UNIVERSIDAD TECNICA FEDERICO SANTA MARIA

Repositorio Digital USM **https://repositorio.usm.cl**

Tesis USM Tesis de Postgrado de Acceso Abierto

2016

DIESEÑO DE UN MODELO DE CONTROL DE GESTIÓN DE RIESGO BASADO EN ISO 31.000 Y COSO ERM PARA SU APLICACIÓN EN GEOLAQUIM LTDA.

FLORES MADRID, CAROLINA MAGDALENA

http://hdl.handle.net/11673/23147

Repositorio Digital USM, UNIVERSIDAD TECNICA FEDERICO SANTA MARIA

UNIVERSIDAD TÉCNICA FEDERIO SANTA MARÍA
Departamento de Ingeniería Comercial
MBA

DISEÑO DE UN MODELO DE CONTROL DE GESTIÓN DE RIESGO BASADO EN ISO 31.000 Y COSO ERM PARA SU APLICACIÓN EN GEOLAQUIM LTDA

Carolina Magdalena Flores Madrid

MBA. Magíster en Gestión Empresarial

Julio 2016

UNIVERSIDAD TÉCNICA FEDERIO SANTA MARÍA
Departamento de Ingeniería Comercial
MBA

DISEÑO DE UN MODELO DE CONTROL DE GESTIÓN DE RIESGO BASADO EN ISO 31.000 Y COSO ERM PARA SU APLICACIÓN EN GEOLAQUIM LTDA

Tesis de Grado presentada por

Carolina Magdalena Flores Madrid

Como requisito para optar al grado de

MBA. Magíster en Gestión Empresarial

Director de Tesis: Dr. Lionel Valenzuela O.

Julio 2016

TITULO DE TESIS:

“Diseño de un modelo de control de gestión de riesgo basado en ISO 31.000 y COSO ERM para su aplicación en Geolaquim Ltda.”

AUTOR:

CAROLINA MAGDALENA FLORES MADRID

TRABAJO DE TESIS, presentando en cumplimiento parcial de los requisitos para el Grado de MBA Magíster en Gestión Empresarial de la Universidad Técnica Federico Santa María.

Observaciones:

_____

_____

Sr. Lionel Valenzuela O. .....

Santiago , Julio 2017

Todo el contenido, análisis, conclusiones y opiniones vertidas en este estudio son de mi exclusiva responsabilidad.

Nombre CAROLINA MAGDALENA FLORES MADRID

Firma…….

Fecha……

Resumen Ejecutivo

~~"Nadie busca lo que no conoce". Es necesario conocer los riesgos para enfrentarse a ellos, este es el mayor desafío que tiene hoy las organizaciones, por ello existe una búsqueda creciente de herramientas para la gestión integral del riesgo, que permite a las empresas administrar sus riesgos para la creación de valor y entregar una seguridad razonable a sus procesos tanto estratégicos como operacionales.~~

~~Por lo anterior, es que la presente investigación, propone un nuevo modelo de control de gestión de riesgos basado en COSO ERM e ISO 31000 y su aplicación en la empresa Geolaquim, donde la metodología de trabajo utilizada es la integración y complementariedad de ambas herramientas de gestión, la evaluación del cumplimiento de aspectos claves del nuevo modelo, estableciendo los requerimientos que la empresa debe cumplir, además de la estrategia para la aplicación del nuevo modelo en la empresa Geolaquim.~~

~~La complementariedad e integración de ambos sistemas en el nuevo modelo de gestión de riesgos, permite a las empresas, un control de gestión de riesgos con un enfoque en la estrategia y robusto, debido a COSO ERM, y con un enfoque en los procesos, simple y practico, debido a la ISO 31000, logrando el objetivo de esta investigación, y permitiendo entregar una herramienta a la empresa para gestionar sus riesgos y mejorar sus prácticas para diseñar, documentar e implantar, controles eficaces y eficientes orientados a reducir los riesgos estratégicos y sobre todo sobre la base de un mejoramiento continuo.~~

La presente investigación consiste en el diseño de un nuevo sistema de control de gestión de riesgos, en base a complementar e integrar dos herramientas internacionales de gestión de riesgo, COSO ERM, con enfoque financiero y ISO 31000, con enfoque de proceso, y su aplicación en la empresa Geolaquim, con el objeto de proporcionar a la organización una herramienta para la gestión integral del riesgos que le permita administrar sus riesgos para la creación de valor y

Con formato: Justificado, Interlineado: 1,5 líneas

entregar una seguridad razonable a sus procesos tanto estratégicos como operacionales, necesidad que hoy es el mayor desafío para las organizaciones.

Con esto se logra gestionar riesgos estratégicos en función de los objetivos de la empresa, además de una metodología apropiada para identificar, analizar, documentar, evaluar, controlar y monitorear los eventos de riesgo estratégicos, en el "Sistemas de Gestión de Riesgos", sobre la base de un lenguaje común y lineamientos de los marcos de referencia ISO 31000:2009 y COSO ERM.

Como resultado de la investigación, la empresa Geolaquim, cuenta con una estrategia de aplicación del nuevo sistema de control de gestión de integral de riesgos, en base a la determinación de la brecha en cuanto al cumplimientos de aspectos claves del nuevo modelo de gestión. Además de, conocimientos y procedimientos necesarios para gestionar los riesgos estratégicos en función de los objetivos de la empresa, asegurando con ello evitar que se refuercen las debilidades, que se desarrollen las amenazas del entorno, que no se aprovechen las oportunidades y que se pierdan las fortalezas de la organización.

Con formato: Fuente: Sin Negrita

TABLA DE CONTENIDOS

1. INTRODUCCIÓN ..... 8~~7~~

2. OBJETIVOS ..... 11~~10~~

2.1. OBJETIVO GENERAL ..... 11~~10~~

2.2. OBJETIVOS ESPECÍFICOS ..... 12~~11~~

3. ALCANCE DEL ESTUDIO ..... 12~~11~~

4. METODOLOGÍA DE TRABAJO ..... 13~~12~~

5. ESTADO DEL ARTE ..... 14~~13~~

6. MARCO TEÓRICO ..... 15~~14~~

6.1. GESTIÓN DEL RIESGO ..... 15~~14~~

6.2. QUÉ ES RIESGO Y OPORTUNIDAD ..... 16~~15~~

6.3. GESTIÓN DE RIESGOS SEGÚN COSO ERM 17

6.4. GESTIÓN DE RIESGOS SEGÚN ISO 31000 ..... 51~~50~~

6.6. GEOLAQUIM LTDA. ..... 66~~64~~

7. DISEÑO Y APLICACIÓN DEL MODELO DE CONTROL DE GESTIÓN DEL RIESGO ..... 69~~67~~

7.1. EVALUACIÓN DE CUMPLIMIENTO DE ASPECTOS CLAVES DE MODELO INTEGRADO DE GESTIÓN DEL RIESGO 75~~73~~

7.2. DETERMINACIÓN DE BRECHA CON LA ORGANIZACIÓN ..... 104~~102~~

7.3. ESTRATEGIA DE APLICACIÓN DEL NUEVO SISTEMA DE CONTROL DE GESTIÓN DE RIESGOS EN GEOLAQUIM ..... 107~~105~~

8. CONCLUSIONES ..... 118~~116~~

9. BIBLIOGRAFÍA ..... 120~~118~~

TABLA DE ILUSTRACIONES

ILUSTRACIÓN 1 MATRIZ TRIDIMENSIONAL DE GESTIÓN DE RIESGOS ..... 25~~24~~

ILUSTRACIÓN 2. ESTRUCTURA NORMA ISO 31.000. ENFOQUE Y RELACIÓN DE LOS ELEMENTOS CLAVES. ..... 53~~52~~

ILUSTRACIÓN 3. RELACIÓN DE COMPLEMENTARIEDAD COSO ERM E ISO 31.000 ..... 64~~63~~

ILUSTRACIÓN 4. MAPA DE PROCESOS DE GEOLAQUIM LTDA. ..... 68~~66~~

1. Introducción

El gran tamaño y la complejidad de las organizaciones que introducen nuevos y diferentes riesgos; la incapacidad de las técnicas tradicionales y del seguimiento para mantenerse actualizados con los cambiantes perfiles de riesgo; las crecientes demandas, expectativas y atención de parte de los grupos de interés; la intolerancia ante los “contratiempos” y sorpresas causadas por insuficiente control de riesgos y el manejo poco efectivo de ciertos riesgos que puede conducir a una exposición involuntaria a otros, crean en las organizaciones la necesidad de una creciente importancia a la Gestión Integral de Riesgos, por lo que las organizaciones tienen el desafío de adoptar un enfoque formal para gestionar el riesgo de manera efectiva e integrar la gestión de riesgos en los procesos operativos.

La Gestión de Riesgos de las organizaciones constituyen un medio para ayudar a perfeccionar la forma en que una empresa entiende y administra los riesgos para lograr transparencia, crecimiento futuro (creación de valor) y activo existente (protección de valor).

Una Gestión de Riesgos es un medio para entregar una seguridad razonable de que se han identificado los riesgos críticos para la misión y que éstos están administrados correctamente; un enfoque integrado establecido desde el más alto nivel; una visión de portfolio de riesgos a nivel de toda la empresa para el reporte de los ejecutivos y el directorio; un medio para alinear las especializaciones y estrategias de riesgo para la empresa como un todo; un medio para apoyar el establecimiento de estrategias y la toma de decisiones basadas en la inteligencia sobre los riesgos; y un medio para mejorar la “inteligencia sobre los riesgos” para una ventaja competitiva.

Con esto, la gestión de riesgo se está moviendo más allá de la tradicional mitigación de riesgos, de aplicar controles para limitar la exposición a los problemas, hacia la optimización de la cartera de riesgos, determinando el apetito y la capacidad de riesgo de la organización entre un grupo de riesgos a través de los negocios, tomando oportunidades dentro de esos parámetros definidos y capitalizando las

utilidades resultantes. Como consecuencia, la gestión de riesgo está comenzando a ser percibida como una nueva forma de administración estratégica de negocios, relacionando la estrategia del negocio con los riesgos cotidianos. La gestión de riesgo empresarial en este contexto, es una forma significativa de identificar los riesgos críticos que la organización enfrenta, incluyendo, por ejemplo, reputación, ética, e-business, o riesgos de salud, seguridad, y medio ambiente (no solamente riesgos financieros o asegurables) y luego administrar y optimizar esa cartera de riesgos para obtener los retornos financieros necesarios.

Por lo anterior, las empresas están experimentando la necesidad de unificar el lenguaje y los procedimientos en los diferentes sistemas de administración de riesgos que utilizan, estandarizarlos y articularlos con otros sistemas de gestión y con estándares internacionales vigentes de Sistemas de Control Interno, tales como, COSO, MECI, COBIT e ISO 27001, basándose en la norma ISO 31000:2009, principios y el marco de referencia para el proceso de administración de riesgos.

Es por ello, que mediante la presente investigación, se busca proponer un modelo de Control de Gestión del Riesgo, que permita obtener un marco de referencia y metodológico, práctico y eficiente para implantar la gestión de riesgos empresariales, específicamente para identificar, analizar, documentar, evaluar, controlar, monitorear y mejorar continuamente los sistemas en la organización, basado en COSO ERM e ISO 31.000, que se encuentre integrado a los Objetivos del Negocio.

COSO es un sistema que permite implementar el control interno en cualquier tipo de entidad u organización. Sus siglas se refieren al Committee of Sponsoring Organizations of The Treadway Commission, quienes evaluaron y llegaron a la conclusión que la ausencia de orden en los procesos de una entidad, representa una diversidad de riesgos, por lo tanto, es necesario evaluarlos y darles una respuesta inmediata para evitar los posibles fraudes o errores que pudieren surgir.

La evolución a lo largo de la historia de la estructura del Sistema COSO ha sido efectiva a partir del año 1992, en cuyo año se denominó Marco del Control Interno (COSO I), para el año 2004 se da a conocer la mejora en el Sistema de COSO I con

el Marco Integral de Riesgos (COSO II ERM), y para el año 2006 se da a conocer el Sistema de COSO III para pequeñas y medianas empresas.

La implementación del Sistema COSO, genera beneficios, evita riesgos, detecta fraudes y aporta la eficiencia en los controles en una entidad. La elección adecuada del Sistema COSO debe ser acorde al grado de desarrollo que posea la entidad.

Para el caso, el modelo del sistema COSO, es el COSO II ERM, en este modelo se buscó la mejora en los elementos potenciales, como resultado de ello se integra a 8 elementos potenciales: a) ambiente interno; b) establecimiento de objetivos; c) identificación de eventos; d) evaluación de riesgos; e) respuesta a los riesgos; f) actividades de control; g) información y comunicación y h) supervisión.

Los modelos del Sistema COSO buscan la eficiencia y eficacia de los recursos, la fiabilidad de la información interna y externa, financiera y no financiera, la alineación de los elementos a la misión de la entidad, la verificación del cumplimiento de las leyes y normas vigentes. Este sistema debe ser aplicado por la dirección, la administración y el resto del personal de una entidad.

A su vez, la norma internacional ISO 31000, proporciona principios y directrices para la gestión de riesgos, ayudando a las organizaciones en sus análisis y evaluaciones de riesgos, tanto en una empresa pública, privada o comunitaria, siendo sus beneficios son aplicables a la mayoría de las actividades empresariales, incluyendo la planificación, operaciones de gestión y procesos de comunicación. Aunque todas las organizaciones gestionan los riesgos de algún modo, las recomendaciones de mejores prácticas de esta norma internacional se desarrollaron para mejorar las técnicas de gestión y garantizar la seguridad en el lugar de trabajo en todo momento.

Mediante la implantación de los principios y guía de la norma ISO 31000 las organizaciones mejoran su eficacia operativa, su gobernanza y la confianza de las partes interesadas, al mismo tiempo que minimiza cualquier posible pérdida. Esta norma internacional también ayuda a fomentar el desempeño de Seguridad y Salud, establecer una base sólida para la toma de decisiones y fomenta una gestión proactiva en todas las áreas.

Las principales ventajas con que cuenta son mejorar de forma proactiva la eficacia operativa y la gobernanza, generar confianza entre las partes interesadas con el uso de técnicas de riesgos, aplica controles de sistemas de gestión para analizar riesgos y minimizar posibles pérdidas, mejora el desempeño y resiliencia de los sistemas de gestión, responde a los cambios de forma eficaz y protege su empresa mientras crece.

El nuevo modelo de Control de Gestión del Riesgo será aplicado en la empresa Geolaquim Ltda., que corresponde a un laboratorio químico geológico ubicado en la ciudad de Copiapó, región de Atacama, que presta servicios a la minería. Geolaquim es una mediana empresa según categorización de Corfo, sus facturaciones anuales promedian los 1500 millones de pesos, con una planilla de personal de 60 personas, variable según los contratos que ejecuten.

Geolaquim, al igual que otras empresas y compañías, opera en ambientes muy dinámicos y de alto nivel competitivo, caracterizado por factores tales como: mayor índice de globalización en los negocios, incremento del uso de tecnología de información, reestructuraciones organizativas y reingeniería de los procesos, constantes cambios en los mercados y la competencia, lo que ha creado un nivel de riesgo e incertidumbre importante, por lo que se hace necesario la Gestión de Riesgos a nivel estratégico, para lograr una reducción de los niveles de riesgo existentes en la empresa y en sus procesos en general como son los operativos, financieros, administrativos, entre otros.

2. Objetivos

2.1. Objetivo General

- Diseñar un nuevo sistema de control de gestión de riesgos basado en COSO ERM e ISO 31000, el cual será aplicado en la empresa Geolaquim Ltda.

2.2. Objetivos Específicos

- Proporcionar conocimientos y procedimientos necesarios para gestionar los riesgos estratégicos en función de los objetivos de la empresa, asegurando con ello evitar que se refuercen las debilidades, que se desarrollen las amenazas del entorno, que no se aprovechen las oportunidades y que se pierdan las fortalezas de la organización.
- Proveer una metodología apropiada para identificar, analizar, documentar, evaluar, controlar y monitorear los eventos de riesgo estratégicos, en el "Sistemas de Gestión de Riesgos", sobre la base de un lenguaje común y lineamientos de los marcos de referencia ISO 31000:2009 y COSO ERM.
- Proveer la metodología y las mejores prácticas para diseñar, documentar e implantar, controles eficaces y eficientes orientados a reducir los riesgos estratégicos.
- Proveer estrategias para proyectar a mediano y largo plazo, la sostenibilidad y mejoramiento continuo del sistema de gestión de riesgos aplicado a la empresa.

3. Alcance del estudio

La presente investigación tendrá un alcance desde la definición del Nuevo Sistema de Control de Gestión hasta su aplicación en Geolaquim Ltda.

De acuerdo las experiencias existentes en el ámbito de gestión de riesgos, las metodologías que se utilizarán en este trabajo, COSO ERM y ISO 31000 serán aplicadas independientemente, es decir las empresas implementan estas metodologías cada uno por sí sola, es debido a esto, que se visualiza la oportunidad de generar un modelo que control de gestión que integre ambas metodologías, logrando un modelo completo que permita alcanzar desde la estrategia de la empresa hasta el ámbito operacional.

Comentado [LV1]: Redacción

Bajo lo anterior, este estudio se clasifica como Exploratorio, con el propósito de aplicar esta herramienta modelo en la empresa Geolaquim Ltda.

4. Metodología de Trabajo

Con el fin de mostrar la planificación y estrategia que permita abordar el desarrollo de la presente investigación, que se busca proponer un modelo de Control de Gestión del Riesgo, que permita obtener un marco de referencia y metodológico, práctico y eficiente para implantar la gestión de riesgos empresariales, específicamente para identificar, analizar, documentar, evaluar, controlar, monitorear y mejorar continuamente los sistemas en la organización, basado en COSO ERM e ISO 31.000, que se encuentre integrado a los Objetivos del Negocio.

Se consideran las siguientes etapas:

1) Reconocer los componentes y aspectos claves del sistema de gestión de riesgos COSO ERM e ISO 31000
2) Establecer la complementariedad de ambos sistemas de gestión de riesgo
3) Diseñar el nuevo modelo, complementando ambos sistemas de gestión a través de sus componentes y aspectos o principios claves
4) Establecer el método de control para cada componente del nuevo sistema, Modelo Integrado de control de gestión del riesgo
5) Crear evaluación de cumplimiento de aspectos claves del modelo integrado de gestión de riesgos, el cual establece los requerimientos que la empresa debe cumplir una vez implementado el modelo
6) Determinar la brecha de la empresa respecto de los requerimientos del nuevo modelo integrado de gestión del riesgo, con la aplicación de la evaluación en Geolaquim Ltda
7) Establecer la estrategia de aplicación del nuevo sistema de control de gestión de riesgos de la empresa Geolaquim

Con lo anterior, se logra dar respuesta al objetivo general y específicos de la investigación.

5. Estado del Arte

Las organizaciones de cualquier naturaleza (privadas, publicas, sin lucro, productivas, financiera, etc.) están expuestas a la posible materialización de riesgos en el desarrollo de sus actividades propias del negocio, lo cual puede impactar negativamente al logro de sus objetivos estratégicos y afectar los resultados financieros.

Por ello, a lo largo de la historia, se han creado múltiples modelos que permiten las gestionar los riesgos, por mencionar algunos en un marco internacional, se encuentran:

- COSO: es la metodología más extendida e implementada a nivel internacional, dedicada a proveer marcos y orientaciones sobre la gestión del riesgo empresarial, control interno y la disuasión del fraude.
- ERM: son estándares de gerencia de riesgos que considera las consecuencias positivas y negativas en todo tipo de organizaciones y actividades en el corto y largo plazo.
- AZ/NZ 4360:2004: publicado por la organización de estandarización de Australia y Nueva Zelanda, acaba de ser sustituido por el estándar AZ/NZ ISO 31000:2009.
- NS 5814:1991: es un estándar noruego que propone unas líneas de actuación para el tratamiento de los riesgos enfocado a la propuesta de mejoras y la consecución de las mismas.
- ISO 31000:2009: «Gestión del Riesgo. Principios y Orientaciones», que recoge y unifica todos los estándares mencionados. Está diseñado para que cualquier tipo de organización pueda identificar y evaluar todos sus riesgos de una forma estructurada.
- ISO 30010:2009: «Gestión del Riesgo. Técnicas de Evaluación del Riesgo», diseñadas para facilitar la aplicación de la norma ISO 31000 en los procesos de identificación y evaluación del riesgo.

En la actualidad, las organizaciones se encuentran frente a un desafío a raíz de la actualización de la norma internacional ISO 9001 a versión 2015, la que incluye un cambio importante incorporando la gestión del riesgo o un enfoque basado en riesgos, haciendo que cada vez más organizaciones sean conscientes de la importancia de gestionar adecuadamente la incertidumbre que presentan sus actividades y construir ventajas competitivas mediante la identificación, evaluación y gestión de los riesgos que afrontan.

La gestión de los riesgos, aspecto de enorme relevancia dentro de la nueva versión de la ISO 9001, es uno de los puntos más novedosos y seguramente el más laborioso, porque una adecuada gestión de riesgos permite alcanzar los resultados previstos y la satisfacción del cliente.

Principalmente, el enfoque de riesgos de la norma ISO 9001:2015, toma como guía los principios básicos que establece la norma ISO 31000, dejando abierta la posibilidad de utilizar alguna metodología de gestión de riesgo que más convenga a la organización.

COSO ERM es una metodología de gestión del riesgo que permite una gran complementariedad con la ISO 31000, con su enfoque integrador.

6. Marco teórico

6.1. Gestión del Riesgo

La gestión integral de los riesgos es un proceso estructurado, consistente y continúo implementado a través de toda la organización para identificar, evaluar, medir y reportar amenazas y oportunidades que afectan el poder alcanzar el logro de los objetivos.

La Gestión de riesgos también puede definirse como la identificación, medición y evaluación colectiva de todos los riesgos que afectan el valor de la organización, así como la definición e implementación de una estrategia en el negocio y en la operación para gestionar efectivamente esos riesgos.

Para una Gestión de Riesgo Eficaz se debe buscar:

- Definir criterios de aceptación general de riesgos, de acuerdo a la actividad comercial de la organización (matriz segmento, mercado, producto, canal).
- Uso de un mapa de riesgo para definir el área aceptable de exposición, el riesgo máximo aceptable (área de peligro) y el área no aceptable de exposición al riesgo.
- Definir el tipo de pérdida que se desea estimar, su horizonte temporal, metodología o modelo.
- Diseñar mecanismos de cobertura de los riesgos, con una visión integral y comprensiva del negocio.
- Definir y estimar medidas de desempeño ajustadas por riesgo.

Los procesos de gestión de riesgos en organizaciones no complejas son distintos a los que se utilizan en las organizaciones de mayor complejidad. Sin embargo, no hay normas estrictas que dicten cómo debe una entidad manejar el proceso. Su grado de rigor debe cumplir con los dictados de la alta dirección, y ser apropiado en función de los riesgos en cuestión.

6.2. Qué es riesgo y oportunidad

En una organización se encuentran eventos, estos eventos pueden tener un impacto negativo o positivo o incluso ambos, en si se puede decir que son baches o sorpresas por el camino.

Cuando estos eventos tienen un impacto negativo se dice que son riesgos, que pueden afectar la creación de valor o dañar la existente. Los eventos con impacto positivo oportunidades, los cuales pueden compensar a los impactos negativos o bien la posibilidad que afecte positivamente al logro de los objetivos, ayudando a la

creación de valor, por lo que la organización debe establecer fórmulas para aprovechar estas oportunidades.

También se puede definir riesgo, como la probabilidad que un peligro, causa inminente de pérdida, existente en una actividad determinada durante un período definido, ocasione un incidente de ocurrencia incierta, pero con consecuencias factibles de ser estimadas. Además, riesgo como el potencial de pérdidas que existe asociado a una operación productiva, cuando cambian en forma no planeada las condiciones definidas como estándares para garantizar el funcionamiento de un proceso o del sistema productivo en su conjunto.

De acuerdo a lo definido anteriormente, para las organizaciones es imprescindible identificar aquellos riesgos y oportunidades relevantes, a los cuales se pueda ver enfrentado y que conlleven un impacto para la consecución de sus objetivos, más aún cuando la rentabilidad de su negocio está íntimamente ligada a dichos riesgos.

La identificación de estos riesgos y oportunidades es un proceso iterativo y generalmente integrado a la estrategia y planificación y su análisis se relaciona con la criticidad del proceso o actividad y con la importancia del objetivo, más allá que éste sea explícito o implícito.

Se puede mencionar al respecto, que en las organizaciones se requiere identificar, valorar y cuantificar su exposición al riesgo, optimizando al mismo tiempo la rentabilidad, que se traslada directamente al cliente mediante unos precios más competitivos y la generación de mayores beneficios.

6.3. Gestión de riesgos según COSO ERM

Tratar eficazmente la incertidumbre y sus riesgos y oportunidades asociados, para mejorar la capacidad de generar valor es la premisa fundamental de la Gestión de Riesgos para COSO ERM, por lo cual permite, maximizar el valor cuando las organizaciones encuentran un equilibrio óptimo entre los objetivos de crecimiento y rentabilidad y los riesgos asociados, en base a una estrategia y objetivos establecidos.

La gestión de riesgos, entonces, se ocupa de los riesgos y oportunidades que afectan a la creación de valor o su preservación, definiéndolo como sigue:

"La gestión de riesgos corporativos es un proceso efectuado por el consejo de administración de una entidad, su dirección y restante personal, aplicable a la definición de estrategias en toda la empresa y diseñado para identificar eventos potenciales que puedan afectar a la organización, gestionar sus riesgos dentro del riesgo aceptado y proporcionar una seguridad razonable sobre el logro de los objetivos"

Por lo tanto, de acuerdo a esta definición se puede decir que, la gestión del riesgo corporativo es un proceso continuo que fluye en toda la organización, es realizado por su personal en todos los niveles, se aplica desde la estrategia y está diseñada para identificar acontecimientos potenciales que afectaría a la organización y para gestionar los riesgos dentro del nivel de riesgo aceptado.

La gestión de riesgos para COSO ERM capta los conceptos claves de como las empresas gestionan el riesgo y proporcionan una base para su aplicación en todas las organizaciones. Se centra directamente en el cumplimiento de los objetivos establecidos y proporciona un base para definir la eficacia en la gestión de riesgos corporativos.

Dentro de los conceptos fundamentales de la gestión de riesgos corporativos se puede destacar:

a. Un proceso: La gestión de riesgos no es estática, sino más bien un intercambio continuo de acciones que fluyen por toda la organización, que se difunden y está implícitas en la forma que la dirección lleva el negocio.

b. Realizado por personas: La gestión de riesgos es realizada por todas las personas de la organización, en los distintos niveles, lo que hacen y dicen la hacen realidad. Las personas establecen la misión, estrategia y objetivos de la organización y colocan los mecanismos de dicha gestión en el lugar adecuado. La gestión de riesgos proporciona los mecanismos

para que a las personas puedan entender el riesgo en el contexto de los objetivos de la organización.

c. Aplicado al establecimiento de la estrategia: Una organización fija su misión o visión y establece sus objetivos estratégicos, que son las metas. Para alcanzar los objetivos estratégicos, la organización fija una estrategia y fija los objetivos conexos que se desea realizar y derivan de ella fluyendo en cascada hacia las unidades de negocios y procesos. La gestión de riesgos se aplica durante el establecimiento de la estrategia, con sus técnicas para ayudar a la dirección a evaluar y elegir la estrategia de la organización y los objetivos asociados a ella.

d. Aplicado a toda la empresa: La gestión de riesgos debe ser aplicada en toda la organización y debe considerar toda la gama de actividades de la organización, desde aquellas a nivel de empresa como la planificación estratégica y la asignación de recursos, hasta las unidades de negocios como son la producción.

e. Riesgo aceptado: El riesgo aceptado es el volumen de riesgo, a un nivel amplio, que una entidad está dispuesta a aceptar en su búsqueda de valor. El riesgo aceptado se relaciona directamente con la estrategia de la organización, y se tiene en cuenta para establecerla, ya que distintas estrategias exponen a una entidad a riesgos distintos. Las tolerancias al riesgo están relacionadas con los objetivos de la organización, el cual es el nivel aceptable de variación relativa al logro de un objetivo. Operar dentro de la tolerancia al riesgo ayuda que la empresa se mantenga dentro de su riesgo aceptado y por consiguiente la empresa consiga sus objetivos.

f. Proporciona una seguridad razonable: Una gestión de riesgos corporativa bien diseñada y realizada puede facilitar a la dirección una seguridad razonable sobre la consecución de los objetivos de la organización. La

seguridad razonable está dada por la idea que la incertidumbre y el riesgo están relacionado con el futuro, no se puede predecir con precisión. La seguridad razonable no es una seguridad absoluta.

Beneficios de la Gestión de Riesgos

Ninguna entidad -independientemente de que sea con o sin fines lucro, e incluso una entidad gubernamental-, opera en un ambiente libre de riesgos, y la gestión de riesgos corporativos tampoco crea un ambiente sin riesgos. Lo que sí permite es operar mucho más eficientemente en un ambiente colmado de riesgos.

La gestión de riesgos incluye las siguientes capacidades inherentes:

- Alinear el riesgo aceptado y la estrategia

En su evaluación de alternativas estratégicas considera el riesgo aceptado, estableciendo los objetivos y desarrollando mecanismos para gestionar los riesgos asociados.

- Mejorar las decisiones de respuesta a los riesgos

La gestión de riesgos proporciona rigor para identificar los riesgos y seleccionar entre las posibles alternativas de respuesta a ellos: evitar, reducir, compartir o aceptar.

- Reducir las sorpresas y pérdidas operativas

Las entidades consiguen mejorar su capacidad para identificar los eventos potenciales y establecer respuestas, reduciendo las sorpresas y los costes o pérdidas asociados.

- Identificar y gestionar la diversidad de riesgos para toda la entidad

Cada entidad se enfrenta a múltiples riesgos que afectan a la organización y la gestión de riesgos corporativos facilita respuestas eficaces e integradas a los impactos de dichos riesgos.

- Aprovechar las oportunidades

Mediante la consideración de una amplia gama de potenciales eventos, se está en posición de identificar y aprovechar las oportunidades de modo proactivo.

- Mejorar la dotación de capital

La obtención de información sólida sobre el riesgo permite a la dirección evaluar eficazmente las necesidades globales de capital y mejorar su asignación.

Estas capacidades, inherentes en la gestión de riesgos corporativos, ayudan a la dirección a alcanzar los objetivos de rendimiento y rentabilidad de la organización y prevenir la pérdida de recursos.

La gestión de riesgos corporativos permite asegurar una información eficaz, el cumplimiento de leyes y normas, ayudar a evitar daños a la reputación de la entidad y sus consecuencias derivadas.

6.3.1. Estructura COSO ERM.

La gestión de riesgos corporativos consta de ocho componentes relacionados entre sí, que se derivan de la manera en que la dirección conduce la empresa y cómo están integrados en el proceso de gestión.

A continuación, se describen estos componentes:

a. Ambiente interno: El ambiente interno abarca el tono de una organización y establece la base de cómo el personal de la entidad percibe y trata los riesgos, incluyendo la filosofía de administración de riesgo y el riesgo aceptado, la integridad, valores éticos y el ambiente en el cual ellos operan.

b. Establecimiento de objetivos: Los objetivos deben existir antes de que la dirección pueda identificar potenciales eventos que afecten su consecución.

La administración de riesgos corporativos asegura que la dirección ha establecido un proceso para fijar objetivos y que los objetivos seleccionados apoyan la misión de la entidad y están en línea con ella, además de ser consecuentes con el riesgo aceptado.

c. Identificación de riesgos: Los eventos internos y externos que afectan a los objetivos de la entidad deben ser identificados, diferenciando entre riesgos y oportunidades. Estas últimas revierten hacia la estrategia de la dirección o los procesos para fijar objetivos.

d. Evaluación de riesgos: Los riesgos se analizan considerando su probabilidad e impacto como base para determinar cómo deben ser administrados. Los riesgos son evaluados sobre una base inherente (propio de cada empresa de acuerdo a su actividad) y residual (después de la implementación del tratamiento del riesgo) bajo las perspectivas de probabilidad (posibilidad de que ocurra un evento) e impacto (su efecto debido a su ocurrencia), con base en datos pasados internos (pueden considerarse de carácter subjetivo) y externos (más objetivos).

e. Respuesta al riesgo: La dirección selecciona las posibles respuestas - evitar, aceptar, reducir o compartir los riesgos - desarrollando una serie de acciones para alinearlos con el riesgo aceptado y las tolerancias al riesgo de la entidad.

f. Actividades de control: Son las políticas y procedimientos específicos que se establecen e implantan en los procesos para ayudar a asegurar que las respuestas a los riesgos se llevan a cabo efectivamente.

g. Información y comunicación: La información relevante se identifica, captura y comunica en forma y plazo adecuado para permitir al personal afrontar sus responsabilidades. Una comunicación efectiva debe producirse en un sentido amplio, fluyendo hacia abajo, a través, y hacia arriba de la entidad.

h. Monitoreo (Supervisión): La totalidad de la administración de riesgos corporativos es monitoreada y se efectúan las modificaciones necesarias. Este monitoreo se lleva a cabo mediante actividades permanentes de la dirección, evaluaciones independientes o ambas actuaciones a la vez. La administración de riesgos corporativos no constituye estrictamente un proceso en serie, donde cada componente afecta sólo al siguiente, sino un proceso multidireccional e iterativo en el cual casi cualquier componente puede e influye en otro.

Consecución de Objetivos

Cabe aclarar que los componentes mencionados no se llevan a cabo en serie como si fueran las etapas de un proceso lineal; por el contrario, se trata de un proceso multidireccional e iterativo, en donde cada una de los componentes genera información que influye en los restantes.

Todas las organizaciones poseen una misión y una visión. Ya sea que las mismas estén apropiadamente formalizadas o no, y que se hayan comunicado en forma adecuada o no, cada entidad tiene desde el momento de su creación una misión y una visión particulares.

A partir de las mismas, la dirección establece la estrategia y fija un árbol de objetivos a lograr durante el ciclo de vida de la entidad. Este árbol de objetivos comienza con objetivos a un nivel macro, que luego se van “bajando a tierra” hasta convertirse en objetivos más detallados y más fáciles de medir.

Como ya se mencionó, la idea subyacente de la gestión de riesgos corporativos, es proporcionar una seguridad razonable sobre el logro de los objetivos organizacionales. Los mismos suelen dividirse en cuatro categorías:

- Estrategia: objetivos a alto nivel, alineados con la misión de la entidad;
- Operaciones: objetivos vinculados al uso eficaz y eficiente de recursos;
- Información: objetivos de fiabilidad de la información suministrada;

- Cumplimiento: objetivos relativos al cumplimiento de leyes y normas aplicables.

Estas categorías están directamente relacionadas con las diferentes necesidades de las entidades y si bien la mencionada clasificación es útil con fines teóricos, muchas veces estas categorías pueden solaparse, puesto que un mismo objetivo puede incluirse en más de una categoría.

En este punto es necesario realizar una aclaración: es con respecto a las dos últimas categorías de objetivos (información y cumplimiento), en donde la gestión de riesgos corporativos facilita directamente su consecución, puesto que son categorías “internas”. En cambio, en relación a las dos categorías restantes (estrategia y operaciones), la gestión de riesgos sólo puede proporcionar una seguridad razonable de que la dirección está adecuadamente informada sobre el progreso de su consecución, pero la misma no puede asegurar su logro, puesto que existen factores externos que no se encuentran bajo el control de la entidad.

Relación entre objetivos y componentes:

La relación entre los diferentes conceptos hasta aquí enunciados puede graficarse como un cubo, tal como se muestra en la figura 1, en donde las cuatro categorías de objetivos – estratégicos, operativos, reporte y cumplimiento – están representadas por las columnas verticales, los ocho componentes de la gestión de riesgos corporativos por las filas horizontales y los diferentes niveles organizacionales por la tercera dimensión del cubo.

Esta matriz tridimensional refleja la capacidad de centrarse sobre la totalidad de la administración de riesgos de una entidad o bien por categoría de objetivos, por componente, por unidad de negocio o por cualquier subconjunto de ellos.

Ilustración 1 Matriz Tridimensional de gestión de riesgos

La eficacia de la gestión de riesgos corporativos

Puede afirmarse que la gestión de riesgos corporativos en una entidad es eficaz cuando los ocho componentes están presentes y funcionan de un modo eficaz, o en otras palabras, cuando no existe ninguna debilidad significativa relacionada con los mismos y cuando los riesgos se encuentran dentro de los niveles aceptados por la organización.

Cuando se determine que la gestión de riesgos corporativos es eficaz para cada una de las cuatro categorías de objetivos, lo que se intenta decir es que:

- la dirección tiene la seguridad razonable de que conoce el grado de consecución de los objetivos estratégicos;
- la dirección también conoce el nivel de logro de los objetivos operativos, siempre con un grado de seguridad razonable;
- la información generada por la entidad es fiable;

- se cumple con las leyes y las normas aplicables.

Es importante destacar que siempre se habla de un grado de “seguridad razonable” debido a que la gestión de riesgos corporativos, si bien proporciona grandes ventajas, también posee algunas limitaciones, como el juicio humano, o la posibilidad de fallas por error humano. Estas limitaciones son las que impiden que la dirección tenga un grado de seguridad absoluta.

Principios Claves de COSO ERM

A continuación, se destacan los principios claves inherentes a los ocho componentes de la gestión de riesgos corporativos:

1) ÁMBIENTE INTERNO

a) Filosofía de la gestión de riesgos:

La filosofía de gestión de riesgos de una entidad es el conjunto de creencias y actitudes compartidas que caracterizan cómo se contempla el riesgo en ella, desde el desarrollo e implantación de la estrategia hasta sus actividades cotidianas. Refleja los valores de la entidad, influye en su cultura y estilo operativo y afecta a cómo se aplican los componentes de dicha gestión, incluyendo la identificación de riesgos, los tipos de riesgo aceptados y cómo son gestionados.

b) Riesgo Aceptado

El riesgo aceptado es el volumen de riesgo, a un nivel amplio, que una entidad está dispuesta a aceptar en su búsqueda de valor. Refleja la filosofía de gestión de riesgo de la entidad e impacta a su vez en su cultura y estilo operativo. El riesgo aceptado debe tenerse en cuenta al fijar la estrategia, pues el rendimiento deseado de la estrategia debe estar alineado con el riesgo aceptado de la entidad. Diferentes estrategias expondrán a la entidad a niveles diferentes de riesgo y la gestión de riesgos corporativos, aplicada en esta fase de fijación de estrategias, ayuda a la dirección a seleccionar una estrategia coherente con el riesgo aceptado. Las

entidades pueden considerar el riesgo aceptado de un modo cualitativo, usando categorías como alto, moderado o bajo, o bien optar por un enfoque cuantitativo, que refleje los objetivos de crecimiento y rendimiento y los equilibre con los riesgos.

c) El Consejo de Administración

El consejo de administración de una entidad es una parte crítica del ámbito interno e influye de modo significativo en sus elementos. Su independencia frente a la dirección, la experiencia y reputación de sus miembros, su grado de implicación y supervisión de las actividades y la adecuación de sus acciones juegan un papel muy importante. Otras características son el alcance con que se plantean y persiguen, junto con la dirección, cuestiones difíciles relativas a estrategias, planes y rendimientos y su interacción o la del comité de auditoría con los auditores internos y externos.

Un consejo de administración u organismo similar activo e implicado debería poseer una adecuada experiencia directiva, técnica y de otro tipo, junto con la necesaria mentalidad para llevar a cabo sus responsabilidades de supervisión. Esto es crítico para un entorno eficaz de gestión de riesgos corporativos.

d) Integridad y Valores éticos

La estrategia y objetivos de una entidad y la manera en que se ponen en práctica se basan en las preferencias, juicios de valor y estilos de gestión. La integridad de la dirección y su compromiso con los valores éticos influyen en dichas preferencias y juicios, que se traducen en normas de conducta. Dado que la reputación de una entidad es tan valiosa, las normas de conducta deben ir más allá del mero cumplimiento de la ley. Los directivos de empresas bien gestionadas aceptan cada vez más la idea de que la ética es rentable y que una conducta íntegra es un buen negocio.

La integridad de la dirección es un requisito previo de la conducta ética en todos los aspectos de la actividad de una entidad. La eficacia de la gestión de riesgos

corporativos no debe sobreponerse a la integridad y los valores éticos de las personas que crean, administran y controlan sus actividades. La integridad y valores éticos son ele-mentos esenciales del ámbito interno de una entidad y afectan al diseño, administración y seguimiento de los otros componentes de la gestión de riesgos corporativos.

e) Compromiso con la Competencia

La competencia refleja los conocimientos y habilidades necesarios para realizar el cometido asignado. La dirección decide el nivel de realización de los cometidos, sopesando la estrategia y objetivos de la entidad respecto a sus planes de implantación y realización. Existe a menudo un conflicto entre competencia y costo -no es necesario, por ejemplo, contratar a un ingeniero eléctrico para cambiar una bombilla.

La dirección establece los niveles de competencia para trabajos concretos y los transforma en conocimientos y habilidades requeridos. A su vez, éstos pueden depender de la inteligencia, formación y experiencia del individuo. Los factores a tener en cuenta en el desarrollo de niveles de conocimiento y habilidad incluyen la naturaleza y grado del juicio a aplicar en un trabajo concreto. A menudo, existe un conflicto entre el grado de supervisión y el nivel de competencia requerido del individuo.

f) Estructura Organizativa

La estructura organizativa de una entidad proporciona el marco para planificar, ejecutar, controlar y supervisar sus actividades. Una estructura organizativa relevante incluye la definición de áreas claves de autoridad y responsabilidad y el establecimiento de líneas adecuadas de información.

Una entidad desarrolla una estructura organizativa ajustada a sus necesidades. Algunas son centralizadas y otras descentralizadas. Unas presentan relaciones directas de dependencia, mientras otras tienen una organización del tipo matricial.

Ciertas entidades están organizadas por sector de actividad o línea de producto, por ubicación geográfica, por un modo concreto de distribución o por una determinada red comercial. Otras entidades, incluyendo muchos organismos gubernamentales, estatales o locales, y entidades sin ánimo de lucro, están organizadas por funciones.

La adecuación de la estructura organizativa de una entidad depende en parte de su dimensión y de la naturaleza de sus actividades. Una organización muy estructurada con líneas formales de dependencia y responsabilidad puede resultar adecuada para una entidad grande con muchas divisiones operativas, incluyendo las operaciones en el extranjero. Sin embargo, en una empresa reducida, esta estructura podría impedir el flujo necesario de información. Sea cual sea dicha estructura, una entidad debería organizarse para permitir una gestión eficaz de riesgos corporativos, desarrollar sus actividades y alcanzar sus objetivos.

g) Asignación de Autoridad y Responsabilidad

La asignación de autoridad y responsabilidad implica el punto hasta el que los individuos y equipos están autorizados y animados a utilizar su iniciativa para tratar los temas y resolver problemas, así como los límites de dicha autoridad. Incluye el establecimiento de relaciones de información y protocolos de autorización, además de políticas que describan las prácticas empresariales adecuadas, los conocimientos y experiencia del personal clave y los recursos proporcionados para que lleven a cabo sus cometidos.

h) Normas para Recursos Humanos

Las prácticas de recursos humanos relacionadas con la contratación, orientación, formación, evaluación, tutoría, promoción, compensación y adopción de acciones remediadoras transmiten mensajes a los empleados en relación con los niveles esperados de integridad, conducta ética y competencia. Por ejemplo, las normas de contratación de las personas más cualificadas, poniendo el énfasis en su historial académico, experiencia laboral previa, logros anteriores y pruebas de su integridad y conducta ética, muestran el compromiso de una entidad con las personas

competentes y de confianza. Lo mismo se aplica cuando las prácticas de selección e incorporación de personal incluyen entrevistas formales y unos cursos de formación sobre la historia, cultura y estilo operativo de la entidad.

2) ESTABLECIMIENTO DE OBJETIVOS

a) Objetivos Estratégicos

La misión de una entidad establece en amplios términos lo que se aspira a alcanzar. Sea cual sea el término empleado, como "misión", "visión" o "finalidad", es importante que la dirección -con la supervisión del consejo- establezca expresamente la razón de ser de la entidad en términos generales. A partir de esto, la dirección fija los objetivos estratégicos, formula la estrategia y establece los correspondientes objetivos operativos, de información y de cumplimiento para la organización. Aunque la misión de una entidad y sus objetivos estratégicos sean generalmente estables, su estrategia y muchos objetivos relacionados con ella son más dinámicos y se adecuan mejor a las cambiantes condiciones internas y externas. A medida que éstas cambian, la estrategia y los objetivos conexos deben volver a situarse en línea con los objetivos estratégicos.

Estos objetivos estratégicos son de alto nivel, están alineados con la misión/visión de la entidad y la dan su apoyo. Reflejan la opción que ha elegido la dirección en cuanto a cómo la entidad creará valor para sus grupos de interés.

b) Objetivos Relacionados

Constituye un factor crítico de éxito el establecimiento de objetivos adecuados que apoyen a la estrategia seleccionada, correspondiente a todas las actividades de la entidad, y estén en línea con ella. Al enfocar primero los objetivos estratégicos y la estrategia, una entidad está en posición de desarrollar los objetivos globales, cuya consecución creará y conservará el valor. Los objetivos al nivel de empresa están vinculados y se integran con otros objetivos más específicos, que repercuten en

cascada en la organización hasta llegar a sus bobjetivos establecidos, por ejemplo, en las diversas actividades de ventas, producción, ingeniería e infraestructura.

Al fijar sus objetivos a los niveles de entidad y actividades, la organización puede identificar los factores críticos de éxito, que han de funcionar bien si se quieren alcanzar los objetivos. Estos factores críticos afectan a la entidad, a cada unidad de negocio, función o departamento y a los individuos. Al fijar sus objetivos, la dirección puede identificar los criterios de medida del rendimiento, con atención a los factores críticos de éxito.

Los objetivos deben ser fácilmente entendibles y mensurables. La gestión de riesgos corporativos exige que el personal a todos los niveles tenga un entendimiento necesario de los objetivos de la entidad, en cuanto se relacionan con el ámbito del individuo. Todos los empleados deben tener una comprensión mutua de lo que se ha de lograr y de los medios para medir lo que se consiga.

Categorías de Objetivos Relacionados:

A pesar de la diversidad de objetivos entre entidades, se pueden establecer algunas categorías amplias:

- Objetivos operativos

Se corresponden con la eficacia y eficiencia de las operaciones de la entidad, incluyendo los objetivos de rendimiento y rentabilidad y de salvaguarda de recursos frente a pérdidas. Varían según las opciones de la dirección respecto a estructura y rendimiento. Los objetivos operativos deben reflejar los entornos, empresarial, sectorial y económico en los que actúa la entidad. Necesitan, por ejemplo, ser relevantes respecto a las presiones competitivas hacia la calidad, una menor duración del ciclo de puesta a disposición del producto en el mercado o hacia los cambios tecnológicos. La dirección debe asegurar que los objetivos reflejan la realidad y las exigencias del mercado y que están expresados en términos que permitan conocer las principales medidas del rendimiento. Un conjunto claro de objetivos operativos, vinculados a subobjetivos, es esencial para el éxito. Los objetivos operativos proporcionan un punto de focalización para orientar la

asignación de recursos. Si los objetivos no son claros o no están bien concebidos, dicha asignación puede resultar desenfocada.

- Objetivos de información

Relativos a la fiabilidad de la información. Incluyen información interna y externa e implican la financiera y no financiera.

Una información fiable proporciona a la dirección datos seguros y completos, adecuados para la finalidad pretendida, y la presta apoyo en su toma de decisiones y en el seguimiento de las actividades y rendimientos de la entidad. Ejemplos de dicha información son los resultados de las campañas de marketing, los informes de ventas diarias, la calidad de producción y los resultados de encuestas sobre la satisfacción de clientes y empleados. La información también está relacionada con los documentos preparados para su difusión externa, como es el caso de los estados financieros y sus notas de detalle, los comentarios y análisis de la dirección y los informes presentados a entidades reguladoras.

- Objetivos de cumplimiento

Se refieren al cumplimiento de leyes y normas relevantes. Dependen de factores externos y tienden a ser similares entre entidades, en algunos casos, y sectorialmente, en otros.

Las entidades deben llevar a cabo sus actividades y a menudo acciones concretas de acuerdo con las leyes y normas relevantes. Estos requisitos pueden referirse al mercado, precios e impuestos, medioambiente, bienestar de los empleados y comercio exterior. Las leyes y normas aplicables establecen pautas mínimas de conducta, que la entidad integra en sus objetivos de cumplimiento. Por ejemplo, las normas sobre higiene y salud laboral hacen que una empresa defina uno de sus objetivos como "Empaquetar y etiquetar todos los productos químicos según normativa". En este caso, las políticas y procedimientos se dirigen a los programas de comunicación, inspecciones in situ y formación. El historial del cumplimiento de

una entidad puede afectar de modo significativo -positiva o negativamente- a su reputación en la comunidad y el mercado.

c) Objetivos Seleccionados

Como parte de la gestión de riesgos corporativos, la dirección no sólo elige los objetivos y considera cómo apoyan la misión de la entidad, sino que también asegura que estén alineados con el riesgo aceptado por la entidad. Un error en dicha alineación podría dar como resultado una aceptación insuficiente del riesgo existente en el logro de objetivos o, por el contrario, una aceptación de un riesgo excesivo. Una gestión eficaz de riesgos corporativos no dicta los objetivos que la dirección debe elegir, pero le proporciona un proceso para alinear los objetivos estratégicos con la misión de la entidad y asegurar que éstos, junto con sus correspondientes objetivos conexos, concuerdan con el riesgo aceptado por la entidad.

d) Riesgo Aceptado

El riesgo aceptado, establecido por la dirección bajo control del consejo de administración, es una orientación para establecer los objetivos. Las empresas pueden expresar su riesgo aceptado como un equilibrio adecuado entre crecimiento, riesgo y rendimiento o como unas medidas de adición de valor para el accionista, ajustadas a su propio nivel de riesgo. Algunas entidades, como son las organizaciones sin ánimo de lucro, expresan su riesgo aceptado como el nivel de riesgo que aceptarían a cambio de crear valor para sus grupos de interés.

Existe una relación entre el riesgo aceptado de una entidad y su estrategia. Normalmente se pueden diseñar muchas estrategias diferentes para conseguir los objetivos deseados de crecimiento y rendimiento, cada uno con riesgos diferentes. La gestión de riesgos corporativos, aplicada al establecimiento de la estrategia, ayuda a la dirección a seleccionar una estrategia consecuente con su riesgo acepta-do. Si el riesgo asociado a la estrategia no está alineado con el riesgo aceptado por la entidad, se revisa la estrategia, lo que puede ocurrir cuando la

dirección formule inicialmente una estrategia que exceda del riesgo aceptado por la entidad o cuando dicha estrategia no contemple riesgo suficiente para permitir que la entidad alcance sus objetivos estratégicos y su misión.

e) Tolerancias al Riesgo

Las tolerancias al riesgo son los niveles aceptables de desviación relativa a la consecución de objetivos. Pueden medirse, y a menudo resulta mejor, con las mismas unidades que los objetivos correspondientes.

Las medidas de rendimiento se usan para ayudar a asegurar que los resultados reales se ciñen a las tolerancias al riesgo establecidas. Por ejemplo, una empresa fija un objetivo del 98% de puntualidad para sus entregas, con una desviación aceptable entre el 97% y el 100%; fija como objetivo de formación una nota de aprobado del 90%, con un rendimiento aceptable mínimo del 75%; y espera que el personal responda a todas las reclamaciones de los clientes en un plazo de 24 horas, aunque acepta que hasta un 25% de ellas se atiendan entre 24 y 36 horas.

Al fijar las tolerancias al riesgo, la dirección tiene en cuenta la importancia relativa de los objetivos correspondientes y alinea aquellas con el riesgo aceptado. Operar dentro de las tolerancias al riesgo proporciona a la dirección una mayor confianza en que la entidad permanece dentro de su riesgo aceptado, que, a su vez, proporciona una seguridad más elevada de que la entidad alcanzará sus objetivos.

3) IDENTIFICACION DE EVENTOS

a) Eventos

Un evento es un incidente o acontecimiento, derivado de fuentes internas o externas, que afecta a la implantación de la estrategia o la consecución de objetivos. Los eventos pueden tener un impacto positivo, negativo o de ambos tipos a la vez.

Al identificar eventos, la dirección reconoce que existen incertidumbres, por lo que no sabe si alguno en particular tendrá lugar y, de tenerlo, cuándo será, ni su impacto exacto. La dirección considera inicialmente una gama de eventos potenciales, derivados de fuentes internas o externas, sin tener que centrarse necesariamente sobre si su impac-to es positivo o negativo. De esta forma, la dirección identifica no sólo los eventos poten-ciales negativos, sino también aquellos que representan oportunidades a aprovechar.

Los eventos abarcan desde lo evidente a lo desconocido y sus efectos, desde lo inconsecuente a lo muy significativo. Para evitar una consideración excesiva de eventos relevantes, procede realizar de forma separada su identificación y la evaluación de su probabilidad de ocurrencia e impacto, aspecto este último que corresponde a la Evaluación de Riesgos. Sin embargo, existen limitaciones prácticas y a menudo es difícil saber distinguirlas. Pero incluso los eventos con una probabilidad de ocurrencia relativamente baja no deberían ignorarse si es grande su impacto sobre la consecución de un objetivo importante.

b) Factores Influyentes

Son muchos los factores externos e internos que provocan eventos que afectan a la implantación de la estrategia y la consecución de objetivos. Como parte de la gestión de riesgos corporativos, la dirección reconoce la importancia de entender dichos factores y el tipo de evento que puede derivarse de ellos. Los factores externos, junto con ejemplos de eventos relacionados y sus implicaciones, incluyen los siguientes:

- Económicos

Eventos tales como los cambios de precios, la disponibilidad de capital o unas menores barreras a la entrada de la competencia, que generan mayores o menores costes de capital y competidores nuevos.

- Medioambientales

Incluyen las inundaciones, incendios y terremotos, que provocan daños a las insta-laciones o edificios, un acceso restringido a las materias primas o la pérdida de capital humano.

- Políticos

Incluyen la elección de gobiernos con nuevos programas políticos, leyes y normas, que provocan, por ejemplo, nuevas restricciones o aperturas en el acceso a merca-dos extranjeros o impuestos mayores o menores.

- Sociales

Relacionados con los cambios demográficos, costumbres sociales, estructuras familiares, prioridades trabajo/ocio y actividades terroristas, que tienen como resul-tado cambios en la demanda de productos y servicios, nuevos puntos de venta, aspectos relacionados con recursos humanos y paros en la producción.

- Tecnológicos

Relativos a los nuevos medios de comercio electrónico, que generan una mayor dis-ponibilidad de datos, reducciones de costes de infraestructura y un mayor aumen-to en la demanda de servicios basados en la tecnología.

c) Técnicas de Identificación de Eventos

La metodología de identificación de eventos de una entidad puede comprender una combinación de técnicas, junto con herramientas de apoyo. Por ejemplo, la dirección puede usar talleres interactivos de trabajo como parte de dicha metodología, con un monitor que emplee alguna herramienta tecnológica para ayudar a los participantes.

Las técnicas varían ampliamente en su nivel de sofisticación. Aunque muchas de las más sofisticadas corresponden a sectores específicos, la mayoría se derivan de un enfoque común. Por ejemplo, tanto los servicios financieros como los del sector de la seguridad e higiene utilizan técnicas de rastreo e identificación de eventos que generen pérdidas. Estas técnicas empiezan con un enfoque sobre los eventos

históricos comunes -los enfoques más básicos estudian acontecimientos derivados de percepciones del personal, mientras que las técnicas más avanzadas se basan en fuentes reales de eventos observables- y luego, se introducen los datos en modelos de previsión más sofisticados. Las empresas más avanzadas en la gestión de riesgos corporativos normalmente aplican una combinación de técnicas que contemplan a la vez eventos pasados y futuros potenciales.

Las técnicas también varían según dónde se estén aplicando dentro de una entidad. Algunas se centran en el análisis detallado de datos y crean una perspectiva ascendente de eventos, mientras que otras lo enfocan, al contrario.

d) Interdependencias

Frecuentemente, los eventos no ocurren de forma aislada. Un acontecimiento puede hacer que se desencadene otro, por lo que pueden ocurrir de forma concurrente. En la identificación de eventos, la dirección debería entender cómo éstos se relacionan entre sí. Evaluando estas relaciones, se puede determinar dónde mejor deberían aplicarse los esfuerzos en la gestión de riesgos. Por ejemplo, un cambio en el tipo de interés de un banco central afecta a los tipos de cambio de moneda extranjera, relevantes para las ganancias y pérdidas en las transacciones de una entidad. Una decisión para reducir la inversión en capital pospone una actualización de los sistemas de gestión de distribución, provocando más tiempo de inactividad y un aumento de costes operativos. Una decisión para ampliar la formación en marketing puede mejorar las capacidades de venta y la calidad de servicio, lo que dará lugar a un aumento de la frecuencia y volumen de los pedidos recurrentes de clientes. Una decisión para entrar en una nueva línea de negocio, con incentivos importantes vinculados al rendimiento, puede incrementar los riesgos de error en la aplicación de principios contables y de que se genere una información fraudulenta.

Puede ser útil agrupar los eventos potenciales en categorías. Al agregarlos horizontalmente en toda la entidad y verticalmente dentro de las unidades operativas, la dirección desarrolla un entendimiento de las relaciones entre eventos,

obteniendo una mejor información como base para la evaluación los riesgos. Mediante esta agregación de eventos similares, la dirección puede determinar mejor las oportunidades y riesgos.

La clasificación de eventos por categorías también permite a la dirección considerar la totalidad de los esfuerzos aplicados a su identificación. Por ejemplo, una empresa puede haber clasificado los eventos relacionados con los cobros de deudores en una única categoría denominada impago de deudores. Si la dirección estudia los eventos relacionados con esta categoría, puede evaluar si se han identificado todos los posibles eventos significativos relacionados con dicho impago.

Algunas empresas desarrollan categorías de eventos basadas en la clasificación de sus objetivos por categorías, usando una jerarquía que empieza con los objetivos de alto nivel y luego, en cascada hasta los objetivos relevantes para las unidades organizativas, funciones o procesos de negocio.

e) Distinción entre Riesgos y Oportunidades

Los eventos, si ocurren, tienen un impacto negativo, positivo o de ambos tipos a la vez. Los de signo negativo representan riesgos, que requieren la evaluación y res-puesta de la dirección. Por tanto, un riesgo es la posibilidad de que ocurra un evento que afecte de modo adverso a la consecución de objetivos.

Los eventos de signo positivo representan oportunidades, que compensan los impactos negativos de los riesgos. Una oportunidad es la posibilidad de que ocurra un evento que afecte positivamente a la consecución de objetivos y la creación de valor. Los eventos que implican oportunidades son canalizados hacia los procesos de la dirección en que se establecen la estrategia y objetivos de la entidad, de forma que puedan formularse acciones para aprovechar las oportunidades. Los eventos que compensen el impacto negativo de los riesgos deben tenerse en cuenta por parte de la dirección al evaluar los riesgos y darles respuesta.

4) EVALUACION DE RIESGOS

a) Riesgo Inherente y Riesgo Residual

La dirección considera a la vez ambos conceptos de riesgo. El riesgo inherente es aquél al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto. El riesgo residual es el que permanece después de que la dirección desarrolle sus respuestas a los riesgos.

b) Estimación de Probabilidad e Impacto

La incertidumbre de los eventos potenciales se evalúa desde dos perspectivas - probabilidad e impacto. La primera representa la posibilidad de que ocurra un evento determinado, mientras que la segunda refleja su efecto. Ambos términos se aplican de forma común, aunque algunas entidades usen otros, tales como frecuencia, severidad, seriedad o consecuencia. A veces, las palabras adquieren connotaciones más específicas y el concepto "probabilidad" puede indicar tanto la posibilidad de que ocurra cierto evento en términos cualitativos como alta, media y baja o derivados de otras escalas de medida o bien en términos cuantitativos como porcentaje, frecuencia y ocurrencia o derivados de otras métricas numéricas.

El horizonte temporal usado para evaluar los riesgos debería ser consecuente con el horizonte temporal de la estrategia y objetivos correspondientes. Como estos dos conceptos apuntan en muchas entidades a horizontes de tiempo entre el corto y medio plazo, la dirección se centra naturalmente en los riesgos asociados con estos plazos de tiempo. Sin embargo, algunos aspectos de la orientación y objetivos estra-tégicos se extienden hasta el largo plazo. Como resultado, la dirección necesita ser consciente de los marcos temporales más dilatados y no obviar los riesgos que pueda deparar un futuro distante.

La dirección usa a menudo medidas del funcionamiento para determinar el grado de consecución de objetivos y normalmente aplica la misma unidad de medida, u otra congruente con ella, que la utilizada para considerar el impacto potencial de un riesgo sobre la consecución de un objetivo concreto. Una empresa, por ejemplo,

que tiene establecido el objetivo de mantener un nivel determinado de servicio al cliente, habrá diseñado un coeficiente u otro tipo de medida para dicho objetivo -tales como el índice de satisfacción del cliente, el número de reclamaciones o el volumen de negocio recurrente. Cuando se evalúa el impacto de un riesgo que podría afectar al servicio al cliente -tal como la posibilidad de que la web de la empresa pueda estar no disponible durante un periodo de tiempo- se determina mejor el impacto usando las mismas medidas.

c) Técnicas de Evaluación

La metodología de evaluación de riesgos de una entidad consiste en una combinación de técnicas cualitativas y cuantitativas. La dirección aplica a menudo técnicas cualitativas cuando los riesgos no se prestan a la cuantificación o cuando no están disponibles datos suficientes y creíbles para una evaluación cuantitativa o la obtención y análisis de ellos no resulte eficaz por su coste. Las técnicas cuantitativas típicamente aportan más precisión y se usan en actividades más complejas y sofisticadas, para complementar las técnicas cualitativas.

Las técnicas cuantitativas de evaluación normalmente exigen un mayor grado de esfuerzo y rigor y a veces emplean modelos matemáticos. Estas técnicas dependen mucho de la calidad de los datos e hipótesis de soporte y resultan más relevantes para riesgos con un historial y una frecuencia de variabilidad conocidos, pues permiten una proyección fiable.

Para conseguir un consenso sobre probabilidad e impacto usando técnicas cualitativas de evaluación, las entidades pueden aplicar el mismo enfoque que usan en la identificación de eventos, tales como las entrevistas y grupos de trabajo. Un proceso de autoevaluación del riesgo capta los puntos de vista de los participantes sobre la probabilidad y el impacto potencial de eventos futuros, usando escalas descriptivas o numéricas.

La dirección puede generar una medida del impacto cuantitativo de un evento en toda la entidad cuando todas las evaluaciones individuales de riesgo referentes al mismo se expresen en términos cuantitativos. Por ejemplo, el impacto de un cambio

en el precio de la energía sobre el margen bruto se calcula en todas las unidades de negocio y se determina así el impacto global para toda la entidad. Cuando exista una mezcla de medidas cualitativas y cuantitativas, la dirección desarrolla una evaluación cualitativa a través de ambos tipos de medición, con el resultado de una evaluación compuesta expresada en términos cualitativos. La generación de estas evaluaciones compuestas se facilita estableciendo términos comunes de probabilidad e impacto para toda la entidad y categorías comunes de riesgo para las medidas cualitativas.

d) Relaciones entre Eventos

Cuando los eventos potenciales no están relacionados entre sí, la dirección los evalúa individualmente. Por ejemplo, una empresa con unidades de negocio expuestas a diferentes fluctuaciones de precios -tales como el de la pasta de papel o el de monedas extranjeras- evaluaría los riesgos independientemente de los movimientos del mercado. Pero cuando exista correlación entre los eventos o éstos se combinen e interaccionen para crear probabilidades o impactos significativamente diferentes, la dirección los evaluará en conjunto. Aunque el impacto de un solo evento pueda ser ligero, el impacto de una secuencia o combinación de eventos puede ser más significativo.

Por ejemplo, una válvula defectuosa de un depósito de propano en un almacén de distribución origina un escape de gas, mientras se mantienen cerradas las puertas de la instalación para retener el calor de las oficinas adyacentes. Cuando el conductor de un camión que se acerca al almacén activa un dispositivo a control remoto para abrir las puertas, la presencia conjunta del gas y la chispa del motor de la puerta cau-san una explosión. Eventos distintos interaccionan y dan como resultado un riesgo significativo.

La observación de interrelaciones entre probabilidad e impacto de los riesgos constituye una importante responsabilidad de la dirección. Una gestión eficaz de riesgos corporativos requiere que su evaluación se realice atendiendo tanto al riesgo inherente como a la repuesta a él, como se expone en el capítulo siguiente.

5) RESPUESTA A LOS RIESGOS

a) Evaluación de Posibles Respuestas

Los riesgos inherentes se analizan y las respuestas a ellos se evalúan con el propósito de conseguir un nivel de riesgo residual en línea con las tolerancias al riesgo de la entidad. A menudo, cualquiera de las diversas respuestas posibles situará dicho riesgo residual dentro del marco de esas tolerancias y, a veces, una combinación de ellas proporcionará el resultado óptimo. Por otro lado, a veces una respuesta afectará a múltiples riesgos, en cuyo caso la dirección puede decidir que no se precisan acciones adicionales para tratar un riesgo determinado.

Al evaluar las opciones de respuesta, la dirección considera el efecto sobre la probabilidad del riesgo y su impacto, reconociendo que una respuesta puede afectarlas de modo diferente. Por ejemplo, una empresa con un centro informático ubicado en una región con fuerte actividad tormentosa establece un plan de continuidad de negocio que, aunque no tiene efecto alguno sobre la probabilidad de que se produzca una tormenta, mitiga el impacto de los daños en el edificio o de la dificultad para que el personal acceda a su trabajo. Por otro lado, la opción de trasladar el centro informático a otra región no reducirá el impacto de posibles tormentas que puedan producirse, pero sí reduce la probabilidad de que tengan lugar en este nuevo centro.

Al analizar las respuestas, la dirección puede tener en cuenta los eventos y tendencias pasadas y los posibles escenarios futuros. Al evaluar las respuestas alternativas, la dirección típicamente determina su efecto potencial usando las mismas unidades de medición, u otras congruentes, que las usadas para el objetivo correspondiente.

b) Respuestas Seleccionadas

Una vez evaluados los efectos de las respuestas alternativas a los riesgos, la dirección decide cómo pretende gestionar los riesgos, seleccionando una respuesta

o una combinación de ellas diseñada para situar la probabilidad e impacto del riesgo dentro de las tolerancias establecidas. Sin embargo, cuando una respuesta a los riesgos pudiera desembocar en que el riesgo residual superará la tolerancia establecida, la dirección tiene que volver sobre sus pasos y revisar su respuesta o, bajo ciertas circunstancias, reconsiderar la tolerancia al riesgo establecida. Por tanto, el equilibrio entre riesgo y tolerancia al riesgo puede implicar un proceso iterativo.

Evaluar las respuestas alternativas a los riesgos inherentes requiere tener en cuenta los riesgos adicionales que pueden derivarse de cada respuesta, lo que puede iniciar un proceso iterativo en que la dirección, antes de tomar su decisión, considere dichos riesgos adicionales, incluyendo aquellos que pudieran no ser evidentes de modo inmediato.

Una vez que la dirección selecciona una respuesta, es posible que necesite desarrollar un plan de implantación para ejecutarla. Una parte crítica de dicho plan es el establecimiento de acciones de control para asegurar que se lleva a cabo la respuesta a los riesgos.

La dirección reconoce que siempre existirá algún nivel de riesgo residual, no sólo por las limitaciones de los recursos, sino también por la incertidumbre del futuro y demás limitaciones inherentes a todas las actividades.

c) Perspectiva de Carteras de Riesgos

La gestión de riesgos corporativos requiere que el riesgo se considere desde una perspectiva: de toda la entidad o desde otra perspectiva de carteras de riesgos. Normalmente, la dirección elige un enfoque en que primero se contemplan los riesgos de cada unidad de negocio, departamento o función y luego su director responsable desarrolla una evaluación compuesta de ellos, que refleja su perfil de riesgo residual respecto a sus objetivos y tolerancias al riesgo.

Con una perspectiva del riesgo para cada unidad individual, la alta dirección de una empresa está bien situada para tener una perspectiva de carteras y determinar si el perfil de riesgo residual de la entidad está a la par del riesgo aceptado global

respecto a sus objetivos. Los riesgos de las diferentes unidades pueden estar dentro de sus respectivas tolerancias individuales, pero en conjunto pueden superar al riesgo aceptado globalmente por la entidad, en cuyo caso hacen falta respuestas adicionales o diferentes para emplazar el riesgo dentro del nivel de riesgo aceptado. A la inversa, los riesgos pueden compensarse naturalmente a través de la entidad cuando, por ejemplo, algunas unidades individuales tienen un mayor riesgo y otras son relativamente adversas a él, de tal modo que el riesgo global está dentro del riesgo aceptado por la entidad, evitando la necesidad de una respuesta diferente a los ries-gos.

Una perspectiva de carteras de riesgos puede ser representada de muchas maneras. Puede alcanzarse centrándose en los principales riesgos o categorías de riesgo de las unidades de negocio o de la empresa en su totalidad, usando métricas como el capital ajustado al riesgo o el capital en riesgo. Dichas medidas compuestas son particularmente útiles para medir el riesgo frente a objetivos establecidos en términos de resultados, crecimiento u otras medidas de funcionamiento, a veces relacionadas con el capital asignado o disponible. Estas medidas de la perspectiva de carteras pueden facilitar información útil para la reasignación del capital entre unidades y la modifica-ción de la orientación estratégica.

6) ACTIVIDADES DE CONTROL

a) Integración con la respuesta al riesgo

Después de haber seleccionado las respuestas al riesgo, la dirección identifica las actividades de control necesarias para ayudar a asegurar que las respuestas a los riesgos se lleven a cabo adecuada y oportunamente.

El siguiente ejemplo sirve para ilustrar el vínculo entre objetivos, respuestas a los ries-gos y actividades de control. Una empresa fija un objetivo de alcanzar o superar las ventas presupuestadas, identificando como riesgo la falta de conocimientos suficien-tes sobre factores externos tales como las necesidades actuales y potenciales de los clientes. Para reducir la probabilidad de ocurrencia y el impacto

del riesgo, la direc-ción establece historiales de compra de los clientes actuales y realiza unas nuevas iniciativas de investigación de mercado. Estas respuestas al riesgo sirven como pun-tos básicos para establecer las actividades de control, incluyendo el seguimiento del desarrollo de dichos historiales en comparación con los calendarios establecidos y la adopción de medidas para asegurar la exactitud de los datos informados. En este sentido, las actividades de control están integradas directamente en el proceso de gestión.

Al seleccionar las actividades de control, la dirección considera cómo se relacionan entre sí. En algunos ejemplos, una sola de ellas afecta a riesgos múltiples. En otros, son necesarias muchas actividades de control para una respuesta al riesgo. Incluso, en otros, la dirección puede descubrir que las actividades de control existentes son suficientes para asegurar que las nuevas respuestas a los riesgos se ejecutan eficaz-mente.

Aunque las actividades de control se establecen generalmente para asegurar que las respuestas a los riesgos se lleven a cabo de modo adecuado, con respecto a ciertos objetivos, también constituyen por sí mismas una respuesta al riesgo. Por ejemplo, para un objetivo que establece que unas transacciones específicas deben estar debi-damente autorizadas, la respuesta será probablemente unas actividades de control tales como la segregación de funciones o la aprobación por personal supervisor.

b) Tipos de actividades de control

Se han propuesto muchas descripciones diferentes de los tipos de actividades de control, incluyendo los controles de prevención, detección, manuales, informáticos y de dirección. Las actividades de control también pueden tipificarse según objetivos concretos de control, tales como los de asegurar la integridad y exactitud del procesamiento de datos.

Son solo unos cuantos de entre muchos procedimientos normalmente aplicados por el personal en distintos niveles de la organización que sirven para potenciar la adhesión a los planes de acción establecidos y mantener el rumbo de las entidades

hacia el logro de sus objetivos. Se presentan a continuación para ilustrar la amplitud y variedad de las actividades de control y no para sugerir una determinada clasificación: revisión de alto nivel, gestión directa de funciones o actividades, procesamiento de la información, controles físicos, Indicadores de rendimiento y segregación de funciones, por mencionar algunas.

c) Políticas y procedimientos

Las actividades de control normalmente implican dos componentes: una política que establece lo que debe hacerse y procedimientos para llevarla a cabo. Por ejemplo, una política podría exigir la revisión de las actividades de contratación de clientes por parte de un director de oficina de una entidad de gestión bursátil. El procedimiento lo constituye dicha revisión en sí misma, realizada de manera oportuna y con atención a los factores establecidos en la política, tales como la naturaleza y volumen de los valores contratados y su relación con el patrimonio y edad del cliente.

Muchas veces, las políticas se comunican verbalmente. Las políticas no escritas pueden ser eficaces cuando la política lleve años en vigor y constituya una práctica bien comprendida y en organizaciones reducidas donde los canales de comunicación impliquen pocos niveles directivos y una interacción estrecha, junto con la supervi-sión del personal. Pero independientemente de si está escrita o no, una política debería implantarse de forma meditada, consciente y consecuente. Un procedimiento no será útil si se lleva a cabo mecánicamente y sin un enfoque claro y continuo sobre las condiciones a las que se orienta la política. Posteriormente, es esencial investigar las condiciones identificadas como resultado del procedimiento y adoptar las acciones correctivas necesarias. Las acciones de seguimiento podrían variar según la dimen-sión y estructura organizativa de una empresa. Pueden abarcar desde procesos for-males de información de una empresa grande -donde las unidades de negocio expli-can por qué no se alcanzan los objetivos y qué acciones se están adoptando para evitar la repetición de ello- hasta el caso de un director-propietario de una empresa pequeña que se desplaza personalmente para

hablar con el responsable de planta sobre lo que ha fallado y qué es necesario hacer.

d) Controles sobre los sistemas de información

Con una dependencia importante de los sistemas de información para operar una empresa y alcanzar los objetivos de información y cumplimiento, hacen falta controles sobre dichos sistemas. Pueden usarse dos amplios grupos de actividades de control de los sistemas de información. El primero lo forman los controles generales, que se aplican a muchos de esos sistemas, si no a todos, y ayudan a asegurar que siguen funcionando continua y adecuadamente. El segundo son los controles de aplicación, que incluyen fases informatizadas dentro del software para controlar el proceso. Ambos tipos de controles, combinados con controles manuales de proceso cuando sea necesario, operan juntos para asegurar la integridad, exactitud y validez de la información.

7) INFORMACION Y COMUNICACIÓN

a) Información

La información se necesita a todos los niveles de la organización para identificar, evaluar y responder a los riesgos y por otra parte dirigir la entidad y conseguir sus objetivos. Se usa mucha información, relevante para una o más categorías de objetivos.

La información operativa de fuentes internas y externas, tanto financiera como no financiera, es relevante para múltiples objetivos de negocio. La información financiera, por ejemplo, se usa para elaborar los estados financieros con fines de información y también para tomar decisiones operativas, tales como la supervisión del funciona-miento y la asignación de recursos. Una información financiera fiable es básica para planificar, presupuestar, fijar precios, evaluar el rendimiento del vendedor, evaluar joint ventures y alianzas y llevar a cabo otras actividades de gestión.

De forma similar, la información operativa es esencial para elaborar los informes financieros y de otro tipo. Esto incluye aquella más rutinaria -compras, ventas y demás transacciones- junto con la correspondiente a nuevas versiones de producto o condiciones económicas de los competidores, que pueden afectar a las existencias y las valoraciones de cuentas a cobrar. La información necesaria a efectos de cumplimiento, tal como la relativa a las emisiones de partículas a la atmósfera o datos del personal, también puede aplicarse a objetivos de información financiera.

La información procede de muchas fuentes -internas y externas, de forma cuantitativa y cualitativa- y facilita respuesta a las condiciones cambiantes. Un reto para la dirección es cómo procesar y depurar grandes volúmenes de datos para convertirlos en información manejable y se enfrenta a él estableciendo una infraestructura de sistemas de información para buscar, captar, procesar, analizar y comunicar la información relevante. Estos sistemas -habitualmente informatizados, pero conteniendo también entradas manuales o interfaces- se ven a menudo dentro del contexto del procesamiento de datos generados internamente. Pero los sistemas de información tienen una aplicación más amplia. También abordan características o circunstancias de eventos externos, por ejemplo, datos económicos específicos de un mercado o sector que muestran cambios en la demanda de los productos o servicios de una empresa, datos sobre productos y servicios para los procesos de producción, información de mercado sobre la evolución de preferencias o demandas del consumidor, información sobre las actividades de desarrollo de productos de los competidores e iniciativas legislativas o normativas.

Los sistemas de información pueden ser formales o informales. Las conversaciones con clientes, proveedores, reguladores y personal de la entidad a menudo proporcionan información crítica necesaria para identificar riesgos y oportunidades. De forma similar, la asistencia a seminarios profesionales o del sector y la participación en asociaciones mercantiles o de otro tipo pueden ser una fuente de información valiosa.

Es particularmente importante mantener la información en forma coherente con las necesidades cuando una entidad se enfrenta a cambios fundamentales en el sector.

Comunicación

La comunicación es inherente a los sistemas de información. Como ya se ha comentado antes, estos sistemas deben proporcionar información al personal adecuado, para que pueda llevar a cabo sus responsabilidades operativas, de información y de cumplimiento. Pero la comunicación también debe tener lugar en un sentido más amplio, abordando las expectativas, las responsabilidades de los individuos y grupos y otros temas importantes.

La dirección proporciona comunicaciones específicas y orientadas que se dirigen a las expectativas de comportamiento y las responsabilidades del personal. Esto incluye una exposición clara de la filosofía y enfoque de la gestión de riesgos corporativos de la entidad y una delegación clara de autoridad. La comunicación sobre procesos y procedimientos debería alinearse con la cultura deseada y reforzarla.

Existe la necesidad de una comunicación adecuada no sólo dentro de la entidad, sino también con el mundo exterior. Con canales de comunicación externos abiertos, los clientes y proveedores pueden proporcionar inputs muy significativos sobre el diseño o la calidad de los productos o servicios, permitiendo a la empresa tratar las demandas o preferencias del cliente en evolución.

La comunicación puede tomar formas tales como un manual de políticas, escritos internos, correos electrónicos, novedades en los tablones de anuncios, mensajes en la web y de vídeo. Cuando los mensajes se transmiten verbalmente -en grandes gru-pos, reuniones reducidas o entrevistas personales- el tono de voz y el lenguaje cor-poral ponen énfasis a lo que se está diciendo.

8) SUPERVISION

a) Actividades de Supervisión Permanente

Muchas actividades sirven para seguir la eficacia de la gestión de riesgos corporati-vos durante el transcurso normal del negocio. Se derivan de las actividades norma-les de gestión, que podrían implicar análisis de varianza, comparaciones de informa-ción procedente de fuentes diferentes y el análisis y tratamiento de acontecimientos inesperados.

Son los directivos de línea o función de apoyo quienes llevan a cabo las actividades de supervisión y dan meditada consideración a las implicaciones de la información que reciben. Al centrarse en relaciones, incoherencias u otras implicaciones relevan-tes, plantean cuestiones y las siguen con otro personal, según sea necesario, para determinar si es precisa una acción correctiva o de otro tipo. Las actividades perma-nentes de supervisión se distinguen de las actividades de funcionamiento según lo requiera la política de procesos de negocio. Por ejemplo, se definen mejor como acti-vidades de control las aprobaciones de transacciones, las conciliaciones de saldos y la verificación de exactitud de los cambios en los ficheros maestros, realizadas según las pautas marcadas por los sistemas informáticos o los procesos de contabilidad.

b) Evaluaciones independientes

Aunque los procedimientos de seguimiento permanente normalmente proporcionan una retroalimentación importante sobre la eficacia de otros componentes de la gestión de riesgos corporativos, puede resultar provechoso echar un nuevo vistazo de vez en cuando, centrándose directamente sobre la eficacia de dicha gestión. Esto también proporciona una oportunidad de tener en cuenta la eficacia continuada de los procedimientos de supervisión permanente.

Las evaluaciones de la gestión de riesgos corporativos varían en alcance y frecuen-cia según la significatividad de los riesgos y la importancia de las respuestas a ellos, así como los correspondientes controles disponibles para gestionarlos.

A menudo, las evaluaciones tienen la forma de autoevaluaciones, en las que los res-ponsables de una determinada unidad o función establecen la eficacia de la gestión de riesgos corporativos en sus actividades.

c) Información de deficiencias

Las deficiencias en la gestión de riesgos corporativos de una entidad pueden proceder de muchas fuentes, incluyendo los procedimientos de supervisión permanente de la entidad, las evaluaciones independientes e información de terceros. Una deficiencia es una situación dentro de la gestión de riesgos corporativos que merece atención y que puede representar una debilidad percibida, potencial o real, o una oportunidad para fortalecer la gestión de riesgos corporativos y aumentar la probabilidad de que se logren los objetivos de la entidad.

6.4. Gestión de riesgos según ISO 31000

La norma internacional ISO 31.000 define la gestión del riesgo como *actividades coordinadas para dirigir y controlar una organización en lo relativo al riesgo*.

El diseño e implantación de este modelo de gestión del riesgo, permite a la organización:

- Fomentar la gestión proactiva en lugar de la reactiva.
- Ser consciente de la necesidad de identificar y tratar el riesgo en todos los niveles de la organización.
- Mejorar la identificación de oportunidades y amenazas.
- Cumplir con los requisitos legales y normativos aplicables, así como las normas internacionales.
- Mejorar la información financiera.
- Mejorar la gestión empresarial.
- Mejorar la confianza de los grupos de interés (stakeholders).
- Establecer una base fiable para la toma de decisiones y planificación.

- Mejorar los controles.
- Repartir y utilizar de forma efectiva los recursos para la gestión de riesgos.
- Mejorar la eficacia y la eficiencia operacional.
- Aumentar la seguridad y salud.
- Mejorar la prevención, así como la gestión de incidentes.
- Minimizar las pérdidas.
- Mejorar el aprendizaje organizativo.
- Mejorar la resistencia organizativa.

6.4.1. Estructura ISO 31000.

El enfoque está estructurado en tres elementos claves para una efectiva gestión de riesgos:

1. Los principios de gestión del riesgo
2. El marco de trabajo para la gestión del riesgo
3. El proceso de gestión del riesgo.

La relación entre los principios de gestión, el marco de referencia, así como el proceso de gestión del riesgo desarrollado en la norma se resume en la figura siguiente:

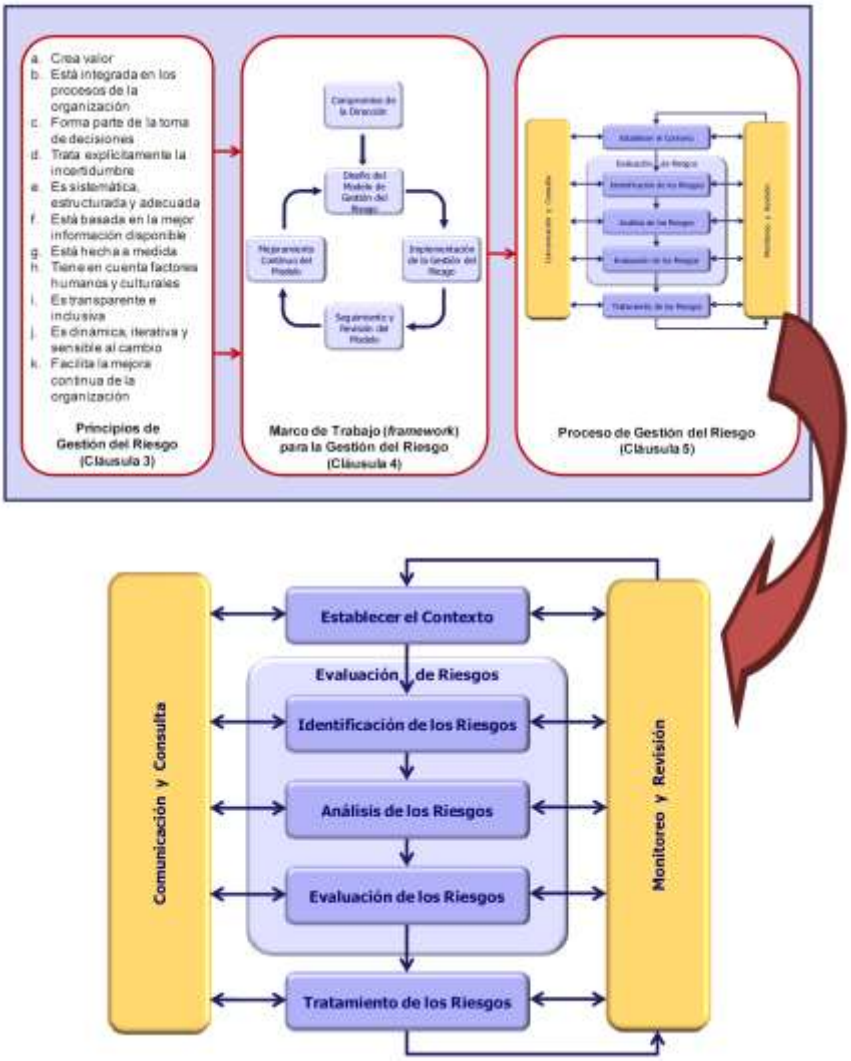


Ilustración 2. Estructura Norma ISO 31.000. Enfoque y relación de los elementos claves. fuente

Principios Básicos para la Gestión de Riesgos

La norma ISO 31000:2009 establece los principios y directrices de carácter genérico sobre la gestión del riesgo.

Para una mayor eficacia de la gestión del riesgo en una organización debe tner en cuenta los siguientes principios:

a) Crea valor y protege valor

La gestión del riesgo contribuye de manera tangible al logro de los objetivos y la mejora del desempeño, por ejemplo, en lo referente a la salud y seguridad de las personas, a la conformidad con los requisitos legales y reglamentos, a la aceptación por el público, a la protección ambiental, a la calidad del producto, a la gestión del proyecto, a la eficacia en las operaciones y a su gobierno y reputación.

b) Está integrada en los procesos de la organización

La gestión de riesgo no es una actividad separada de las actividades y procesos principales de la organización. La gestión del riesgo es parte de las responsabilidades de gestión y una parte integral de todos los procesos de la organización, incluyendo la planificación estratégica y todos los procesos de la gestión de proyectos y de cambios.

c) Forma parte de la toma de decisiones

La gestión de riesgos ayuda a las personas que toman decisiones a realizar elecciones informadas, a definir las prioridades de las acciones y a distinguir entre planes de acciones diferentes.

d) Trata explícitamente la incertidumbre

La gestión del riesgo tiene en cuenta explícitamente la incertidumbre, la naturaleza de esa incertidumbre, y la manera en que se puede tratar.

e) Es sistemática, estructurada y adecuada

Un enfoque sistémico, oportuno y estructurado de la gestión de riesgos contribuye a la eficacia y a resultados coherentes, comparables y fiables.

f) Está basada en la mejor información disponible

Los elementos de entrada del proceso de gestión del ri3esgo se basan en fuentes de información tales como datos históricos, experiencia, retroalimentación de las partes interesadas, observación, previsiones y juicios de expertos. No obstante, las personas que toman decisiones deberían informarse y tener en cuenta todas las limitaciones de los datos o modelos utilizados ¿, asi como las posibles divergencias entre expertos.

g) Está hecha a medida, se adapta.

La gestión del riesgo se alinea con el contexto externo e interno de la organización y con el perfil del riesgo.

h) Tiene en cuenta factores humanos y culturales.

La gestión del riesgo permite identificar las aptitudes, las percepciones y las intenciones de las personas externas e internas que pueden facilitar u obstruir el logro de los objetivos de la organización.

i) Es transparente e participativa.

La implicación apropiada y oportuna de las partes interesadas y, en particular, de las personas que toman decisiones a todos los niveles de la organización, asegura

que la gestión del riesgo se mantenga pertinente y actualizada. La implicación también permite a las partes interesadas estar correctamente representadas y que sus opiniones se tengan en cuanta en la determinación de los criterios de riesgos.

j) Es dinámica, iterativa y sensible al cambio

La gestión del riesgo es sensible de manera continuada a los cambios y responde a ello. Como se producen sucesos externos e interno, el contexto y los conocimientos cambian, se realiza el seguimiento y la revisión de riesgos, surgen nuevos riesgos, algunos cambian y otros desaparecen.

k) Facilita la mejora continua de la organización

Las organizaciones deberían desarrollar e implementar estrategias para mejorar su madurez en la gestión del riesgo en todos los demás aspectos de la organización.

Marco de Trabajo de la ISO 31.000

El éxito de la gestión de riesgos dependerá de la efectividad del marco para manejar los riesgos, que provee las bases y fundamentos que traspasa la organización en todos sus niveles. El marco colabora en la gestión efectiva de los riesgos, a través de procesos de administración de riesgos en varios escenarios y contextos del Servicio o entidad. El marco asegura que la información derivada de ese proceso sea adecuadamente comunicada y se utilice como una base para la toma de decisiones por parte de la autoridad y para la rendición de cuentas o accountability de las mismas.

El marco de trabajo no pretende prescribir un sistema de gestión, sino más bien ayudar a la organización a integrar la gestión del riesgo en su sistema de gestión global. Por ello, las organizaciones deberían adaptar los componentes del marco de trabajo a sus necesidades específicas.

Si las prácticas y procesos de gestión existentes en una organización incluyen componentes de gestión del riesgo, o si la organización ya ha adoptado un proceso formal de gestión del riesgo para tipos o situaciones particulares de riesgo, entonces éstos se deberían revisar y evaluar de forma crítica de acuerdo con esta norma, a fin de determinar si la gestión de riesgos ha sido adecuada y eficaz.

El marco describe los elementos necesarios para la gestión de riesgos y la forma cómo estos componentes se interrelacionan entre sí, como se señala en la Ilustración N° 2.

La descripción de los elementos del marco de trabajo de la gestión del riesgo comprende:

1. Mandato y Compromiso

La introducción de la gestión del riesgo y el aseguramiento de su eficacia continua requieren un compromiso fuerte y sostenido de la dirección de la organización gubernamental, así como establecimiento de una planificación estratégica y rigurosa para lograr el compromiso a todos los niveles.

2. Diseño del Marco de Trabajo de la Gestión del Riesgo
   - 2.1. Comprensión de la Organización y de su Contexto. Antes de iniciar el diseño y la implementación del marco de trabajo de la gestión del riesgo, es importante evaluar y entender el contexto externo y el contexto interno de la organización, dado que ambos pueden influir significativamente en el diseño del marco de trabajo.
   - 2.2. Establecimiento de la Política de Gestión del Riesgo. La política de gestión del riesgo debería indicar claramente los objetivos y el compromiso de la organización en materia de la gestión del riesgo.
   - 2.3. Obligación de Rendir Cuentas (Accountability). La organización se debería asegurar que la obligación de rendir cuentas, la autoridad y las competencias apropiadas para gestionar el riesgo están establecidas,

incluyendo la implementación y la mantención del proceso de gestión del riesgo y asegurando la idoneidad, eficacia y eficiencia de todos los controles.

2.4. Integración en los Procesos de la Organización. La gestión del riesgo debería estar integrada en todas las prácticas y procesos de la organización, de una manera que sea pertinente, eficaz y eficiente. El proceso de gestión del riesgo debería formar parte de los procesos de la organización, y no ser independiente de ellos. En particular, la gestión del riesgo debería estar integrada en el desarrollo de la política, en la planificación y revisión de la actividad y la estrategia, y en los procesos de gestión de cambios.

2.5. Recursos. La organización debería proporcionar los recursos adecuados para gestión del riesgo.

2.6. Establecimiento de los Mecanismos Internos de Comunicación y de Reporte. La organización debería establecer mecanismos internos de comunicación y de reporte con objeto de apoyar y fomentar la obligación de rendir cuentas y la propiedad del riesgo.

2.7. Establecimiento de los Mecanismos Externos de Comunicación y de Reporte. La organización debería desarrollar e implementar un plan para comunicarse con las partes interesadas externas.

3. Implementación del Marco de Trabajo de la Gestión del Riesgo y del Proceso de Gestión del Riesgo.

3.1. Implementación del Marco de Trabajo de la Gestión del Riesgo. Para esta actividad la organización debería:

- Definir el calendario y la estrategia apropiados para la implementación del marco de trabajo;
- Aplicar la política y el proceso de gestión del riesgo a los procesos de la organización;
- Cumplir los requisitos legales y reglamentarios;
- Asegurar que la toma de decisiones, incluyendo el desarrollo y el establecimiento de los objetivos, se alinean con los resultados de los procesos de gestión del riesgo;
- Organizar sesiones de información y de entrenamiento; y

- Comunicar y consultar a las partes interesadas para garantizar que su marco de trabajo de la gestión del riesgo continúa siendo apropiado.

3.2. Implementación del Proceso de Gestión del Riesgo. La gestión del riesgo se debería implementar de manera que se asegure que el proceso de gestión del riesgo, se aplica mediante un plan de gestión del riesgo en todos los niveles y funciones pertinentes de la organización, como parte de sus prácticas y procesos.

4. Monitoreo y Revisión del Marco de Trabajo

Con objeto de asegurar que la gestión del riesgo es eficaz y contribuye a ayudar al desempeño de la organización ésta debería:

- Medir el desempeño de la gestión del riesgo respecto a los indicadores, que se revisan periódicamente en cuanto a su idoneidad;
- Medir periódicamente el progreso y las desviaciones respecto al plan de gestión del riesgo.
- Revisar periódicamente si el marco de trabajo, la política y el plan de gestión del riesgo siguen siendo apropiados, a la vista del contexto interno y externo de la organización;
- Establecer informes sobre los riesgos, sobre el progreso del plan de gestión del riesgo y sobre la forma en que se está siguiendo la política de gestión del riesgo; y
- Revisar la eficacia del marco de trabajo de gestión del riesgo.

5. Mejora Continua del Marco de Trabajo

En base a los resultados obtenidos del monitoreo y de las revisiones, se deberían tomar decisiones sobre cómo mejorar el marco de trabajo, la política y el plan de gestión del riesgo. Estas decisiones deberían conducir a mejoras en la gestión del riesgo por parte de la organización, así como a mejoras de su cultura de gestión del riesgo.

Fases Genéricas en el Proceso de Gestión de Riesgos

Sin perjuicio que en la actualidad existen una serie de modelos para la gestión de riesgos de mayor o menor difusión, se ha decidido utilizar un modelo genérico, que recoge en su mayor parte los elementos del Proceso de Gestión de Riesgos contenidos en la Norma NCh-ISO 31000, que en su desarrollo y mejora a través del tiempo permita a las entidades gubernamentales adecuarlo a otros más específicos, si es que aquello fuese necesario.

Las fases en que se desagrega este modelo genérico y que deben desarrollarse para implementar el Proceso de Gestión de Riesgos, se señalan a continuación:

5.1. Establecimiento del Contexto: Definición de los parámetros externos e internos a tener en cuenta cuando se gestiona el riesgo, y se establecen el alcance y los criterios de riesgo para la política de gestión del riesgo. Comprende establecer los contextos estratégicos, organizacional y de gestión en los cuales tendrá lugar el Proceso de Gestión de Riesgos. Deben establecerse los objetivos de la evaluación del riesgo, los criterios contra los cuales se evaluarán los riesgos, el programa de evaluación del riesgo y definirse la estructura de análisis, los roles y responsabilidades.

5.2. Evaluación del Riesgo: La evaluación del riesgo es el proceso global de identificación del riesgo, de análisis del riesgo y de valoración del riesgo.

5.3. Identificación del Riesgo: Proceso de búsqueda, reconocimiento y descripción de riesgos. Comprende identificar los riesgos que podrían impedir, degradar o demorar el cumplimiento de los objetivos estratégicos y operativos de la organización, así como las oportunidades que puedan contribuir al logro de los referidos objetivos.

5.4. Análisis del Riesgo: Proceso que permite comprender la naturaleza del riesgo y determinar el nivel de riesgo. El análisis del riesgo proporciona las bases para la valoración del riesgo y para tomar las decisiones relativas al tratamiento del riesgo. El análisis debería considerar el rango de consecuencias potenciales y cuán probable es que los riesgos puedan ocurrir. Consecuencia y probabilidad se combinan para producir un nivel estimado de riesgo según la definición de la organización. Adicionalmente se debe identificar y analizar los controles mitigantes existentes.

5.5. Valoración del Riesgo: Proceso de comparación de los resultados del análisis del riesgo con los criterios de riesgo para determinar si el riesgo y/o su magnitud es aceptable o tolerable. Comprende comparar los niveles de riesgo encontrados contra los criterios de riesgo aceptado preestablecidos por la organización, considerando el balance entre beneficios potenciales y resultados adversos. Ordenar y priorizar mediante un ranking los riesgos analizados.

5.6. Tratamiento del Riesgo: Una vez completada la evaluación del riesgo, el tratamiento del riesgo involucra la selección y el acuerdo para aplicar una o varias opciones pertinentes para cambiar la probabilidad de que los riesgos ocurran, los efectos de los riesgos, o ambas, y la implementación de estas opciones. A continuación de esto, sigue un proceso crítico de reevaluación del nuevo nivel de riesgo, con la intención de determinar su tolerancia con respecto a los criterios previamente establecidos, para decidir si se requiere tratamiento adicional. De acuerdo al ranking de riesgos y al nivel de riesgo aceptado preestablecido por la organización, definir su tratamiento y/o monitoreo, desarrollando e implementando estrategias y planes de acción específicos, que mantengan el riesgo dentro de los niveles aceptados por la organización.

5.7. Monitoreo y Revisión: Como parte del proceso de gestión del riesgo, los riesgos y los controles se deben monitorear y revisar de manera regular.

Comprende definir y utilizar mecanismos para la verificación, supervisión, observación crítica o determinación del estado de los riesgos y controles con objeto de identificar de una manera continua los cambios que se puedan producir en el nivel de desempeño requerido o esperado y dar cuenta de la evolución del nivel del riesgo en procesos críticos para la administración.

5.8. Comunicación y Consulta: Los procesos continuos e iterativos que realiza una organización para proporcionar, compartir u obtener información y para comprometer el diálogo con las partes interesadas en relación con la gestión del riesgo. Comprende definir y utilizar mecanismos para comunicar y consultar con los interesados internos y externos, según resulte apropiado en cada etapa del Proceso de Gestión de Riesgos. Dichos mecanismos deben permitir a las autoridades tomar decisiones en forma oportuna respecto de los riesgos con mayores desviaciones en relación a los niveles aceptados.

6.5. Complementariedad de COSO ERM e ISO 31000

Para establecer los aspectos en que estos dos modelos de gestión del riesgo se complementan, primero se analizará las diferencias entre ambos.

En relación al Riesgo, en la ISO 31000 los riesgos pueden ser considerados positivos como negativos, en cambio para COSO ERM, sólo los eventos con consecuencias negativas son considerados como riesgos, y los con consecuencias positivas se les considera como oportunidades y quedan fuera de la evaluación de riesgo, por ende, de todos los pasos siguientes.

COSO ERM, respecto de la respuesta al riesgo, no considera que se pueda producir un aumento de riesgo, esto es por no considerar eventos que tengan consecuencias positivas, por lo que sólo atiende a la reducción del riesgo. La ISO 31000 si considera este aumento de riesgos y dos respuestas ante un riesgo, cambiar las

probabilidades o cambiar las consecuencias, lo que hace que tenga una lista más extensa de respuesta ante un riesgo, cubriendo sólo el riesgo residual. COSO ERM cubre el riesgo residual e inherente.

Para el análisis de las probabilidades del riesgo, COSO ERM lo realiza en la identificación del evento, en cambio ISO 31000 recomienda este análisis en la evaluación de las consecuencias de los riesgos. Provee más análisis en detalle de las consecuencias por realizarlo en este paso que en comparación con COSO ERM.

ISO 31000 guía para una política de riesgo. COSO ERM no se enfoca en una política.

ISO 31000 provee mayor guía en como describir un potencial riesgo durante la identificación de este y se centra más en entender las consecuencias de éstos. Además, considera el riesgo de que no ocurra un riesgo, siendo más minucioso.

A pesar de haber visto las diferencias, COSO ERM e ISO 31000 tienen más similitudes o complementariedad que diferencias, las cuales se mencionan a continuación:

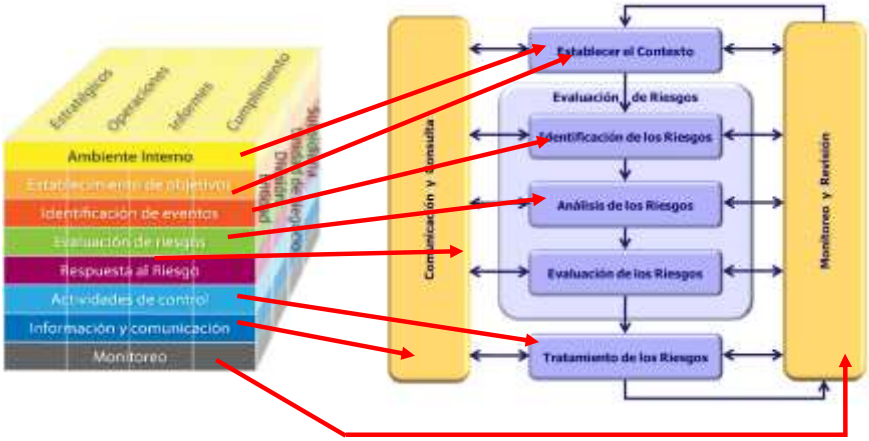
- Facilitan la identificación y el manejo de incertidumbres que están asociadas a cualquier tipo de organización.
- Se adaptan de acuerdo al contexto de la organización.
- El soporte ejecutivo es muy importante para el riesgo.
- No es un proceso estático sino dinámico, el cual puede ir modificándose en la marcha.
- El sistema de gestión de riesgos debe ser integrado al núcleo de la empresa y no ser separado, además, de ser considerado una estrategia.
- Ambas modelos reconocen la importancia del contexto.
- Reconocen la importancia de los stakeholders o partes interesadas.
- Reconocen la importancia de hacer rendición de cuentas y asignar responsabilidades a través de toda la organización para la efectiva implementación de la ERM.
- Consideran la importancia de identificar eventos que puedan tener impacto sobre los objetivos de la organización, como parte de la identificación de riesgos.

- Consideran técnicas cualitativas y cuantitativas en el análisis de riesgos.
- Tienen en cuenta la posible existencia de riesgos interrelacionados o que uno de origen a otro.
- Realización de un análisis de costo beneficio al elegir la forma de tratar un riego.
- La vital importancia de COMUNICAR la información a las partes interesadas (stakeholders)
- Monitorear riesgos e implementar medidas.

En cuanto a los componentes que ambos modelos de gestión del riesgo presentan, se visualiza su complementariedad en la tabla e ilustración a continuación.

COSO (ERM)	**ISO 31000**
Ambiente interno Establecimiento de objetivos	Establecer el contexto
Identificación de eventos	Identificación del riesgo
Evaluación de riesgos	Análisis del riesgo
Respuesta a los riesgos	Evaluación del riesgo Tratamiento del riesgo
Actividades de control	
Información y comunicación	Comunicación y consulta
Monitoreo	Monitoreo y revisión

Ilustración 3. Relación de Complementariedad COSO ERM e ISO 31.000


Estratégicos
Operaciones
Informes
Cumplimiento
Ambiente Interno
Establecimiento de objetivos
Identificación de eventos
Evaluación de riesgos
Respuesta al Riesgo
Actividades de control
Información y comunicación
Monitoreo
Unidad
División
Área
Establecer el Contexto
Evaluación de Riesgos
Identificación de los Riesgos
Análisis de los Riesgos
Evaluación de los Riesgos
Tratamiento de los Riesgos
Comunicación y Consulta
Monitoreo y Revisión

6.6. Geolaquim Ltda.

GEOLAQUIM LTDA., Laboratorio Químico Geológico, ubicado en el Barrio Industrial de la ciudad de Copiapó, inicia sus actividades en el año 2002, logrando establecerse en el mercado y experimentar un gran crecimiento.

En Marzo del 2004 se Certifica bajo la norma ISO 9001:2000, otorgado por DetNorske Veritas, DNV, y acreditado por RvA, cuyo alcance cubre las actividades desde la evaluación y generación de cotizaciones hasta las etapas de producción, control y despacho de los mismos, lo que respalda, aún más, la Confiabilidad de los Resultados y la Calidad del Servicio.

En Octubre de 2015, es aprobado para la Acreditación por la norma NCh-ISO 17025:2005 para la competencia de los laboratorios de ensayos por el INN.

está orientado a satisfacer los requerimientos de la Gran Minería, de acuerdo a las más exigentes normas de Calidad, Medio Ambiente y Seguridad, que avalan su seriedad y solidez. Por supuesto, con importantes fortalezas como lo son un Capital humano altamente calificado y de vasta experiencia, preparado para responder a grandes desafíos y una infraestructura de primer nivel, equipamiento técnico de última generación y sistema de administración de datos analíticos que permiten un servicio confiable y adecuado control de calidad.

Desde sus inicios, contamos con una importante cartera de Cliente de la gran minería, por mencionar algunos: Anglo American Chile con sus división Manto Verde, Los Bronces, El Soldado y Exploraciones, Minera Spence, Exploraciones mineras S. A. (Filial de Codelco Norte), Sociedad Contractual Minera Carola, Coemin S.A., Compañía Minera Carmen Bajo, Minera MMX, Sociedad Contractual Minera Atacama Kozan, Nittetsu Chile Ltda., Minera Catania Verde S.A, entre otros y la atención de la demanda de la mediana minería de la zona.

Entre los principales servicios que ofrece **GEOLAQUIM LTDA**., se puede encontrar:

- Corte de Testigo con Sierra
- Preparación Mecánica de Muestra

- Análisis granulométrico.
- Análisis de Oro por ensayo al fuego y detección por Espectrofotometría de Absorción Atómica.
- Análisis Geoquímica por E.A.A para los elementos Cu, Ag, Pb, Zn, Sb, Mo ,As, Co
- Análisis de mena mineral Cu, Ag, Pb, Zn
- Análisis de Hierro por Espectrofotometría de Absorción Atómica.
- Análisis de Hierro por volumetría.
- Análisis de Hierro Magnético con Tubo Davis.
- Análisis de cobre Volumétrico.
- Análisis de óxidos de cobre en ácido cítrico o sulfúrico
- Análisis de óxidos de aluminio, Sílice, sodio, Potasio, Calcio, Manganeso, Magnesio, Titanio por fusión o detección por E. A.A.
- Análisis de Carbonato de Calcio o Azufre en Analizador LECO
- Análisis de fósforo por Colorimetría.
- Análisis de Cu y Fe total en Solución.
- Análisis de Acides (libre) por Grahm en muestras de Solución.
- Análisis de PH en muestras de Solución.
- Determinación de potencial oxido reducción (ORP).
- Determinación de hierro (II) por Volumetría con Dicromato de Potasio.
- Determinación de Cloruro en muestras de Solución.

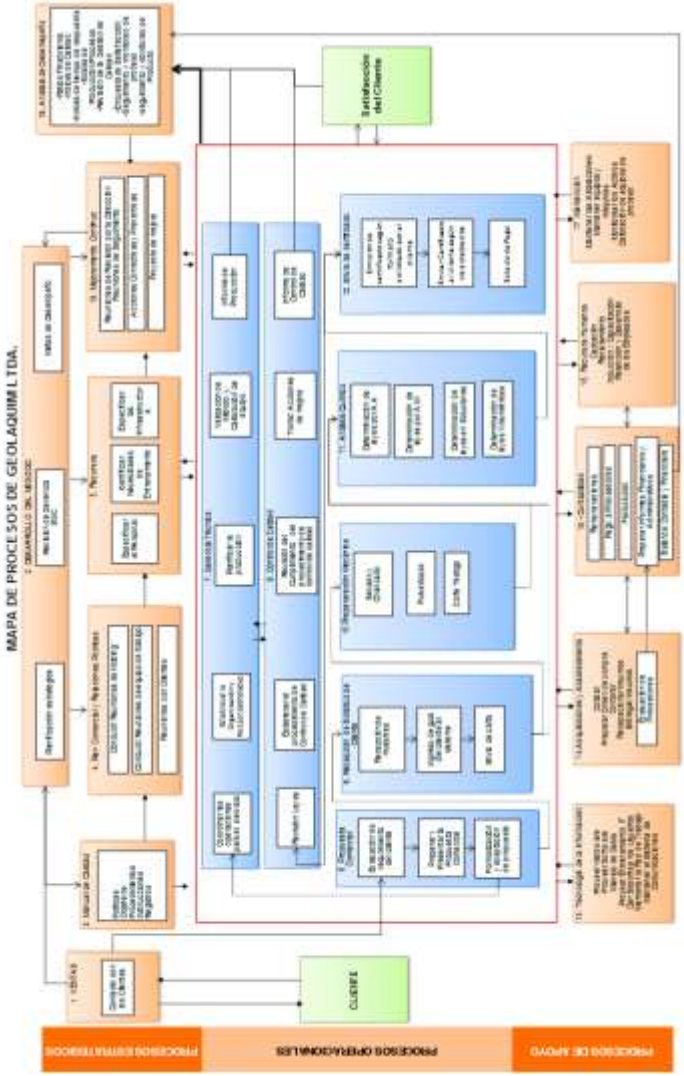


Ilustración 4. Mapa de Procesos de Geolaquim Ltda.

7. Diseño y aplicación del Modelo de Control de Gestión del Riesgo

De acuerdo a las complementariedades entre ambos modelos de gestión de riesgo COSO ERM e ISO 31000, se puede obtener un MODELO INTEGRADO DE GESTIÓN DEL RIESGO, que permite obtener un marco de referencia y metodológico, practico y eficiente para implantar la gestión de riesgos empresarial y mejorar continuamente los sistemas en la organización, que se encuentre integrado a los Objetivos del Negocio.

El cual se presenta a continuación, donde se aprecian 7 componentes, que se integran a los principios de COSO ERM y al proceso de gestión de riesgo de ISO 31000, con el cual, la organización cuenta con una metodología y mejores prácticas para diseñar, documentar e implantar controles eficaces y eficientes orientados a reducir los riesgos estratégicos.

MODELO INTEGRADO DE GESTION DEL RIESGO
Establecimiento del contexto
Identificación de eventos
Análisis del riesgo
Respuesta a los riesgos
Actividad de control
Información y comunicación
Monitoreo de Actividades

De acuerdo a los aspectos claves y principios de cada modelo de gestión del riesgo, se establecen los aspectos claves para el MODELO INTEGRADO DE GESTION DEL RIESGO:

COSO (ERM)	ISO 31000	MODELO INTEGRADO		COSO (ERM)	ISO 31000
• Ambiente interno • Establecimiento de objetivos	Establecer el contexto	Establecimiento del contexto	Contexto interno	• Filosofía de la gestión del riesgo • Riesgo aceptado • Consejo de administración • Integridad y valores éticos • Compromiso con las competencias • Estructura organizativa • Delegación de autorizada • Normas de recursos humanos	
			Contexto externo		• Entorno externo • Objetivos de las partes interesadas externas • Requisitos legales y reglamentarios
			Contexto del proceso de riesgo	• Objetivos Estratégicos • Objetivos conexos	• Criterios de riesgo • Contexto de los objetivos

				• Objetivos seleccionados • Riesgo aceptado • Tolerancia al riesgo	de la organización
Identificación de eventos	Identificación del riesgo	Identificación de eventos	• Identificación de eventos positivos y negativos • Identificación de riesgos y oportunidades	• Eventos • Factores influyentes • Técnicas de identificación de eventos • Interdependencias • Distinción entre riesgos y oportunidades	
Evaluación de riesgos	Análisis del riesgo	Análisis del riesgo		• Riesgo Inherente y residual • Estimación de probabilidad e impacto • Técnicas de evaluación • Relaciones entre los eventos	
Respuesta a los riesgos	• Evaluación del riesgo • Tratamiento del riesgo	Respuesta a los riesgos	• Evaluación del riesgo • Tratamiento del riesgo	• Evaluación de las posibles respuestas • Respuestas seleccionadas • Perspectiva de cartera de riesgos	
Actividad de control		Actividad de control		• Integración con la respuesta a los riesgos • Tipos de actividades de control • Políticas y procedimientos • Controles informáticos	

Información y comunicación	Comunicación y consulta	Información y comunicación		• Información • Comunicación	
Monitoreo / Supervisión	Monitoreo y revisión	Monitoreo de Actividades		• Actividades permanentes de supervisión • Evaluaciones independientes • Información de deficiencias	

De acuerdo a lo anterior, se establece una metodología apropiada para identificar, analizar, documentar, evaluar, controlar y monitorear los eventos de riesgos estratégicos, en un Sistema de Gestión de Riesgos en la organización, la cual está en relación directa con cada componente del MODELO INTEGRADO DE GESTION DE RIESGOS planteado.

MODELO INTEGRADO DE GESTION DEL RIESGO		
COMPONENTES	**ASPECTOS CLAVES**	**METODO DE CONTROL**
Establecimiento del contexto	• Contexto interno ○ Filosofía de la gestión del riesgo ○ Riesgo aceptado ○ Consejo de administración ○ Integridad y valores éticos ○ Compromiso con las competencias ○ Estructura organizativa ○ Delegación de autorizada ○ Normas de recursos humanos	• FODA (INTERNO – EXTERNO) • APETITO DEL RIESGO
	• Contexto externo ○ Entorno externo ○ Objetivos de las partes interesadas externas ○ Requisitos legales y reglamentarios	

	• Contexto del proceso de riesgo
	  ○ Objetivos Estratégicos
	  ○ Objetivos conexos
	  ○ Objetivos seleccionados
	  ○ Riesgo aceptado
	  ○ Tolerancia al riesgo
	  ○ Criterios de riesgo
	  ○ Contexto de los objetivos de la organización	

Identificación de eventos	• Eventos positivos y negativos / riesgos y oportunidades • Factores influyentes • Técnicas de identificación de eventos • Interdependencias • Distinción entre riesgos y oportunidades	MATRIZ DE RIESGO (DESCRIPCION DEL PELIGRO)
Análisis del riesgo	• Riesgo Inherente y residual • Estimación de probabilidad e impacto • Técnicas de evaluación • Relaciones entre los eventos	MATRIZ DE RIESGOS (EVALUACION DEL RIESGO)
Respuesta a los riesgos	• Evaluación de las posibles respuestas • Respuestas seleccionadas • Tratamiento del riesgo • Perspectiva de cartera de riesgos	MATRIZ DE RIESGOS (PLANES DE ACCION Y MEDIDAS DE CONTROL)

Actividad de control	• Integración con la respuesta a los riesgos • Tipos de actividades de control • Políticas y procedimientos • Controles informáticos	SEGUIMIENTO Y CONTROL
Información y comunicación	• Información • Comunicación	INFORMACION DOCUMENTADA
Monitoreo de Actividades	• Actividades permanentes de supervisión • Evaluaciones independientes • Información de deficiencias	AUDITORIA INTERNA

7.1. Evaluación de cumplimiento de aspectos claves de modelo integrado de gestión del riesgo

Con el propósito de conocer el nivel de cumplimiento de los requerimientos del nuevo modelo integrado de gestión de riesgo en la organización, se crea una "evaluación de cumplimiento de aspectos claves del modelo integrado de gestión del riesgo", a partir de cada componente del nuevo modelo, con una serie de afirmaciones que permiten que la empresa sea evaluada con una escala porcentual.

Con la aplicación de la evaluación en la empresa se establece la brecha existente entre la organización y los requerimientos del modelo, permitiendo con la información establecer una estrategia de mejoramiento del Sistema de Gestión de Riesgo en base al Modelo integrado y su metodología de aplicación.

EVALUACIÓN DE CUMPLIMIENTO DE ASPECTOS CLAVES DE MODELO INTEGRADO DE GESTIÓN DEL RIESGO

La presente evaluación mide el nivel de cumplimiento en la empresa respecto de la implementación del Modelo Integrado de Gestión del Riesgo basado en COSO ERM e ISO 31000, por cada aspecto clave de los componentes del modelo.

A continuación, se presentan una serie de afirmaciones por cada componente sobre la empresa a ser evaluada con la escala porcentual aquí detallada.

ESCALA DE EVALUACIÓN DE CUMPLIMIENTO				
NUNCA	**CASI NUNCA**	**A VECES**	**CASI SIEMPRE**	**SIEMPRE**
0%	**25%**	**50%**	**75%**	**100%**

Por favor marque con una "x" el recuadro que corresponda según el nivel de cumplimiento de la empresa. La casilla final - % Cumplimiento - ha de ser rellenada por el evaluador en relación al cumplimiento de la empresa según ítem.

		ESCALA DE EVALUACIÓN DE CUMPLIMIENTO					
		NUNCA	CASI NUNCA	A VECES	CASI SIEMPRE	SIEMPRE	% CUMPLIMIENTO
		0%	25%	50%	75%	100%	
1. **ESTABLECIMIENTO DEL CONTEXTO**							
1.1. CONTEXTO INTERNO							
Filosofía de la gestión de	La empresa cuenta con una filosofía de la gestión de riesgos declarada						

riesgos de la empresa	Representa las convicciones y actitudes compartidas que caracterizan cómo la entidad contempla el riesgo en todas sus actividades						
	La empresa refleja los valores de la entidad, influyendo en su cultura y estilo operativo						
	Está bien desarrollada, entendida y aceptada por el personal de la empresa						
	La filosofía de gestión de riesgo se ha integrado en las declaraciones de políticas de la empresa, las comunicaciones verbales y escritas y la toma de decisiones						
	La gerencia refuerza la filosofía de gestión de riesgo no sólo con palabras, sino también con acciones cotidianas						
Riesgo aceptado por la empresa	Refleja la filosofía de gestión de riesgos e influye en la cultura y estilo operativo						
	Es considerado en el establecimiento de la estrategia, la cual queda en línea con el riesgo aceptado						
	El proceso de gestión del riesgo se alinea con la						

Gestión de Riesgo	cultura, los procesos, la estructura y la estrategia de la organización						
	La gestión del riesgo se realiza en el contexto de los objetivos de la organización						
	Los objetivos y los criterios de un proyecto, de un proceso, de una actividad específicos en la empresa, se consideran a la vista de los objetivos de la organización en su conjunto						
	La empresa reconoce las oportunidades que le permiten conseguir sus objetivos en materia de la estrategia, de proyecto o de negocio, permitiendo la continuidad del compromiso, la credibilidad, la confianza y los valores de la empresa						
Dirección de la empresa	La dirección incluye las estructuras de la organización, las funciones y las responsabilidades						
	La dirección incluye las políticas, los objetivos y las estrategias que se establecen para conseguirlos						

	La dirección incluye las aptitudes, entendidas en términos de recursos y conocimientos						
	La dirección incluye las relaciones con las partes internas interesadas, sus percepciones y sus valores						
	La dirección incluye la cultura de la organización						
	La dirección incluye los sistemas de información, los flujos de información y los procesos de toma de decisiones						
	La dirección incluye las normas, las directrices y los modelos adoptados por la organización, y la forma y extensión de las relaciones contractuales						
Consejo de administración de la empresa	Es activo y posee una adecuada experiencia directiva, técnica y de otro tipo, junto con la mentalidad necesaria para realizar sus funciones supervisoras						
	Está preparado para cuestionar y fiscalizar las actividades de la dirección, presentar perspectivas alternativas y actuar contra el dolo						

	Posee al menos una mayoría de consejeros externos e independientes						
	Proporciona la supervisión de la gestión de riesgos corporativos y es consciente del riesgo aceptado por la empresa y está de acuerdo con el						
Integridad y Valores éticos de la empresa	Las normas de conducta de la empresa reflejan su integridad y valores éticos						
	Los valores éticos no sólo se comunican, sino que también van acompañados de una orientación explícita sobre lo que es correcto e incorrecto						
	Son comunicados a través de un código formal de conducta						
	Existen canales ascendentes de comunicación donde los empleados se sienten cómodos aportando información relevante						
	Sanciones se aplican a los empleados que violan el código						
	Los mecanismos animan al empleado a presentar denuncias por sospechas de violaciones al código						

	Se toman acciones disciplinarias contra empleados que conscientemente optan por no informar sobre violaciones al código						
	La integridad y los valores éticos se comunican a través de acciones de la dirección y sus ejemplos						
Compromiso con la competencia	Las competencias de los empleados de la empresa reflejan los conocimientos y habilidades necesarias para realizar las tareas asignadas						
	La dirección alinea las competencias y el coste						
Estructura Organizada	Define las áreas claves de responsabilidad						
	Establece las líneas de información						
	Se desarrolla teniendo en cuenta la dimensión de la entidad y la naturaleza de sus actividades						
	Permite una gestión eficaz de riesgos corporativos						
Delegación de autoridad y responsabilidad (dentro de la empresa)	Las delegaciones marcan los límites de la autoridad y establece hasta qué punto se confiere ésta a los equipos y personas y se les anima a usar su						

	iniciativa para abordar temas y resolver problemas						
	Las asignaciones correspondientes establecen las relaciones de información y los protocolos de autorización						
	Las políticas describen las prácticas empresariales adecuadas, el conocimiento y experiencia del personal clave y los recursos asociados						
	Las personas conocen cómo sus acciones se relacionan entre sí y contribuyen a la consecución de objetivos						
Norma de recursos humanos	Abordan la contratación, orientación, formación, evaluación, asesoramiento, promoción, compensación y acciones correctoras						
	Impulsan los niveles esperados de integridad, comportamiento ético y competencias						
	Las secciones disciplinarias transmiten el mensaje de que las violaciones del comportamiento esperado no serán toleradas						

1.2. CONTEXTO EXTERNO							
Entorno externo	La empresa establece el entorno social y cultural, a nivel internacional, nacional, regional o local, según sus necesidades						
	La empresa establece el entorno político, legal, reglamentario, a nivel internacional, nacional, regional o local, según sus necesidades.						
	La empresa establece el entorno económico, natural y competitivo, a nivel internacional, nacional, regional o local, según sus necesidades.						
	Es considerado en el desarrollo de los criterios de riesgo de la empresa.						
	Establece los factores y tendencias claves del contexto externo que afecten los objetivos de la empresa.						
Objetivo de las partes interesadas externas	Establece las relaciones con las partes interesadas externas, sus percepciones y sus valores						
	La empresa asegura los objetivos e inquietudes de las partes interesadas externas						

Requisitos legales y reglamentarios	La empresa cumple con los requisitos legales y reglamentarios inherentes a su negocio que afectan a las partes interesadas u otro agente externo						
1.3. CONTEXTO DEL PROCESO DE RIESGO							
Objetivos estratégicos de la empresa	Establecen objetivos de alto nivel, en línea con su misión/visión y dando apoyo a la empresa						
	Reflejan las decisiones estratégicas de la dirección respecto a cómo la empresa pretenderá crear valor para sus grupos de interés						
	La dirección identifica los riesgos asociados a las decisiones estratégicas y considera sus implicaciones						
Objetivos conexos de la empresa	Apoyan la estrategia seleccionada, relativa a todas las actividades de la empresa						
	Cada nivel de objetivos está vinculado a objetivos más específicos que fluyen en cascada por toda la empresa						
	Los objetivos son fácilmente comprensibles y medibles						

	Están en línea con el riesgo aceptado						
Objetivos seleccionados de la empresa	La dirección tiene un proceso que alinea los objetivos estratégicos con la misión de la entidad, asegurando que los objetivos estratégicos y relacionados son consecuentes con el riesgo aceptado por la entidad						
Riesgo aceptado por la empresa	Es la guía principal para establecer la estrategia						
	Orienta la dotación de recursos						
	Alinea a la organización, personas, procesos e infraestructura						
Tolerancia al Riesgo	Son medibles, preferiblemente en las mismas unidades que los objetivos conexos						
	Están en línea con el riesgo aceptado						
Criterios de Riesgo	La empresa define los criterios que se aplican para evaluar la importancia del riesgo de forma que refleja los valores, los objetivos y los recursos de la organización						
	Los criterios de riesgo son coherentes con la política						

	de gestión del riesgo de la empresa						
	La política de gestión de riesgo es definida al comienzo de cualquier proceso de gestión del riesgo, y es revisada continuamente						
	Se considera la naturaleza y los tipos de las causas y de las consecuencias que se pueden producir, y como se deben medir al definir los criterios de riesgo						
	Se establece el método de definición de la probabilidad, los plazos de la probabilidad y/o de las consecuencias al definir los criterios de riesgo						
	Se establece el método para determinar el nivel de riesgo, el nivel al que el riesgo comienza a ser aceptable o tolerable						
Contexto de los objetivos de la empresa respecto al riesgo	La empresa especifica los recursos requeridos, las responsabilidades y autoridades, y los registros que se deben conservar						
	Define las metas y objetivos de las actividades de gestión del riesgo						

	La empresa incorpora la definición de las responsabilidades relativas al proceso de gestión del riesgo						
	Se establece la definición del alcance, así como el grado y la amplitud de las actividades de gestión del riesgo a realizar						
	Establece la definición de la actividad, del proceso, de la función, del proyecto, del producto, del servicio o del activo, en términos de tiempo y de ubicación						
	La empresa establece metodologías de apreciación del riesgo						
	Se establece o define el método para evaluar el desempeño y la eficacia en la gestión del riesgo						
1. IDENTIFICACIÓN DE EVENTOS							
	Se tienen en cuenta incluso los eventos con una posibilidad de ocurrencia relativamente baja siempre que su impacto sobre la consecución de algún objetivo sea importante						
Identificación del riesgo	La empresa identifica los orígenes de riesgo, las áreas de impactos, los sucesos, así como sus						

	causas y sus consecuencias potenciales						
	La empresa identifica sus riesgos generando una lista exhaustiva basada en aquellos sucesos que podrían crear, mejorar, prevenir, degradar, acelerar o retrasar el logro de los objetivos						
	Se identifican todo tipo de riesgos, incluyendo los riesgos asociados al hecho de no buscar una oportunidad						
	En la identificación incluye los riesgos, tanto si su origen está o no bajo el control de la organización, incluso aunque el origen o la causa del riesgo no pueda ser evidente						
	La identificación del riesgo incluye el examen de los efectos en cadena de consecuencias particulares, incluyendo los efectos en cascada o acumulativos						
	Considera un amplio rango de consecuencias, incluso aunque el origen o la causa del riesgo no puedan ser evidentes						

	Identifica lo que podría ocurrir, considerando las posibles causas y escenarios que muestran las consecuencias que se pueden producir; todas las causas y consecuencias significativas son consideradas						
	La empresa aplica herramientas y técnicas de identificación del riesgo que se adaptan a sus objetivos y aptitudes, así como a los riesgos a los que está expuesta						
	La información relacionada a la identificación de riesgos es pertinente y actualizada, siempre que sea posible, está acompañada de antecedentes apropiados						
Factores influyentes	La dirección reconoce la importancia de entender los factores internos y externos y el tipo de eventos que pueden emanar de ellos						
	Se identifican los eventos tanto a nivel de empresa como de actividad						
Técnicas de identificación de eventos	Las técnicas aplicadas miran tanto el pasado como al futuro						

	La dirección selecciona técnicas adecuadas para su filosofía de gestión de riesgos y asegura que la empresa desarrolle las capacidades de identificación de eventos						
	La identificación de los eventos es sólida, formando la base de la evaluación de riesgos y los componentes de respuestas a ellos						
Interdependencias	La dirección entiende como los eventos se relacionan entre sí						
Distinción entre riesgos y oportunidades	Los eventos con impactos negativos representan riesgos, que la dirección evalúa y a los cuales responde						
	Los eventos que representan oportunidades son canalizados hacia el proceso de establecimiento de estrategias y objetivos						
2. ANÁLISIS DEL RIESGO							
Riesgo inherente y residual	Al evaluar los riesgos, la dirección considera los eventos esperados e inesperados						

	La dirección evalúa los riesgos inherentes previamente						
	Una vez desarrolladas las respuestas, la dirección considera el riesgo residual						
Estimación de probabilidad e impacto	Los eventos potenciales son evaluados desde dos perspectivas: probabilidad e impacto						
	Identifica los factores que afectan a las consecuencias y a la probabilidad						
	El riesgo se analiza determinando las consecuencias y su probabilidad, así como otros atributos del riesgo						
	Al evaluar el impacto, la gerencia utiliza la misma unidad de medición, u otra coherente, que la empleada en el objetivo						
	Las consecuencias y su probabilidad se determinan realizando el modelo de los resultados de un suceso o conjunto de sucesos, o por extrapolación de estudios experimentales o de datos disponibles						
	El horizonte temporal aplicado para evaluar los riesgos es consecuente						

	con el horizonte de tiempo de la estrategia y objetivos correspondientes						
	Las consecuencias se expresan en términos de impactos tangibles o intangibles, en algunos casos, se utiliza un valor numérico o descriptor para especificar las consecuencias y su probabilidad.						
Técnicas de evaluación	La empresa al realizar el análisis del riesgo considera los diferentes grados de detalle, dependiendo del riesgo, de la finalidad del análisis y de la información, así como de los datos y los recursos disponibles.						
	La dirección usa una combinación de técnicas cualitativas y cuantitativas						
	Las técnicas apoyan el desarrollo de una evaluación compuesta de los riesgos						
	En base a los resultados del análisis del riesgo, la evaluación del riesgo favorece la toma de decisiones, determinando los riesgos a tratar y la prioridad para implementar el tratamiento						

	Para las decisiones se toma en cuenta el contexto más amplio del riesgo y se incluye la consideración de la tolerancia del riesgo						
	Las decisiones se toman de acuerdo con requisitos legales, reglamentarios y requisitos de otro tipo						
	Las decisiones están influenciadas por la actitud ante el riesgo por parte de la organización y por los criterios de riesgo que se hayan establecido						
Relaciones entre los eventos	La dirección los evalúa en conjunto cuando existe una correlación entre eventos o donde se combinan e interaccionan						
3. RESPUESTA AL RIESGO							
	La dirección considera sus costos y beneficios, además de las nuevas oportunidades						
Respuestas seleccionadas	Las respuestas elegidas por la dirección están diseñadas para enmarcar la probabilidad de riesgo esperada y el impacto dentro de las tolerancias de riesgo						
	La dirección considera los riesgos adicionales que						

	pueden derivarse de una respuesta						
Tratamiento del riesgo	Se evalúa el tratamiento del riesgo y se decide si los niveles de riesgo residual son tolerables						
	De no ser tolerables los niveles de riesgo residual se genera un nuevo tratamiento de riesgo						
	Se evalúa la eficacia del tratamiento constantemente, el seguimiento es parte integral del tratamiento de riesgo						
	La selección de tratamiento de riesgo implica una compensación de los costos y los esfuerzos de implementación en función de las ventajas que se obtengan						
	La selección de tratamiento de riesgo toma en cuenta los requisitos legales, reglamentarios y de otro tipo, tales como responsabilidad social y la protección del entorno natural						
	La selección de tratamiento de riesgo considera los riesgos cuyo tratamiento no es						

	justificable en el plano económico						
	La selección de tratamiento de riesgo toma en cuenta otras partes de la empresa o partes interesadas en las que pueda impactar el riesgo						
	La empresa considera los valores y percepciones de las partes interesadas y los medios más apropiados para comunicarse con ellas						
	El plan de tratamiento identifica con claridad el orden de prioridad en que se deberían implementar los tratamientos de riesgo individuales						
	Los riesgos secundarios producidos por el tratamiento de riesgo están incluidos en el plan de tratamiento original						
	Los planes de tratamiento de riesgo incluyen las razones que justifican la selección de tratamiento, incluyendo los beneficios previstos						
	Los planes de tratamiento de riesgo establecen las personas responsables de la aprobación del plan y las						

	personas responsables de la implementación del plan						
	Los planes de tratamiento de riesgo incluyen las acciones propuestas						
	Los planes de tratamiento de riesgo establecen las necesidades de recursos incluyendo las contingencias						
	Los planes de tratamiento de riesgo incluyen las medidas del desempeño y las restricciones						
	Los planes de tratamiento de riesgo establecen los requisitos en materia de información y de seguimiento						
	Los planes de tratamiento de riesgo incluyen el calendario y la programación						
	Los planes de tratamiento se integran en los procesos de gestión de la empresa y se discuten con las partes interesadas apropiadas						
	Las personas que toman decisiones y las otras partes interesadas están enteradas de la naturaleza y amplitud del riesgo						

	residual después del tratamiento del riesgo						
	El riesgo residual se documenta y somete a seguimiento, revisión y, cuando sea apropiado, a tratamiento adicional						
	La dirección considera los riesgos desde la perspectiva de toda la empresa o la de carteras de riesgos						
Perspectiva de cartera de riesgos	La dirección determina si el perfil de riesgos residual de la empresa es consecuente con su riesgo aceptado global						
4. ACTIVIDAD DE CONTROL							
Tipos de actividades de control	La dirección selecciona varios tipos de actividad de control, incluyendo los controles de detección, manuales, informáticos y de gestión						
Políticas y procedimientos	Las políticas se implantan de forma meditada, consciente y coherente						
	Los procedimientos se llevan a cabo con un enfoque claro y permanente sobre las condiciones hacia las que se orienta la política						

	Las condiciones identificadas como resultado del procedimiento son investigadas y se toman las acciones correctoras adecuadas						
Controles informáticos	Se implantan adecuados controles generales y de aplicaciones						
5. INFORMACION Y COMUNICACIÓN							
	La información se facilita con profundidad, forma y marco temporal adecuados para que resulte disponible, utilizable y vinculada a responsabilidades definidas incluyendo la necesidad de identificar y evaluar el riesgo y responder al mismo						
	Los datos e información son fiables y facilitados a tiempo en el lugar adecuado para permitir una toma eficaz de decisiones						
	La oportunidad de flujo de información es coherente con el ritmo de cambios en los entornos externos e internos de la entidad						
	Los asistentes de información cambian						

	según se necesite para apoyar a los objetivos nuevos						
Comunicación	La dirección proporciona una comunicación específica y directa relativa a las expectativas de comportamiento y responsabilidades del personal, incluyendo una nítida exposición de la filosofía y enfoque de gestión de riesgos corporativos de la empresa y una clara delegación de autoridad						
	La comunicación sobre procesos y procedimientos está en línea con la cultura y se ajusta a ella						
	Todo el personal recibe un mensaje claro desde la alta dirección de que la gestión de riesgos corporativos ha de tomarse en serio						
	El personal sabe cómo sus actividades se relacionan con el trabajo de los demás, permitiéndoles reconocer los problemas, determinar sus causas y tomar acciones correctoras						
	El personal sabe qué comportamiento se						

	considera aceptable y no aceptable						
	Existen canales abiertos de comunicación y una disposición a escuchar. El personal cree que sus superiores realmente desean conocer los problemas y que los abordarán eficazmente						
	Hay canales de comunicación independientes de las líneas normales de información y el personal entiende que no habrá represalias por trasladar información relevante						
	Un canal abierto de comunicaciones existe entre la alta dirección y el consejo de administración, siendo comunicada oportunamente la información adecuada						
	Están abiertos unos canales externos de comunicaciones y a través de ellos los clientes y proveedores pueden facilitar información significativa						
6. MONITOREO DE ACTIVIDADES							

Evaluaciones independientes	El evaluador entiende cada una de las actividades de la empresa y cada componente de la gestión de riesgos corporativos que está siendo abordado						
	El evaluador analiza el diseño de la gestión de riesgos corporativos de la empresa y los resultados de las pruebas realizadas frente al trasfondo de normas establecidas por la dirección, determinando si dicha gestión proporciona una seguridad razonable respecto a los objetivos fijados						
	Las deficiencias informadas desde fuentes internas o externas se consideran cuidadosamente por sus implicaciones para la gestión de riesgos corporativos y se adoptan las acciones correctoras adecuadas						
Información de deficiencias	Todas las deficiencias identificadas que afectan a la capacidad de la entidad para desarrollar e implementar su estrategia y alcanzar sus objetivos establecidos se comunican a aquellas personas en posición de efectuar las acciones necesarias						

	No solo se informa de las transacciones o eventos investigados y corregidos, sino que también se vuelven a evaluar los procedimientos subyacentes potencialmente defectuosos						
	Se establecen protocolos para identificar qué información es necesaria a un nivel determinado para tomar decisiones eficazmente						
	El seguimiento y la revisión se planifican en el proceso de tratamiento del riesgo y se someten a una verificación o una vigilancia regular						
Seguimiento y revisión	La verificación o vigilancia es periódica o eventual, con una frecuencia definida						
	Las responsabilidades del seguimiento y de la revisión están claramente definidas						
	Los procesos de seguimiento y de revisión de la organización abarcan todos los aspectos del proceso de gestión del riesgo, asegurando que los controles son eficaces y eficientes tanto en su						

	diseño como en su utilización						
	Los procesos de seguimiento y de revisión de la organización abarcan todos los aspectos del proceso de gestión del riesgo, obteniendo la información adicional para mejorar la apreciación del riesgo						
	Los procesos de seguimiento y de revisión de la organización abarcan todos los aspectos del proceso de gestión del riesgo, analizando y concluyendo de los sucesos (incluyendo los cuasi-accidentes), cambios, tendencias, éxitos y fallos						
	Los procesos de seguimiento y de revisión de la organización abarcan todos los aspectos del proceso de gestión del riesgo, detectando los cambios en el contexto interno y externo, incluidos los cambios en los criterios de riesgo y en el propio riesgo, que puedan requerir la revisión de los tratamientos de riesgo y de las prioridades e identificar los riesgos emergentes						

	Los resultados se incorporan en la gestión del funcionamiento global de la organización, en su medición y en las actividades externas e internas						
	Los resultados del seguimiento y de la revisión se registran e incluyen en informes internos y externos, según corresponda						
	Los resultados del seguimiento y de la revisión se utilizan como elementos de entrada para la revisión del marco de trabajo de la gestión del riesgo						

7.2. Determinación de brecha con la organización

Para la determinación de la brecha en Geolaquim, se aplica la evaluación de cumplimiento de aspectos claves de modelo integrado de gestión del riesgo, la cual es respondida por el comité de calidad de la organización, compuesto por gerente general, gerente técnico, supervisor de calidad, supervisor de laboratorio, jefe de informática y jefe de administración.

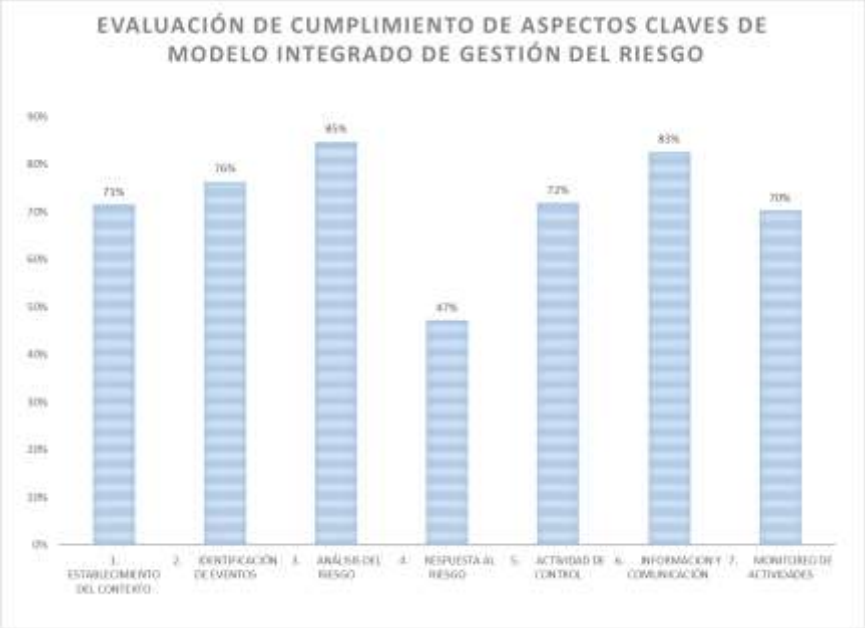
Se determina la brecha en base a cada componente y aspecto clave del modelo, dando como resultado un 72% de cumplimiento de los aspectos claves del modelo integrado de gestión del riesgo.

Mayor debilidad en el sistema se encuentra en el componente de respuesta al riesgo, donde el tratamiento al riesgo es el aspecto de preocupación para la mejora de la gestión de riesgos.

A continuación, se muestra tabla de resultados de la evaluación y gráfico con los siete componentes y su evaluación final.

TABLA DE RESULTADOS EVALUACIÓN DE CUMPLIMIENTO DE ASPECTOS CLAVES		
1. ESTABLECIMIENTO DEL CONTEXTO		**71%**
1.1. CONTEXTO INTERNO		
Filosofía de la gestión de riesgos	79%	
Riesgo aceptado por la empresa	75%	
Gestión de Riesgo	69%	
Dirección de la empresa	86%	
Consejo de administración de la empresa	75%	
Integridad y Valores éticos de la empresa	50%	
Compromiso con la competencia	75%	
Estructura Organizada	63%	
Delegación de autoridad y responsabilidad (dentro de la empresa)	63%	
Norma de recursos humanos	58%	
1.2. CONTEXTO EXTERNO		
Entorno externo	40%	
Objetivo de las partes interesadas externas	50%	
Requisitos legales y reglamentarios	100%	
1.3. CONTEXTO DEL PROCESO DE RIESGO		
Objetivos estratégicos de la empresa	92%	
Objetivos conexos de la empresa	75%	
Objetivos seleccionados de la empresa	75%	
Riesgo aceptado por la empresa	100%	
Tolerancia al Riesgo	75%	
Criterios de Riesgo	100%	
Contexto de los objetivos de la empresa respecto al riesgo	64%	
2. IDENTIFICACIÓN DE EVENTOS		**76%**

Identificación del riesgo	70%	
Factores influyentes	100%	
Técnicas de identificación de eventos	75%	
Interdependencias	100%	
Distinción entre riesgos y oportunidades	75%	
3. ANÁLISIS DEL RIESGO		**85%**
Riesgo inherente y residual	92%	
Estimación de probabilidad e impacto	86%	
Técnicas de evaluación	82%	
Relaciones entre los eventos	75%	
4. RESPUESTA AL RIESGO		**47%**
Evaluación de posibles respuestas	94%	
Respuestas seleccionadas	63%	
Tratamiento del riesgo	34%	
Perspectiva de cartera de riesgos	88%	
5. ACTIVIDAD DE CONTROL		**72%**
Integración con la respuesta a los riesgos	50%	
Tipos de actividades de control	75%	
Políticas y procedimientos	92%	
Controles informáticos	75%	
6. INFORMACION Y COMUNICACIÓN		**83%**
Información	70%	
Comunicación	91%	
7. MONITOREO DE ACTIVIDADES		**70%**
Evaluaciones independientes	81%	
Información de deficiencias	56%	
Seguimiento y revisión	72%	
TOTAL DE CUMOLIMIENTO DE GEOLAQUIM		**72%**



7.3. Estrategia de aplicación del nuevo sistema de control de gestión de riesgos en Geolaquim

ESTRATEGIA DE APLICACIÓN	
1. ESTABLECIMIENTO DEL CONTEXTO	
1.1. CONTEXTO INTERNO	
Filosofía de la gestión de riesgos	• Mejorar filosofía de la gestión del riesgo de la empresa, de manera que incluya una declaración clara de las convicciones de la empresa de cómo se contempla el riesgo. • La filosofía debe ser un documento publicado, comunicado y conocido

	por toda la organización, se debe generar evidencia de ello. • Establecer un plan de acción de cumplimiento de la filosofía de gestión de riesgos a todo nivel de la organización.
Riesgo aceptado por la empresa	• Incorporar en la filosofía el riesgos aceptado según el estilo operativo de la empresa, ya que esté tiene una estrecha relación con la cultura de ella.
Gestión de Riesgo	• Incorporar aspectos de la cultura de la empresa en el proceso de gestión del riesgo. • Definir el alcance de la aplicación de la gestión de riesgos de la empresa, en cuento a que proyectos, actividades y/o procesos incorpora. • Establecer un programa de revisión frecuente de oportunidades presentes en línea con la estrategia de la organización que permitan un mejoramiento en la gestión de riesgo.
Dirección de la empresa	• Definir, declarar y comunicar las partes interesadas de la empresa, y sus relaciones con ellas, de manera que sean incluidas en el proceso de gestión de riesgo.

Consejo de administración de la empresa	• Incorporar al consejo administrativo a lo menos un miembro asesor externo permanente con participación activa, que permita tener otro punto de vista del sistema y sobre todo con la autoridad de supervisión.
Integridad y Valores éticos de la empresa	• Establecer una planificación de capacitación o charlas que permitan una frecuencia definida en la comunicación a los distintos nivel de ls organización sobre valores ético, integridad, filosofía, sanciones, acciones disciplinarias, canales de comunicación formales, etc.
Compromiso con la competencia	• Realizar una revisión que todos los cargos se encuentre con su perfil de competencias actualizado y en línea con la estrategia y el proceso de gestión de riesgo.
Estructura Organizada	• Mejorar las líneas de información y comunicación de la estructura organizacional de la empresa, de maneras que sean más eficaces.
Delegación de autoridad y responsabilidad (dentro de la empresa)	• Formalizar y documentar la delegación de autoridad y responsabilidad, que quede claramente definida, conocida y comunicada a todos los niveles de la organización, y su relación con los objetivos de la organización.

Norma de recursos humanos	• Establecer, documentar y comunicar formalmente las normas de recurso humanos referente a evaluación, promoción, compensación y acciones correctoras.
1.2. CONTEXTO EXTERNO	
Entorno externo	• Establecer el entorno social y cultural a nivel local y regional que afecte a la empresa en su proceso de gestión del riesgo. • Establecer los factores y tendencias claves del entorno externo que afectan a los objetivos de la empresa.
Objetivo de las partes interesadas externas	• Establecer cuáles son las partes interesadas externas que afectan el proceso de gestión de riesgo de la empresa y su relación.
Requisitos legales y reglamentarios	
1.3. CONTEXTO DEL PROCESO DE RIESGO	
Objetivos estratégicos de la empresa	• Realizar una revisión por parte de la dirección, si están considerados todos los riesgos y sus implicaciones inherentes a la estrategia de la empresa.
Objetivos conexos de la empresa	• Establecer y definir objetivos específicos en los niveles operativos de la organización, en relación a los objetivos principales del sistema de gestión.

Objetivos seleccionados de la empresa	• Revisar que todos los objetivos estratégicos sean consecuentes con el riesgo aceptado en el sistema de gestión.
Riesgo aceptado por la empresa	
Tolerancia al Riesgo	• Revisar y evaluar que los objetivos estratégicos y conexos en todos los niveles dela empresa sean de preferencia medidos cuantitativamente.
Criterios de Riesgo	
Contexto de los objetivos de la empresa respecto al riesgo	• Especificar los recursos requeridos para el cumplimiento de los objetivos de la empresa en todos niveles de la organización. • Establecer claramente el alcance de todas las actividades de la gestión del riesgo. • Documentar y evidenciar el proceso de gestión del riesgo de actividades o proyectos nuevos de la empresa, donde quede claramente definido objetivos, alcance proceso, funciones, responsabilidades, recursos, tiempos, etc. • Documentar las metodologías de apreciación del riesgo, de manera de unificar el método en toda la organización. • Definir y documentar la metodología para la evaluación del

	desempeño y eficacia de la gestión de riesgo.
2. IDENTIFICACIÓN DE EVENTOS	
Identificación del riesgo	• Establecer en la metodología de identificación del riesgo, que la aprobación final de la lista de riesgos sea realizada por el comité de calidad o consejo de administración del sistema, de manera que no queda dua que se espusieron todos los aspectos relevantes en relación al logro de los objetivos a todo nivel de la organización. • Identificar riesgos que estén fuera del control de la organización y afecten al logro de los objetivos de la empresa. • Identificar los riesgos en relación con objetivos específicos de niveles operativos de la empresa, se debe trabajar en el efecto cascada de los objetivos y riesgos inherentes.
Factores influyentes	
Técnicas de identificación de eventos	• Establecer y documentar una metodología única para la identificación de los riesgos en todos los niveles de la organización. • Definir un plan de capacitación permanente sobre la identificación de los riesgos.

Interdependencias	
Distinción entre riesgos y oportunidades	• Establecer y documentar una metodología para la identificación riesgos provenientes de oportunidades que impacten a la estrategia y los objetivos de la empresa. Además, establecer frecuencia de revisión de ello.
3. ANÁLISIS DEL RIESGO	
Riesgo Inherente y residual	• Establecer y documentar una metodología para el análisis del riesgo residual, que considere una planificación para la revisión de este riesgo, frecuencia y responsables.
Estimación de probabilidad e impacto	• Definir el horizonte de tiempo para la evaluación de los riesgos, en consecuencia, con la estrategia de la empresa.
Técnicas de evaluación	• Establecer en la técnica de evaluación de los riesgos, lo siguiente: o Recursos disponibles para el tratamiento del riesgo o Medición cuantitativa del riesgo o Evaluación compuesta de riesgos, con mediciones cuantitativas y considerando interdependencia de riesgos en las distintas áreas

	○ Prioridad para el tratamiento del riesgo
Relaciones entre los eventos	
4. RESPUESTA AL RIESGO	
Evaluación de posibles respuestas	
Respuestas seleccionadas	• Establecer en la metodología de respuesta al riesgo, que se analicen los riesgos adicionales de consecuencia del tratamiento del riesgo.
Tratamiento del riesgo	• Establecer en la metodología de respuesta al riesgo, el tratamiento de los riesgos, considerando: ○ El tratamiento de los riesgos residuales y su análisis de la tolerancia del riesgo. Etapas. ○ La evaluación de la eficacia del tratamiento del riesgo ○ Análisis de costo/beneficio de la opción de tratamiento seleccionada. ○ Impacto del tratamiento en partes interesadas ○ Plan de tratamiento de riesgos con priorización de implementación ○ Tratamiento de riesgos secundario ○ Razones o justificación de la selección del tratamiento del riesgo

	○ Responsabilidades y autoridad para el tratamiento de riesgos y su implementación ○ Necesidades de recursos para la implementación del tratamiento del riesgo y posibles contingencias ○ Evaluación del desempeño y eficacia del tratamiento del riesgo ○ Seguimiento de la implementación del tratamiento y su planificación y programación de realización.
Perspectiva de cartera de riesgos	
6. ACTIVIDAD DE CONTROL	
Integración con la respuesta a los riesgos	• Establecer una metodología para las actividades de control y seguimiento, que aseguren la implementación del tratamiento del riesgo
Tipos de actividades de control	• Establecer una metodología aplicada a todos los niveles de la organización para unificar los tipos de actividades de control según el origen del riesgo.
Políticas y procedimientos	

Controles informáticos	• Incorporar el sistema de gestión de riesgos al actual sistema informático del sistema de gestión de calidad, de manera de integrar los sistemas y mejorara el acceso a la información documental.
6. INFORMACION Y COMUNICACION	
Información	• Establecer una programación única de todo el sistema de gestión de riesgos que facilite el acceso a la información, tiempos, frecuencias, controles, responsabilidades, etc. Y permita un oportuno flujo de información para la toma de decisiones.
Comunicación	• Establecer canales de comunicación independientes de lo formal establecido que permita canalizar información relevante a la gerencia.
7. MONITOREO DE ACTIVIDADES	
Evaluaciones independientes	• Establecer en la metodología de monitoreo de actividades, las deficiencias informadas de fuentes externas, con su tratamiento y acciones correctivas necesarias.
Información de deficiencias	• Establecer frecuencia definida para el monitoreo y verificación en cada actividad y nivel de la organización
Seguimiento y revisión	• Establecer responsabilidades del seguimiento y revisión de los

	riesgos, por cada nivel de la empresa. • Medir eficacia y eficiencia del control y seguimiento de la gestión de los riesgos

7.4. Ventajas y Desventajas del nuevo modelo propuesto

En el nuevo modelo integrado de gestión de riesgo presentado en esta investigación, se puede ver las siguientes ventajas y desventajas de su aplicación en la organización:

Ventajas

- Considera la combinación de dos herramientas desarrolladas para la gestión del riesgo muy utilizadas y bien consideradas, en el mundo financiero COSO y en el mundo producción ISO 31000, lo que permite aplicar el nuevo modelo a toda la organización desde líneas estratégicas hasta líneas operativas o productivas.
- El cuestionario que se presenta como evaluación de brechas entre el modelo y la organización es amigable de fácil interpretación y respuesta, además que cubre aspectos internos y externos de la organización.
- El modelo de gestión de riesgos se encuentra alineado con la visión de riesgos incorporada en la ISO 9001:2015, lo que permite a la organización integración de normas con mayor facilidad, así cumplir con los requisitos de manera ágil y práctica.
- El nuevo modelo de gestión de riesgos es un punto de partida importante para la generación de nuevos estudios, sobre todo con la aplicación en distintas empresas o organizaciones.

Desventajas

- La validación del instrumento de evaluación de brecha del modelo de gestión de riesgos es una debilidad importante en esta investigación al ser solo aplicado a una empresa.
- Falta la aplicación del modelo de gestión de riesgos en más de una empresa, de manera de validar el modelo y permita realizar una velicación de eficacia de la aplicación a las organizaciones.

8. Conclusiones

En vista de la importancia que reviste hoy en dia la gestión de riesgos para las empresas y la necesidad que existe de implementar una gestión de riesgos efectiva e integrada a los procesos estratégicos y operativos de la organización, es que fue propuesto, en esta investigación, el diseño de un nuevo modelo de control de gestión de riesgos y su aplicación en la empresa Geolaquim. Lo cual se realizó con la integración de dos sistemas internaciones de gestión de riesgo COSO ERM e ISO 31000, permitiendo lograr la anhelada seguridad razonable en la empresa, esto por la implementación de un eficiente sistema de gestión de riesgos, alineado con la estrategia y objetivos.

Al complementar e integrar ambos sistemas en el nuevo modelo de gestión de riesgos, permitió a la empresa, un control de gestión de riesgos con un enfoque en la estrategia y robusto, debido a COSO ERM, y con un enfoque en los procesos, simple y practico, debido a la ISO 31000.

Al tener un enfoque en la estrategia y en los procesos, permitió lograr gestionar los riesgos estratégicos con mayor profundidad en función de los objetivos de la empresa, asegurando con ello, evitar que se refuercen las debilidades, que se desarrollen las amenazas del entorno, que no se aprovechen las oportunidades y que se pierdan las fortalezas de la organización, y alcanzar todos los niveles de la organización logrando una interrelación e interactuación entre las actividades de los procesos de la empresa.

Al ser robusto y simple, permitió lograr una gestión de riesgos con un enfoque proactivo y de cumplimiento o control, práctico y flexible, que entregó una metodología apropiada para identificar, analizar, documentar, evaluar, controlar y monitorear los eventos de riesgo estratégicos y de todos los procesos de la organización, además, de un sistema de gestión de riesgos, sobre la base de un lenguaje común y lineamientos claros y entendibles por toda la empresa.

Por lo tanto, se demuestra que la integración de ambos sistemas internacionales de gestión de riesgos, COSO ERM e ISO 31000, permite lograr el objetivo principal de esta investigación.

Además, de entregar una herramienta a la empresa Geolaquim, para gestionar sus riesgos y mejorar sus prácticas para diseñar, documentar e implantar, controles eficaces y eficientes orientados a reducir los riesgos estratégicos y sobre todo sobre la base de un mejoramiento continuo.

9. Bibliografía

Libro con editor:

AENOR. (Ed). (2010). ISO 31000 Gestion del Riesgo, Principios y directrices. Madrid, España: AENOR

Versión electrónica de libro impreso:

Abella, R (2006). COSO II y la gestión integral de riesgos del negocio. Recuperado de https://www.estrategiafinanciera.es

Ambrosone, M (2007). La administración del riesgo empresarial: una responsabilidad de todos – el enfoque COSO. Recuperado de http://ayhconsultores.com

Committee of Sponsoring Organization of the Treadway Commission (2009). Gestión de Riesgos Corporativos, Marco Integrado. Recuperado de https://issuu.com/opvallar/docs/coso_erm_-_resumen_marco_integrado

Páginas web:

Avila, I. A. (2015). Gestión del riesgo operacional. Recuperado de http://slideplayer.es/slide/8046030/

Mora, C. (2009). Gestión de riesgos corporativos, marco integrado. Recuperado de http://www.econ.unicen.edu.ar

Valdivieso, C. (2014). CLAIN 2014 , Principales cambios en relación a coso 1992 y su uso en la evaluación del control interno. Recuperado de http://aechile.cl/wp-content/uploads/2014/

Valdivieso, C. (2014). COSO ERM anuncio de actualización. Recuperado de http://aechile.cl/2014/10/29/coso-erm-anuncio-de-actualizacion/

Código de campo cambiado