realizado únicamente por una persona, basándose en sus consideraciones de las actividades que se realizan en el proceso correspondiente y no es consultado con los diferentes agentes que actúan en el proceso como indica el sistema propuesto por COSO (**Debilidad, ver numeral 2.6**).

Para identificar eventos adversos, como ya se mencionó anteriormente, la compañía realiza reuniones de Comité Ejecutivo todos los meses para revisar el estatus de situaciones que ocurren en la organización. Sin embargo, esto no incluye personal operativo que en la mayoría de las ocasiones son quienes detectan falencias de control con más exactitud en un proceso (**Debilidad, ver numeral 2.6**); tampoco se realiza una reunión adicional para este propósito. Las novedades de control en los procesos en muchas de las ocasiones salen a la luz porque se producen y no porque existe una estrategia previa para evitar su ocurrencia.

Otro de los mecanismos que se utilizan para identificar riesgos externos es la comunicación continua con las firmas de abogados contratados por la organización. MM S.A. tiene contratos con abogados societarios, laborales y tributarios los cuales mantienen actualizada a la compañía en relación a los distintos cambios en las regulaciones y leyes locales. Aparte de esto, MM S.A. tiene un Departamento Legal Regional que se

encarga de manejar directamente todos los contingentes que tiene la compañía y en este sentido se considera que los riesgos legales y políticos son identificados oportunamente para una correcta toma de decisiones, además de que posee un buen asesoramiento (**Fortaleza, ver numeral 2.6**).

Una última herramienta que se utiliza para la identificación de eventos es la revisión de control interno que se hace tanto a través de auditoría interna corporativa como a través del Departamento de Contraloría y Compliance (**Fortaleza, ver numeral 2.6**). Estas revisiones se hacen cada año por el equipo local de Control Interno (Contraloría), el cual no cuenta con el personal suficiente para manejar dicha actividad en todos los procesos. Tampoco se utilizan asesores externos para evaluar distintas áreas específicas que necesitan otras aptitudes profesionales para ser evaluadas a cabalidad.

Los procesos y procedimientos formalizados en la compañía demuestran su intención para detectar y controlar riesgos pero no han sido documentados como tal. Tampoco se posee un mapa de riesgos por procesos y por áreas de manera que en este sentido MM S.A. no visualiza correctamente los puntos de control necesarios en todas las áreas (**Debilidad, ver numeral 2.6**). Para profundizar aún más, no todas las actividades de la compañía cuentan con procedimientos

formales; muchas de ellas se vienen realizando de la misma manera que en años anteriores (**Debilidad, ver numeral 2.6**).

2.3 PASO 3 - EVALUACIÓN DE LOS RIESGOS

En esta sección básicamente lo que se realiza es una medición de la probabilidad de ocurrencia de los riesgos y su potencial nivel de impacto. Es necesario que una vez identificado el riesgo se propongan estrategias de mitigación de los mismos, de manera que sean manejados o eliminados. En esta sección también se incluye la asignación de valores financieros a los impactos que pueden causar los riesgos, así la compañía puede dimensionar de mejor manera la importancia de un evento asociado al riesgo identificado.

2.3.1 Componente 4: Asesoría del riesgo

El componente 4 del COSO II es descrito como el núcleo del sistema de riesgos, permite a la compañía entender el impacto final que puede resultar de la ocurrencia de un riesgo identificado y su influencia en el cumplimiento de los objetivos establecidos. Los riesgos deben ser analizados bajo dos perspectivas: la probabilidad de ocurrencia y su impacto potencial.

Adicionalmente, es necesario considerar dos tipos de riesgos que se pueden presentar en todas las operaciones de la organización: inherentes y residuales. Los riesgos inherentes han sido definidos por parte de la Oficina de Administración y Presupuesto de lo Estados Unidos como "El potencial para desperdicio, pérdida, uso no autorizado o apropiación indebida debido a la naturaleza de una actividad propia" (Robert R. Moeller- John Wiley & Sons - Citación de Enterprise Risk Management Integrated Framework 2004, 2011)

Tomando otra perspectiva, el COSO II ha definido a los riesgos residuales como "El riesgo para una entidad en la ausencia de cualquier acción que pueda realizar la administración para alterar la probabilidad o impacto del riesgo" (The Comittee of Sponsoring Organizations of the Treadway Commission, 2004, pág. 33).

En resumen, todos los riesgos pueden tener una porción inherente que puede ser asesorada para mitigar su impacto o riesgo (Solo uno o ninguno de los dos) dejando así un riesgo residual que de igual manera podría presentarse para otros riesgos que no presenten esta característica inherente.

Los factores principales que participan en la presencia de riesgos inherentes son: el tamaño del presupuesto de una organización; la fortaleza y el sistema sofisticado de la administración y la propia naturaleza de sus actividades (Robert R. Moeller- John Wiley & Sons - Citación de Enterprise Risk Management Integrated Framework 2004, 2011).

En la otra mano, los riesgos residuales son aquellos que permanecen luego de que se han aplicado mecanismos de control para mitigar riesgos ya identificados. Se considera que siempre permanecerán niveles mínimos de riesgos en casi todas las situaciones (Robert R. Moeller- John Wiley & Sons - Citación de Enterprise Risk Management Integrated Framework 2004, 2011).

2.3.1.1 Situación actual de la asesoría del riesgo de MM S.A.

MM S.A. en Ecuador no presenta una metodología formal para medir los riesgos identificados en cuanto a su probabilidad e impacto. De manera general, el Comité Ejecutivo considera los impactos en reuniones a base de reportes o por casos específicos previamente identificados pero el proceso no es documentado (**Debilidad, ver numeral 2.6**). Posiblemente no exista una organización grande y exitosa que no identifique los impactos monetarios para el establecimiento de estrategias pero el hecho de no documentarlos dificulta la elaboración de evaluaciones más específicas sobre el comportamiento de un proceso. Se podría decir que el área que más considera impactos por variaciones en cifras es Planificación Financiera cuando hace comparaciones del presupuesto versus la ejecución de las estrategias, sin embargo, esas variaciones se dan por ocurrencia de eventos inesperados que se relacionan directamente con la identificación (**Fortaleza, ver numeral 2.6**).

Por otro lado y basándose en lo antes expuesto, probablemente la empresa no prioriza acciones de remediación de manera correcta al no contar con un cuadro que dimensione los riesgos más importantes a ser mitigados, ni tampoco las oportunidades de mejora resultantes de los análisis de identificación de eventos y cuantificación de los mismos.

2.4 PASO 4 – RESPUESTA AL RIESGO

2.4.1 Componente 5: Respuesta al riesgo

Una vez que se han asesorado e identificado los riesgos más significativos en una compañía es momento de determinar las acciones que se llevarán a cabo para mitigarlos. La respuesta al riesgo se fundamenta en las consideraciones que se tomaron acerca de la probabilidad y nivel de impacto para luego analizar el costo y beneficio que traerán estas estrategias de respuesta. La gerencia o dirección debe desarrollar una estrategia general ara responder ante la identificación de eventos ya sean favorables o desfavorables.

2.4.1.1 Situación actual de la respuesta al riesgo de MM S.A.

Las estrategias que MM S.A. utiliza para mitigar riesgos y sus impactos se enmarcan en las políticas y procedimientos corporativos y locales,

así como en las leyes y en el código de conducta (**Fortaleza, ver numeral 2.6**); además, como ya se mencionó anteriormente existen varias actividades que se llevan a cabo en la compañía para identificar riesgos pero no para medirlos.

A pesar de que MM S.A. no esté documentando las estrategias para mitigar riesgos en todos los casos, como se menciona en el COSO II (en base a las 4 categorías de respuesta al riesgo que se verán en la propuesta del capítulo III), es relevante reconocer que la compañía si realiza un análisis detenido para definir estrategias que permitan mitigar los riesgos identificados, basándose en conocimientos técnicos y profesionales de todos sus empleados (**Fortaleza, ver numeral 2.6**).

En este sentido es necesario hacer un paréntesis para aclarar un punto importante. MM S.A. es una de las corporaciones multinacionales más grandes e innovadoras del mundo que tiene prácticas de excelencia muy reconocidas. Sería ilógico considerar que no lleva procesos eficientes de control en sus procesos. El problema radica específicamente en que en Ecuador y otros países de Latinoamérica la compañía no se utiliza un sistema tan elaborado y técnico como se propone en el COSO II y para el cual se han explicado las ventajas que propone. Dentro de las actividades de la compañía existen algunas debilidades que podrían ser mejoradas si se aplica lo propuesto en el capítulo III.

Continuando con la evaluación de la respuesta al riesgo, MM S.A. obtiene sus estrategias de mitigación a través de las siguientes acciones (**Fortaleza, ver numeral 2.6**):

- Reuniones de Comité Ejecutivo

- Análisis de impactos monetarios (Esto se hace generalmente cuando se presenta la oportunidad, es decir, es un análisis que surge de una solicitud más no de un sistema como el mencionado)

- Consultas con abogados

- Consultas corporativas a más alto nivel

- Revisión de políticas corporativas y locales

- Revisión de Código de Conducta

- Objetivos de la compañía a nivel corporativo y local

- Six Sigma en base a eventos históricos

Como ya se detalló antes no existe un formato predeterminado o sistema elaborado para la toma de decisiones en factores más específicos como lo menciona el COSO II. Sin embargo se utilizan reportes y otros tipos de análisis que podrían o no estar disponibles en el momento que se identifica el problema (**Debilidad, ver numeral 2.6**).

Además, al no presentarse una correcta definición de objetivos, apetito al riesgo y portafolio de riesgos con niveles de ocurrencia e impacto, la compañía no está en las posibilidades de ligar las estrategias con los objetivos de la organización o determinar consistentemente que los riesgos serán mitigados con las estrategias propuestas (**Debilidad, ver numeral 2.6**).

Los documentos que apoyan a la implementación de una estrategia en MM S.A. son (**Fortaleza, ver numeral 2.6**):

- Elaboración de nuevas políticas y procedimientos

- Contratos con proveedores y empleados

- Comunicados internos con instrucciones específicas

- Memos

- Informes de control interno o compliance

- Otros

Cabe recalcar que esto no está definido en un documento, procedimiento o política.

2.5 PASO 5 – CONTROL DE RIESGOS

Para monitorear la gestión realizada en la mitigación de los riesgos, es necesario llevar una serie de indicadores que deben ser identificados dentro de cada proceso. De esta manera, es posible hacer una evaluación del funcionamiento de las estrategias propuestas y de ser necesario se deberán llevar a cabo los anteriores pasos reconsiderando cualquier factor que haya quedado desapercibido en la revisión inicial.

2.5.1 Componente 6: Actividades de control

Las actividades de control comprenden las políticas y procedimientos necesarios para asegurar que las respuestas a los riesgos aprobadas son implementadas correctamente. Para lo cual una organización puede tomar varias acciones dependiendo del proceso y nivel jerárquico.

Una vez que se han realizado los pasos anteriores, una organización debe seleccionar diversas formas de control para asegurar que las respuestas al riesgo se estén llevando a cabo en tiempo y forma. Los controles deben ser aplicados por todos los funcionarios de la organización de acuerdo a sus procesos relacionados (Silva, 2013). En este sentido, se deben definir puntos de control a ser verificados por diferentes empleados dentro del área operativa como también a nivel de supervisión.

2.5.1.1 Situación actual de las actividades de control de MM S.A.

MM S.A. utiliza una práctica corporativa para controlar procesos o estrategias ya establecidas, reguladas por políticas y procedimientos. Este se llama Selfassessment of Internal Controls y básicamente lo que se hace es un control de los controles de los procesos (**Fortaleza, ver numeral 2.6**). Si bien es cierto en secciones anteriores se mencionó que muchas personas de la compañía no estaban al tanto de los controles

que se mantienen en cada proceso, las políticas y procedimientos para cada área mencionan algunos lineamientos (no todos) que deben ser controlados.

En casos puntuales se ha identificado que MM S.A. no utiliza indicadores específicos de control mensual o trimestral para todos los procesos, se usan los que se consideran más importantes (**Debilidad, ver numeral 2.6**). Sin embargo, cada semestre el Departamento Financiero realiza una reunión para revisar los diferentes indicadores de la compañía relacionados a la materia. Por ejemplo, gastos administrativos, de ventas, promocionales, liquidez, prueba ácida, retorno sobre la inversión, rentabilidad operativa y neta, peso de devoluciones sobre ventas. Con estas revisiones se establecen estrategias para evitar riesgo y aprovechar oportunidades de mejora (**Fortaleza, ver numeral 2.6**).

En cuanto a actividades de control para las respuestas al riesgo, MM S.A. no establece mecanismos inmediatos para estas estrategias; de manera general, estos son definidos posteriormente por las áreas participantes sin comunicar a un Equipo de Riesgos, no se asignan responsables en todos los casos y no se documentan. Es decir, se establecen indefinidamente para unas estrategias y para otras no. Además, no hay un departamento o función que compendie y verifique que se estén llevando a cabo las acciones correctas. Falta definición

formal y procedimiento para esta actividad (**Debilidad, ver numeral 2.6**).

Por otro lado, la compañía ha desarrollado un nuevo sistema que contiene las bases de datos de casi todos los archivos que maneja el sistema contable. Este nuevo sistema es bastante flexible y puede ser de mucha utilidad para la organización. Para indicadores de gestión para otras áreas de información no contable, la compañía mantiene contratos con diferentes proveedores nacionales e internacionales que proveen de estos datos muy relevantes para la gestión (**Fortaleza, ver numeral 2.6**).

A pesar de lo antes mencionado, la compañía no tiene asignados indicadores a personas específicas encargadas del control para cada área. Por lo tanto, el Selfassessment de Control Interno tampoco ha definido qué indicadores seleccionar para realizar sus controles (**Debilidad, ver numeral 2.6**).

Profundizando un poco más acerca de las funciones del Selfassessment de Control Interno, en la actualidad se están diseñando formatos de control para cada proceso en base a los flujos, políticas y procedimientos relacionados para verificar los puntos de control claves en el negocio. Este es un trabajo extenso que se viene realizando desde el 2013 y se ha propuesto ser finalizado hasta el primer semestre del

2015. Además, muchas áreas como Planning y Cuentas por Cobrar han desarrollado en este año nuevos reportes necesarios para la gestión del negocio con el fin de soportar adecuadamente las decisiones de la gerencia (**Fortaleza, ver numeral 2.6**).

Otra falencia de control identificada en este componente es que no se han documentado en un portafolio todas las observaciones de control resultantes de los Selfassessments, por lo que se podría decir que no se está haciendo un seguimiento adecuado de las observaciones y las estrategias de mitigación de eventos adversos (**Debilidad, ver numeral 2.6**).

Hasta esta parte finaliza lo relacionado al Diagnóstico del Sistema de Gestión de Riesgos en MM S.A. Se hicieron encuestas e investigaciones en las herramientas informáticas de la compañía tomando en cuenta todas sus prácticas para cada punto en base a la información que fue posible extraer para ser incluida en este trabajo. Los componentes 7 y 8 del COSO II serán analizados en el siguiente capítulo como ya se recalcó en los primeros párrafos. A continuación se adjunta un cuadro resumen de las debilidades encontradas en el Sistema de Gestión de Riesgos de MM S.A.

2.6 CUADRO RESUMEN DE GUÍAS, DEBILIDADES Y FORTALEZAS DEL SISTEMA DE GESTIÓN DE RIESGOS DE MM S.A.

2.1.1 Ambiente Interno				
Situación actual de la filosofía del manejo de riesgos en MM S.A.				
No.	**Debilidades**	**Pág. Deb.**	**Fortalezas**	**Pág. Fort.**
2.1.1.1.1/3.1.1.1	Políticas y procedimientos no contienen consideraciones expresas del riesgo y en otros casos tampoco mencionan el motivo por el cual los controles se llevan a cabo.	Pág. 38	N/A	N/A
	Integrantes de los procesos no tienen una visión clara del control (puntos de control) y se considera que ésta es una función única del área de Contraloría.	Pág. 39	N/A	N/A
	Empleados no conocen todas las políticas y procedimientos que influyen en sus procesos.	Pág. 40	N/A	N/A
	El Departamento de Contraloría que se encarga del control interno no tiene conocimiento preciso de todas las políticas y procedimientos locales existentes y tampoco se muestra en estándar para desarrollarlos. Aparte, no se definen de manera específica puntos de control claves.	Pág. 41	N/A	N/A
	No se presenta una política local de control interno o Sistema de Gestión de Riesgos.	Pág. 41	N/A	N/A
	Procedimientos formales no contienen diagramas de flujos.	Pág. 42	N/A	N/A
Situación actual del apetito al riesgo de MM S.A.				
No.	**Debilidades**	**Pág. Deb.**	**Fortalezas**	**Pág. Fort.**
2.1.1.2.1/3.1.1.2	MM S.A. no presenta un conocimiento escrito, documentado o formalizado de los niveles de riesgo que se aceptan en sus procesos.	Pág. 44	N/A	N/A

Situación actual de la actitud de la Junta Directiva de MM S.A., estrategia y organización.				
No.	**Debilidades**	**Pág. Deb.**	**Fortalezas**	**Pág. Fort.**
2.1.1.3.1/3.1.1.3	MM S.A. en la localidad no cuenta con un Comité de Auditoría o de Riesgos. Estas funciones las asume de manera parcial el Área de Contraloría. Las funciones como comité se realizan de manera parcial debido a que el Área de Contraloría no reporta ni cuestiona asuntos de control directamente con el Comité Ejecutivo mencionado anteriormente y en pocas ocasiones forma parte de la elaboración de nuevos modelos y estrategias de negocio que se proponen en la compañía.	Pág. 47	Cada sucursal de MM S.A. cuenta con su propio Comité Ejecutivo que podría ser considerado como el Consejo de Administración, mismo que se reúne constantemente para revisar las condiciones del negocio dentro del país.	Pág. 46
	El Área de Contraloría no cuenta con ayuda externa para realizar revisiones de control o aseguramiento de gestión de riesgos.	Pág. 48	El Departamento de Auditoría Interna Corporativa realiza revisiones generales de los procesos más importantes en cada país.	Pág. 48
	La revisión de Auditoría Interna Corporativa se hace cada dos años aproximadamente y no incluye todos los procesos que se manejan localmente, además, se fundamenta en la detección de eventos en base a guías corporativas y que en algunos casos no se ajustan a las actividades locales que se realizan en la sucursal.	Pág. 48	Otras de las estrategias que utiliza el Departamento de Contraloría para detectar riesgos es un selfassessment de los procesos financieros más importantes como parte del control interno.	Pág. 49
	El selfassessment se basa en lineamientos corporativos diseñados para un sistema contable distinto al que utiliza la sucursal en Ecuador.	Pág. 49		

No.	Debilidades	Pág. Deb.	Fortalezas	Pág. Fort.
2.1.1.3.1/3.1.1.3	No existe un procedimiento estandarizado para las revisiones de control interno que realiza Contraloría con los puntos más importantes en cada proceso, se identificó que para ciertas observaciones no se realiza un seguimiento específico posterior.	Pág. 49	Se emiten informes de las revisiones de Auditoría Interna Corporativa y revisiones locales del Área de Contraloría que se comunican al Comité Ejecutivo.	Pág. 49
Situación actual de la integridad y valores éticos de MM S.A.				
No.	**Debilidades**	**Pág. Deb.**	**Fortalezas**	**Pág. Fort.**
2.1.1.4.1	N/A	N/A	A nivel general, el código de conducta de MM S.A. está completamente compuesto de todos los puntos necesarios tal y como lo menciona el COSO II. Además, MM S.A. cuenta con una Pirámide de Políticas que resalta los estándares generales y específicos como guía para las actividades de la compañía.	Pág. 54-58

No.	Debilidades	Pág. Deb.	Fortalezas	Pág. Fort.
2.1.1.4.1	N/A	N/A	MM S.A. cuenta con un robusto sistema tecnológico de entrenamientos online que permiten certificar a todos los empleados en el conocimiento de valores éticos y conductas de comportamiento necesarios para el cumplimiento de objetivos de manera ética. Por otro lado, existe un departamento que se enfoca específicamente en la recepción y procesamiento de quejas por prácticas incorrectas que se pueden presentar en la industria en sus múltiples áreas.	Pág. 58
Situación actual del compromiso con la competencia de MM S.A.				
No.	**Debilidades**	**Pág. Deb.**	**Fortalezas**	**Pág. Fort.**
2.1.1.5.1/2.1.2.1	Los proyectos pequeños que se llevan a cabo en MM S.A. en ocasiones no se materializan y se podría considerar que se necesitan mayores acciones para que todos los proyectos independientemente de su tamaño puedan cumplir con su propósito.	Pág. 61	Las estrategias para implementar proyectos nuevos o para aprovechar oportunidades identificadas en el mercado son revisadas minuciosamente por MM S.A. antes de ser llevadas a cabo. Se llevan cronogramas y se asignan responsables para cada punto.	Pág. 60

No.	Debilidades	Pág. Deb.	Fortalezas	Pág. Fort.
2.1.1.5.1/2.1.2.1	N/A	N/A	MM S.A. presenta una herramienta informática corporativa que ayuda a alinear los objetivos estratégicos y relacionados en todas las sucursales y áreas.	Pág. 61
	El seguimiento para el cumplimiento de objetivos lo debe manejar cada empleado con ayuda de su supervisor sin un cronograma establecido o indicadores específicos para su monitoreo. En ocasiones esto podría provocar el incumplimiento de algunos objetivos o que sean llevados a cabo a último momento, antes que finalice el año. Esto afecta a la competencia profesional que se maneja a nivel gerencial para el cumplimiento de objetivos más específicos.	Pág. 61	Los proyectos grandes (objetivos prioritarios) son monitoreados constantemente para que se lleven a cabo, con minutas, reuniones, cronogramas y responsables.	Pág. 62
			A nivel de Recursos Humanos en MM S.A. se manejan descripciones específicas para cada puesto de trabajo, así como también, se han identificado los conocimientos y habilidades necesarias para ejercer una determinada función. Estas características son comunicadas detalladamente a una consultora externa que se encarga de la selección del personal avalada por diferentes estándares reconocidos a nivel nacional.	Pág. 62

Situación actual de la estructura organizacional de MM S.A.				
No.	**Debilidades**	**Pág. Deb.**	**Fortalezas**	**Pág. Fort.**
2.1.1.6.1/3.1.1.3	No se presenta una estructura sistemática específica para administrar un Sistema de Gestión de Riesgos de manera adecuada, el enfoque está más centrado en el control interno. Es necesario establecer un Departamento de Riesgos dentro de la sucursal que permita una mejor coordinación de las actividades de control basada en riesgos.	Pág. 65	El Área Comercial cuenta con un Oficial de Compliance que enfoca su trabajo en asegurar el cumplimiento de las políticas y procedimientos del área Comercial, reporta Directamente al Director General de MM S.A. en Ecuador. También participa en reuniones del Comité Ejecutivo para certificar que las nuevas actividades y proyectos que surjan en la organización estén dentro de los lineamientos de la compañía.	Pág. 66
	El Oficial de Compliance no realiza actividades relacionadas a gestión de riesgos, únicamente identifica asuntos de control en las estrategias comerciales, así como también asesora a los distintos departamentos de la compañía en temas relacionados a compliance.	Pág. 66		
	Contraloría y Compliance trabajan de manera separada, ciertas revisiones de control que realiza Compliance son comunicadas a Contraloría pero esto no se da en sentido contrario. Además, se ha detectado que no existe una comunicación adecuada entre las dos áreas y hay una poca coordinación para las actividades de control en conjunto.	Pág. 66	Para reportar hallazgos de control el Departamento de Contraloría emite informes de los procesos revisados durante todo el año que son entregados en primera instancia al Director Financiero para que los comunique al Comité Ejecutivo en sus reuniones mensuales.	Pág. 67

No.	Debilidades	Pág. Deb.	Fortalezas	Pág. Fort.
2.1.1.6.1/3.1.1.3	La compañía carece de un procedimiento de control definido para que las dos áreas utilicen sistemas estándar de revisión que estén certificadas, de esta manera, las revisiones de control podrían no abarcar los puntos necesarios para mitigar riesgos que estén de acuerdo a las necesidades del negocio.	Pág. 67	N/A	N/A
	Los informes de control emitidos por Compliance no son comunicados al Área de Contraloría, tampoco (de manera general) las decisiones de los informes entregados por las dos áreas.	Pág. 67	N/A	N/A
	El alcance de las revisiones que realiza Contraloría está limitado a procesos Financieros.	Pág. 68	N/A	N/A
Situación actual de la designación de autoridad y responsabilidad de MM S.A.				
No.	**Debilidades**	**Pág. Deb.**	**Fortalezas**	**Pág. Fort.**
2.1.1.7.1	N/A	N/A	MM S.A. tiene bien definidos sus niveles de autoridad y las maneras de delegarlos (GOA), el mismo que se encuentra detallado específicamente en un documento formalizado emitido por Casa Matriz en el cual constan las firmas del Presidente y Vicepresidente Ejecutivo de la compañía. Esta normativa cae como cascada en todas las sucursales de la compañía alrededor del mundo.	Pág. 70

No.	Debilidades	Pág. Deb.	Fortalezas	Pág. Fort.
2.1.1.7.1	N/A	N/A	El GOA define que un Supervisor inmediato directo siempre deberá tener un GOA superior al de su subordinado y que siempre exista el consentimiento del Supervisor para cualquier transacción.	Pág. 70
Situación actual de los estándares de recursos humanos de MM S.A.				
No.	**Debilidades**	**Pág. Deb.**	**Fortalezas**	**Pág. Fort.**
2.1.1.8.1/3.1.1.1/3.1.1.3	MM S.A. en la localidad no cuenta con procedimientos formalizados para recursos humanos.	Pág. 72	MM S.A. tiene una política corporativa para el Área de Recursos Humanos la cual determina que se deben realizar investigaciones previas de los empleados contratados, así como también revisiones posteriores en cuanto a las condiciones legales y éticas alrededor de mundo, utilizando un sistema que tiene una interface con la base de datos de diferentes instituciones de control en los Estados Unidos de América y otros países de relevancia en el mundo.	Pág. 72

No.	Debilidades	Pág. Deb.	Fortalezas	Pág. Fort.
2.1.1.8.1/3.1.1.1/3.1.1.3	N/A	N/A	MM S.A. utiliza a un tercero reconocido en el medio para la contratación garantizada de profesionales competentes para una función vacante.	Pág. 72
	No se realizan entrenamientos semestrales o anuales para refrescamiento de políticas y procedimientos locales en la mayoría de los casos.	Pág. 73	En relación a las actividades de entrenamiento para el conocimiento de políticas y procedimientos, MM S.A. tiene un sofisticado sistema de entrenamiento continuo a través de intranet.	Pág. 72
			Cuando ingresan nuevos empleados a la compañía se realizan entrenamientos para el conocimiento de procesos importantes de la corporación pero el Área de Recursos Humanos no conoce específicamente si todos los procesos fundamentales han sido tomados en cuenta.	Pág. 73

2.1.2 Establecimiento de Objetivos				
No.	**Debilidades**	**Pág. Deb.**	**Fortalezas**	**Pág. Fort.**
2.1.2.1	Se identificaron las siguientes debilidades en los objetivos estratégicos y relacionados de MM S.A.: • No se utiliza el mismo idioma de clasificación de objetivos. • Los objetivos en ciertos casos son determinados en base a las consideraciones del área, más no fundamentados en las estrategias de Dirección. • Los objetivos en general no tienen KPI´s específicos que permitan establecer niveles de evaluación y cumplimiento de objetivos. • Las fechas de cumplimiento son muy flexibles y podrían afectar en la planificación para los propósitos propuestos. • El objetivo estratégico si permite que la compañía pueda alcanzar la misión general. • No se han determinado aspectos específicos en relación al apetito al riesgo aunque de cierta manera las políticas y procedimientos de la compañía si establecen lineamientos claros para determinadas situaciones. • No es posible determinar niveles de flexibilidad de objetivos si las circunstancias del mercado cambian. • No hay un cuadro formato que una los objetivos de las diferentes áreas que soportan a un negocio para visualizar los diferentes aspectos mencionados.	Pág. 77-80	Los objetivos de MM S.A. se establecen por departamento y son revisados de manera anual para mantener dentro de sus necesidades los cambios del mercado y la tecnología.	Pág. 75
			En MM S.A. los objetivos de casa matriz son cascadeados a todas sus subsidiarias en todo el mundo y reflejan la misión y visión de la compañía global.	Pág. 75
			MM S.A. elabora varios objetivos relacionados a operación, reportaje y compliance.	Pág. 75, 76
			En MM S.A. los objetivos de compliance forman parte de todos los objetivos operativos y de reportaje.	Pág. 77

2.2.1 Identificación de Eventos				
No.	**Debilidades**	**Pág. Deb.**	**Fortalezas**	**Pág. Fort.**
2.2.1.1/3.2.1	La compañía no presenta un procedimiento y flujo específico para la identificación de riesgos. Los eventos son identificados cuando se producen.	Pág. 84	Corporativamente MM S.A. reporta los riesgos asociados a la sucursal en Ecuador, sin embargo no existe un procedimiento formal para identificarlos.	Pág. 85
	El reporte de riesgos entregado a Contraloría Regional es realizado únicamente por una persona, basándose en sus consideraciones de las actividades que se realizan en el proceso correspondiente y no es consultado con los diferentes agentes que actúan en el proceso.	Pág. 85		
	No se incluye a personal operativo dentro de las reuniones de Comité Ejecutivo para identificación de eventos; tampoco se realiza una reunión adicional para este propósito.	Pág. 85	MM S.A. se asesora de abogados societarios, laborales y tributarios los cuales mantienen actualizada a la compañía en relación a los distintos cambios en las regulaciones y leyes locales. Aparte de esto, MM S.A. tiene un Departamento Legal Regional que se encarga de manejar directamente todos los contingentes que tiene la compañía y en este sentido se considera que los riesgos legales y políticos son identificados oportunamente para una correcta toma de decisiones.	Pág. 86

No.	Debilidades	Pág. Deb.	Fortalezas	Pág. Fort.
2.2.1.1/3.2.1	Los riesgos identificados no son documentados. Tampoco se posee un mapa de riesgos por procesos y por áreas de manera que en este sentido MM S.A. no visualiza correctamente los puntos de control necesarios en todas las áreas.	Pág. 86	Se realizan revisiones de auditoría interna corporativa y selfassessments para identificación de eventos.	Pág. 86
	No todas las actividades de la compañía cuentan con procedimientos formales; muchas de ellas se vienen realizando de la misma manera que en años anteriores.	Pág. 87		
2.3.1 Asesoría de riesgos				
No.	**Debilidades**	**Pág. Deb.**	**Fortalezas**	**Pág. Fort.**
2.3.1.1/3.3.1	MM S.A. en Ecuador no presenta una metodología formal para medir los riesgos identificados en cuanto a su probabilidad e impacto. De manera general, el Comité Ejecutivo considera los impactos en reuniones a base de reportes o por casos específicos previamente identificados pero el proceso no es documentado.	Pág. 89	El Área de Planificación Financiera realiza comparaciones de presupuesto versus ejecución real para identificar brechas, sin embargo, esas variaciones se dan por ocurrencia de eventos inesperados que se relacionan directamente con la identificación.	Pág. 89
2.4.1 Respuesta al riesgo				
No.	**Debilidades**	**Pág. Deb.**	**Fortalezas**	**Pág. Fort.**
2.4.1.1/3.4.1	No existe un formato predeterminado, política o sistema elaborado para la toma de decisiones en factores más específicos como lo menciona el COSO II. Sin embargo se utilizan reportes y otros tipos de análisis que podrían o no estar disponibles en el momento que se identifica el problema.	Pág. 93	Las estrategias que MM S.A. utiliza para mitigar riesgos y sus impactos se enmarcan en las políticas y procedimientos corporativos y locales, así como en las leyes y el código de conducta.	Pág. 91

No.	Debilidades	Pág. Deb.	Fortalezas	Pág. Fort.
2.4.1.1/3.4.1	N/A	N/A	La compañía realiza un análisis detenido en ocasiones no documentado para definir estrategias que permitan mitigar los riesgos identificados, basándose en conocimientos técnicos y profesionales de todos sus empleados.	Pág. 91
			MM S.A. obtiene sus estrategias de mitigación a través de las siguientes acciones: Reuniones de Comité Ejecutivo; Análisis de impactos monetarios (Esto se hace generalmente cuando se presenta la oportunidad, es decir, es un análisis que surge de una solicitud más no de un sistema como el mencionado); Consultas con abogados; Consultas corporativas a más alto nivel; Revisión de políticas corporativas y locales; Revisión de Código de Conducta; Objetivos de la compañía a nivel corporativo.	Pág. 92

No.	Debilidades	Pág. Deb.	Fortalezas	Pág. Fort.
2.4.1.1/3.4.1	Al no presentarse una correcta definición de objetivos, apetito al riesgo y portafolio de riesgos con niveles de ocurrencia e impacto, la compañía no está en las posibilidades de ligar las estrategias con los objetivos de la organización o determinar consistentemente que los riesgos serán mitigados con las estrategias propuestas.	Pág. 93	Los documentos que apoyan a la implementación de una estrategia en MM S.A. son: • Elaboración de nuevas políticas y procedimientos • Contratos con proveedores y empleados • Comunicados internos con instrucciones específicas • Memos • Informes de control interno o compliance • Otros	Pág. 93
2.5.1 Actividades de control				
No.	**Debilidades**	**Pág. Deb.**	**Fortalezas**	**Pág. Fort.**
2.5.1.1/3.5.1	En casos puntuales se ha identificado que MM S.A. no utiliza indicadores específicos de control mensual o trimestral para todos los procesos, se usan los que se consideran más importantes.	Pág. 96	MM S.A. utiliza una práctica corporativa para controlar procesos o estrategias ya establecidas, reguladas por políticas y procedimientos. Este se llama Selfassessment of Internal Controls y básicamente lo que se hace es un control de los controles de los procesos.	Pág. 95

No.	Debilidades	Pág. Deb.	Fortalezas	Pág. Fort.
2.5.1.1/3.5.1	En cuanto a actividades de control para las respuestas al riesgo, MM S.A. no establece mecanismos inmediatos para el control de estas estrategias; de manera general, son definidos posteriormente por las áreas participantes sin comunicar a un Equipo de Riesgos, no se asignan responsables en todos los casos y no se documentan. Es decir, se establecen indefinidamente para unas estrategias y para otras no. Además, no hay un departamento o función que compendie y verifique que se estén llevando a cabo las acciones correctas. Falta definición formal y procedimiento para esta actividad.	Pág. 97	Cada semestre el Departamento Financiero realiza una reunión para revisar los diferentes indicadores de la compañía relacionados al área donde se identifican riesgos y oportunidades de mejora.	Pág. 96
			La compañía ha desarrollado un nuevo sistema que contiene las bases de datos de casi todos los archivos que maneja el sistema contable. Este nuevo sistema es bastante flexible y puede ser de mucha utilidad para la organización. Para indicadores de gestión para otras áreas de información no contable, la compañía mantiene contratos con diferentes proveedores nacionales e internacionales que proveen de estos datos muy relevantes para la gestión.	Pág. 97

No.	Debilidades	Pág. Deb.	Fortalezas	Pág. Fort.
2.5.1.1/3.5.1	En algunos casos el área que realiza el Selfassessment de Control Interno no ha definido los indicadores a revisar a falta de una definición formal por parte de los integrantes del área involucrada.	Pág. 97	En la actualidad se están diseñando formatos de control para cada proceso en base a los flujos, políticas y procedimientos relacionados para verificar los puntos de control claves en el negocio. Este es un trabajo extenso que se viene realizando desde el 2013 y se ha propuesto ser finalizado hasta el primer semestre del 2015. Además, muchas áreas como Planning y Cuentas por Cobrar han desarrollado en este año nuevos reportes necesarios para la gestión del negocio con el fin de soportar adecuadamente las decisiones de la gerencia.	Pág. 98
	Otra falencia de control identificada en este componente es que no se han documentado en un portafolio todas las observaciones de control resultantes de los Selfassessments, por lo que se podría decir que no se está haciendo un seguimiento adecuado de las observaciones y las estrategias de mitigación de eventos adversos.	Pág. 98		
3.6.1 Información y Comunicación				
No.	**Debilidades**	**Pág. Deb.**	**Fortalezas**	**Pág. Fort.**
3.6.1			MM S.A. cuenta con un sistema en intranet para reportar actividades de control y procedimientos existentes en el mercado que será aplicado en 2015.	

3. CAPÍTULO III: PROPUESTA DEL SISTEMA DE GESTIÓN DE RIESGOS EN MM S.A.

Este capítulo se fundamenta principalmente en las estrategias de gestión de riesgos empresariales detalladas en el Enterprise Risk Management Integrated Framework elaborado por COSO y en las aplicaciones prácticas del mismo documento. El punto de partida para el contenido de este capítulo es el diagnóstico que se realizó para cada una de los pasos del Sistema de Gestión de Riesgos en conjunto con los componentes del COSO II.

3.1 PASO 1 – ESTRUCTURACIÓN DE LA GESTIÓN DE RIESGOS

3.1.1 Componente 1: Ambiente interno

Dentro del componente de ambiente interno se detallan a continuación actividades recomendadas a MM S.A. para evaluar y mejorar sus prácticas que se requieren para gestionar correctamente los riesgos.

3.1.1.1 Filosofía del manejo de riesgos

Se recomienda que MM S.A. mencione en sus comunicados, políticas y procedimientos a la importancia de la detección de riesgos en los procesos de la compañía. La Filosofía del Riesgo puede ser reforzada implementando una campaña de concienciación sobre el tema dirigida a toda la compañía con pequeños comunicados que pueden ser e-mails, mensajes de texto o reuniones presenciales. Estos deben funcionar como recordatorios por un cierto periodo de tiempo (puede ser tres meses) con tips de control y conceptos claves relacionados a riesgos.

Para los responsables del control en cada proceso este reforzamiento debe ser aún mayor asignando tareas como por ejemplo, repasos de políticas y procedimientos ya existentes, reportes de eventos adversos identificados en el día a día, identificación de "áreas grises" en los procesos involucrados, asignación de responsabilidades a manejar al ser responsable del control en un punto del proceso, importancia del control en el proceso, certificado de conocimiento de las políticas e indicadores y las que se consideren necesarias. Es muy relevante recalcar el hecho de que cada empleado de la compañía debe efectuar un control en sus actividades, no solo del trabajo sino también en la vida cotidiana **(Propuesta, ver numeral 3.8)**.

La filosofía del riesgo como parte del componente No.1 del COSO II está compuesto por los siguientes atributos adicionales que se deben tomar en cuenta por parte de MM S.A. para identificar si una compañía tiene la filosofía del riesgo correctamente definida en sus integrantes (The Comittee of Sponsoring Organizations of the Treadway Commission, 2004):

- **Liderazgo y Estrategia:** Se enfoca en demostrar ética y valores; comunicar la visión y los objetivos.

- **Gente y Comunicación:** Que menciona el compromiso con la competencia en relación a los compañeros de trabajo; compartir la información y el conocimiento.

- **Responsabilidad y Reforzamiento:** Estructura organizacional; medición de rendimiento e incentivos.

- **Manejo del Riesgo e Infraestructura:** Asesorar y medir el riesgo; accesos al sistema y seguridad.

MM S.A. deberá utilizar una encuesta muy sencilla para ubicar puntos en los atributos mencionados que necesiten de un mayor refuerzo para contar con un ambiente interno favorable y alineado a la filosofía del

riesgo. La **Figura 3.1** muestra el cuestionario que se propone en el COSO II **(Propuesta, ver numeral 3.8)**:

Figura 3.1: Cuestionario de Evaluación de Filosofía del Manejo de Riesgos

No.	Pregunta	Atributos	Rango Promedio		Des. Stand.	Conteo	Tot. de acuerdo	De acuerdo	Neutral	Desacuerdo	Tot. Desacuerdo
1	Los líderes de mi unidad son ejemplo positivo de conducta ética	Liderazgo y Estrategia	1.42	Fuerte	0.71	186	1	3	9	77	96
2	Entiendo la misión y estrategia de la compañía	Liderazgo y Estrategia	1.05	Bueno	0.69	186	0	7	18	119	42
3	Se toman acciones disciplinarias para conductas no apropiadas	Responsabilidad y Reforzamiento	0.21	Necesita Acción	1.20	175	11	55	18	68	23
4	La rotación de personal no ha afectado de manera significativa nuestra habilidad para alcanzar objetivos	Gente y Comunicación	0.81	Precaución	0.88	145	4	3	39	69	30
5	Los líderes de mi unidad de negocio son receptivos a cualquier comunicación acerca de riesgos, incluyendo malas noticias	Manejo del Riesgo e Infraestructura	0.99	Bueno	0.85	183	2	13	16	106	46

Tiene 5 preguntas que deberán ser respondidas por una muestra importante de la compañía y que debe ser realizada al menos una vez al año. Las preguntas son las siguientes:

- ¿Los líderes de mi unidad dan un ejemplo positivo de conducta ética?

- ¿Entiendo la visión general de la compañía y la estrategia?

- ¿Se toman acciones disciplinarias cuando se han detectado conductas profesionales inadecuadas de los empleados?

- ¿La salida del personal no ha afectado de manera significativa nuestra habilidad de alcanzar objetivos?
- ¿Los líderes de mi unidad de negocios son receptivos a cualquier comunicación relacionada a riesgos identificados, aun si se trata de malas noticias?

Las respuestas deben ser calificadas de +2 a -2 considerando que, +2 es totalmente de acuerdo, +1 de acuerdo, 0 neutral o desconocimiento, -1 desacuerdo y -2 totalmente en desacuerdo. Como se muestra en el cuadro existen dos medidas que permiten tener una visión de lo que está ocurriendo, una es el promedio de los resultados obtenidos y otra es la desviación estándar. Para el promedio, de -2 a 0,8 se necesita atención inmediata; de 0,8 a 0,95 se necesita tener precaución, de 0,95 a 1,2 se considera bueno y de 1,2 a 2 se considera una fortaleza. La desviación estándar permite ver el nivel de consenso del resultado obtenido, relacionado al promedio (The Comittee of Sponsoring Organizations of the Treadway Commission, 2004).

Con los resultados obtenidos se pueden establecer medidas de remediación para reforzar la filosofía del riesgo basándose en los atributos mencionados. Para un mayor detalle de qué quieren decir cada

uno de los atributos se recomienda revisar la materia teórica en el ERM Integrated Framework.

Regresando al tema del establecimiento de **políticas** y procedimientos, se recomienda a MM S.A. que realice un inventario total de todos los documentos que reflejen lineamientos para las actividades de los empleados en la compañía. Adicionalmente, se deberán archivar los mencionados papeles dentro del Área de Contraloría, considerada en este trabajo como el equipo ERM. Como segundo paso se debe identificar la validez de dichos documentos y relacionarlos con las políticas corporativas a las que hacen mención o se fundamentan. Posterior a esto, se debe analizar cada documento con las áreas correspondientes para identificar actualizaciones u oportunidades de mejora (inclusión de flujos) y actualizar las políticas que deberán ser firmadas por las autoridades competentes **(Propuesta, ver numeral 3.8)**.

Como otra actividad relacionada al mapeo de políticas y procedimientos, es necesario que el equipo de ERM elabore un documento que norme y describa los nuevos procedimientos a realizarse en base a los puntos contenidos en este capítulo, para lo cual se debe contar con asesoría del Director de Riesgos en este caso Dirección Financiera y otro documento para las revisiones de Selfassessments de Controles Internos como ya se verá en párrafos

posteriores. Este documento deberá contener como mínimo los siguientes aspectos **(Propuesta, ver numeral 3.8)**:

- Nombre del documento
- Tipo de Documento
- Vigencia
- Fecha de nueva revisión
- Alcance
- Glosario de términos
- Objetivo del Sistema de Riesgos
- Fundamentos
- Políticas corporativas relacionadas

- Responsables

- Lineamientos

- Diagramas de flujo

Para que estas políticas y procedimientos tengan una correcta validez en una compañía es imperante que sean documentados y firmados por las autoridades pertinentes. Estos dos elementos son los brazos a través de los cuales se realiza el control interno y a su vez éstos componen la columna vertebral de una organización. La afectividad del control interno estará dada por cuán sumergido se encuentre este concepto en las actividades "core" del negocio.

3.1.1.2 Apetito al riesgo

Para este punto se ha sugerido a MM S.A. que se tome en cuenta los siguientes pasos para determinar sus niveles aceptables de riesgo en todos sus procesos (Committee of Sponsoring Organizations of the Treadway Commission, 2012, pág. 8) **(Propuesta, ver numeral 3.8)**:

- Desarrollar su apetito al riesgo, en este sentido no es correcto evitar incurrir en riesgos ya que la estrategia podría ser muy conservadora y con bajos resultados. No existe un estándar para determinación del apetito al riesgo en el mundo, para esto MM S.A. debe definirlo de acuerdo a sus necesidades y estructura de negocio.

- Comunicar su apetito al riesgo, para esto es necesario diseñar un documento formal que sea claro para todas las áreas de la organización. Se deberán tomar los lineamientos contenidos en las políticas corporativas, locales y código de conducta vigentes, así como también analizar aspectos no definidos en cada proceso. Posteriormente se puede completar esta actividad con el establecimiento de objetivos para el 2015. Como tercer paso se deben comunicar estas consideraciones enfocadas a cada categoría de riesgo identificada como ya se explica más adelante.

- Monitorear y actualizar su apetito al riesgo, el equipo ERM, la Dirección de riesgos y Compliance debe encargarse de revisar cada vez que sea necesario su declaración de apetito al riesgo más aún cuando el modelo de negocio ha cambiado, esto debe estar mencionado en la política del Sistema de Gestión de Riesgos. De esta manera se asegura que los riesgos estén considerados en todo momento. El concepto también conlleva a

realizar las acciones necesarias para que la cultura organizacional esté compuesta por una fuerte filosofía del riesgo.

El apetito al riesgo no se debe medir de forma aislada, está compuesto por cuatro consideraciones que se muestran en la **Figura 3.2** (Committee of Sponsoring Organizations of the Treadway Commission, 2012, pág. 10):

Figura 3.2: Composición del Apetito al Riesgo

Visión General de las Consideraciones que Afectan al Apetito al Riesgo		
Perfil de los Riesgos Existentes	El nivel actual y distribución de los riesgos en la organización a través de varias categorías.	**Determinación del Apetito al Riesgo**
Capacidad del Riesgo	Cantidad de riesgo que una entidad está dispuesta a soportar en su persecución de objetivos.	
Tolerancia al Riesgo	Nivel aceptable de variación que una entidad está dispuesta a aceptar en la persecución de sus objetivos.	
Actitud hacia el Riesgo	Actitudes en relación al crecimiento, riesgo y retorno	

Como se muestra en el cuadro, se debe considerar el perfil de riesgos alrededor de la organización, en el caso de MM S.A. ha sido desarrollado únicamente de manera parcial para ciertos procesos y excluyendo las características del mercado local, este perfil se obtiene de la identificación de eventos en todos los procesos. Por otro lado, determinar la capacidad de riesgo que la organización está dispuesta a asumir basándose en las declaraciones de las políticas, procedimientos

y código de conducta de MM S.A. A través del correcto establecimiento de objetivos se deberán definir los niveles de tolerancia, atados a indicadores de gestión específicos para cada estrategia, esta actividad se realiza en el establecimiento de objetivos. Por último es importante elaborar una definición clara de la actitud que la compañía tendrá ante ciertos eventos que ponen en riesgo a su estabilidad. Esta definición debe estar declarada en un documento de alto nivel jerárquico que esté al alcance de todos los empleados de MM S.A. Esta parte está explicada adecuadamente en las funciones y responsabilidades del Director de Riesgos y su equipo ERM.

Se podría decir que los últimos tres puntos tienen muy poca presencia en MM S.A. a pesar de que si existen lineamientos para responder ante eventos adversos, los cuales se relacionan a la forma en cómo se deben comunicar asuntos que van en contra de los intereses de la compañía en varias categorías, por ejemplo, eventos relacionados a compliance de políticas y procedimientos, eventos adversos en calidad de los productos que fabrica y comercializa la compañía, lineamientos para el desarrollo y entrega de materiales promocionales a profesionales de salud y otros terceros, discriminación y otros asuntos relacionados al personal, entre otros.

El apetito al riesgo está intensamente ligado a la tolerancia al riesgo y a su vez estos son determinados en base a los objetivos que mantiene

cada área dentro de la organización y sus estrategias. Es decir, debe existir una conexión muy clara y evidente entre los objetivos, las estrategias, el apetito y tolerancia al riesgo. Ligado a los objetivos, la tolerancia al riesgo se ubica dentro de las categorías que se mencionaron dentro del COSO I y COSO II que son: estratégicos, operacionales, reportaje y compliance. Mientras que el apetito al riesgo es más general, la tolerancia al riesgo es mucho más específica y se establece en base a las operaciones y estrategias.

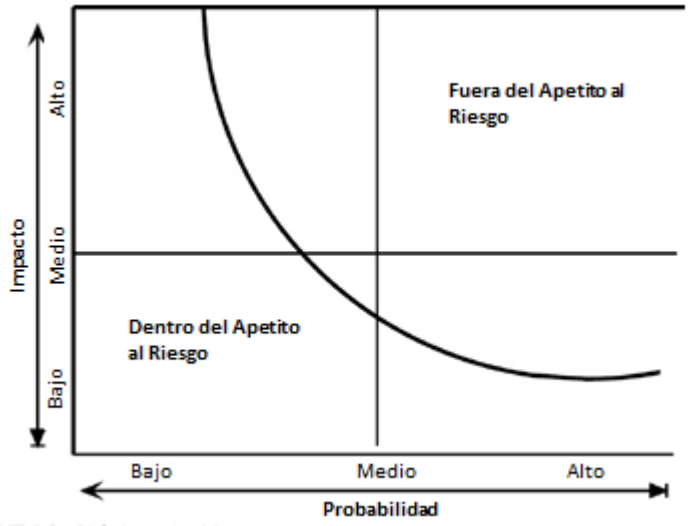
Por ejemplo, MM S.A. tiene un elevado apetito al riesgo en relación al retorno que traerán los gastos operacionales destinados para tener un mayor acceso a nuevas regiones dentro del país. Sin embargo, no aceptará una mayor inversión de 30 mil USD en el desarrollo y contratación de terceros para manejar planes que faciliten el acceso, ni tampoco aceptará una participación en el mercado menor al 5% en el país.

El ejemplo mostrado en el párrafo anterior facilita el entendimiento de la vital relación entre los dos componentes para un correcto establecimiento del apetito al riesgo. Además, esto permitirá a MM S.A detectar eventos no deseados (riesgos) y de qué manera estos pueden ser definidos como de alto, medio y bajo impacto para la organización. Para mostrar el efecto en la práctica de los antes expuesto, se analizará

este punto de manera completa en los componentes 3, 4 y 5 del ERM Integrated Framework que se expone más adelante.

Para finalizar este punto, el ERM Integrated Framework (COSO II) ilustra al lector con la **Figura 3.3** gráfico donde se unen los conceptos de la filosofía del riesgo y el apetito al riesgo denominado Mapa de Apetito al Riesgo como se muestra a continuación (Robert R. Moeller-John Wiley & Sons - Citación de Enterprise Risk Management Integrated Framework 2004, 2011):

Figura 3.3: Mapa de Apetito al Riesgo



Básicamente, lo que muestra este gráfico es que MM S.A. deberá aceptar los riesgos del negocio en relación a su probabilidad de ocurrencia y nivel de impacto y de la misma manera rechazará otros en

este mismo sentido dependiendo de sus niveles: Alto, medio o bajo. La línea curva determina dos sectores, el primero hace referencia a los riesgos que la compañía debería estar dispuesta a aceptar denominada el área dentro del apetito al riesgo y el segundo indica el área fuera del apetito al riesgo en relación a los riesgos que la empresa no debería estar dispuesta a aceptar. De todas maneras, se podría considerar una tercera dimensión para este diagrama considerando la variable del retorno. En este sentido MM S.A. podría aceptar más o menos riesgo dependiendo del porcentaje del retorno que espera obtener y basada en su apetito al riesgo.

3.1.1.3 Actitud de la Junta Directiva, estructura organizacional y estándares de recursos humanos

En cuanto a la **organización y estructura** del Departamento de Riesgos que se debe instalar en MM S.A., se considerarán los mismos integrantes con los que cuenta ahora la organización.

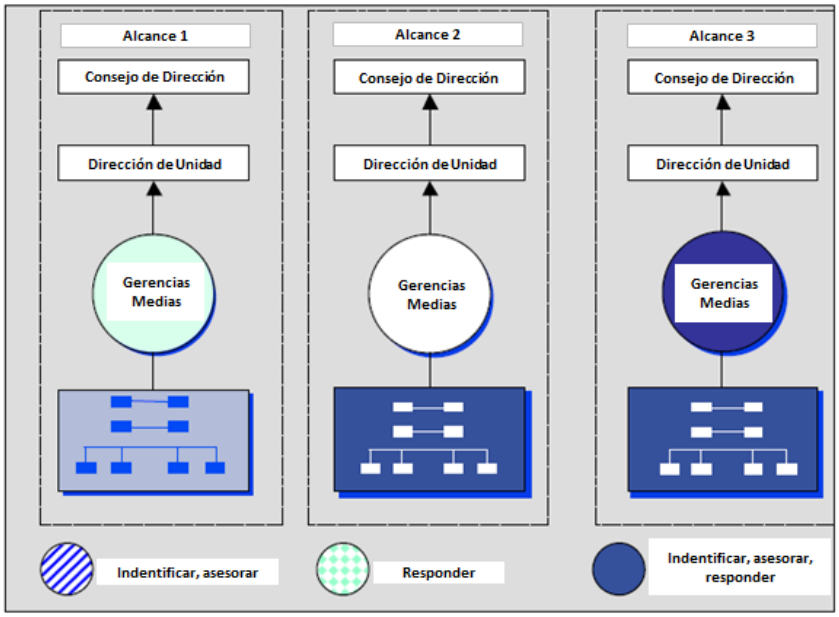
Es importante rescatar la filosofía que menciona el COSO II en relación a la responsabilidad en el Sistema de Gestión de Riesgos (Committee of Sponsoring Organizations of the Treadway Commission, 2004, pág. 101):

> Todos en una entidad tienen cierta responsabilidad para el manejo de riesgos. El Director de Riesgos es el responsable primordial y debe

adueñarse del sistema. Otros Gerentes soportan la filosofía del manejo del riesgo, promueven el compliance con el apetito al riesgo, y administran los riesgos dentro de la esfera de sus responsabilidades en consistencia con la tolerancia al riesgo. Otro personal es responsable de ejecutar el Sistema de Gestión de Riesgos en concordancia a las directrices y protocolos. El Consejo de Directores provee una importante visión del Sistema de Gestión de Riesgos. Un número de participantes externos a menudo proveen información útil para efectuar el sistema de Gestión de Riesgos pero no son responsables de la efectividad del Sistema Integral de Gestión de Riesgos de la compañía.

De esta manera se resume rápidamente la participación del Departamento de Riesgos y los empleados en general de la organización. Para que esta realidad se lleve a cabo en MM S.A. primeramente es necesario establecer el tipo de organización para el sistema propuesto como se muestra en la **Figura 3.4** a continuación (Committee of Sponsoring Organizations of the Treadway Commission, 2004) **(Propuesta, ver numeral 3.8)**:

Figura 3.4: Tipos de Organizaciones de Riesgos



Los tres alcances tienen diferentes beneficios y desafíos (esto puede ser consultado a detalle en el texto COSO II Técnicas de Aplicación), sin embargo y de acuerdo a los fundamentos mencionados con anterioridad para incrementar la filosofía del riesgo, MM S.A. necesita el modelo 3. En este modelo las líneas del negocio y las gerencias medias son las encargadas de identificar, asesorar y responder a los riesgos identificados. Esta consideración también se da por la escasez de recursos que se presenta en el equipo ERM y que por ende necesitará ayuda crucial por parte de las gerencias medias para ejecutar las acciones del Sistema de Gestión de Riesgos.

Por otro lado existen riesgos que solo pueden ser conocidos por las gerencias medias que presentan una visión más global de la compañía. En un nivel más arriba se encuentran las diferentes directivas como las Unidades de Negocio, Dirección Médica, etc. En el último punto se encuentra el Director de Finanzas que en este caso va a ser el Director de Riesgos de MM S.A. en Ecuador junto con el Director General de la compañía cuya participación es crucial para complementar el enfoque de gobierno.

Para la propuesta de la **organización** del Sistema de Riesgos se van a realizar modificaciones en relación a lo que menciona el ERM Integrated Framework de acuerdo a la estructura que actualmente posee

MM S.A. En este sentido lo que se recomienda es que exista la siguiente estructura:

- Direcciones Regionales a quienes se reportan las actividades de control y riesgos del país, específicamente al Contralor Regional.

- El Consejo de Directores en Ecuador cuyos integrantes se acaban de mencionar.

- El Director de Riesgos en Ecuador que será el Director Financiero, cabe recalcar que el actual Director tiene mucha experiencia en Auditoría Interna Corporativa en MM S.A.

- El Comité Ejecutivo en Ecuador que está conformado de todos los Directores de las diferentes áreas y algunas gerencias estratégicas como el Oficial de Compliance y el Contralor.

- Equipo ERM conformado por el Contralor y el Coordinador de Contabilidad.

- Gerencias Medias conformada por los gerentes de las distintas áreas.

- Empleados en general.

El Consejo de Directores conformado por el Director Financiero y el Director General en este caso se va a encargar de supervisar desde arriba el Sistema de Gestión de Riesgos. De acuerdo a lo que determine la organización es posible que se puedan incluir más personas a este Consejo, por ejemplo un elemento interno del Departamento Legal de alto nivel. Este Consejo deberá estar al tanto de manera oportuna de los riesgos más significativos de MM S.A., así como también del asesoramiento y de las respuestas al riesgo propuestas para dichos riesgos identificados. Además dentro de sus funciones, deberá determinar sanciones por actos no permitidos realizados por empleados de la compañía en conjunto con la Dirección de Recursos Humanos preservando el cumplimiento de las políticas corporativas relacionadas a esta materia.

Existen varias necesidades del Consejo de Directores para sentirse confidentes de que la información proporcionada por el Comité Ejecutivo y el equipo ERM es correcta y se presenta de manera oportuna, para esto se deben establecer funciones claras en las líneas que se ubican debajo de esta estructura.

Las funciones de Directivas Regionales no se mencionarán ya que estos reportan a un Comité mucho más arriba del país y la región.

Las funciones y responsabilidades del Director de Riesgos en Ecuador deben integrar al menos lo siguiente (Committee of Sponsoring Organizations of the Treadway Commission, 2004, pág. 109):

- El Director de Riesgos reportará sus actividades al Director Financiero Regional. El reporte directo de controles y riesgos a las Direcciones Regionales será realizado por el Equipo ERM específicamente por el Contralor.

- Ser el auspiciante principal del Equipo ERM para que se den a cabo las actividades del Sistema de Gestión de Riesgos.

- Comunicar y administrar el establecimiento y mantenimiento continuo del Sistema de Gestión de Riesgos en base a objetivos.

- Asegurar el apropiamiento del Sistema de Gestión de Riesgos por parte de los Directores de cada área de acuerdo al alcance.

- Validar que todos los riesgos de la compañía están siendo identificados y asesorados de manera correcta y oportuna.

- Establecer un flujo adecuado de comunicación con el Equipo ERM con respecto al estatus del Sistema de Gestión de Riesgos y la estandarización de los selfassessments.

- Promover el Sistema de Gestión de Riesgos en todas las unidades y ser un facilitador para apoyar a la implementación en cada una.

- Verificar que el Sistema se esté aplicando en todas las unidades de una manera correcta a través de los reportes entregados por el equipo ERM.

- Revisar y aprobar procedimientos completos para reportar riesgos significativos.

- Asistir a las Reuniones de Comité Ejecutivo para promover la filosofía del riesgo en todas las unidades.

- Promover el desarrollo de información estandarizada de riesgos y la automatización de procesos que sea utilizable en toda la compañía.

- Asegurar que el Equipo ERM está realizando actividades para focalizar las acciones de remediación en análisis de costo beneficio en las diferentes unidades.

- Asegurar que los empleados sean entrenados en gestión de riesgos para desarrollar una cultura apropiada focalizada en riesgos.

- Trabajar en conjunto con las diferentes direcciones de unidad para asegurar que las nuevas estrategias y planificaciones financieras consideren al riesgo dentro del análisis.

- Comunicar adecuadamente las observaciones presentadas en las reuniones de Comité Ejecutivo y Consejo de Dirección en relación a reportes de riesgos y estatus del Sistema de Gestión de Riesgos e informar al equipo ERM.

Las funciones y responsabilidades del Equipo ERM en MM S.A. deberán ser al menos las siguientes:

- Asegurar que las Gerencias Medias y Empleados en General entiendan y acepten su responsabilidad en identificar, asesorar y manejar los riesgos.

- Realizar pruebas para determinar que las diferentes unidades de negocio están enfocadas en estrategias resultantes del Sistema de Gestión de Riesgos, esto también se puede realizar a través de selfassessments.

- Proporcionar el material suficiente que sirva de apoyo a las otras áreas para aplicar el Sistema de Gestión de Riesgos.

- Apoyar a la organización en cualquier duda para la implementación de sistema en cuestión.

- Asegurar que las estrategias de riesgos se están llevando a cabo de una manera correcta a través de actividades de control

- Verificar que las transacciones contables están siendo registradas correctamente de acuerdo a las políticas contables que apliquen a MM S.A.

- Realizar selfassessments de control para identificar ineficiencias en los controles determinados para cada proceso.

- Determinar y asignar responsables en los procesos para efectuar controles determinados.

- Establecer reuniones trimestrales para revisar el estatus del sistema con las diferentes áreas.

- Revisar y ajustar el apetito al riesgo y sus tolerancias.

- Reportar cualquier actividad inusual al Director de Riesgos.

- Desarrollar y evaluar reportes de control en relación al manejo de riesgos.

- Otros.

Las funciones del Comité Ejecutivo, las Gerencias Medias y los Empleados en General deberán ser:

- Apoyar el Equipo ERM en la aplicación de las técnicas propuestas en este Sistema de Gestión de Riesgos

- Reportar eventos adversos u oportunidades identificadas de manera oportuna al Equipo ERM para la inclusión de las mismas en el portafolio de riesgos.

- Comunicar adecuadamente en las reuniones de Comité Ejecutivo los hallazgos encontrados en asesoría de riesgos y reportarlos inmediatamente al Equipo ERM.

- Definir estrategias de mitigación de riesgos en base a los procedimientos establecidos.

- Entregar reportes anuales sobre identificación, asesoría y respuesta al riesgo de los procesos relacionados al Equipo ERM para que posteriormente sea presentado y aprobado por el Consejo de Dirección.

- Aplicar las técnicas del Sistema de Gestión de Riesgos para la elaboración de nuevas estrategias.

- Otras relacionadas a la aplicación del Sistema de Gestión de Riesgos.

Si MM S.A. modifica su estructura organizacional de manera que Contraloría (equipo ERM) y Compliance trabajen en conjunto con un alcance integral para todos los procesos de la compañía, el control y la gestión de riesgos podrían tener una mayor participación a nivel gerencial que permita la aplicación de todos los componentes del Marco Integrado para la Gestión de Riesgos Empresariales.

Un Sistema de Gestión de Riesgos debe contar con ayuda externa para asesorar correctamente su administración, así como también, para brindar un enfoque de independencia y objetividad. Para lo cual se recomienda a MM S.A. que identifique opciones dentro del mercado de empresas que puedan brindar este servicio a la organización en coordinación con el Equipo ERM y su Director para la contratación de expertos en el tema, de no ser posible en el corto plazo por varios factores, se importante que al menos se lo realice luego de la primera estructuración del sistema y posteriormente cada dos años **(Propuesta, ver numeral 3.8)**.

En relación a las revisiones de Auditoría Interna que se enfocan en estándares corporativos y que no incluyen necesariamente aspectos

relevantes del mercado, es fundamental que MM S.A. haga un levantamiento de todos los procesos de la compañía y realice los pasos de identificación, asesoría y control de riesgos. En este sentido, establecer puntos clave de control y documentarlo para cada proceso. Esta será la base para estandarizar los selfassessments que contengan las variables importantes para la localidad, asimismo, esto servirá para que la compañía pueda hacer revisiones concisas y que fluyan rápidamente en el futuro **(Propuesta, ver numeral 3.8)**.

Las recomendaciones antes mencionadas tendrán efecto en las debilidades halladas en los elementos: Estructura organizacional y estándares de recursos humanos. De todas maneras es necesario que el Departamento de Recursos Humanos haga un levantamiento de los cursos principales que debe realizar cada empleado en relación a su función y establecer periodos de actualización. La compañía tiene recursos suficientes para programar cursos online y que emitan certificados de cumplimiento para obtención de estadísticas anuales **(Propuesta, ver numeral 3.8)**. Las debilidades identificadas en el elemento compromiso con la competencia se remedian con las acciones que se deben tomar para el componente: Establecimiento de objetivos.

Estas son las recomendaciones principales que se proponen a MM S.A. en relación al primer componente del COSO II.

3.1.2 Componente 2: Establecimiento de objetivos

En primera instancia se recomienda que MM S.A. comunique adecuadamente los objetivos propuestos por la dirección de cada unidad de negocio o área. De esta manera los subordinados tendrán una mejor guía para enfocar los esfuerzos en soportar las estrategias de su supervisor.

Por otro lado, es imperante conocer que la secuencia indispensable que MM S.A. debe seguir para implementar un correcto sistema de objetivos basados en riesgos parte de la misión de la compañía. La misión es un elemento crucial en la planificación estratégica, crea una declaración general y formalizada del propósito de la organización y es la base para la planificación de los objetivos y estrategias más específicas. Luego de la misión, cada Dirección de Unidad o Área debe desarrollar uno o varios objetivos estratégicos con medidas o indicadores de gestión denominados KPI´s; posteriormente se deben establecer objetivos operacionales, de reportaje y compliance por parte de cada empleado o subordinado directo de dirección. Estos deberán estar alineados con el apetito al riesgo que a su vez debe contar con otros indicadores de gestión o los denominados KPI's (Key Performance Indicator). Estos últimos objetivos y medidas darán los lineamientos finales para determinar los niveles de tolerancia para cada uno de los objetivos relacionados mismos que servirán de guía para que MM S.A. pueda determinar si los objetivos fueron alcanzados a cabalidad, sobrepasando las expectativas, dentro de los niveles aceptables o por debajo de los niveles aceptables **(Propuesta, ver numeral 3.8)**. Con estas consideraciones

se pueden identificar oportunidades de mejora y además MM S.A. podrá establecer medidas de riesgos de una manera más sencilla y basada en objetivos. La **Figura 3.5** muestra esta relación con un ejemplo ilustrativo que se utilizará para este y los siguientes componentes (Committee of Sponsoring Organizations of the Treadway Commission, 2004, pág. 28) :

Figura 3.5: Establecimiento de Objetivos basados en Riesgos

Misión		
Ser el productor líder de productos premium para el hogar en las regiones que operamos		
Objetivos Estratégicos	**Estrategia**	**Apetito al Riesgo**
Estar en el cuartil tope de ventas de productos de hogar para vendedores minoristas	Expandir la producción de nuestros 5 productos top de venta al por menor para satisfacer el incremento en la demanda	Aceptar que la compañía esta dispuesta a invertir grandes cantidades de dinero en nuevos activos, gente y procesos
	Objetivo Relacionado	Aceptar que la competencia puede incrementar su participación en el mercado a través de reducciones considerables de precios y por lo tanto reduciendo niveles de rentabilidad para la compañía
	Incrementar la producción del producto X en un 15% en los siguientes meses Contratar 180 empleados nuevos calificados para todas las divisiones manufactureras Mantener la calidad del producto en 4.0 Sigma Mantener el costo de la mano de obra en un 22% por cada orden de 1 dólar	No se acepta faltas en la calidad de los productos de la compañía
KPI	**KPI**	
Participación en el mercado	Unidades de Producción Número de Personas Contratadas Calidad del Producto bajo Sigma	
Tolerancia al Riesgo		
KPI	**Target**	**Tolerancias - Rango Aceptable**
Participación en el mercado	Primer Percentil	20%-30%
Unidades de Producción	150000 Unidades	-7500/+10000
Número de Personal Contratado	180 Contrataciones	-15/+20
Indicador de Calidad para Producción	4.0 Sigma	4.0 - 4.5 Sigma

Como se puede evidenciar de esta manera se establecen el apetito al riesgo y sus tolerancias a través de objetivos, punto que es un elemento del apetito al riesgo mostrado en la **Figura 3.2.**

3.2 PASO 2 - IDENTIFICACIÓN DE LOS RIESGOS

El paso 2 y 3 se fundamentarán en las técnicas propuestas por el Ingeniero Wilson Silva, Director de este Trabajo de Titulación y experto en asesoría corporativa para auditoría externa e interna que están basadas en el COSO II.

3.2.1 Componente 3: Identificación de eventos

Se propone que MM S.A. considere lo siguientes aspectos para la identificación de riesgos (Robert R. Moeller- John Wiley & Sons - Citación de Enterprise Risk Management Integrated Framework 2004, 2011) **(Propuesta, ver numeral 3.8)**:

- **Eventos Económicos Externos:** Es necesario que se enlisten todos los eventos económicos del Ecuador que podrían tener impactos a corto, mediano y largo plazo ya que los mismos podrían tener una influencia importante en el alcance de los objetivos de la sucursal. Es importante asimismo adelantarse a los hechos económicos que el país podría estar sufriendo en el futuro.

- **Eventos Naturales de Medioambiente:** En relación a catástrofes naturales como terremotos, incendios, tormentas, entre otros.

- **Eventos Políticos:** En relación a nuevas leyes, gobernantes, como por ejemplo el decreto 400, el establecimiento del nuevo código monetario, etc.

- **Factores Sociales:** Cambios demográficos, cambios en las culturas, desarrollo de preferencias nuevas del consumidor, por ejemplo la tendencia de los pacientes para la adquisición de medicamentos genéricos.

- **Eventos de Infraestructura Interna:** Es necesario verificar que riesgos pueden producir nuevas estrategias de mercado, por ejemplo el establecimiento de un programa de pacientes para aumentar la adherencia al tratamiento, qué impactos puede tener en el control, en el paciente, etc.

- **Eventos de Procesos Internos:** Cambios en procesos para mejorar el flujo podrían causar riesgos en otros procesos, por ejemplo en MM S.A. el cambio de un sistema automático de pagos a empleados por uno manual.

- **Eventos de Tecnología Interna o Externa:** En este sentido se deben considerar los cambios en la tecnología alrededor del mundo, dentro del

país en la misma sucursal, por ejemplo almacenamiento en nubes de información, hackers especializados en filtración de información confidencial, utilización de nueva maquinaria para procesamiento de medicinas con menores costos, desarrollo de nuevos sistemas para controlar inventarios, etc.

La identificación de riesgos se vuelve más sencilla si se asignan diferentes responsables de riesgos en las varias áreas funcionales de la organización. Específicamente, se debe contar con personas claves y comprometidas en identificación de riesgos para actividades operacionales, finanzas y contabilidad, IT y gerencias de unidad. Más adelante en el componente de actividades de control se ejemplifica como MM S.A. puede asignar estas responsabilidades; claro está que se necesitan tareas de entrenamiento para que estas personas puedan asumir ese rol.

La propuesta de este trabajo hacia MM S.A. es que actividad la detección de riesgos sea coordinada a través del Equipo ERM.

Existen varias técnicas recomendadas para identificación de eventos, estas pueden aplicarse dependiendo de los recursos que podría disponer una compañía, principalmente tiempo y otros factores específicos del proceso o situación sujeta a análisis. En base a los recursos que puede disponer MM S.A. se recomienda que se utilicen las siguientes metodologías (The Comittee of Sponsoring Organizations of the Treadway Commission, 2004):

- Un listado de eventos desfavorables que se han presentado en las compañías de la industria farmacéutica no solo en el país sino también en el mundo. Esto debe ser documentado y archivado de manera que puedan ser revisadas las veces que sea necesario con el fin de establecer puntos de control que son comunes en el medio. Estos eventos desfavorables pueden ser consultados en internet o a través del servicio de un tercero.

- Análisis de Diagramas de Flujo: Es necesario que se elaboren diagramas de flujo en todos los procesos de la compañía, como se había explicado únicamente existen para ciertos procesos. Se podrían aprovechar la iniciativa de levantamiento de políticas para completar esta acción. Con estos diagramas de flujo se pueden identificar visualmente los puntos de control y también crear escenarios negativos en un sentido de ¿Qué pasa si….? para cada una de las actividades del flujo.

La técnica principal que se propone en esta sección es el denominado Taller Simple de Reconocimiento que funciona a través de reuniones con el personal de diferentes especialidades involucrado en el proceso, para hacer una **lluvia de ideas.** Este trabajo puede servir como ejemplo para todas las áreas funcionales que necesiten identificar sus propios riesgos. El equipo ERM no necesita convocar necesariamente estas reuniones porque podría ser impracticable estar presente en todas, se puede asignar un líder que cuente con el conocimiento suficiente en la metodología. Con la lluvia de ideas se podrían identifican

además los alcances de las actividades de cada proceso y permitirá al equipo de ERM que se enfoque principalmente en la gestión y mitigación de los riesgos.

Antes de que se realice el taller se deben aplicar los siguientes pasos (The Comittee of Sponsoring Organizations of the Treadway Commission, 2004):

- Identificar un facilitador con experiencia para liderar sesiones, manejar grupos dinámicos y planificar la mejor manera de capturar ideas útiles

- Establecer reglas del juego para el desarrollo de la reunión

- Reconocer las diferentes personalidades de los participantes, considerando las maneras de optimizar su contribución.

- Identificar qué objetivos, categorías de objetivos y de eventos serán tratados

- Invitar a un número no mayor de 15 participantes, de preferencia menos

- Establecer expectativas realísticas en relación a lo que el taller podría conseguir

La agenda del taller debe tener una introducción que explique el propósito del mismo, el motivo por el que los participantes han sido invitados y el mecanismo de las actividades. Como segundo punto la agenda debe explicar el proceso que se llevará a cabo en base a los objetivos corporativos designados para el proceso objeto de revisión.

El objetivo de utilizar esta técnica en MM S.A. es presentar los diferentes puntos de vista de las personas involucradas en los procesos. La actividad puede funcionar de manera sencilla utilizando una fórmula simple (Votos = No. de riesgos/2 + 1) partiendo de los diferentes riesgos que han salido de dicha tarea, la cual determina la cantidad de votos que se pueden asignar por persona a cada riesgo. Aquellos ítems que no llegan a ocupar al menos el 25% de los votos deberán ser descartados. Este procedimiento debe ser realizado hasta que se satisfaga el objetivo que consideren los involucrados en cuanto al número de riesgos identificados, generalmente quedan de 4 a 7 ítems (podría variar de acuerdo al caso) (Robert R. Moeller- John Wiley & Sons - Citación de Enterprise Risk Management Integrated Framework 2004, 2011).

Cuando el equipo ERM revise el listado de riesgos resultante de las reuniones antes mencionadas, deberá clasificarlos en el portafolio de riesgos de alto nivel ya mencionado anteriormente y además identificar los siguientes parámetros (no limita a que otros sean considerados):

- El riesgo es común en todos los procesos o se trata de un caso puntual.

- Es generado de factores externos (Económico, medio ambiente, político, social, tecnológico) o internos (Infraestructura, personal, procesos, tecnología).

- Los riesgos están relacionados y causan otros o son aislados dentro del alcance del área.

Es posible que dentro de las reuniones establecidas para la identificación de riesgos salten a la luz situaciones que están causando variados tipos de problemas a la compañía y que las mismas ya se hayan identificado anteriormente y que además, se hayan establecido lineamientos de control en documentos formales para que las mismas no se den. Estas actividades serán tratadas como GAPS. Un GAP es un espacio de diferencia entre lo que es y lo que debería ser una actividad específica. Estos GAPS de control deberán ser enlistados en cada proceso analizado. Cabe recalcar que las personas involucradas en estos talleres deben conocer las políticas y procedimientos en la compañía para que estos casos sean identificados en el acto. Posteriormente en los pasos y componentes de control del ERM Integrated Framework los GAPS serán tomados en cuenta para incluirlos dentro de los informes de control.

Continuando con la metodología se deben analizar los objetivos de las áreas y de los procesos en cuestión para identificar los riesgos asociados a su incumplimiento. Siguiendo el ejemplo dado para los objetivos, esta actividad se

debe desarrollar ligando los eventos a los objetivos de acuerdo a la **Figura 3.6** de la siguiente manera:

Figura 3.6: Identificación de Riesgos Corporativos

Misión	Ser el productor líder de productos premium para el hogar en las regiones que operamos
Objetivo Estratégico	Estar en el cuartil tope de ventas de productos de hogar para vendedores minoristas
Objetivos Relacionados	Contratar 180 empleados nuevos calificados para todas las divisiones manufactureras Mantener el costo de la mano de obra en un 22% por cada dólar ordenado
KPI	Número de Personas Contratadas Costo de Mano de Obra por cada dólar ordenado
Tolerancia	165 - 200 Contrataciones Costo de Mano de Obra entre 20% y 23% por cada dólar ordenado
Eventos potenciales/riesgos y su impacto relacionado	Reducción de la demanda en el mercado en el mercado, provocando que se contraten más personas de lo necesario Aceleración inesperada en el mercado laboral, reduciendo la oferta laboral y contratando menos personal de lo necesitado Descripciones inadecuadas de las posiciones requeridas, resultando en contrataciones de personal no calificado

Posteriormente, se pueden dar una serie de consideraciones adicionales por parte del área encargada del Equipo ERM para definir de una manera más específica a cada uno de los casos y que esa consideración tenga más o menos peso dentro de las funciones más importantes de la compañía. La idea es contar con un conocimiento profundo de los riesgos asociados a cada proceso y departamento e identificar si estos afectan a las áreas "core" de la compañía. A pesar de que este primer set de riesgos no será el definitivo, es un excelente comienzo para desarrollar un sistema más complejo.

Una vez que los riesgos han sido definidos, deben ser compartidos con los responsables de cada unidad, la Dirección de Riesgos y los involucrados en la lluvia de ideas. Los riesgos identificados en estas sesiones también deben ser compartidos con otras áreas que no participaron en las mismas; en fin deben ser divulgados a los miembros de toda la compañía que se considere necesario, esto puede ser llevado a cabo en las reuniones de Comité Ejecutivo.

Es probable que el método de la lluvia de ideas no satisfaga las necesidades de la gerencia y podría ser considerada como una metodología informal. Para estos casos existen otras técnicas de igual importancia y validez como la lluvia de ideas pero que necesitan de mayor tiempo y dedicación por parte de las personas involucradas. Las técnicas adicionales presentadas en el Marco para la Gestión de Riesgos Empresariales para identificación de riesgos y estimación de probabilidad e impacto están resumidas en el **Anexo 1** de este trabajo y son:

- Método Delphi (Identificación de riesgos)

- Simulación Montecarlo (Estimación de probabilidad e impacto)

- Árbol de Decisiones (Estimación de probabilidad de múltiples riesgos)

Cabe recalcar que uno de los propósitos de este trabajo no es profundizar mucho en las técnicas probabilísticas sino más bien establecer claros y entendibles criterios para la administración de riesgos empresariales.

Finalmente, con los eventos identificados es posible realizar un mapeo de los riesgos y oportunidades para cada proceso categorizándolos por los factores relacionados a los mismos ya sean internos o externos. Un ejemplo de esta categorización se puede encontrar en el **Anexo 2**.

Esta es la primera actividad que se debe realizar para cumplir con el primer punto para la determinación de la tolerancia al riesgo ubicado en la **Figura 3.2**.

3.3 PASO 3 - EVALUACIÓN DE RIESGOS

Con fines prácticos, en lo que sigue de la evaluación cuantitativa y cualitativa de los riesgos se propone a MM S.A. tomar como técnica para la identificación de riesgos al Taller Simple de Reconocimiento (más utilizado en las corporaciones de acuerdo al COSO II).

3.3.1 Componente 4: Administración del riesgo

El primer paso en esta sección es determinar la probabilidad de ocurrencia de los riesgos identificados y también su impacto en términos de costos monetarios.

Existe más de una técnica para realizar esta cuantificación, sin embargo, cuando el set de riesgos no es tan amplio generalmente se utiliza una técnica bastante sencilla y que en muchas ocasiones ha funcionado muy bien. Esta técnica es la que se recomienda a MM S.A. utilizar por su practicidad y eficiencia. Por otro lado, si se presenta una cantidad importante de riesgos, la compañía podría también utilizar técnicas más precisas para diferenciar los niveles entre unos y otros.

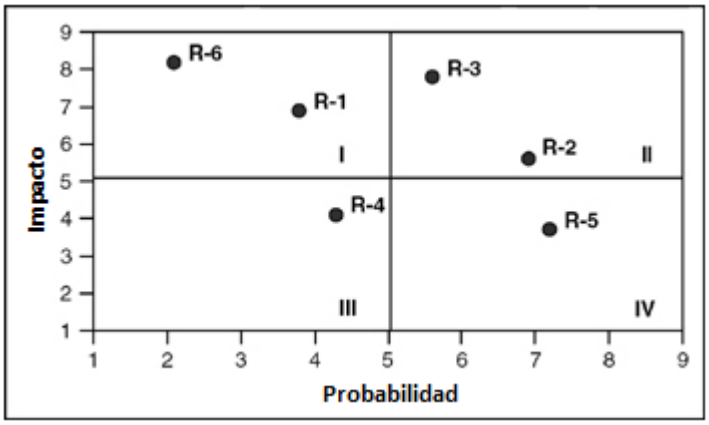
La primera metodología inicia realizando dos preguntas muy sencillas y prácticas por parte de la persona que está guiando el taller a los integrantes del mismo (Robert R. Moeller- John Wiley & Sons - Citación de Enterprise Risk Management Integrated Framework 2004, 2011) **(Propuesta, ver numeral 3.8)**:

- ¿Cuál es la probabilidad de ocurrencia del riesgo identificado en el periodo de un año? Calificar del 1 al 9 considerando que 1 quiere decir que casi no existe probabilidad de ocurrencia; 9 si se cree que el evento ocurrirá durante el periodo y de 2 a 8 para calificar niveles mixtos, es decir, probabilidades medias, medias bajas y medias altas.

- ¿Qué impacto puede tener el riesgo en términos de costos monetarios? De igual manera para esta pregunta se debe utilizar la escala antes mencionada del 1 al 9.

Posteriormente, se debe realizar un promedio de los dos factores para determinar el peso de cada uno y su importancia. Se utiliza una tabla sencilla con cuatro cuadrantes: en el eje de las "x" se ubica a la probabilidad y en el eje de las "y" el impacto monetario. Los cuadrantes e dividen a partir del número 5 en los dos ejes dejando cuatro espacios en donde se deberán ubicar cada uno de los riesgos analizados como se enseña en la **Figura 3.7**:

Figura 3.7: Mapa de Riesgos



El cuadrante No. II debe ser atendido inmediatamente entendiéndose como riesgos que tienen una alta probabilidad y un impacto financiero importante. Estas características deben ser consolidadas por el Equipo ERM una vez

finalizados los talleres para incluirlas en el portafolio de riesgos integral de la compañía.

Esta forma de medir los riesgos puede no tener una precisión estricta debido a que se basa en consideraciones de los distintos puntos de vista de los involucrados pero al menos brinda una visión cualitativa muy cercana de lo que un riesgo puede significar en las operaciones de la compañía. Cabe recalcar que esto no limita a que se establezcan parámetros para la calificación de las dos variables, de manera que el análisis tenga un efecto más acercado a la realidad.

Esto dependerá también de la predisposición de los integrantes de los talleres y la información disponible en MM S.A. En este sentido se considera que se pueden asignar muchos otros indicadores para la consideración de la probabilidad e impacto en la compañía para los cuales que se han desarrollado varios sistemas para recolección de indicadores, nada más es cuestión de identificar qué indicadores son útiles en cada proceso.

Cuando se ha detectado un número mucho mayor de riesgos es recomendable utilizar dos dígitos porcentuales para las calificaciones de ocurrencia e impacto. Esto permite al ejercicio diferenciar las categorías en donde debe ser ubicado cada riesgo. Esto también quiere decir que el equipo ERM debe prestar mayor atención en la diferenciación de cada riesgo y las posibles amenazas que se pueden presentar en el negocio.

Ahora bien, una vez identificados los riesgos a través de la lluvia de ideas, es necesario mirar a cada uno de forma individual. En este sentido es necesario asesorar en primera instancia la porción de riesgo inherente que potencialmente podría tener cada uno. Para estos riesgos, de manera general, no se pueden realizar muchas acciones para mitigar su impacto o su riesgo y siempre quedará un riesgo residual. Sin embargo, se pueden realizar consideraciones en base a la siguiente **Figura 3.8** como ilustración y que sigue la línea de los ejemplos anteriores tomando otros riesgos:

Figura 3.8: Asesoramiento de Riesgos Inherentes

Objetivo Operacional	Ingreso operativo de ventas al exterior de 100 millones				
KPI	Cambio en el ingreso operativo proveniente de ventas al exterior				
Riesgo	Variación en la tasa de cambio afecta de manera negativa el ingreso operacional de ventas al exterior				
Tolerancia	Variación aceptable de +/- 10 millones				
Riesgo	**Asesoramiento de Riesgo Inherente**		**Respuesta al Riesgo**	**Asesoramiento de Riesgo Residual**	
	Probabilidad	**Impacto**		**Probabilidad**	**Impacto**
La tasa de cambio sube en 1 punto dentro de 90 días	10%	$ 5.000.000,00	Aceptación	10%	$ 5.000.000,00
La tasa de cambio sube en 1,5 puntos dentro de 90 días	4%	$ 10.000.000,00	Obtener instrumentos de cobertura para tasas de cambio en monedas internacionales para	4%	$ 5.000.000,00
La tasa de cambio sube en 3 puntos dentro de 90 días	1%	$ 20.000.000,00		1%	$ 8.000.000,00

Como se puede observar las estrategias de respuesta al riesgo minimizan de cierta manera el impacto pero no el riesgo, este es el principio del riesgo inherente. Posteriormente se debe realizar un análisis del riesgo residual que

quedará de las acciones de mitigación determinadas para este riesgo inherente en caso de que exista la posibilidad de implementarlas.

Para estos y aquellos riesgos no ubicados en la categoría de inherentes se pueden realizar una serie de técnicas más específicas mucho más complejas de acuerdo a la realidad del negocio y disponibilidad de indicadores. Por ejemplo, el ERM Integrated Framework propone técnicas cualitativas; cuantitativas estadísticas y no estadísticas; atribuciones de capital y otras que deben ser llevadas a cabo por un equipo mucho más especializado en riesgos**.** Esta alternativa debe ser analizada por cada área de MM S.A. luego de implementar el primer alcance propuesto en esta sección y que se asegura tendrá excelentes resultados como un primer paso.

Por otro lado, es posible determinar la probabilidad de riesgos conjuntos multiplicando las calificaciones en términos de decimales (%) por ejemplo 0,70. Esto quiere decir que si un riesgo tiene la probabilidad de ocurrencia de un 0,70 y otro un 0,40 al multiplicarlos obtenemos un factor de 0,28, lo que significa que hay una probabilidad del 28% de que los dos riesgos se lleguen a dar. De la misma manera funciona entre el nivel de ocurrencia e impacto. Utilizando el mismo ejemplo anterior, si un riesgo tiene un nivel de ocurrencia de 0,70 y un nivel de impacto 0,40 existe una probabilidad ponderada del riesgo individual de que ocurra en un 28%, a esto se lo llama rango individual del riesgo (Robert R. Moeller- John Wiley & Sons - Citación de Enterprise Risk Management Integrated Framework 2004, 2011).

La calificación de un riesgo no debe terminar en lo antes explicado, el alcance podría ser mayor si se revisa de manera más profunda. Pueden haber varias implicaciones resultantes de ese riesgo y en muchas de las ocasiones es recomendable siempre realizar un poco más de investigación al respecto antes de asignarle un factor porcentual de ocurrencia o significancia (impacto). Por este motivo se recomienda a MM S.A. que los talleres que se analicen para identificación de riesgos se hagan con personal de todas las áreas, generalmente esto ocurre porque los procesos son multifuncionales.

Es importante que la identificación de riesgos sea realizada por la compañía para el mismo periodo en todos los procesos, generalmente el periodo es de un año. Además, es indispensable considerar que cada riesgo a pesar de que sea visto de manera independiente en cada unidad, posiblemente se refleje en las actividades de otras; inclusive podría no impactar las actividades de otros departamentos pero tener consecuencias catastróficas a nivel de toda la corporación. Es por este motivo que es necesario que cada unidad esté al tanto de los riesgos que se presentan en otras unidades de manera que pueda estar preparada para un impacto de esta dimensión. Es decir, los riesgos pueden ser interdependientes entre distintas divisiones, áreas, procesos, compañías relacionadas, etc. y deben ser analizados de esta manera.

Retomando lo revisado en párrafos anteriores, es tiempo de clasificar a los riesgos en rangos de importancia; para esto se utilizan los dos factores antes mencionados y que son la clave de la segunda etapa del asesoramiento en

riesgos; ocurrencia e impacto. Esto es sumamente sencillo y se puede resumir en la siguiente **Figura 3.9**:

Figura 3.9: Cuadro Resumen de Riesgos e Impactos en Talleres Simples de Reconocimiento

Riesgos Identificado	Nivel de Ocurrencia	Nivel de Impacto	Puntuación Individual	Rango
a	0,68	0,75	0,51	1
b	0,15	0,22	0,03	8
c	0,46	0,49	0,23	4
d	0,41	0,9	0,37	3
e	0,19	0,44	0,08	6
f	0,28	0,18	0,05	7
g	0,76	0,28	0,21	5
h	0,55	0,87	0,48	2

Es importante recalcar aquí que se deben considerar las interdependencias de los riesgos para cada unidad en cuanto a la afectación que un determinado riesgo pueda tener en otra unidad. El trabajo no es tan fácil como hacer una tabla; el equipo ERM debe centrarse en ajustar y dar una correcta calificación a cada riesgo en base a lo que se ha expuesto previamente. Precisamente de esto dependerá la exactitud de un sistema fundamental de riesgos.

A continuación de la obtención del rango de cada riesgo viene una de las partes más difíciles del sistema, esto es la cuantificación del riesgo en costos monetarios. La intención general de esta actividad es identificar el costo resultante del riesgo si se llegara dar y luego aplicarlo al rango. Si bien es cierto

los pasos anteriores permiten dar una valoración importante de cada riesgo potencial, no es suficiente para apreciar su nivel de impacto e importancia.

La actividad debe ser desarrollada con la participación de los miembros del proceso en cuestión, que tengan el conocimiento suficiente en relación al riesgo identificado para que puedan dar una valoración razonable del impacto. En esta parte también se deben definir los responsables de dar seguimiento a cada riesgo en cada proceso como se recomendó en el Paso 1 del Sistema de Gestión de Riesgos. La actividad no resultará de un análisis sencillo y es fundamental entender el camino por el cual se debe direccionar el razonamiento para conseguir una estimación acertada. El sentido en general es determinar de cierta manera el costo en el que se debe incurrir para que la organización se recupere de la ocurrencia de un riesgo o la pérdida que este podría causar.

MM S.A. debe realizar las siguientes preguntas a los integrantes del taller, en conjunto, como guía para estimar adecuadamente el costo de un riesgo (Robert R. Moeller- John Wiley & Sons - Citación de Enterprise Risk Management Integrated Framework 2004, 2011):

- ¿Cuál es el costo en el mejor de los casos si se tuviera que incurrir en el riesgo? Esta pregunta funciona comúnmente en los casos en los que el impacto es limitado si el riesgo ocurre.

- ¿Qué costo estimarían las personas conocedoras del proceso para el riesgo identificado? Esta pregunta se la puede realizar al director del área o unidad.

- ¿Cuál es el valor o costo esperado de incurrir en el riesgo? Esta se utiliza para los tipos de riesgos que incluyen costos bases u otros costos relacionados.

- ¿Cuál es el costo en el peor de los casos si se tuviera que incurrir en el riesgo? Esta pregunta básicamente apunta al peor de los escenarios para estimar el impacto.

Las respuestas a estas 4 preguntas darán resultados estimados de los costos en los que se pueden incurrir si el riesgo se llagara a dar. Sin embargo, es preciso definir el impacto tomando solo una, la mejor. En la práctica, la pregunta 2 y 3 suelen presentar las mejores estimaciones y para escoger la correcta, el equipo ERM debe involucrarse en esta actividad como guía. Adicionalmente, todo este trabajo debe ser documentado y el impacto escogido debe estar representado en otra tabla que tendrá la planificación de respuesta al riesgo como se muestra en la **Figura 3.10** continuación:

Figura 3.10: Ocurrencia, Impacto y Costos Esperados

Riesgos Identificados	Nivel de Ocurrencia	Nivel de Impacto	Punutación Individual	Rango	Impacto en Costo	Valor o Costo Esperado	Planificación para Mitigar Riesgo?
a	0,68	0,75	0,51	1	$ 500.000,00	$ 255.000,00	Si
h	0,55	0,87	0,48	2	$ 420.000,00	$ 200.970,00	No
d	0,41	0,9	0,37	3	$ 130.000,00	$ 47.970,00	Si
c	0,46	0,49	0,23	4	$ 10.000,00	$ 2.254,00	Si
g	0,76	0,28	0,21	5	$ 45.000,00	$ 9.576,00	Si
e	0,19	0,44	0,08	6	$ 88.000,00	$ 7.356,80	No
f	0,28	0,18	0,05	7	$ 230.000,00	$ 11.592,00	No
b	0,15	0,22	0,03	8	$ 225.000,00	$ 7.425,00	No

Como se puede observar en el cuadro, los riesgos han sido ordenados por rangos y sus impactos en costos estimados han sido ubicados también en la tabla utilizando el mismo ejemplo de la tabla anterior. La columna "Valor o Costo Esperado" es la multiplicación de la "Puntuación Individual" y el "Impacto en Costo" y se entiende como el costo de incurrir en ese riesgo determinado. En la columna "Planificación para Mitigar Riesgo" se menciona si los grupos encargados de definir la respuesta al riesgo están dispuestos en incurrir en los costos necesarios para mitigarlos o simplemente la organización ha decidido convivir con ese riesgo pese al posible impacto identificado, esto se revisará más detenidamente en el Paso 4 del Sistema de Gestión de Riesgos.

Esta tabla contiene valores que no pueden expresarse por sí solos, es necesaria la interpretación de un especialista dentro del equipo ERM o del Director de Riesgos. Las conclusiones que se asignarán a cada riesgo identificado utilizando la tabla dependerán de las perspectivas de los analizadores. Por ejemplo, el riesgo **a** tiene un nivel de ocurrencia e impacto alto, así como también el costo esperado más elevado en el caso de que se incurra en el riesgo. Este es uno de

los riesgos que debe ser analizado de inicio a fin como un potencial candidato para su mitigación, utilizando distintas acciones correctivas. Si se sigue el orden de la tabla, el riesgo **h** de igual manera tiene niveles altos de impacto y ocurrencia, así como también un alto costo; sin embargo, el costo de saneamiento para la mitigación de este riesgo es demasiado elevado y la organización no cuenta con los recursos necesarios para realizar acciones correctivas. En este caso, el Consejo Directivo ha decidido vivir con el riesgo dentro de su tolerabilidad y realizar un análisis individual para el mismo en búsqueda de otras alternativas de saneamiento. Otros riesgos podrán tener altos niveles de impacto pero bajos niveles de ocurrencia o viceversa y podría considerarse como innecesaria la implementación de acciones costosas para mitigarlos e inclusive encontrarse dentro de los niveles aceptables de riesgo e impacto.

Este cuadro resumen de los riesgos identificados con los pasos anteriormente expuestos se compone como una de las herramientas más útiles para el mapeo de riesgos de una empresa. Asimismo, es una excelente ayuda en la toma de decisiones para la remediación de aquellos riesgos peligrosos para la empresa y también como una guía para definir prioridades en proyectos. En el **Anexo 3** se muestran las matrices de riesgos consolidadas que debe utilizar MM S.A. una vez finalizadas las reuniones de identificación y asesoramiento de riesgos, estas fueron desarrolladas por el Ing. Wilson Silva. Además se incluye un formato para el programa de revisiones de Selfassessments de Controles Internos y otros para la determinación de las consideraciones que se tomaron en cuenta para

definir los niveles de ocurrencia de los riesgos y niveles de impacto en base al apetito al riesgo y sus tolerancias.

3.4 PASO 4 – RESPUESTA AL RIESGO

3.4.1 Componente 5: Respuesta al riesgo

La respuesta que se debe dar a los riesgos identificados se basa como ya se mencionó anteriormente en las consideraciones de probabilidad, impacto, costo y beneficio. Esta no es una tarea fácil, sin embargo, para clasificar de mejor manera estas estrategias se recomienda que MM S.A. considere las siguientes categorías de respuestas (Robert R. Moeller- John Wiley & Sons - Citación de Enterprise Risk Management Integrated Framework 2004, 2011) **(Propuesta, ver numeral 3.8)**:

- **Abandonar:** Esto se refiere a abortar la actividad que causa el riesgo, es decir, dejar de realizarla, cambiar su espacio geográfico, desatender una unidad, etc. Es difícil que una compañía decida finalmente dejar de realizar una actividad para la cual ha invertido muchos recursos, por ejemplo en el caso de productos, maquinarias nuevas, bodegas o fábricas, inversiones, contratos, etc. Generalmente una empresa podría considerar permanecer con el riesgo hasta que se produzca en el peor de los casos. Se considera que una de las mayores razones para que se

utilice esta estrategia es la consideración que tenga la compañía en relación al apetito al riesgo para el objetivo de la actividad o procesos que envuelve el riesgo mencionado

- **Reducir:** Esta es generalmente la respuesta que una compañía esperaría aplicar. Existen varias acciones que MM S.A. podría efectuar para evitar un riesgo, estas acciones surgen de las reuniones que se mantienen con los participantes del proceso; hay muchas posibilidades para este tipo de estrategias, sin embargo, muchas veces podría no ser conveniente por los costos asociados o por desviaciones en relación al apetito al riesgo.

- **Compartir:** Esta estrategia permite a una compañía dividir los costos asociados al riesgo en caso de que ocurra a través de algunas alternativas como por ejemplo pólizas de seguros. Se ha visto que en la actualidad prácticamente todo puede ser asegurado, sin embargo existe un costo significativo para hacerlo. Otra práctica que se realiza a nivel financiero son compras o ventas de opciones en bolsas de valores internacionales, en el caso de MM S.A. esto podría ser impracticable a causa de que en Ecuador la Bolsa de Valores es relativamente primitiva comparada con los instrumentos financieros existentes en el mundo. La mejor acción que podría acceder MM S.A. en este sentido es la contratación de seguros para respaldar sus activos y otras acciones como contratación de terceros para la realización de actividades operativas de la organización a esto se le llama Outsourcing.

- **Aceptar:** Se podría presentar esta estrategia en caso de riesgos inherentes que no pueden ser controladas por la compañía, es decir, no existen acciones que mitiguen la probabilidad de ocurrencia del riesgo o su impacto y se decide convivir con el riesgo independientemente de los impactos que este traiga. En ciertos casos los costos de aplicar una estrategia de reducción pueden ser tan altos que la compañía no estaría al alcance de implementarla, en estos casos se recomienda a MM S.A. que se determine esta acción de manera documentada y que se modifique el apetito al riesgo en caso de que no se hayan estipulado estas consideraciones en el establecimiento de objetivos.

MM S.A. debe identificar meticulosamente las estrategias que se deben aplicar para cada uno de los riesgos identificados en base a las 4 categorías que se mostraron en la sección anterior, inclusive la respuesta al riesgo puede tener fusiones de dos estrategias distintas en base a condicionantes para su aplicación por ejemplo. Por otro lado la identificación de un riesgo podría desencadenar acciones que deben ser tratadas como un proyecto a futuro con actividades que duren varios meses y con costos bastante significativos.

La respuesta al riesgo es un tema más profundo ya que necesita de mucho análisis en ciertos casos, en otros la respuesta podría ser obvia y reconocida por la experiencia de la misma u otras compañías del medio. También demanda una gran responsabilidad para los Gerentes/Directivos que deciden optar por cualquiera de las estrategias en consideración a los costos y otras variables que

podrían afectar a la estabilidad de las operaciones y por ende al alcance de los objetivos propuestos. Cabe mencionar que el apetito al riesgo es la guía primordial para la toma de decisiones en este aspecto.

Para que MM S.A. empiece con el análisis de las respuestas al riesgo, debe priorizar los ya identificados como se muestra en la **Figura 3.7** de la sección de administración del riesgo en donde se detallan 4 cuadrantes de riesgos por probabilidad e impacto de la ocurrencia. Esta matriz es de gran utilidad para iniciar las estrategias de mitigación priorizando aquellos riesgos que se encuentra en el cuadrante dos (Alta probabilidad y alto impacto).

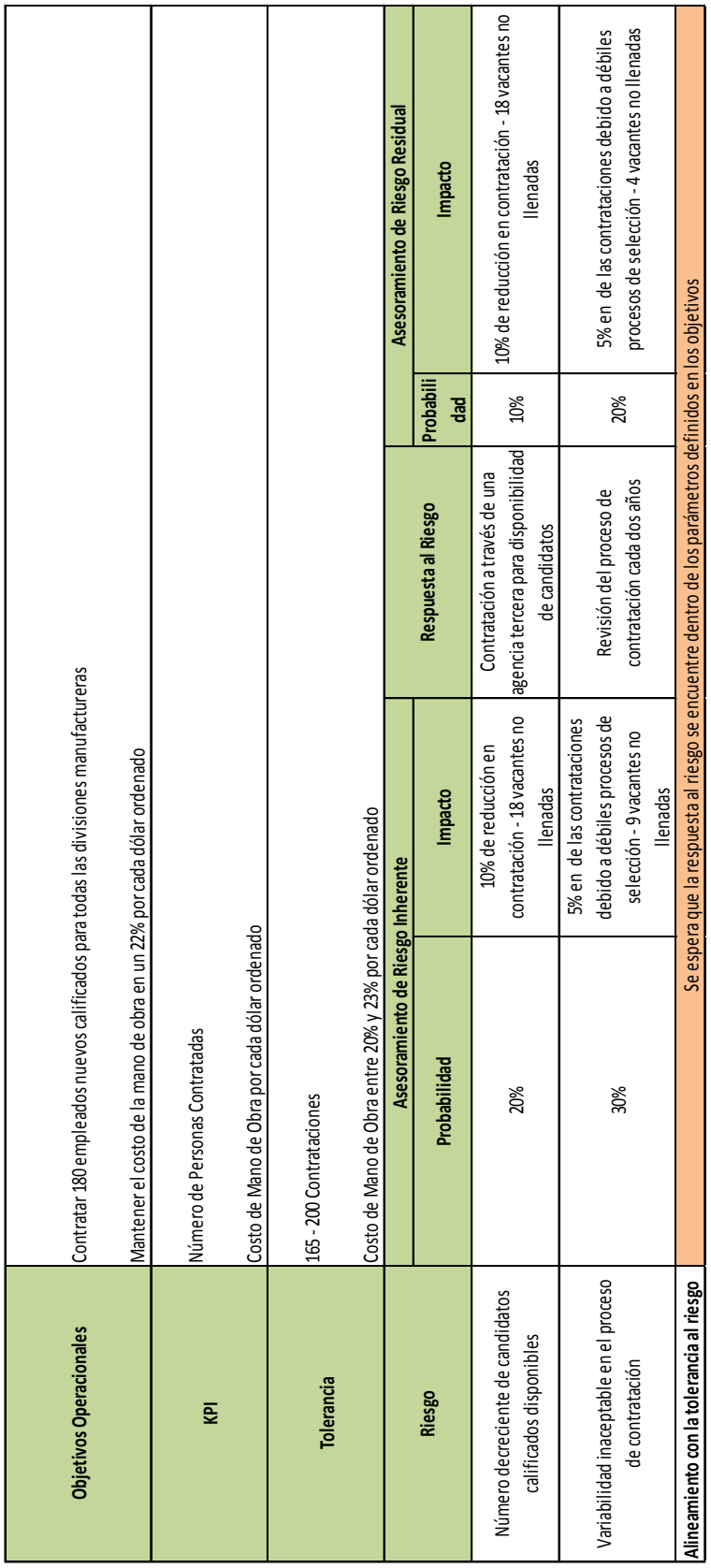
Las alternativas para mitigar los riesgos identificados deben ser propuestas por los participantes de los Talleres Simples de Reconocimiento posterior al análisis de priorización. Los responsables de los riesgos designados para cada proceso deberán comunicar los eventos identificados a los Directores de Unidad en caso de que los mismos no hayan asistido a los talleres. El Director de Unidad comunicará los riesgos y estrategias de mitigación propuestas en los talleres en la reunión de Comité Ejecutivo. Finalmente, con las estrategias definidas se consolidará la información por parte del Equipo ERM para el envío de un reporte completo para aprobación al Consejo Directivo.

Es imperante detallar todos los costos asociados a las estrategias para un análisis de costos versus beneficios. Además, se debe intentar asociar a los diferentes riesgos identificados con los mismos impactos, por ejemplo, impacto en

ingresos, gastos, contingentes legales, participación en el mercado, indicadores de preferencia del consumidor, etc. Es posible que sea necesaria una nueva estimación de los impactos identificados en las secciones anteriores para incluir los costos de la respuesta al riesgo. Este análisis puede ser complicado pero tiene excelentes resultados en la organización.

A continuación se muestra un ejemplo ilustrativo en la **Figura 3.11** para la propuesta que se hace a MM S.A. en este sentido, tomando el ejemplo que se ha venido manejando desde el establecimiento de objetivos (Committee of Sponsoring Organizations of the Treadway Commission, 2004):

Figura 3.11: Respuesta al Riesgo en Riesgos Inherentes y su Impacto en Riesgos Residuales



Objetivos Operacionales	Contratar 180 empleados nuevos calificados para todas las divisiones manufactureras Mantener el costo de la mano de obra en un 22% por cada dólar ordenado					
KPI	Número de Personas Contratadas Costo de Mano de Obra por cada dólar ordenado					
Tolerancia	165 - 200 Contrataciones Costo de Mano de Obra entre 20% y 23% por cada dólar ordenado					
Riesgo	Asesoramiento de Riesgo Inherente		Respuesta al Riesgo	Asesoramiento de Riesgo Residual		
	Probabilidad	Impacto		Probabilidad	Impacto	
Número decreciente de candidatos calificados disponibles	20%	10% de reducción en contratación - 18 vacantes no llenadas	Contratación a través de una agencia tercera para disponibilidad de candidatos	10%	10% de reducción en contratación - 18 vacantes no llenadas	
Variabilidad inaceptable en el proceso de contratación	30%	5% en de las contrataciones debido a débiles procesos de selección - 9 vacantes no llenadas	Revisión del proceso de contratación cada dos años	20%	5% en de las contrataciones debido a débiles procesos de selección - 4 vacantes no llenadas	
Alineamiento con la tolerancia al riesgo	Se espera que la respuesta al riesgo se encuentre dentro de los parámetros definidos en los objetivos					

Una vez que se han realizado estas actividades es primordial que MM S.A. detalle todos los riesgos identificados, probabilidades de ocurrencia, impactos, respuestas al riesgo con costo versus beneficio ligados con los objetivos de la organización y se compendien en un denominado **Portafolio de Riesgos**. Este es el objetivo principal que Contraloría como equipo ERM debe presentar a Dirección General para soportar adecuadamente la toma de decisiones basado en un sistema técnico y completo de riesgos para toda la entidad. El formato del portafolio de riesgos puede ser elaborado de acuerdo a las necesidades del Consejo de Dirección. De todas maneras se recomienda que se revisen los formatos establecidos por COSO II en su texto ERM Application Techniques como referencia.

Posteriormente, Dirección General en conjunto con las diferentes Directivas de MM S.A. deberá analizar las propuestas generadas en las reuniones de Comité Ejecutivo para lo cual se recomienda que se aumente una reunión adicional cada vez que esto suceda, es decir, una vez al año y cuando existan nuevas propuestas de negocios. Las estrategias de respuesta al riesgo deberán ser aprobadas por Dirección General, Compliance y Dirección Financiera físicamente en el reporte entregado por ERM. Se pueden presentar cambios a las estrategias u otras consideraciones relacionadas al procedimiento de establecimiento de objetivos para lo cual el equipo ERM debe coordinar dichos cambios con las diferentes áreas involucradas en los procesos y proceder nuevamente a la aprobación.

Otros documentos que resultarán de este análisis son nuevas políticas y procedimientos en relación a las respuestas al riesgo aprobaciones físicas de los reportes enviados por el equipo ERM, comunicados internos para nuevas directrices, contratos con proveedores y todo documento concerniente a las estrategias escogidas.

3.5 PASO 5 – CONTROL DE RIESGOS

3.5.1 Componente 6: Actividades de control

Las actividades de control que se deben realizar por parte de MM S.A. para identificar que las estrategias de respuesta al riesgo y políticas y procedimientos resultantes del anterior paso, son similares a las prácticas que se realizan en la actualidad en la compañía llamadas Selfassessments of Internal Controls pero enfocadas en riesgos en base a los puntos ya revisados. Se recomienda que se consideren los siguientes conceptos al momento de realizar estas revisiones (Robert R. Moeller- John Wiley & Sons - Citación de Enterprise Risk Management Integrated Framework 2004, 2011) **(Propuesta, ver numeral 3.8)**:

- Desarrollar un profundo entendimiento de los riesgos identificados y elaborar procedimientos de control para monitorearlos.

- Crear procedimientos de pruebas para determinar si los controles establecidos están funcionando correctamente.

- Aplicar los procedimientos de pruebas.

- Realizar ajustes o mejoras de estos procedimientos en caso de que sean necesarios.

En el ERM Integrated Framework se mencionan consideraciones mínimas que deben contener los procedimientos de control en los procesos de la compañía. Sin embargo, MM S.A. ya presenta en ciertos casos actividades de control para determinar que una estrategia implementada en una política se está llevando a cabo. Lo que se puede recomendar en este caso es que esta práctica sea definida para todos los procesos de la compañía y no solo para aquellos "core" del negocio y que por otro lado se estandaricen estos procedimientos en documentos formales firmados por el Director de Riesgos y el Equipo ERM como ya se explicó en secciones anteriores.

Otra consideración que debe tener la compañía es que se asignen responsables para cada proceso con sus respectivos indicadores para que se formalicen sus responsabilidades como agente de control interno y riesgo. Es decir, cada proceso debe contar con puntos de control que deben ser monitoreados constantemente por los responsables asignados a través de los indicadores que ya

genera la compañía con los varios sistemas desarrollados y explicados en el capítulo II. Esto también ayudará a que la compañía refuerce la filosofía del riesgo y control como uno de los pilares más importantes del sistema. Es necesario también que estas responsabilidades sean documentadas por parte del equipo de ERM y firmadas por el Director de Riesgos que en este caso será el Director Financiero. En MM S.A. se pueden asignar las responsabilidades de control de la siguiente manera y reportando sus novedades el equipo ERM:

- **Proceso de OtC (Order to Cash):** 1 responsable para las funciones de cuentas por cobrar y emisión de notas de crédito y facturas por descuentos, bonificaciones, regularizaciones y otros, 1 responsable para las liberaciones y procedimiento general de devoluciones en finanzas, 1 responsable para las funciones de despacho de ventas, recepción de devoluciones y canjes en bodega, 1 responsable para los controles en la coordinación logística para los mismos movimientos de inventarios, 1 responsable para el manejo de precios, costos, mantenimiento y ajustes de inventario, 1 responsable para las actividades de facturación, 1 responsable para las negociaciones institucionales, 1 responsable para asuntos comerciales relacionados con ventas y comunicación con los clientes.

- **Proceso de PtP:** 1 responsable para cuentas por pagar y administración de los sistemas, 1 responsable para el manejo de tesorería, todos los

usuarios que ingresan y aprueban responsables de la correcta facturación para pago y reportes de gastos de empleados.

Todas estas personas deben seguir una capacitación correspondiente acerca de cómo se deben comunicar los eventos adversos identificados y se deberá desarrollar un formato estandarizado para reportar estas actividades. También es necesario asegurar que cada uno de los responsables conozca perfectamente las actividades de control que deben realizar, así como también las políticas y procedimientos relacionados.

Como último punto relevante en monitoreo, se recomienda a MM S.A. que se haga un cuadro resumen de todas las observaciones obtenidas a través de los Selfassessments de manera que sea posible realizar un seguimiento mensual posterior y verificar que las estrategias establecidas se están aplicando eficientemente o establecer nuevas medidas de control.

3.6 PASO 6 – CAPTACIÓN DE INFORMACIÓN Y REPORTAJE

3.6.1 Componente 7: Información y comunicación

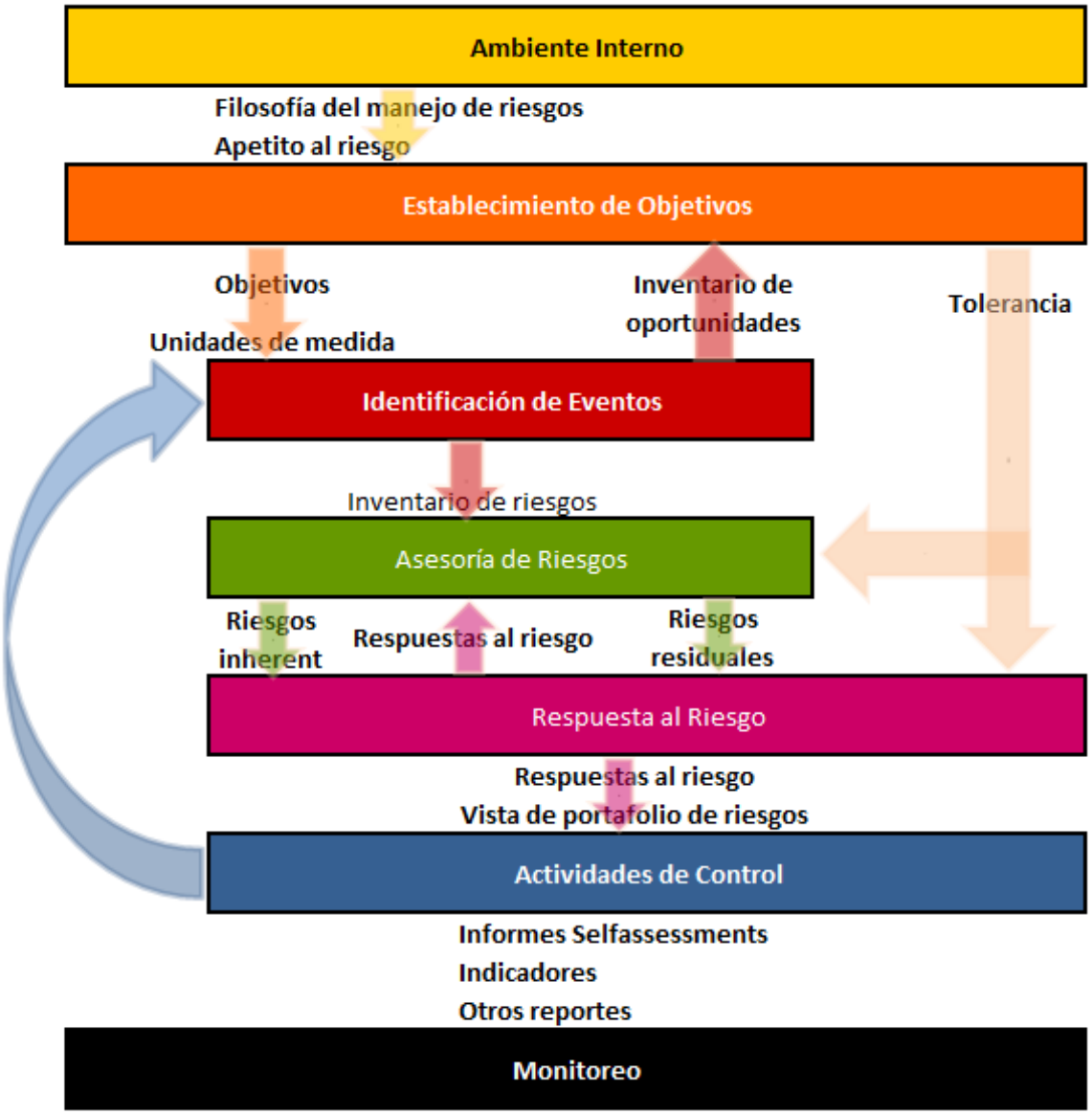
En esta parte básicamente se realizarán recomendaciones en relación a cómo se debe manejar la información del Sistema de Gestión de Riesgos de MM S.A.

para que cumpla con sus propósitos y que se puedan realizar acciones oportunas. Por otro lado se retomarán acciones importantes en cuanto a la comunicación que se debe impartir por parte de la Dirección General para reforzar ciertos componentes revisados anteriormente como la filosofía del manejo del riesgo.

El Sistema de Gestión de Riesgos propuesto necesita de un trabajo eficiente en cuanto a los mecanismos de comunicación entre cada paso. Además se deben definir las maneras en que la compañía deberá llevar su información de manera que se puedan tomar decisiones en un tiempo adecuado.

La **Figura 3.12** a continuación muestra el flujo de información y comunicación que recorren las actividades del Sistema de Gestión de Riesgos, se podría decir que este componente es el engranaje a través del cual toda la metodología funciona **(Propuesta, ver numeral 3.8)**:

Figura 3.12 Flujo del Sistema de Gestión de Riesgos en MM S.A.



Como se muestra en la gráfica todo el sistema tiene una serie de documentos resultantes del sistema como tal para los cuales se han asignado sus respectivos responsables y que se resumen de la siguiente manera:

- **Componente 1:** Filosofía del manejo de riesgos (Consejo de Dirección, Equipo ERM) que está compuesto por el cuestionario de la **Figura 3.1**; Apetito al riesgo (Consejo de Dirección, Director de Riesgos, Equipo ERM, Comité Ejecutivo, Gerencias Medias, Empleados en General) que está compuesto por los pasos expuestos para la identificación de riesgos y los objetivos de la compañía.

- **Componente 2:** Objetivos, KPI, Tolerancia al riesgo (Todos los empleados), Inventario de oportunidades (Equipo ERM, Comité Ejecutivo, Gerencias Medias, Empleados en General).

- **Componente 3:** Inventario de Riesgos (Equipo ERM).

- **Componente 4:** Riesgos Inherentes y Residuales (Equipo ERM, Comité Ejecutivo, Gerencias Medias, Empleados en General).

- **Componente 5:** Respuestas al riesgo y Portafolio de riesgos (Consejo de Dirección, Director de Riesgos, Equipo ERM, Comité Ejecutivo, Gerencias Medias, Empleados en General).

- **Componente 6:** Informes de Selfasessments; Indicadores de Gestión; Otros reportes (Equipo ERM, Director de Riesgos, Responsables de riesgos para cada proceso).

- **Componente 8:** Monitoreo que se hablará más adelante.

Toda la información es alimentada en cada estructura o componente en base a las flechas que se han establecido en la gráfica. En el COSOII se muestra cómo el Sistema de Gestión de Riesgos fluye con sus componentes en un proceso de ventas de una empresa ejemplo.

Las tareas que se deben llevar a cabo para presentar la información de una manera adecuada a través de todo el flujo son cruciales y puede requerir de muchas medidas, como formatos estandarizados que de hecho deben ser desarrollados por el Equipo ERM. En este sentido se recomienda a MM S.A. que desarrolle un proyecto con la participación indispensable del Departamento de IT para identificar alternativas para llevar esta información y que pueda ser monitoreada constantemente por el Equipo ERM. El Sistema de Gestión de Riesgos no tendrá ningún efecto positivo si no se establece un mecanismo a través de sistemas para el flujo de la información y comunicación de las partes.

Por lo pronto MM S.A. puede utilizar un sistema que ya se ha desarrollado a nivel corporativo y que se fundamenta en los conceptos del GRC. Este sistema

aún no ha sido aplicado para las regiones de Latinoamérica pero está previsto que los mercados de la región mencionada lo utilicen a partir del primer trimestre del 2015, fecha en la cual se deben incluir todos los mecanismos de control que tiene MM S.A. para identificación de riesgos y actividades de monitoreo. De esta manera MM S.A. se estaría alineando con los requerimientos corporativos y tendrá un sistema que puede contener todo el flujo de información resultante de la implementación de la metodología abarcada en este documento.

Aparte de estas acciones se recomienda también que se haga un levantamiento de todos los indicadores de gestión que están disponibles para MM S.A. en la actualidad a través de los diferentes sistemas y servicios de terceros para introducir esta data dentro de los componentes del Sistema de Gestión de Riesgos como sea necesario. Por ejemplo es evidente que para que los empleados responsables de riesgos en cada proceso puedan controlar sus actividades, cuenten con indicadores de sus procesos asignados. De otra manera no podrán evaluar adecuadamente el funcionamiento de estrategias de respuesta a riesgos y oportunidades que han sido aprobadas por el Consejo de Dirección y materializadas en políticas y procedimientos.

Siguiendo con lo propuesto en el COSO II, MM S.A. debe, a través de Dirección General y el Consejo de Dirección, realizar una declaración de la filosofía del manejo del riesgo en la compañía y su importancia. A pesar de que el Código de

Conducta es modificado y comunicado por Casa Matriz, MM S.A. puede utilizar otros medios para comunicar este particular:

- E-mails

- Noticias Corporativas a través de una iniciativa interna que en la actualidad ya realiza acciones en este sentido para encontrar recursos en la web.

- Grupos de discusión a través de la web.

- Acceso a información de riesgos identificados para el personal autorizado.

- Mensajes de Texto.

- Reuniones presenciales o remotas.

- Comunicados escritos pegados en las instalaciones de la compañía.

- Reuniones con el Equipo ERM, Director de Riesgos, Comité Ejecutivo para riesgos.

- Entrenamientos para el Equipo ERM especializando nuevas habilidades en la materia.

- Auspicio y comunicación a todos los empleados sobre nuevas tecnologías y procedimientos establecidos para detección de riesgos.

- Noticias sobre eventos adversos ocurridos en la industria y en otros campos.

- Otros.

3.7 PASO 7 – MONITOREO DEL PERFORMANCE Y CUMPLIMIENTO

3.7.1 Componente 8: Monitoreo

Para que MM S.A. pueda asegurarse que el Sistema de Gestión de Riesgos está funcionando adecuadamente en todos sus componentes, debe establecer mecanismos de monitoreo de alta visualización. Esto se puede llevar a cabo

determinando controles de revisión continuo o a través de pruebas separadas en varios aspectos del sistema.

En el Paso 6 – Actividades de Control se mencionaron ya algunos mecanismos para evaluar el funcionamiento de los controles establecidos por cada área. Esta misma actividad puede ser implementada para el funcionamiento del Sistema de Gestión de Riesgos. Se había también acotado que MM S.A. presenta varios indicadores de gestión que se obtienen interna y externamente, sin embargo, la periodicidad de la revisión de esos indicadores o su disponibilidad son cruciales en el componente del monitoreo.

Algunos procesos de MM S.A. tienen ya sus propios indicadores que se generan automáticamente o a través de la utilización de sistemas simples de manera diaria, semanal o mensual. Generalmente estos indicadores se presentan en áreas bastante sensibles como Calidad, Inventarios, Reporte de Eventos Adversos, Logística, otros. Estos indicadores permitirán a los responsables de riesgos designados para cada proceso y función, como también al Equipo ERM, a evaluar el funcionamiento del Sistema de Gestión de Riesgos en relación a los puntos de control identificados y a las estrategias propuestas. Es bastante similar a las actividades de control, sin embargo, para la realización de este trabajo se ha identificado la necesidad de establecer otros mecanismos para revisar el flujo de la información por parte del sistema como tal.

En este sentido se recomienda a MM S.A. que se mantengan reuniones cada dos meses con los responsables de riesgos para cada proceso y el Equipo ERM con el fin de levantar novedades de control en cada área y realizar cuestionarios prefabricados que especifiquen puntos de monitoreo en el Sistema de Gestión de Riesgos. Además, para el nuevo sistema corporativo se deben realizar pruebas comprobando que toda la información ingresada está actualizada con respecto a las novedades obtenidas cada dos meses basado en las reuniones mencionadas. También se debe considerar la posibilidad de introducir personal externo a la compañía para asesorar ciertos puntos del Sistema de Gestión de Riesgos con conocimientos técnicos en cada área **(Propuesta, ver numeral 3.8)**.

Otra actividad que es importante para presentar un correcto monitoreo es incentivar a los empleados en general que reporten falencias en el sistema y otras consideraciones no tomadas en cuenta el momento de implementarlo por primera vez. Además, se recomienda documentar el flujo de todos los primeros procesos analizados para detectar ineficiencias y mejorar el Sistema de Gestión de Riesgos una y otra vez.

El COSO II propone estrategias para revisiones específicas que se pueden dar cada determinado lapso de tiempo, estos de cierta manera ya fueron mencionados en otros componentes del sistema, sin embargo se recomienda a MM S.A. que considere la realización de las siguientes revisiones (Robert R. Moeller- John Wiley & Sons - Citación de Enterprise Risk Management Integrated Framework 2004, 2011):

- **Diagramas de Flujo:** Como se había mencionado anteriormente, los diagramas de flujo forman una parte fundamental de la documentación de un determinado proceso. El Equipo ERM debe revisar, en determinados tiempos, los procedimientos definidos en cada área y verificar si en el momento revisado se ajustan a la realidad. De esta manera, se deben actualizar los mencionados documentos junto con sus políticas y los diagramas de flujo, así también es posible determinar si los riesgos en un proceso están correctamente determinados y si se están cumpliendo las estrategias propuestas.

- **Revisión de los documentos del Sistema de Gestión de Riesgos:** Se recomienda que MM S.A. cada trimestre revise los documentos del proceso del Sistema de Gestión de riesgos para identificar eficiencias de las acciones que se están implementando, esto puede ser realizado por el equipo ERM junto con los responsables de riesgos en cada proceso.

- **Benchmarking:** Es importante identificar otras empresas en el medio que utilicen Sistemas de Gestión de Riesgos y verificar prácticas que podrían servir a MM S.A. Es posible que esta información sea muy difícil de conseguir dado que podría ser considerada confidencial en otras compañías, sin embargo, puede ser de mucha utilidad. Sin embargo, MM S.A. puede intentar realizar esta actividad en otras sucursales alrededor del mundo.

- **Grupos Focales:** Otra actividad que se recomienda en MM S.A. es realizar reuniones con grupos focales que brinden sus perspectivas acerca del funcionamiento del sistema de Gestión de Riesgos implementado en la compañía con sugerencias e información sobre el estatus de los riesgos identificados en sus áreas. Esto también se podría realizar con la iniciativa del Equipo ERM y el auspicio del Director de Riesgos.

Hasta este punto finaliza la propuesta realizada a MM S.A. para el establecimiento de un Sistema de Gestión de Riesgos en base a los fundamentos teóricos y técnicas prácticas emitidas por COSO en su libro Enterprise Risk Management Integrated Framework. La propuesta podría cambiar de cierta manera el enfoque que en la actualidad tiene la compañía para manejar sus procedimientos de control interno; sin embargo, como se ha observado en todos los componentes del COSO II, el sistema tiene fundamentos muy interesantes que tienen efectos muy positivos en la salud organizacional y pueden ser puestos en práctica con acciones y actitudes basadas en la filosofía del manejo de riesgos.

Se finaliza esta sección con un cuadro resumen de las propuestas formuladas para cada componente y los pasos que una empresa multinacional en general debe seguir para implementar un sistema de gestión de riesgos:

3.8 RESUMEN DE DEBILIDADES Y PROPUESTAS DEL SISTEMA DE GESTIÓN DE RIESGOS DE MM S.A.

2.1.1 Ambiente Interno				
Situación actual de la filosofía del manejo de riesgos en MM S.A.				
No.	**Debilidades**	**Pág. Deb.**	**Propuestas**	**Pág. Prop.**
2.1.1.1.1/3.1.1.1	Políticas y procedimientos no contienen consideraciones expresas del riesgo y en otros casos tampoco mencionan el motivo por el cual los controles se llevan a cabo.	Pág. 38	Mencionar en los comunicados, políticas y procedimientos a la importancia de la detección de riesgos. Implementar una campaña de concienciación sobre el riesgo a través de e-mails, mensajes de texto o reuniones presenciales. Hacer una encuesta sobre los atributos de la filosofía del riesgo.	Pág. 118
	Integrantes de los procesos no tienen una visión clara del control (puntos de control) y se considera que ésta es una función única del área de Contraloría.	Pág. 39	Para los responsables del control en cada proceso, asignar tareas ej. Repasos de políticas y procedimientos ya existentes, reportes de eventos adversos identificados en el día a día, identificación de "áreas grises" en los procesos involucrados, asignación de responsabilidades en un punto del proceso, importancia del control en el proceso, certificado de conocimiento de políticas e indicadores, etc. Cada empleado de la compañía debe efectuar un control en sus actividades.	Pág. 116
	Empleados no conocen todas las políticas y procedimientos que influyen en sus procesos.	Pág. 40		

No.	Debilidades	Pág. Deb.	Propuestas	Pág. Prop.
2.1.1.1.1/3.1.1.1	El Departamento de Contraloría que se encarga del control interno no tiene conocimiento preciso de todas las políticas y procedimientos locales existentes y tampoco se muestra en estándar para desarrollarlos. Aparte, no se definen de manera específica puntos de control claves.	Pág. 41	Realizar un inventario total de todos los documentos que reflejen lineamientos. Archivar los documentos dentro del Área de Contraloría. Identificar la validez de dichos documentos y relacionarlos con las políticas corporativas a las que hacen mención. Analizar cada documento con las áreas correspondientes para identificar actualizaciones u oportunidades de mejora y actualizar.	Pág. 120
	No se presenta una política local de control interno o Sistema de Gestión de Riesgos.	Pág. 41	Elaborar un documento que norme y describa los nuevos procedimientos del Sistema de Gestión de Riesgos, contar con asesoría del Director de Riesgos. Otro documento para las revisiones de Selfassessments de Controles Internos con aspectos mencionados en la página 121. MM S.A. deberá incluir diagramas de flujo en todos los procesos nuevos y antiguos.	Pág. 121
	Procedimientos formales no contienen diagramas de flujos.	Pág. 42		

Situación actual del apetito al riesgo de MM S.A.				
No.	**Debilidades**	**Pág. Deb.**	**Propuestas**	**Pág. Prop.**
2.1.1.2.1/3.1.1.2	MM S.A. no presenta un conocimiento escrito, documentado o formalizado de los niveles de riesgo que se aceptan en sus procesos.	Pág. 44	Se recomienda desarrollar, comunicar a través de un documento formal, monitorear y actualiza el apetito al riesgo. Para esto se deben identificar los riesgos de acuerdo al componente de identificación de eventos en todas las áreas (iniciar con los más sensibles de la operación), determinar los niveles aceptables de riesgos para cada proceso en base a las políticas, procedimientos, declaraciones de código de conducta y la asesoría de riesgos. A través del establecimiento de objetivos se deberá identificar niveles de tolerancia de riesgos y definir una actitud clara acerca del riesgo en diversas situaciones fundamentándose en las prácticas recomendadas en el componente de ambiente interno. Además se recomienda utilizar un mapa de apetito al riesgo que sea práctico y utilizable por todos los miembros de la compañía.	Pág. 122

Situación actual de la actitud de la Junta Directiva de MM S.A., estrategia y organización.				
No.	**Debilidades**	**Pág. Deb.**	**Propuestas**	**Pág. Prop.**
2.1.1.3.1/3.1.1.3	MM S.A. en la localidad no cuenta con un Comité de Auditoría o de Riesgos. Estas funciones las asume de manera parcial el Área de Contraloría. Las funciones como comité se realizan de manera parcial debido a que el Área de Contraloría no reporta ni cuestiona asuntos de control directamente con el Comité Ejecutivo mencionado anteriormente y en pocas ocasiones forma parte de la elaboración de nuevos modelos y estrategias de negocio que se proponen en la compañía.	Pág. 47	Establecer un Departamento de Riesgos de acuerdo al tipo de organización para el sistema propuesto (**Figura 3.4),** las líneas del negocio y las gerencias medias son las encargadas de identificar, asesorar y responder a los riesgos identificados. Esta consideración se da por la escasez de recursos en el equipo ERM. En un nivel más arriba se encuentran las diferentes directivas como las Unidades de Negocio. En el último punto se encuentra el Director de Finanzas que en este caso va a ser el Director de Riesgos de MM S.A. en Ecuador junto con el Director General de la compañía cuya participación es crucial para complementar el enfoque de gobierno. La estructura específica y funciones de cada uno de los miembros se deben establecer de acuerdo a lo mencionado en el numeral 3.1.1.3, ver índice.	Pág. 129
	El Área de Contraloría no cuenta con ayuda externa para realizar revisiones de control o aseguramiento de gestión de riesgos.	Pág. 48	Se recomienda a MM S.A. que identifique opciones de proveedores dentro del mercado que brinden asesoría en gestión de riesgos y que se coordine con el Equipo ERM y su Director para la contratación de expertos en el tema, de no ser posible en el corto plazo por varios factores, es importante que al menos se lo realice luego de la primera estructuración del sistema y posteriormente cada dos años.	Pág. 139

No.	Debilidades	Pág. Deb.	Propuestas	Pág. Prop.
2.1.1.3.1/3.1.1.3	La revisión de Auditoría Interna Corporativa se hace cada dos años aproximadamente y no incluye todos los procesos que se manejan localmente, además, se fundamenta en la detección de eventos en base a guías corporativas y que en algunos casos no se ajustan a las actividades locales que se realizan en la sucursal.	Pág. 48	Es fundamental que MM S.A. haga un levantamiento de todos los procesos de la compañía y realice los pasos de identificación, asesoría y control de riesgos. En este sentido, establecer puntos clave de control y documentarlo para cada proceso. Esta será la base para estandarizar los selfassessments y que contengan las variables importantes para la localidad, asimismo, esto servirá para que la compañía pueda hacer revisiones concisas y que fluyan rápidamente en el futuro.	Pág. 140
	El selfassessment se basa en lineamientos corporativos diseñados para un sistema contable distinto al que utiliza la sucursal en Ecuador. .	Pág. 49		
	No existe un procedimiento estandarizado para las revisiones de control interno que realiza Contraloría con los puntos más importantes en cada proceso, se identificó que para ciertas observaciones no se realiza un seguimiento específico posterior.	Pág. 49		
Situación actual del compromiso con la competencia de MM S.A.:				
No.	**Debilidades**	**Pág. Deb.**	**Propuestas**	**Pág. Prop.**
2.1.1.5.1/2.1.2.1	Los proyectos pequeños que se llevan a cabo en MM S.A. en ocasiones no se materializan y se podría considerar que se necesitan mayores acciones para que todos los proyectos independientemente de su tamaño puedan cumplir con su propósito.	Pág. 61	Este punto se remedia con las acciones que se deben realizar en el componente de establecimiento de objetivos.	Pág. 141

No.	Debilidades	Pág. Deb.	Propuestas	Pág. Prop.
2.1.1.5.1/2.1.2.1	El seguimiento para el cumplimiento de objetivos lo debe manejar cada empleado con ayuda de su supervisor sin un cronograma establecido o indicadores específicos para su monitoreo. En ocasiones esto podría provocar el incumplimiento de algunos objetivos o que sean llevados a cabo a último momento, antes que finalice el año. Esto afecta a la competencia profesional que se maneja a nivel gerencial para el cumplimiento de objetivos más específicos.	Pág. 61	Este punto se remedia con las acciones que se deben realizar en el componente de establecimiento de objetivos.	Pág. 141
Situación actual de la estructura organizacional de MM S.A.				
No.	**Debilidades**	**Pág. Deb.**	**Propuestas**	**Pág. Prop.**
2.1.1.6.1/3.1.1.3	No se presenta una estructura sistemática específica para administrar un Sistema de Gestión de Riesgos de manera adecuada, el enfoque está más centrado en el control interno. Es necesario establecer un Departamento de Riesgos dentro de la sucursal que permita una mejor coordinación de las actividades de control basada en riesgos.	Pág. 65	Establecer un Departamento de Riesgos de acuerdo al tipo de organización para el sistema propuesto (**Figura 3.4),** las líneas del negocio y las gerencias medias son las encargadas de identificar, asesorar y responder a los riesgos identificados. Esta consideración se da por la escasez de recursos en el equipo ERM. En un nivel más arriba se encuentran las diferentes directivas como las Unidades de Negocio. En el último punto se encuentra el Director de Finanzas que en este caso va a ser el Director de Riesgos de MM S.A. en Ecuador junto con el Director General de la compañía cuya participación es crucial para complementar el enfoque de gobierno. La estructura específica y funciones de cada uno de los miembros se deben establecer de acuerdo a lo mencionado en numeral 3.1.1.3, ver índice.	Pág. 129
	El Oficial de Compliance no realiza actividades relacionadas a gestión de riesgos, únicamente identifica asuntos de control en las estrategias comerciales, así como también asesora a los distintos departamentos de la compañía en temas relacionados a compliance.	Pág. 66		

No.	Debilidades	Pág. Deb.	Propuestas	Pág. Prop.
2.1.1.6.1/3.1.1.3	Contraloría y Compliance trabajan de manera separada, ciertas revisiones de control que realiza Compliance son comunicadas a Contraloría pero esto no se da en sentido contrario. Además, se ha detectado que no existe una comunicación adecuada entre las dos áreas y hay una poca coordinación para las actividades de control en conjunto.	Pág. 66	Establecer un Departamento de Riesgos de acuerdo al tipo de organización para el sistema propuesto (**Figura 3.4),** las líneas del negocio y las gerencias medias son las encargadas de identificar, asesorar y responder a los riesgos identificados. Esta consideración se da por la escasez de recursos en el equipo ERM. En un nivel más arriba se encuentran las diferentes directivas como las Unidades de Negocio. En el último punto se encuentra el Director de Finanzas que en este caso va a ser el Director de Riesgos de MM S.A. en Ecuador junto con el Director General de la compañía cuya participación es crucial para complementar el enfoque de gobierno. La estructura específica y funciones de cada uno de los miembros se deben establecer de acuerdo a lo mencionado en numeral **3.1.1.3**, ver índice.	Pág. 129
	La compañía carece de un procedimiento de control definido para que las dos áreas utilicen sistemas estándar de revisión que estén certificadas, de esta manera, las revisiones de control podrían no abarcar los puntos necesarios para mitigar riesgos que estén de acuerdo a las necesidades del negocio.	Pág. 67		
	Los informes de control emitidos por Compliance no son comunicados al Área de Contraloría, tampoco (de manera general) las decisiones de los informes entregados por las dos áreas.	Pág. 67		
	El alcance de las revisiones que realiza Contraloría está limitado a procesos Financieros.	Pág. 68		
Situación actual de los estándares de recursos humanos de MM S.A.				
No.	**Debilidades**	**Pág. Deb.**	**Propuestas**	**Pág. Prop.**
2.1.1.8.1/3.1.1.1/3.1.1.3	MM S.A. en la localidad no cuenta con procedimientos formalizados para recursos humanos.	Pág. 72	Es fundamental que MM S.A. haga un levantamiento de todos los procesos de la compañía y realice los pasos de identificación, asesoría y control de riesgos. En este sentido, establecer puntos clave de control y documentarlo para cada proceso. Esta será la base para estandarizar los selfassessments y que contengan las variables importantes para la localidad.	Pág. 140

No.	Debilidades	Pág. Deb.	Propuestas	Pág. Prop.
2.1.1.8.1/3.1.1.1/3.1.1.3	No se realizan entrenamientos semestrales o anuales para refrescamiento de políticas y procedimientos locales en la mayoría de los casos.	Pág. 73	Es necesario que el Departamento de Recursos Humanos haga un levantamiento de los cursos principales que debe realizar cada empleado en relación a su función y establecer periodos de actualización. La compañía tiene recursos suficientes para programar cursos online y que emitan certificados de cumplimiento para obtención de estadísticas anuales.	Pág. 140
2.1.2 Establecimiento de Objetivos				
No.	**Debilidades**	**Pág. Deb.**	**Propuestas**	**Pág. Prop.**
	Se identificaron las siguientes debilidades en los objetivos estratégicos y relacionados de MM S.A.: • No se utiliza el mismo idioma de clasificación de objetivos. • Los objetivos en ciertos casos son determinados en base a las consideraciones del área, más no fundamentados en las estrategias de Dirección. • Los objetivos en general no tienen KPI´s específicos que permitan establecer niveles de evaluación y cumplimiento de objetivos. • Las fechas de cumplimiento son muy flexibles y podrían afectar en la planificación para los propósitos propuestos. • El objetivo estratégico si permite que la compañía pueda alcanzar la misión general. • No se han determinado aspectos específicos en relación al apetito al riesgo aunque de cierta manera las políticas y procedimientos de la compañía si establecen lineamientos claros para determinadas situaciones.	Pág. 77,80	Se recomienda a MM S.A. que aplique los siguientes fundamentos: La misión (MM S.A. si cuenta con una misión corporativa), que es un elemento crucial en la planificación estratégica. Luego de la misión, cada Dirección de Unidad o Área debe desarrollar uno o varios objetivos estratégicos con medidas o indicadores de gestión denominados KPI´s; posteriormente se deben establecer objetivos operacionales, de reportaje y compliance por parte de cada empleado o subordinado directo de dirección. Estos deberán estar alineados con el apetito al riesgo que a su vez debe contar con otros indicadores de gestión o los denominados KPI's. Estos últimos objetivos y medidas darán los lineamientos finales para determinar los niveles de tolerancia para cada uno de los objetivos relacionados mismos que servirán de guía para que MM S.A. pueda determinar si los objetivos fueron alcanzados a cabalidad. **(Figura 3.5)**	Pág. 141

2.2.1 Identificación de Eventos				
No.	**Debilidades**	**Pág. Deb.**	**Propuestas**	**Pág. Prop.**
2.2.1.1/3.2.1	La compañía no presenta un procedimiento y flujo específico para la identificación de riesgos. Los eventos son identificados cuando se producen.	Pág. 84	Se propone que MM S.A. considere lo siguientes aspectos para la identificación de riesgos: • Eventos Económicos Externos. • Eventos Naturales de Medioambiente. • Eventos Políticos. • Factores Sociales. • Eventos de Infraestructura Interna. • Eventos de Procesos Internos. • Eventos de Tecnología Interna o Externa. El equipo ERM en coordinación con las distintas áreas debe asignar diferentes responsables de riesgos en actividades operacionales, finanzas y contabilidad, IT y gerencias de unidad. En base a los recursos de MM S.A. se recomienda las siguientes metodologías: • Un listado de eventos desfavorables que se han presentado en las compañías de la industria farmacéutica no solo en el país sino también en el mundo, pueden ser consultados en internet o a través del servicio de un tercero. • Análisis de Diagramas de Flujo: Es necesario que se elaboren diagramas de flujo en todos los procesos de la compañía. La técnica principal es el Taller Simple de Reconocimiento que funciona a través de reuniones con el personal de diferentes especialidades involucrado en el proceso, para hacer una lluvia de ideas. Referencia **Figura 3.6.** Es posible que dentro de las reuniones salten a la luz	Pág. 143
	El reporte de riesgos entregado a Contraloría Regional es realizado únicamente por una persona, basándose en sus consideraciones de las actividades que se realizan en el proceso correspondiente y no es consultado con los diferentes agentes que actúan en el proceso.	Pág. 85		

No.	Debilidades	Pág. Deb.	Propuestas	Pág. Prop.
2.2.1.1/3.2.1	No se incluye a personal operativo dentro de las reuniones de Comité Ejecutivo para identificación de eventos; tampoco se realiza una reunión adicional para este propósito.	Pág. 85	…….**(Continuación propuesta anterior)** situaciones que están causando variados tipos de problemas a la compañía y que las mismas ya se hayan identificado anteriormente y que además, se hayan establecido lineamientos de control en documentos formales para que las mismas no se den. Estas actividades serán tratadas como GAPS y deberán ser enlistados en cada proceso analizado. Finalmente, con los eventos identificados es posible realizar un mapeo de los riesgos y oportunidades para cada proceso categorizándolos por los factores relacionados a los mismos ya sean internos o externos **(Anexo 2)**.	Pág. 143
	Los riesgos identificados no son documentados. Tampoco se posee un mapa de riesgos por procesos y por áreas de manera que en este sentido MM S.A. no visualiza correctamente los puntos de control necesarios en todas las áreas.	Pág. 86		
	No todas las actividades de la compañía cuentan con procedimientos formales; muchas de ellas se vienen realizando de la misma manera que en años anteriores.	Pág. 87	Este punto se remedia con las acciones que se deben realizar en el elemento: Actitud de la Junta Directiva, estrategia y organización; filosofía del manejo de riesgos.	Pág. 120, 140

2.3.1 Asesoría de riesgos				
No.	**Debilidades**	**Pág. Deb.**	**Propuestas**	**Pág. Prop.**
2.3.1.1/3.3.1	MM S.A. en Ecuador no presenta una metodología formal para medir los riesgos identificados en cuanto a su probabilidad e impacto. De manera general, el Comité Ejecutivo considera los impactos en reuniones a base de reportes o por casos específicos previamente identificados pero el proceso no es documentado.	Pág. 89	La metodología recomendada inicia con dos preguntas por parte de la persona que está guiando el taller: • ¿Cuál es la probabilidad de ocurrencia del riesgo identificado en el periodo de un año? Calificar del 1 al 9 (Bajo, medio, alto). • ¿Qué impacto puede tener el riesgo en términos de costos monetarios? Calificar del 1 al 9. Realizar un promedio de los dos factores para determinar el peso de cada uno y su importancia **(Figura 3.7).** Se pueden utilizar decimales para una división más específica de los riesgos. Para asesoramiento de riesgos residuales se debe empezar realizando las actividades relacionadas a la **Figura 3.8.** Para asesoría de riesgos más generales se debe seguir lo mencionado para la **Figura 3.9 y 3.10** con probabilidad e impacto.	Pág. 153

2.4.1 Respuesta al riesgo				
No.	**Debilidades**	**Pág. Deb.**	**Propuestas**	**Pág. Prop.**
2.4.1.1/3.4.1	No existe un formato predeterminado, política o sistema elaborado para la toma de decisiones en factores más específicos como lo menciona el COSO II. Sin embargo se utilizan reportes y otros tipos de análisis que podrían o no estar disponibles en el momento que se identifica el problema.	Pág. 93	Para clasificar las estrategias se recomienda que MM S.A. considere las siguientes categorías: Abandonar, reducir, compartir, aceptar. La respuesta al riesgo puede tener fusiones de dos estrategias distintas en base a condicionantes para su aplicación por ejemplo. MM S.A. debe priorizar los riesgos ya identificados **(Figura 3.7)**.tomando los riesgos que se encuentra en el cuadrante dos (Alta probabilidad y alto impacto). Las alternativas para mitigar los riesgos identificados deben ser propuestas por los participantes de los Talleres Simples de Reconocimiento. El Director de Unidad comunicará los riesgos y las estrategias de mitigación en la reunión de Comité Ejecutivo. Con las estrategias definidas se consolidará la información por parte del Equipo ERM. Se deben detallar los costos de las estrategias para un análisis de costos versus beneficios. Es posible que sea necesaria una nueva estimación de los impactos identificados para incluir los costos de la respuesta al riesgo. El equipo ERM deberá detallar los riesgos identificados, probabilidades de ocurrencia, impactos, respuestas al riesgo con costo versus beneficio ligados con los objetivos de la organización y en un denominado Portafolio de Riesgos.	Pág. 164

No.	Debilidades	Pág. Deb.	Propuestas	Pág. Prop.
2.4.1.1/3.4.1	Al no presentarse una correcta definición de objetivos, apetito al riesgo y portafolio de riesgos con niveles de ocurrencia e impacto, la compañía no está en las posibilidades de ligar las estrategias con los objetivos de la organización o determinar consistentemente que los riesgos serán mitigados con las estrategias propuestas.	Pág. 93	Este punto se remedia con las acciones que se deben realizar en el elemento: Apetito al riesgo, identificación de eventos y asesoría de riesgos.	Pág. 122, 143, 153
2.5.1 Actividades de control				
No.	**Debilidades**	**Pág. Deb.**	**Propuestas**	**Pág. Prop.**
2.5.1.1/3.5.1	En casos puntuales se ha identificado que MM S.A. no utiliza indicadores específicos de control mensual o trimestral para todos los procesos, se usan los que se consideran más importantes.	Pág. 96	Las prácticas que se recomiendan en esta sección son similares a las llamadas Selfassessments of Internal Controls pero enfocadas en riesgos. Se recomienda que se consideren los siguientes conceptos al momento de realizar estas revisiones: • Desarrollar un profundo entendimiento de los riesgos identificados y elaborar procedimientos de control para monitorearlos. • Crear procedimientos de pruebas para determinar si los controles establecidos están funcionando correctamente. • Aplicar los procedimientos de pruebas. • Realizar ajustes o mejoras de estos procedimientos en caso de que sean necesarios. MM S.A. deberá asignar responsables en cada proceso con sus respectivos indicadores para que se formalicen sus responsabilidades como agente de control interno y riesgo. Cada proceso debe contar con puntos de control que deben ser monitoreados constantemente por los responsables asignados a través de indicadores.	Pág. 171
	En cuanto a actividades de control para las respuestas al riesgo, MM S.A. no establece mecanismos inmediatos para el control de estas estrategias; de manera general, son definidos posteriormente por las áreas participantes sin comunicar a un Equipo de Riesgos, no se asignan responsables en todos los casos y no se documentan. Es decir, se establecen indefinidamente para unas estrategias y para otras no. Además, no hay un departamento o función que compendie y verifique que se estén llevando a cabo las acciones correctas. Falta definición formal y procedimiento para esta actividad.	Pág. 97		
	En algunos casos el área que realiza el Selfassessment de Control Interno no ha definido los indicadores a revisar a falta de una definición formal por parte de los integrantes del área involucrada.	Pág. 97		

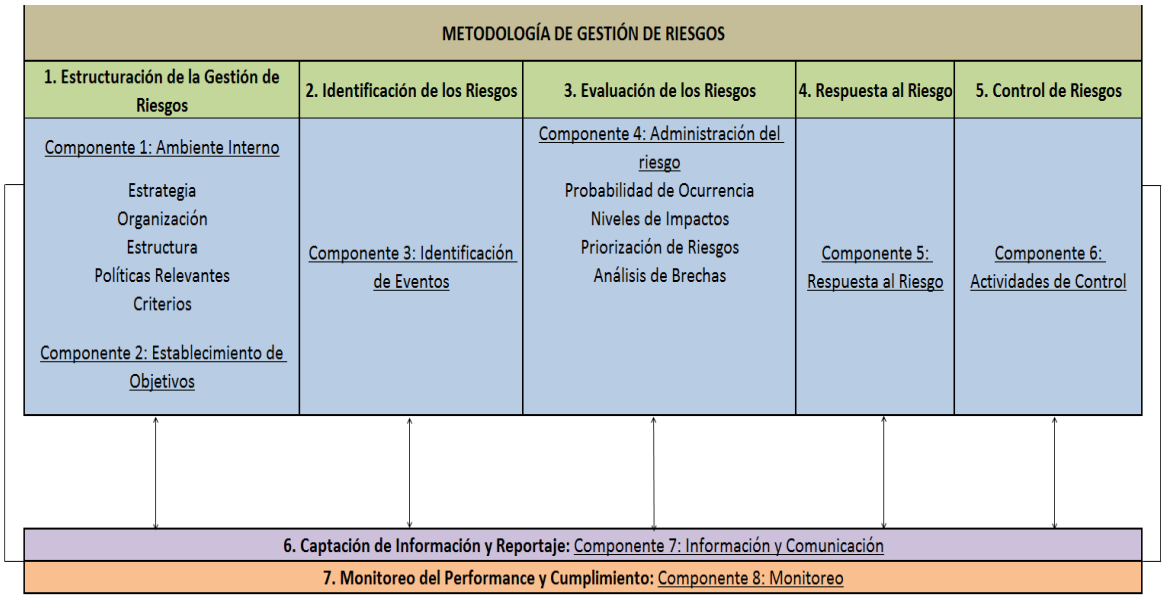
No.	Debilidades	Pág. Deb.	Propuestas	Pág. Prop.
2.5.1.1/3.5.1	Otra falencia de control identificada en este componente es que no se han documentado en un portafolio todas las observaciones de control resultantes de los Selfassessments, por lo que se podría decir que no se está haciendo un seguimiento adecuado de las observaciones y las estrategias de mitigación de eventos adversos.	Pág. 98	**…(Continuación propuesta anterior)** Todas estas personas deben seguir una capacitación correspondiente acerca de cómo se deben comunicar los eventos adversos identificados y se deberá desarrollar un formato estandarizado para reportarlos. Se recomienda a MM S.A. hacer un cuadro resumen de las observaciones obtenidas a través de los Selfassessments para realizar un seguimiento posterior y control. El seguimiento será mensual.	Pág. 171
3.6.1 Información y Comunicación				
No.	**Debilidades**	**Pág. Deb.**	**Propuestas**	**Pág. Prop.**
3.6.1	N/A	N/A	El Sistema de Gestión de Riesgos propuesto necesita de un trabajo eficiente en cuanto a los mecanismos de comunicación entre cada paso. Además se deben definir las maneras en que la compañía deberá llevar su información con el fin de que se puedan tomar decisiones en un tiempo adecuado de acuerdo a la **Figura 3.12**. Todo el sistema tiene una serie de documentos resultantes para los cuales se han asignado sus respectivos responsables: • Componente 1: Filosofía del manejo de riesgos (Consejo de Dirección, Equipo ERM) que está compuesto por el cuestionario de la Figura 3.1; Apetito al riesgo (Consejo de Dirección, Director de Riesgos, Equipo ERM, Comité Ejecutivo, Gerencias Medias, Empleados en General) que está compuesto por los pasos expuestos para la…	Pág. 175

No.	Debilidades	Pág. Deb.	Propuestas	Pág. Prop.
3.6.1	N/A	N/A	**…(Continuación propuesta anterior)** identificación de riesgos y los objetivos de la compañía. • Componente 2: Objetivos, KPI, Tolerancia al riesgo (Todos los empleados), Inventario de oportunidades (Equipo ERM, Comité Ejecutivo, Gerencias Medias, Empleados en General). • Componente 3: Inventario de Riesgos (Equipo ERM). • Componente 4: Riesgos Inherentes y Residuales (Equipo ERM, Comité Ejecutivo, Gerencias Medias, Empleados en General). • Componente 5: Respuestas al riesgo y Portafolio de riesgos (Consejo de Dirección, Director de Riesgos, Equipo ERM, Comité Ejecutivo, Gerencias Medias, Empleados en General). • Componente 6: Informes de Selfasessments; Indicadores de Gestión; Otros reportes (Equipo ERM, Director de Riesgos, Responsables de riesgos para cada proceso).	Pág. 175

3.7.1 Monitoreo				
No.	**Debilidades**	**Pág. Deb.**	**Propuestas**	**Pág. Prop.**
3.7.1	N/A	N/A	Se recomienda a MM S.A. mantener reuniones cada dos meses con los responsables de riesgos para cada proceso y el Equipo ERM con el fin de levantar novedades de control en cada área y realizar cuestionarios prefabricados que especifiquen puntos de monitoreo en el Sistema de Gestión de Riesgos. También se debe considerar la posibilidad de introducir personal externo a la compañía para asesorar ciertos puntos del Sistema de Gestión de Riesgos con conocimientos técnicos en cada área. Incentivar a los empleados en general que reporten falencias en el sistema y otras consideraciones no tomadas en cuenta el momento de implementarlo por primera vez. Además, se recomienda documentar el flujo de todos los primeros procesos analizados para detectar ineficiencias y mejorar el Sistema de Gestión de Riesgos una y otra vez. MM S.A. deberá considerar la realización de las siguientes revisiones : • Diagramas de Flujo • Revisión de los documentos del Sistema de Gestión de Riesgos • Benchmarking • Grupos Focales	Pág. 183

3.9 GUÍA DE PASOS PARA LA IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE RIESGOS EN UNA EMPRESA MULTINACIONAL

Retomando todos los conceptos y guías revisados en los anteriores capítulos, fundamentados en el texto Marco Integrado para la Gestión de Riesgos Empresariales elaborado por COSO, a continuación se detallan los pasos específicos que una empresa multinacional debe considerar para implantar un Sistema de Gestión de Riesgos de acuerdo a la **Figura 2.1** que se muestra nuevamente a continuación**:**



GUÍA DE PASOS PARA LA IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN RIESGOS EN UNA EMPRESA MULTINACIONAL				
Paso 1: Estructuración de la Gestión de Riesgos				
Actitud de la Junta Directiva y Estructura Organizacional				
No.	**Descripción**	**Si**	**No**	**N/A**
1	El área encargada del control interno de la compañía deberá elaborar una presentación detallada del Sistema de Gestión de Riesgos según COSO que incluya la importancia y objetivo del sistema, componentes, beneficios, inversión necesaria (Se deberá considerar un asesor de riesgos externo, desarrollos de sistemas para el flujo de información resultante de la metodología, establecimiento de indicadores a través de sistemas informáticos y cualquier gasto relevante para poner en funcionamiento la propuesta), estructura organizacional piloto, tiempo para la implementación, conceptos del GRC y definiciones de términos importantes como control interno, riesgo, impacto, debilidad, apetito al riesgo, tolerancia al riesgo, compliance y todo lo que se considere necesario para que la información sea entendida a cabalidad. Es importante tomar en cuenta que la presentación debe ser didáctica y con el texto estrictamente necesario, es decir, debe ser una guía resumida de lo que el Sistema de Gestión de Riesgos abarca.			
2	El Director de Riesgos (más adelante se explicará la estructura organizacional) deberá convocar una reunión en donde se incluya al Director General, Directores de Unidad, IT, Oficial de Compliance y Equipo de Control Interno en donde se pondrá en conocimiento la propuesta de implementación del Sistema de Gestión de Riesgos utilizando la presentación antes mencionada. La exposición debe ser elaborada de tal manera que se identifiquen claramente las ventajas del sistema y que sea viable de acuerdo a las condiciones del negocio. Cualquier duda o consulta adicional deberá ser atendida en un periodo máximo de 30 días calendario con el fin de obtener la aprobación final por parte de Dirección General y de Unidad en un tiempo razonable.			
3	Una vez aprobada la iniciativa por parte de Dirección General y de Unidad, el Equipo de Control Interno deberá elaborar una minuta de los acuerdos establecidos en la reunión, misma que deberá ser firmada por todos los participantes. Este es el primer documento que deberá ser archivado en una carpeta que contendrá todos los soportes de la implementación del sistema.			

No.	Descripción	Si	No	N/A
4	A partir de este momento inicia la etapa de estructuración del sistema en donde se diseñará la estructura organizacional. La estructura y organización debe ser elaborada por el Equipo ERM. Para esto se hará un gráfico en Word, Visio o cualquier otro programa similar en donde se muestre la estructura para el funcionamiento del Sistema de Gestión de Riesgos. Se deberá definir al menos los siguientes cargos: Director de Riesgos; Comité de Auditoría o Riesgos (Ejecutivo en el caso de MM S.A.); Gerentes participantes en el sistema; Equipo ERM (Contará con la ayuda del asesor de riesgo externo para todos los pasos de implementación); Consejo de Directores; Asesores Externos; Empleados participantes; es fundamental recalcar en esta parte la importancia de la actitud de la junta directiva enfocada en riesgos en base a los conceptos fundamentales del GRC y la administración de riesgos tal como lo establece COSO. Adicionalmente, se debe definir el tipo de organización de acuerdo a la **Figura 3.4**. Este documento de igual manera deberá ser aprobado por el Consejo de Directores. No es necesario que se cambie la estructura actual de la organización, es posible utilizar las mismos cargos pero asignando nuevas responsabilidades.			
5	Con la estructura definida, se deberán asignar responsabilidades para cada uno de los miembros del sistema. Para esto, el Equipo ERM deberá utilizar las funciones y responsabilidades mencionadas en el numeral **3.1.1.3** y convocar una reunión con el Director de Recursos Humanos y el Oficial de Compliance para alinearlas con los estándares de la compañía. De esta reunión se obtendrá un documento formal bajo los estándares y formatos que utilice la organización con los perfiles de cada función definidos que deberá ser aprobado por el Consejo de Dirección. Estas nuevas responsabilidades deberán ser comunicadas por el Comité de Riesgos y el Consejo de Dirección a todos los involucrados antes de que inicie la ejecución del sistema.			

No.	Descripción	Si	No	N/A
6	El dueño del Sistema de Gestión de Riesgos será el Director de Riesgos y los brazos ejecutores del sistema será el Equipo ERM, el mismo que desarrollará una estrategia y flujo para la identificación, asesoramiento, respuesta, control, comunicación y monitoreo del Sistema de Gestión de Riesgos a implementar. Es necesario que se tome en cuenta lo dispuesto por COSO y que también se definan los roles del Equipo ERM en participación de la revisiones de Auditoría Interna. El documento deberá especificar cada una de las funciones del personal dentro del sistema, los pasos principales que se realizarán en cada etapa, reuniones semanales, mensuales, trimestrales, semestrales y anuales que se deberán mantener para asegurar el correcto funcionamiento del sistema, en fin todo lo necesario para implementarlo. Esta actividad no deberá tomar más de 30 días calendario. Asimismo, la estrategia deberá ser firmada por el Consejo de Directores. Cabe recalcar, que este documento será actualizado una vez implementado todo el proceso como parte de una retroalimentación.			
7	El Equipo ERM coordinará con el Departamento de Compras la identificación de opciones de proveedores dentro del mercado que brinden asesoría en gestión de riesgos; se deberá seguir lo dispuesto en la política de compras vigente que debe incluir al menos dos revisores antes de la adquisición del servicio, es importante tener la asesoría necesaria para el diseño del sistema.			
Integridad y Valores Éticos				
No.	**Descripción**	**Si**	**No**	**N/A**
8	En la actualidad la mayoría de las empresas multinacionales cuentan con códigos de conducta, misión y visión establecidas. En este sentido, es necesario que el Director de Riesgos convoque una reunión en la que participe el Consejo de Dirección, el Comité de Riesgos y el personal que se considere necesario para analizar los puntos del código de conducta y alinearlo a lo dispuesto por COSO en base a lo mencionado en el numeral **2.1.1.4.1**. Una vez identificadas las diferencias se procederá con la actualización respectiva por parte del Comité de Riesgos quien entregará el documento final al Consejo de Dirección y al Oficial de Compliance para su aprobación. Una vez obtenida la aprobación, El Oficial de Compliance será el encargado de difundir el documento a través de los medios masivos pertinentes para asegurar que todos los empleados de la compañía conozcan los puntos principales del código y sus cambios a cabalidad.			

No.	Descripción	Si	No	N/A
9	En caso de que el código de conducta no pueda ser modificado en la localidad por disposiciones corporativas de casa matriz, se deberá realizar un adéndum local del código con las consideraciones necesarias en base a lo antes explicado. Cuando la filosofía del riesgo es plasmada en el código de conducta, documento considerado como el pilar de todos los lineamientos corporativos, el Sistema de Gestión de Riesgos cuenta con el auspicio necesario de alto nivel para su implementación. El entrenamiento del código deberá contener también un examen de verificación de conocimientos y ejemplos de desviaciones para asegurar un correcto entendimiento.			
Filosofía del Manejo de Riesgos				
No.	**Descripción**	**Si**	**No**	**N/A**
10	El Equipo ERM con la ayuda del Oficial de Compliance establecerá reuniones con los involucrados de todos los procesos de la compañía con la finalidad de asignar dueños de cada proceso y responsables de control para cada sector, el documento resultante deberá ser entregado a Recursos Humanos. Los dueños responderán ante cualquier evento que se presente en su proceso y tendrán como responsabilidad el monitoreo del comportamiento de los diferentes indicadores que se manejan dentro de cada actividad y que se asignarán de igual manera a los responsables de cada sector. Se entiende que el dueño del proceso tendrá la suficiente autoridad para administrar el control en su proceso.			
11	El Departamento de Recursos Humanos incluirá las nuevas obligaciones de los dueños y responsables de cada proceso en sus perfiles, los cuales deberán ser firmados por sus Supervisores y Directores de Unidad.			
12	Adicionalmente, los dueños y responsables de cada proceso realizarán repasos de: políticas y procedimientos ya existentes, elaboración de reportes de eventos adversos identificados en el día a día, identificación y reportaje de “áreas grises”, responsabilidades en un punto del proceso, importancia del control en el proceso, obtención de certificado de conocimiento de políticas e indicadores, etc. Actividades que serán diseñadas por el Equipo ERM y los Supervisores.			
13	Posteriormente, el Equipo ERM realizará un inventario total de todos los documentos que reflejan lineamientos, aparte del código de conducta. Archivará los documentos físicos y hará una matriz en un programa, puede ser una simple tabla de Excel que contenga referencias principales de los procesos para su fácil ubicación como el nombre, tipo de documento, fecha de elaboración, fecha de expiración, área responsable, persona responsable del proceso, etc. Se deberá identificar la validez de dichos documentos tomando en cuenta que deben incluir flujogramas y referenciarlos con las políticas corporativas a las que hacen mención.			

No.	Descripción	Si	No	N/A
14	Cada área analizará las normas relacionadas para identificar actualizaciones u oportunidades de mejora tomando en cuenta que el control y la identificación de riesgos son fundamentales para el correcto funcionamiento del sistema y que esta consideración debe ser incluida en la política o procedimiento. Asimismo, la actualización será realizada por los involucrados en cada proceso, asignando la responsabilidad a un solo empleado. Para esto, el equipo ERM deberá realizar un cronograma que contenga las fechas acordadas con cada dueño del proceso para la actualización de la normativa correspondiente, con esto se podrá realizar un seguimiento. Por la magnitud de esta actividad se considera que esta podría ser finalizada en el transcurso de 2 meses aproximadamente.			
15	Para reforzar las creencias y actitudes de todo el personal de la organización enfocándolas al riesgo, es necesario que el Equipo ERM con el apoyo del Consejo de Dirección, realice una encuesta obligatoria para identificar el estatus de los atributos de la filosofía del riesgo que deberá contener las preguntas y tabulación como se muestra en la **Figura 3.1**. Los resultados darán una clara visión de los puntos que se deberán reforzar a través de comunicados formales, talleres, encuestas, conversaciones personalizadas y otro tipo de técnicas. Estas iniciativas deberán ser lideradas por Dirección General para que cuenten con la correcta autoridad.			
16	El Equipo ERM junto con el Director de Riesgos deberá elaborar un documento que norme y describa los nuevos procedimientos del Sistema de Gestión de Riesgos y las actividades de control para la implementación y seguimiento de las respuestas al riesgo. Se incluirán los aspectos mencionados en el numeral **3.1.1.1**.			
Compromiso con la Competencia				
No.	**Descripción**	**Si**	**No**	**N/A**
17	El departamento de Recursos Humanos en conjunto con todas las Direcciones analizará anualmente todos los perfiles de funciones de cada posición por departamento para asegurar que la compañía cuenta con los recursos necesarios para la implementación del Sistema de Gestión de Riesgos y que todos los objetivos se puedan llevar a cabo con los recursos disponibles. Cada perfil será firmado por las dos partes y archivado en los files del departamento otorgando además una copia para cada Director.			

Designación de Autoridad y Responsabilidad				
No.	**Descripción**	**Si**	**No**	**N/A**
18	Para asegurar que exista una correcta asignación de autoridad para los empleados de la organización, el Consejo de Dirección deberá convocar una reunión para hacer un análisis de las políticas corporativas relacionadas y verificar que los niveles de aprobación se ajusten a las necesidades locales para diferentes tipos de transacción por ejemplo, adquisición de activos fijos, ventas, límites de crédito, gastos, relacionado a acciones de rutina y no rutina con el fin de eliminar procedimientos burocráticos e ineficientes. Además, se deberá generar un documento formal elaborado por el Equipo ERM, aprobado por el Consejo de Dirección, Oficial de Compliance y las autoridades regionales competentes. La normativa será comunicada a todos los empleados de la compañía a través de los medios y talleres pertinentes recalcando la importancia del enfoque en riesgos			
Estándares de Recursos Humanos				
No.	**Descripción**	**Si**	**No**	**N/A**
19	Recursos Humanos con ayuda del Oficial de Compliance asegurará que sus normas establezcan estándares adecuados para la contratación, entrenamiento, promoción, disciplina y otras acciones del departamento, enfocándose en la detección y control de riesgos. Asimismo, cualquier modificación que se intente realizar deberá estar autorizada por el Consejo de Dirección. El documento será archivado en los files del departamento. Por otro lado el Departamento de Recursos Humanos deberá verificar que se estén implementando los cursos necesarios para asegurar el cumplimiento de políticas corporativas y locales más importantes para la compañía.			
Apetito al Riesgo				
No.	**Descripción**	**Si**	**No**	**N/A**
20	El apetito al riesgo es un compendio de documentos que se generan de varias actividades relacionadas a diferentes pasos del Sistema de Gestión de Riesgos. Para esto, el Equipo ERM documentará el producto final de cada uno de los pasos mencionados para incluirlos dentro de las siguientes categorías, ver numeral **3.1.1.2**: Portafolio de riesgos (Identificación de eventos), capacidad de riesgo (Establecimiento de objetivos, código de conducta, políticas corporativas y locales), tolerancia al riesgo (Establecimiento de objetivos) y actitud hacia el riesgo (identificado ya en los anteriores pasos – actitud de la junta directiva). Todo deberá ser incluido dentro de un solo documento que deberá ser formalizado con las firmas del Consejo de Dirección y Comité de Riesgos. Se recomienda discreción para la divulgación de estas consideraciones.			

Establecimiento de Objetivos				
No.	**Descripción**	**Si**	**No**	**N/A**
21	El Consejo de Dirección deberá promover una reunión general que incluya a todos los Directores de Unidad y de Área y al Equipo ERM en la cual el Director de Riesgos será el encargado de detallar a profundidad el procedimiento a seguir para el establecimiento de objetivos basados en riesgos. Es decir, misión, objetivos estratégicos, KPI's, estrategias, objetivos relacionados alineados con el apetito al riesgo, KPI´s, tolerancia al riesgo. En esta reunión se explicarán los conceptos de apetito al riesgo, tolerancia al riesgo, objetivos estratégicos y objetivos relacionados para un correcto entendimiento de la metodología.			
22	Cada Director de Unidad y de Área se encargará de transmitir este conocimiento a sus subordinados para la correcta ejecución.			
23	El Equipo ERM elaborará un documento formal con la metodología mencionada en el numeral **3.1.2** en base a los fundamentos del COSO como se muestra en la **Figura 3.5**. El mismo deberá ser firmado por el Consejo de Dirección y el Director de Recursos Humanos para que posteriormente sea divulgado a todos los empleados de la organización.			
24	Luego de las acciones anteriores, todos los empleados de la compañía y dueños de procesos harán un levantamiento de todos los objetivos por departamento y proceso con el fin de reestructurarlos utilizando los siguientes fundamentos: La misión que se compone como la base de los objetivos y funciona como elemento crucial en la planificación estratégica. Para soportar la misión, cada Dirección de Unidad o Área desarrollará uno o varios objetivos estratégicos con medidas o indicadores de gestión denominados KPI´s; posteriormente se establecerán objetivos operacionales, de reportaje y compliance por parte de cada empleado o subordinado directo de dirección. Estos deberán estar alineados con el apetito al riesgo que a su vez debe contar con otros indicadores de gestión o KPI's. Estos últimos objetivos e indicadores darán los lineamientos finales para determinar los niveles de tolerancia para cada uno de los objetivos relacionados mismos que servirán de guía para que la compañía pueda determinar si los mismos fueron alcanzados a cabalidad. (Figura 3.5). Cada objetivo estará mapeado dentro de la clasificación corporativa respectiva de acuerdo al área.			

No.	Descripción	Si	No	N/A
25	Los objetivos deberán ser ingresados por cada empleado y aprobados por los supervisores respectivos en el sistema corporativo siguiendo el procedimiento regular de la organización en el transcurso de 30 días calendario. Cabe recalcar que los objetivos de los procesos estarán fundamentados en los objetivos de los empleados involucrados en el mismo y deberán formar parte de sus procedimientos formales. Adicionalmente, cada Director de Unidad o Área ingresará sus objetivos antes que sus subordinados y los comunicará una vez que sean aprobados con el fin de que los mismos puedan ser soportados por todos los integrantes de los procesos.			
26	El Equipo ERM consolidará la información de cada área y proceso e incluirá la tolerancia al riesgo dentro del documento del apetito al riesgo categorizándolo por área y función.			
Paso 2: Identificación de Riesgos				
No.	**Descripción**	**Si**	**No**	**N/A**
1	El Equipo ERM deberá ser el principal promotor de la identificación de eventos. Se elaborará un cronograma de reuniones para las sesiones de lluvia de ideas, el mismo que será revisado por el Director de Riesgos y presentado en una reunión que incluirá al Consejo de Dirección, Comité de Riesgos, Oficial de Compliance y Directores de Unidad y de Área. En esta reunión se modificará el cronograma de acuerdo a la disponibilidad del personal y las necesidades del negocio.			
2	Además, en la reunión se deberá explicar el objetivo de los talleres y los roles de cada uno de los participantes (Todo el personal involucrado en el proceso, operativo y no operativo), de acuerdo a la estructura organizacional definida en el paso 4, tomando como guía lo mencionado en el numeral **3.2.1**. El Equipo ERM deberá elaborar un documento formal del cronograma en base a lo acordado en la reunión, firmado por el Consejo de Dirección y el Director de Riesgos y archivado en la carpeta de la implementación del Sistema de Gestión de Riesgos.			
3	El Equipo ERM con la ayuda del asesor externo y el Departamento de Compras identificarán proveedores en el mercado que puedan proporcionar a la compañía la siguiente información: Un listado de eventos desfavorables que se han presentado en las compañías de la industria farmacéutica no solo en el país sino también en el mundo, con el fin de asesorar a los participantes de los talleres con eventos similares que podrían ocurrir en la compañía.			

No.	Descripción	Si	No	N/A
4	Pocos días antes de iniciar los talleres, el Equipo ERM enviará una guía preliminar a los participantes de los talleres en donde se mencionará al menos los siguientes aspectos: Cronograma de actividades, duración de las reuniones, objetivos de las reuniones y roles de los participantes, pasos posteriores y análisis de los siguientes aspectos para la identificación de riesgos, explicando cada uno de ellos: •Eventos Económicos Externos. •Eventos Naturales de Medioambiente. •Eventos Políticos. •Factores Sociales. •Eventos de Infraestructura Interna. •Eventos de Procesos Internos. •Eventos de Tecnología Interna o Externa.			
5	La técnica principal que se utilizará es el Taller Simple de Reconocimiento que funciona a través de reuniones con el personal de diferentes especialidades involucrado en el proceso, para hacer una lluvia de ideas. La guía para realizar esta actividad se encuentra en la **Figura 3.6** y lo mencionado en el numeral **3.2.1**. Esta tarea será liderada por el Equipo ERM, no necesita necesariamente estar presente en todas estas reuniones porque podría ser impracticable. Se puede designar al dueño del proceso como el organizador y líder, sin embargo, es necesario que tenga conocimiento suficiente sobre la metodología.			
6	Cuando el equipo ERM revise el listado de riesgos resultante de las reuniones antes mencionadas, deberá clasificarlos en el portafolio de riesgos de alto nivel e identificar los siguientes parámetros (no limita a que otros sean considerados): • El riesgo es común en todos los procesos o se trata de un caso puntual. • Es generado de factores externos (Económico, medio ambiente, político, social, tecnológico) o internos (Infraestructura, personal, procesos, tecnología). • Los riesgos están relacionados y causan otros o son aislados dentro del alcance del área. Esto permitirá al Equipo ERM categorizarlos por factores internos o externos, ver **Anexo 2**. Toda esta actividad generará varios riesgos que serán comunicados a las personas afectadas en el proceso para identificar cambios o sugerencias que requieran modificación. Una vez establecidos los riesgos de manera definitiva se elaborará un documento por proceso que servirá de insumo para el primer punto del apetito al riesgo y para la evaluación de riesgos, firmado por el Comité de Riesgos, el Consejo de Dirección y el Director de Riesgos. Este documento final será comunicado a todas las áreas respectivas en todos los niveles locales involucrados.			

No.	Descripción	Si	No	N/A
7	Es posible que dentro de las reuniones salten a la luz situaciones que están causando variados tipos de problemas a la compañía y que las mismas ya se hayan identificado anteriormente y que además, se hayan establecido lineamientos de control en documentos formales para que las mismas no se den. Estas actividades serán tratadas como GAPS y enlistadas en cada proceso analizado por parte de cada dueño del proceso y el Equipo ERM.			
Paso 3: Evaluación de Riesgos				
No.	**Descripción**	**Si**	**No**	**N/A**
1	Se puede realizar la actividad relacionada a la asesoría de riesgos durante la primera reunión del taller o hacer una segunda convocación. Para esta nueva reunión, el Equipo ERM será el encargado de explicar nuevamente el objetivo y propósito de la evaluación de riesgos.			
2	Para iniciar la metodología recomendada se deberá tomar como insumo el documento elaborado en el paso anterior y se formularán dos preguntas por parte de la persona que está guiando el taller: • ¿Cuál es la probabilidad de ocurrencia del riesgo identificado en el periodo de un año? Calificar del 1 al 9 (Bajo, medio, alto). • ¿Qué impacto puede tener el riesgo en términos de costos monetarios? Calificar del 1 al 9.			
3	Posteriormente, se realizará un promedio de los dos factores para determinar el peso de cada uno y su importancia, **Figura 3.7.** Se pueden utilizar decimales para una división más específica de los riesgos. Para asesoramiento de riesgos residuales se debe empezar realizando las actividades relacionadas a la **Figura 3.8.** Para asesoría de riesgos más generales se debe seguir lo mencionado para la **Figura 3.9 y 3.10** con probabilidad e impacto. Es necesario que se revise toda la guía específica que se encuentra en el numeral **3.3.1.** La calificación de un riesgo no debe terminar en lo antes explicado, el alcance podría ser mayor si se revisa de manera más profunda. Pueden haber varias implicaciones resultantes de ese riesgo y en muchas de las ocasiones es recomendable siempre realizar un poco más de investigación al respecto antes de asignarle un factor porcentual de ocurrencia o significancia (impacto).			

No.	Descripción	Si	No	N/A
4	El líder del taller deberá realizar las siguientes preguntas a los integrantes del taller, en conjunto, como guía para estimar adecuadamente el costo de un riesgo: • ¿Cuál es el costo en el mejor de los casos si se tuviera que incurrir en el riesgo? Esta pregunta funciona comúnmente en los casos en los que el impacto es limitado si el riesgo ocurre. • ¿Qué costo estimarían las personas conocedoras del proceso para el riesgo identificado? Esta pregunta se la puede realizar al director del área o unidad. • ¿Cuál es el valor o costo esperado de incurrir en el riesgo? Esta se utiliza para los tipos de riesgos que incluyen costos bases u otros costos relacionados. • ¿Cuál es el costo en el peor de los casos si se tuviera que incurrir en el riesgo? Esta pregunta básicamente apunta al peor de los escenarios para estimar el impacto. Las respuestas a estas 4 preguntas darán resultados estimados de los costos en los que se pueden incurrir si el riesgo se llagara a dar. Sin embargo, es preciso definir el impacto tomando solo una, la mejor. En la práctica, la pregunta 2 y 3 suelen presentar las mejores estimaciones y para escoger la correcta, el equipo ERM debe involucrarse en esta actividad como guía. Adicionalmente, el impacto escogido debe estar representado en otra tabla que tendrá la planificación de respuesta al riesgo como se muestra en la **Figura 3.10.**			
5	De esta asesoría, el Equipo ERM elaborará un documento por proceso que servirá de insumo para la respuesta al riesgo, así como también se desarrollará un mapa de riesgos **Figura 3.7 y Figura 3.10**, firmado por el Comité de Riesgos, el Consejo de Dirección y el Director de Riesgos. Estos documentos finales serán comunicados a todas las áreas respectivas en todos los niveles locales involucrados.			
Paso 4: Respuesta al Riesgo				
No.	**Descripción**	**Si**	**No**	**N/A**
1	Tomando el insumo del anterior paso y el mapa de riesgos, El Equipo ERM priorizará los riesgos en base a su probabilidad e impacto y serán los primeros en ser atendidos. Adicionalmente, se explicará el objetivo de las reuniones para la respuesta al riesgo y todos los conceptos necesarios para entender la actividad a las personas involucradas en la reunión.			

No.	Descripción	Si	No	N/A
2	Luego, se mantendrán las reuniones respectivas con el Comité de Riesgos, Gerencias y Empleados involucrados en general para definir las respuestas a los riesgos identificados con el propósito de mitigarlos en la mayor manera posible. Se irán revisando uno por uno los riesgos y se consideran las siguientes categorías: Abandonar, reducir, compartir, aceptar. La respuesta al riesgo puede tener fusiones de dos estrategias distintas y deberán tener fechas específicas de implementación, tomando en cuenta los costos versus los beneficios. Es posible que sea necesaria una nueva estimación de los impactos identificados para incluir los costos de la respuesta al riesgo y además muchas de las respuestas al riesgo podrían ser consideradas para ser incluidas dentro de las normativas de la compañía, para lo cual se realizarán actualizaciones en las políticas, procedimientos, código de conducta, etc.			
3	El Equipo ERM consolidará la información de cada área y proceso en el portafolio de riesgos y lo enviará en físico y magnético al Consejo de Dirección, Comité de Riesgos y Director de Riesgos para su aprobación. Se archivará en la carpeta de implementación del Sistema de Gestión de Riesgos. Con los pasos mencionados hasta este punto, el Sistema de Gestión de Riesgos ha concluido con su parte fundamental. Para una guía más específica se debe revisar el numeral **3.4.1.**			
Paso 5: Control de Riesgos				
No.	**Descripción**	**Si**	**No**	**N/A**
1	El Equipo ERM en conjunto con el Departamento de IT desarrollará estrategias que aseguren la correcta implementación de las respuestas al riesgo, políticas y procedimientos resultantes de las estrategias definidas. Estas deben guiarse en lo siguiente: Desarrollar un profundo entendimiento de los riesgos identificados y elaborar procedimientos de control para monitorearlos, crear procedimientos de pruebas para determinar si los controles establecidos están funcionando correctamente, aplicar los procedimientos de pruebas, realizar ajustes o mejoras de estos procedimientos en caso de que sean necesarios.			
2	Es importante que el Equipo ERM con la ayuda del Departamento de Recursos Humanos, el Oficial de Compliance y el Departamento de IT realice una capacitación acerca de cómo se deben reportar los eventos adversos identificados para lo cual se desarrollará una herramienta informática. Se recomienda que estos informes sean siempre canalizados a través del Equipo ERM. El Equipo ERM hará un cuadro resumen de las observaciones obtenidas a través de las actividades de control definidas para realizar un seguimiento posterior y control, el seguimiento será mensual.			

No.	Descripción	Si	No	N/A
3	Los dueños y responsables de cada proceso harán un seguimiento mensual, trimestral, semestral y anual de los indicadores asignados para cada proceso los cuales deberán ser presentados al Equipo ERM dependiendo de la periodicidad, utilizando la herramienta informática antes mencionada. Para un mejor entendimiento se debe revisar el numeral **3.5.1.**			
4	El seguimiento y control será documentado mensualmente por el Equipo ERM y firmado por el Director de Riesgos, quien comunicará los hallazgos en cada reunión de Comité de Riesgos. Para el archivo se utilizará una nueva carpeta de actividades de control.			
Paso 6: Captación de Información y Reportaje				
No.	**Descripción**	**Si**	**No**	**N/A**
1	El Sistema de Gestión de Riesgos propuesto necesita de un trabajo eficiente en cuanto a los mecanismos de comunicación entre cada paso. El Equipo ERM y el Departamento de IT deberán definir las maneras en que la compañía llevará su información para que se puedan tomar decisiones en un tiempo adecuado de acuerdo a la **Figura 3.12**. Se debe revisar como referencia el numeral **3.6.1.** Este paso es el pegamento que uno a todo el sistema en su totalidad y su correcta implementación.			
2	El Equipo ERM trabajará en conjunto con el Departamento de IT para identificar las necesidades de generación de KPI's establecidos en los objetivos y para los cuales funcionarán las actividades de control y monitoreo. Para esto se analizarán todos los indicadores que al momento no se están generando en las herramientas de la compañía y se identificarán estrategias para generarlos estableciendo un presupuesto de acuerdo a las posibilidades del negocio. Estas nuevas necesidades informáticas deberán ser manejadas por el Departamento de IT con fechas específicas de cumplimiento y costos necesarios, documentadas y firmadas por el Equipo ERM, Consejo de Dirección, Director de Riesgos y Direcciones de Unidad y de Área.			

Paso 7: Monitoreo del Performance y Cumplimiento				
No.	**Descripción**	**Si**	**No**	**N/A**
1	El Equipo ERM deberá establecer mecanismos de monitoreo de alta visualización para verificar el funcionamiento global del Sistema de Gestión de Riesgos a través de: reuniones mensuales con responsables de procesos, realización de preguntas específicas de control, verificación periódica de que la información ingresada en el sistema esté actualizada, asesoramiento del asesor externo para asesoría en monitoreo. Se utilizarán al menos las siguientes estrategias de monitoreo para el Sistema de Gestión de Riesgos: Diagramas de flujo actualizados para todos los procesos, revisión periódica de la documentación resultante de los distintos pasos del sistema, benchmarking dentro y fuera de la industria, actividades con grupos focales. La importancia del componente del monitoreo es verificar el estatus de funcionamiento del sistema y mejorarlo a través del tiempo con mejores sistemas y estrategias pero siempre conservando la misma filosofía enfocada en riesgos.			
2	El Equipo ERM documentará las estrategias escogidas con fechas de aplicación y cualquier información relevante para el monitoreo total del sistema considerando además adquisición de sistemas informáticos en gestión de riesgos que al momento se encuentren disponibles en el mercado y que permitan tener ajustes para la realidad del negocio. El documento deberá estar firmado por el Director de Riesgos y el Consejo de Dirección. Como referencia se debe considerar lo mencionado en el numeral **3.7.1**			
3	Como parte de la retroalimentación del sistema, el Equipo ERM deberá emitir reportes semestrales sobre el funcionamiento del Sistema de Gestión de Riesgos en todos los procesos que será presentado en las reuniones semestrales del Comité de Riesgos a partir de la primera implementación, reflejando los tiempos de duración entre cada paso. En términos generales no debería tomar más de ocho meses en su primera implementación y se deberá correr en su totalidad al menos una vez al año para todos los procesos.			

4. CAPÍTULO IV: CONCLUSIONES Y RECOMENDACIONES

4.1 CONCLUSIONES

En base al objetivo general planteado: Implementar un sistema de gestión de riesgos, a fin de mejorar el manejo administrativo de la organización; se hizo un diagnóstico, determinación de fortalezas, propuestas y pasos para la implementación de acuerdo al Sistema de Gestión de Riesgos emitido por COSO como una técnica de gran reconocimiento a nivel mundial, en comparación con el sistema actual de MM S.A. La intención de estas acciones es proveer a la gerencia instrumentos prácticos para mejorar sobremanera los fundamentos para la toma de decisiones, así como también eliminar incertidumbres al momento de definir estrategias para un mejor desempeño organizacional. Además, el mismo permite visualizar de manera transparente el estatus de las actividades en todas las áreas y de qué manera éstas pueden ser mejoradas para potenciar los resultados esperados.

Para los objetivos específicos: Establecer un sistema de gestión de riesgos certificado y estandarizado para los procesos más importantes de la organización; determinar los impactos de los riesgos si se llegaran a producir; establecer acciones para mitigar estos riesgos de manera que se alcancen los niveles de aceptación requeridos por la alta administración; verificar si los procedimientos de la organización se encuentran

enfocados en la consecución de sus objetivos y proponer programas de revisión y evaluación del sistema de gestión de riesgos y controles internos; se elaboraron propuestas y los pasos que MM S.A. y las compañías multinacionales en general deben seguir para implementar un Sistema de Gestión de Riesgos eficiente en base a los estándares del Marco Integrado para la Gestión de Riesgos Empresariales emitido por COSO. De esta manera se establecieron acciones claras y prácticas, certificadas a nivel mundial, que permitirán a la organización alcanzar los objetivos propuestos.

Otro de los aspectos importantes identificados en la realización del trabajo es que MM S.A. aplica los principios del GRC a nivel corporativo pero localmente en Ecuador el componente (R-riesgo) no es manejado con la misma importancia que el (G-gobierno) y el (C-compliance). De aquí surge uno de los motivos principales para la aplicación de esta ideología que utiliza la compañía a nivel global. Obviamente como ya se viene mencionando, este sistema es una herramienta de valor agregado que apoya directamente a la toma de decisiones y a la mejora continua de los varios procesos que maneja MM S.A.

El proceso que se debe llevar a cabo para la implementación de un Sistema de Gestión de Riesgos requiere de un trabajo extenso y más aún en empresas multinacionales como MM S.A. ya que todas sus áreas a través de las cuales fluyen todos los procesos, mantienen una relación horizontal y multifuncional para las cuales se requieren equipos completos y de diferentes especializaciones técnicas.

Un Sistema de Gestión de Riesgos es un instrumento vivo en la organización que se caracteriza por ser flexible y adaptable a las condiciones de cualquier empresa e

industria. Al igual que otras estrategias administrativas que aportan a este sistema, se requiere de mucha creatividad para identificar maneras acertadas de evaluación de los procesos de la compañía de manera que los objetivos propuestos por la misma puedan ser medidos con un enfoque en riesgos.

La experiencia obtenida en este Trabajo de Titulación ha sido totalmente enriquecedora. El tema propuesto tiene una gran variedad de aplicaciones que han levantado un fuerte interés tanto personalmente como en la organización objeto del estudio. Este sistema ha sido de gran ayuda para entender muchos aspectos relevantes de control que deben ser aplicados en la organización de manera adecuada para obtener los resultados esperados.

A pesar de las largas horas de estudio que se aplicaron para la elaboración de este trabajo, es totalmente satisfactorio el conocimiento obtenido. Las estrategias detalladas servirán para generar un valor agregado importantísimo en las organizaciones de la actualidad que cuentan con estructuras enormes de varias unidades, sucursales, departamentos, funciones, políticas, procesos, procedimientos, etc. Inclusive es fundamental para el establecimiento de nuevas compañías que entreguen bienes y servicios a la comunidad y el mundo, estableciendo desde un inicio mecanismos de control adecuados basados en riesgos.

4.2 RECOMENDACIONES

Se necesita mucho compromiso por parte de todos los empleados de la compañía para implementar un sistema como este. Por la experiencia obtenida en el día a día en MM S.A., existe una gran predisposición por parte de los Empleados y Gerentes para el establecimiento de nuevas estrategias con el fin de mejorar controles y establecer mejoras a los procesos. Sin duda el sistema requiere de gran trabajo pero sus resultados como ya se mencionó anteriormente son garantizados.

Se recomienda a MM S.A. aplicar los puntos revisados en este documento de manera paulatina para suavizar el cambio en los procedimientos de la organización ya que el sistema podría ser considerado como impracticable o muy complejo. Lo más importante para reforzar en primera instancia es la filosofía del manejo del riesgo y posteriormente las técnicas para establecimiento de objetivos para lo cual es necesario introducir los conceptos del G.R.C. y la importancia del control y manejo de riesgos. Luego se deberá proceder con la aplicación de los demás componentes.

Los principios del GRC que se han mencionado recaen en todas las actividades de la empresa, así como también, en todo el proceso para el establecimiento de un Sistema de Gestión Riesgos y su futura administración. Cada componente del GRC debe ser analizado por separado pero aplicado en conjunto con la misma importancia para cada uno, de otra manera no se estaría dando el enfoque adecuado.

BIBLIOGRAFÍA

- AICPA. (2012). *Marco Internacional para la Práctica de Auditoría Interna.*
- Arnold, V., Hamptom, C., Khazanchi, D., & Sutton, S. (2004). *Enterprise Risk Management: Identifying Risks in B2B E-Commerce Relationships.* Altamonte Springs - Florida: The Institute of Internal Auditors Research Foundation.
- Borja, D. R. (2004). *Auditoría Interna Un Enfoque Moderno de Planificación, Ejecución y Control.* Guatemala: Artes Gráficas Acropolis.
- Committee of Sponsoring Organizations of the Treadway Commission. (2004). *Gestión de Riesgos Coporativos - Marco Integrado.* NJ EEUU: Instituto de Auditores Internos & PriceWaterHouseCoopers.
- Committee of Sponsoring Organizations of the Treadway Commission. (2011). *Internal Control - Integrated Framework.* AICPA.
- Committee of Sponsoring Organizations of the Treadway Commission. (2012). *Internal Control Integrated Framework.*
- Committee of Sponsoring Organizations of the Treadway Commission. (2012). *Understanding and Communicating Risk Appetite.* Durham: COSO.
- Coopers & Lybrand e Institutos de Auditores Internos. (1997). *Los Nuevos Conceptos del Control Interno (Informe COSO).* Madrid: Días de Santos.
- MacLeod, A., Foster, B., Mcdonald, P., Robertson, A., Stokka, T., & Ybarra, B. (2012). *Coordinating Risk Management and Assurance.* Altamonte Springs Florida: The Institute of Internal Auditors.
- MM S.A. (2014). Misión.
- MM S.A. (2014). Visión.
- Protiviti-Independent Risk Consulting. (2006). Guide to Enterprise Risk Management.
- Reding, K., Sobel, P., Anderson, U., Head, M., Ramamoorti, S., Salamasick, M., & Riddle, C. (2009). *Auditoría Interna: Servicios de Aseguramiento y Consultoría.* Altamonte Springs - Florida: Fundación de Investigaciones del Instituto de Auditores Internos.
- Robert R. Moeller- John Wiley & Sons - Citación de Enterprise Risk Management Integrated Framework 2004. (20 de 01 de 2011). *About Us: Books24x7, Inc*. Obtenido de Books24x7 Web site: http://www.books24x7.com/toc.aspx?bookid=44326

- Silva, W. (2013). *Apuntes de Auditoría Administrativa.* Quito.
- The Comittee of Sponsoring Organizations of the Treadway Commission. (2004). *Enterprise Risk Management Integrated Framework - Application Techniques.* NJ EEUU: AICPA.
- The IIA. (2013). *The Institute of Internal Auditors*. Obtenido de About The IIA: www.theiia.org
- http://auditor2006.comunidadcoomeva.com/blog/uploads/1-PresentacinRafaelRuano-PriceWaterHouseCoopers-COSOII-ERMyelRoldelAuditorInterno.pdf

GLOSARIO

- **GOA:** Grant of Authority, se entiende como el nivel de aprobación que posee cada empleado de MM S.A. para que la empresa realice sus actividades. Generalmente es medido por valores monetarios y difiere del tipo de transacción que se desea realizar y por el tamaño de la sucursal (MM S.A., 2014).

- **Gobierno Corporativo:** Se refiere básicamente a las reglas, procesos o leyes a través de las cuales las corporaciones llevan a cabo sus operaciones, son reguladas y controladas. Este término se refiere tanto a factores internos definidos por los directivos, accionistas o los objetivos generales de la organización, como también a las fuerzas externas como los grupos de consumidores, clientes o regulaciones gubernamentales (Robert R. Moeller- John Wiley & Sons - Citación de Enterprise Risk Management Integrated Framework 2004, 2011).

- **Compliance:** En una organización se refiere al cumplimiento de políticas, normas éticas, regulaciones y condiciones legales internas y del entorno en la que ejerce sus funciones (Robert R. Moeller- John Wiley & Sons - Citación de Enterprise Risk Management Integrated Framework 2004, 2011).

- **Stakeholders:** Son todos aquellos grupos que directa o indirectamente son afectados por las actividades de la compañía. Aquí se pueden incluir a los accionistas, empleados, clientes, proveedores.

- **Apetito al riesgo:** Es el nivel del riesgo que una organización y sus gerentes individuales están dispuestos a aceptar en su persecución de valor. Puede ser medido en categorías como alteo, medio y bajo (Robert R. Moeller- John Wiley & Sons - Citación de Enterprise Risk Management Integrated Framework 2004, 2011).

- **Sistema de Gestión de Riesgos (ERM):** Un proceso ejecutado por el consejo directivo, la administración y otro personal de una entidad, aplicado en el establecimiento de estrategias en toda la empresa, designado para identificar eventos potenciales que pudieran afectar a la entidad, y administrar los riesgos para mantenerlos dentro de su propensión al riesgo, proporcionar seguridad razonable referente al logro de objetivos de la entidad. (MacLeod, y otros, 2012), basado en la definición dada por The Committee of Sponsoring Organizations of the Treadway Commission.

- **C.O.S.O:** The Committee of Sponsoring Organizations of the Treadway Commission. Está conformado por: American Institute of Certified Public Accountants (AICPA), American Accounting Association (AAA), The Institute of Internal Auditors (IIA), Institute of management Accountants (IMA) y el Financial Executives International (FEI). Este comité ha emitido varios informes acerca del

control interno, guías prácticas y otros documentos para la actividad de auditoría interna. (PwC, 2011)

- **Riesgo:** Posibilidad de que ocurra un incidente que afecte negativamente al logro de los objetivos (Reding, y otros, 2009, págs. 10-25)

- **Auditoría Interna:** De acuerdo al Instituto de Auditores Internos de los EEUU es una actividad independiente y objetiva de aseguramiento y consulta, concebida para agregar valor y mejorar las operaciones de una organización. Ayuda a una organización a cumplir sus objetivos aportando un enfoque sistemático y disciplinado para evaluar y mejorar la efectividad de los procesos de gestión, control y dirección. (Borja, 2004, pág. 25)

- **Incertidumbre:** Incapacidad de saber anticipadamente la probabilidad e impacto exactos de eventos futuros. (PriceWaterHouseCoopers LLP, 2004)

- **Debilidad (Auditoría):** Identificación de un evento negativo dentro de un proceso realizado en una entidad, que a su vez determina la consecución de un riesgo con impacto negativo a las actividades de una empresa.

- **Probabilidad:** La posibilidad de que un evento dado ocurra. (PriceWaterHouseCoopers LLP, 2004)

- **Seguridad Razonable:** El concepto de que la gestión de riesgos corporativos, por muy bien diseñada y operativa que esté, no puede proporcionar una garantía de la consecución de objetivos de la entidad, debido a las Limitaciones Inherentes a dicha gestión. (PriceWaterHouseCoopers LLP, 2004)

- **Impactos:** Consecuencia o efecto de la consecución de un riesgo (Robert R. Moeller-John Wiley & Sons - Citación de Enterprise Risk Management Integrated Framework 2004, 2011).

- **Control/es Interno/s:** de acuerdo al COSO promovido por las siguientes organizaciones: American Institute of Certified Public Accountants (AICPA), American Accounting Association (AAA), The Institute of Internal Auditors (IIA), Institute of Management Accountants (IMA) y el Financial Executives International (FEI), patrocinaron un estudio del control interno y en 1992, se publicó el resultado de dicha investigación en el denominado informe COSO, por sus siglas en Inglés; en este documento se define el control interno de la siguiente manera: Es un proceso efectuado por el cuerpo colegiado más alto (Consejo de administración, Directorio, etc.) la gerencia y por el personal de una entidad para dar seguridad razonable del cumplimiento de los objetivos institucionales, comprendidos en uno o más de los siguientes grupos: efectividad y eficiencia de las operaciones, confiabilidad de la información financiera administrativa; y, observación de las leyes reglamentos aplicables (Borja, 2004, pág. 113).

ANEXOS

Anexo 1: Métodos Alternativos para Identificación de Eventos

Aquí una breve explicación de las tres técnicas:

Método Delphi: El nombre de esta técnica nace hace miles de años atrás de los antiguos Griegos. En la ciudad de Delphi en la antigüedad se formó un templo que estaba habitado por unos curas llamados Oráculos, una de sus funciones era responder las preguntas que le hacían los pobladores de la localidad y sus palabras eran vistas como las palabras de los dioses. Las respuestas a las preguntas que se les planteaba no eran entregadas inmediatamente, se hacía una deliberación entorno a la cuestión presentada y su respuesta era entregada a la persona por un miembro anónimo. Este templo era visto como un centro de conocimiento y era parte de las decisiones que se tomaban en el mundo de aquel entonces. A partir de este hecho, la Corporación RAND de Santa Mónica en California diseña este particular método en los años 50 por su semejanza con el Templo en la ciudad Delphi.

El fundamento de esta metodología es la realización de encuestas en varias rondas, entregando a los participantes los resultados de la primera etapa para que sean

reconsideradas y se tome la decisión de permanecer con las mismas o cambiarlas de manera parcial o total. Se ha visto que en ocasiones, con el método de lluvia de ideas, se presentan miembros de la actividad que toman el liderazgo de las sesiones quitando participación a otros integrantes. En este método se elimina este aspecto dado que las consultas son realizadas anónimamente a los participantes, de manera individual y con cierta confidencialidad utilizando cuestionarios.

Básicamente la técnica parte del equipo ERM quienes actúan como los "Oráculos" y serán los administradores de este proceso. Se selecciona un grupo de gerentes involucrados en el área designada para esta actividad quienes identificarán los riesgos. Los "Oráculos" deberán realizar un formato con preguntas básicas para identificación de riesgos, mismo que será entregado a los gerentes seleccionados en esta actividad. Con los resultados, el equipo ERM deberá identificar ideas comunes entre los participantes y proponer un listado de riesgos en las áreas más importantes. Los gerentes seleccionados deberán revisar este nuevo listado y a su vez expresar su acuerdo, desacuerdo o propuesta de modificaciones. El equipo ERM ("Oráculos") podrá desarrollar un listado actualizado en base a esta propuesta y organizar una tercera ronda de ser necesario (The Comittee of Sponsoring Organizations of the Treadway Commission, 2004).

De esta manera el quipo ERM puede obtener un claro listado de riesgos con la participación equitativa de todos los miembros escogidos. Esta, al parecer es una excelente técnica, sin embargo, consume bastante tiempo del cual en muchas ocasionalmente no se dispone. El Método Delphi además propone una participación anónima de los involucrados lo cual otorga una mayor objetividad al ejercicio. Hoy en día la metodología puede ser

realizada de una manera muy eficiente ya que se pueden utilizar herramientas tecnológicas disponibles como el internet y las hojas de cálculo para facilitar el manejo de la información y la recepción – entrega de los cuestionarios en un tiempo relativamente corto. De todas maneras, cabe mencionar que la técnica únicamente puede resultar óptima si existe una participación y compromiso de las personas involucradas, respetando los tiempos establecidos para las respuestas.

Simulación Monte Carlo: Este método proviene del Casino Monte Carlo ubicado en Mónaco y es utilizado para entender y evaluar riesgos de los cuales no se tiene mucho conocimiento o certeza en cuanto a su significancia (costo) e impacto. De manea general, se recomienda que cuando se identifican muchos riesgos en las áreas core de una compañía por ejemplo, 100, 200 o más riesgos; se utilice un sistema más técnico como el Monte Carlo para determinar qué riesgos son realmente prioritarios para iniciar con las estrategias de remediación.

De manera general, lo que se realiza en esta metodología es solicitar a las personas designadas para la identificación de riesgos que establezcan una serie de factores y realicen estimaciones entorno a los mismos; estos podrían ser probabilidad de ocurrencia e impacto monetario si esa es la naturaleza del riesgo. Con estos parámetros se deben considerar el mejor, cuasi real y peor escenario para ser representados en un gráfico simple parecido a una campana que es considerado como un modelo. El propósito de este método es diseñar una serie de modelos que describan los riesgos identificados a través de simulaciones de computadora para así establecer varias combinaciones de riesgos en diferentes escenarios

(Robert R. Moeller- John Wiley & Sons - Citación de Enterprise Risk Management Integrated Framework 2004, 2011).

Este método no es sencillo y se necesita de ayuda técnica especializada para que pueda ser llevado a cabo.

Árbol de Decisiones: Esta técnica es utilizada para determinar la probabilidad de ocurrencia de riesgos combinados. Es útil cuando se trata de estimar resultados para riesgos que se encuentran relacionados o son causantes unos de otros. Básicamente lo que muestra la teoría de esta técnica es que se deben considerar los niveles de probabilidad de ocurrencia de un riesgo en términos porcentuales y multiplicarlo por el nivel de probabilidad de otro riesgo causado a raíz de la ocurrencia del primero. La herramienta es eficaz cuando se trata de determinar el impacto final que tendrá un riesgo considerando que su ocurrencia tendrá un impacto en otras áreas que a su vez podría incrementar la probabilidad de ocurrencia de otros riesgos y ser potencialmente más peligroso de lo que se pensaba.

El árbol de decisiones es llamado de esta manera ya que gráficamente permite detallar los impactos y relaciones de unos riesgos con otros especialmente cuando se cuenta con una cantidad de riesgos conjuntos identificados en una organización, creando así una forma de un árbol con varias ramas y hojas consecutivas.

Las técnicas detalladas de manera muy superficial en los párrafos antecedentes pueden ser muy útiles si son entendidas y estudiadas profundamente; sus teorías pueden ser encontradas en literaturas estadísticas más técnicas.

Anexo 2: Categorización de Eventos por Factores (Committee of Sponsoring Organizations of the Treadway Commission, 2004, pág. 38)

Mecanismo - Entrada	Factores Externos					Factores Internos			
	Economico	Medio Ambiente	Político	Social	Tecnológico	Infraestructura	Empleados	Procesos	Tecnología
Conferencias de industria o técnicas	X	X	X	X	X	X	X	X	X
Página web de la compañía	X				X				
Reuniones de manejo de riesgos internos						X	X	X	X
Reportes de benchmarking	X				X	X	X	X	X
Índices externos	X	X	X	X	X				
Índices internos/otros indicadores						X	X	X	X
Nuevas decisiones legales	X		X	X					
Reportes de análisis	X		X	X					
Publicaciones de la industria, mercado y profesionales	X	X	X	X	X				
Tiempo de lanzamiento de productos vs otros competidores	X						X	X	X

Anexo 3: Matrices de Riesgos y Formatos para Selfassessments de Controles Internos.

(Silva, 2013)

Programa de Trabajo para Selfassessment

D-10 / Programa

MM S.A.
PROGRAMA DE TRABAJO
AREA:
FECHA:
HECHO POR:

RESPONSABLE		ACTIVIDAD	TIEMPO en Horas ESTIMADO	REAL	REF. P/T
		DESCRIPCION GENERAL DEL AREA: PUNTOS DEBILES IMPORTANTES: PUNTOS FUERTES DE CONTROL: OBJETIVOS DEL AUDITOR INTERNO: DESCRIPCION DE LOS PROCEDIMIENTOS DE AUDITORÍA INTERNA:			

Prueba de Cumplimiento

P.T	
Preparado por	
Revisado por	
Fecha	

PRUEBA DE CUMPLIMIENTO
PROCESO:
FECHA:
HECHO POR:

							Aserciones							
PARAMETRO 1	PARAMETRO 2	PARAMETRO 3	PARAMETRO 4	PARAMETRO 5	PARAMETRO 6	a	b	c	d	e	f	g	h

NOTA 1. **OBJETIVO DEL TRABAJO**

NOTA 2. **SELECCIÓN DE LA MUESTRA:**

Significado de Aserciones:

a
b
c
d
e
f
g
h

Marcas:
n/a
ok
otras

Detalle de Excepciones

DETALLE DE EXCEPCIONES
PROCESO:
FECHA:
HECHO POR:

Preparado por:

Nº Excepción	Ref. PT:	DESCRIPCIÓN DE LA EXCEPCIÓN (Problema)	COMENTARIO DEL RESPONSABLE DEL RIESGO	DISPOSICIÓN DEL EQUIPO ERM	POLITICA AFECTADA
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					
16					
17					
18					
19					
20					

Matriz de Riesgos

MATRIZ DE RIESGOS

AREA: MM

FECHA:

HECHO POR:

Nº	Descripción de la debilidad	Descripción del Riesgo	Nivel de ocurrencia del rriesgo				Descripción del Impacto	Nivel del impacto				Puntuación Individual				Impacto en Costo	Costo Esperado	Respuesta al Riesgo	Objetivo Relacionado	Apetito al Riesgo Relacionado al Proceso	Niveles de Tolerancia
			A (9)	M (5)	B (1)	Ning (0)		A (9)	M (5)	B (1)	Ning (0)	A (9)	M (5)	B (1)	Ning (0)						
1																					
2																					
3																					
4																					
5																					

Asesoramiento de Riesgos Residuales

Nº	Descripción de la debilidad	Riesgo Residual	Nivel de ocurrencia del				Descripción del Impacto	Nivel del impacto				Puntuación Individual				Impacto en Costo	Costo Esperado
			A (9)	M (5)	B (1)	Ning (0)		A (9)	M (5)	B (1)	Ning (0)	A (9)	M (5)	B (1)	Ning (0)		
1																	
2																	
3																	
4																	
5																	