Trabajo Monográfico para la obtención del Título de Contador Público
Facultad de Ciencias Económicas y Administración – Universidad de la República

Administración de riesgos – una visión global y moderna

Autores:
Gastón Bueno
Cecilia Correa
Juan Ignacio Echeverry

Orientador: Cr. Luis Sauleda

Marzo 2010

INDICE

AS/NZS 4360:2004 - Administración de Riesgos

BS 31100: Código de prácticas para la Administración de Riesgos

ISO 31000:2009 Gestión de riesgos – principios y directrices

AGRADECIMIENTOS

Queremos expresar nuestro agradecimiento a nuestro coordinador, Cr. Luis Sauleda, por su orientación en la realización del presente trabajo de investigación monográfico, su guía para la obtención del material de referencia y el tiempo dedicado.

Por otra parte también queremos agradecer a nuestros familiares y amigos, por acompañarnos y apoyarnos a lo largo de nuestra carrera.

RESUMEN EJECUTIVO

Los actuales problemas y la realidad del contexto mundial han llevado a las organizaciones a prestar más atención a su gestión de riesgos, considerándola uno de los factores claves para el éxito. En los últimos años han surgido en diversas partes del mundo innumerables estándares nacionales e internacionales buscando lograr un entendimiento global sobre la forma más eficaz de realizarlo.

El objetivo de nuestro trabajo es analizar el estado del arte en la materia procurando componer una visión moderna, revisando las tendencias mundiales hacia una mirada integral de administración, enfatizando la importancia del sistema de gestión de riesgos dentro de la empresa y los beneficios que su implementación puede traer y que aún muchas empresas no han logrado percibir o comprender.

Es así que realizamos un análisis comparativo de los distintos marcos estudiados, procurando presentar los conceptos y prácticas innovadoras para acercarnos a una concepción más actualizada en la materia. Dicha comparación se centra en la evolución de las definiciones y alcances, el proceso de administración de riesgos en sí y sus etapas, y los principios establecidos tanto en los estándares como en otros lineamientos internacionales.

Entendemos conveniente que desde el ámbito académico y profesional se aborde la tarea de difundir los estándares y las ventajas de utilizar esta herramienta por parte de las empresas, enfatizando que la ecuación costo beneficio en el corto o largo plazo es favorable porque la administración integral de riesgos permite a los empresarios evitar o mitigar erogaciones extraordinarias originadas por el surgimiento de circunstancias o situaciones adversas que ellos mismos pueden gestionar.

CAPITULO I: INTRODUCCIÓN Y OBJETIVOS

En el contexto actual del mundo de los negocios, a partir de las sucesivas crisis económicas y financieras de los últimos tiempos, resulta evidente que *nadie está ajeno al riesgo empresarial*, sin importar tamaño, tipo y composición de las organizaciones.

Los negocios operan y operarán en un entorno totalmente distinto a lo que era hace quince años. La globalización de los mercados y las nuevas estrategias competitivas y de expansión impulsadas por los vertiginosos avances de la tecnología; las reestructuraciones organizacionales, las privatizaciones y asociaciones, y el outsourcing de procesos como respuestas habituales a esas nuevas realidades; la constante búsqueda y generación de los nuevos productos materiales e inmateriales así como los grandes proyectos de inversión extranjera y nacional y las nuevas tendencias de financiación, producción y consumo, generan, todos ellos, riesgos inherentes, sean normales o extraordinarios, muchos de los cuales nunca se pensó que pudieran afectar a las organizaciones empresariales privadas o públicas. [1]

Los actuales problemas llevan a las organizaciones a prestar más atención a su gestión de riesgos, considerando la administración de los riesgos como uno de los factores claves para el éxito.

El objetivo de nuestro trabajo es analizar el estado del arte en la materia procurando componer una visión moderna de la gestión de riesgo empresarial, revisando las tendencias mundiales hacia una mirada integral de administración, enfatizando la importancia del sistema de gestión de riesgos dentro de la empresa y los beneficios que su implementación puede traer y que aún muchas empresas no han logrado percibir o comprender.

Con este propósito, desarrollaremos el trabajo según indicamos a continuación:

En primer término, describiremos el enfoque tradicional de riesgo empresarial del Comité de las Organizaciones Patrocinadoras de la Comisión[2], a raíz de la publicación del informe Administración de Riesgos Corporativos – Marco Integrado (ERM)[3].

[1] http://www.javeriana.edu.co/fcea/pos_contaduria/III_revisoria_fiscal/ponencia_rodrigo_estupinan_u_rosario.pdf

[2] Treadway Sponsoring Organizations of the Treadway Commission, en adelante COSO

A continuación nos ocuparemos de otros estándares que tratan del tema. Abordaremos el concepto de gestión empresarial según los siguientes documentos, ordenados en orden cronológico de aparición:

- ✓ Marco de Administración Integrada de Riesgo[4] del gobierno canadiense, cuya primera versión fue en 1997 y la segunda publicación fue en el año 2001,
- ✓ Estándares de Gerencia de Riesgos[5] del Reino Unido, del año 2002,
- ✓ *AS/NZS 4360:2004 - Administración de Riesgos* [6] de los gobiernos de Australia y Nueva Zelanda. Si bien la primera versión fue en 1995, tomamos en nuestro análisis la versión del 2004,
- ✓ BS 31100: Código de prácticas para la Administración de Riesgos[7] del Grupo BSI[8], publicado en octubre 2008,
- ✓ ISO 31000:2009 Gestión de riesgos – principios y directrices[9], del Instituto Internacional de Normalización[10], emitido en noviembre de 2009.

En la tercer parte realizaremos una comparación analítica de los documentos, centrándonos en la evolución del concepto de riesgo y administración de riesgos, las semejanzas y diferencias establecidas en el proceso y otros aspectos a destacar en cada uno.

También analizaremos la vinculación del enfoque de administración de riesgos con los lineamientos de Basilea II y los principios de Gobierno Corporativo, ya que entendemos que están estrechamente relacionados.

Finalmente, presentaremos las conclusiones y recomendaciones resultantes del análisis precedente.

[3] www.coso.org, Enterprise Risk Management - Integrated Framework, en adelante ERM
[4] Integrated Risk Management Framework, en adelante estándar canadiense o IRMF , su siglaen inglés
[5] A Risk Management Standard - AIRMIC, ALARM, IRM: 2002, en adelante ALARM
[6] AS/NZS 4360:2004: Risk Management, en adelante AS/NZS 4360
[7] BS 31100: Code of practice for risk management, en adelante BS 31100
[8] www.bsi**group**.com, The **British Standards** Institution o British Group
[9] ISO 31000:2009 Risk management - Principles and guidelines, en adelante ISO 31000
[10] www.**iso**.org International Organization for Standardization, en adelante ISO

CAPITULO II: COSO-ERM: EL DOCUMENTO MADRE

Administración de Riesgos Corporativos – Marco Integrado

Antecedentes y características:[11]

El Marco Integrado ha sido emitido por el Comité de las Organizaciones Patrocinadoras de la Comisión Treadway[12] con la colaboración para su desarrollo de Pricewaterhouse Coopers[13], con el objetivo de ser considerado como un modelo conceptual común para la administración de riesgos corporativos. Dicho marco de referencia facilita a los gerentes la evaluación y el mejoramiento de su capacidad para administrar los riesgos de sus organizaciones.

El referido documento, conocido como ERM surge a través de la necesidad de desarrollar una terminología común y de tratar de integrar los principios ampliamente aceptados para que puedan ser usados por la dirección como una guía para desarrollar una arquitectura eficaz de gestión de riesgos.

A finales de 2001, COSO inició un estudio orientado a ayudar a las organizaciones a administrar los riesgos. A pesar de la abundancia de literatura existente sobre el tema, COSO concluyó que hacía falta diseñar y construir un marco y las correspondientes técnicas de aplicación del tema. Es por esto que PWC fue contratada para dirigir el proyecto, el cual consistió en desarrollar una estructura o marco de referencia que facilitara a los gerentes la evaluación y el mejoramiento de su capacidad para administrar los riesgos de sus organizaciones.

En el mismo, se define el riesgo y la administración de riesgos corporativos, y entrega definiciones básicas, conceptos, categorías de objetivos, componentes y principios de un proceso integral de la administración de riesgos corporativos.

De este modo, proporciona orientación a las empresas y demás organizaciones para determinar cómo mejorar su gestión, facilitando el contexto y facilitando su aplicación en el mundo real.

[11] ERM Resumen Ejecutivo Marco
[12] COSO
[13] www.pwc.com, en adelante PWC

La premisa principal de ERM es que toda entidad existe para proveer valor a sus interesados. Todas las empresas operan en ambientes cambiantes, enfrentando a la incertidumbre sobre el futuro lo que deriva de la incapacidad de determinar la probabilidad de ocurrencia de eventos inciertos, así como de las consecuencias asociadas; y el desafío para la gerencia es determinar cuanta incertidumbre la entidad está dispuesta a aceptar en su esfuerzo por aumentar el valor para sus grupos de interés[14].

La incertidumbre presenta para la empresa, tanto riesgos como oportunidades, los cuales pueden generar deterioro o crecimiento del valor. ERM provee un marco que permite a la empresa poder manejar eficazmente la incertidumbre y los riesgos y oportunidades asociados, de manera de aumentar su capacidad de generar valor.

La incertidumbre proviene de la dificultad de determinar con precisión la probabilidad de ocurrencia de acontecimientos eventuales y sus consecuencias asociadas.[15]

La incertidumbre también se presenta como consecuencia de las decisiones estratégicas de la entidad. Dichas decisiones presentan tanto riesgo como oportunidades, relacionadas con el ambiente en que operan (entorno político, recursos, mercados, canales). Las decisiones adoptadas por la empresa hacen que el valor sea creado, preservado o deteriorado. El valor es maximizado cuando la estrategia y los objetivos administrativos alcanzan armonizar el crecimiento, retorno, y riesgo.

La creación de valor se produce a través de la correcta utilización de los recursos, incluyendo personas, capital y tecnología. Es por esto que las empresas reconocen el valor cuando los interesados obtienen beneficios reconocibles que ellos a su vez valoran.

Ninguna empresa opera en un ambiente libre de riesgos, y el ERM no crea tal ambiente. ERM permite a los administradores operar más eficazmente en un ambiente pleno de riesgos.

[14] El término “grupos de interés” estaría refiriéndose a lo que en inglés definen como Stakeholders
[15] www.ccee.edu.uy, **Administración del riesgo empresarial**, material publicado por la cátedra de Control Interno, año 2005

El ERM proporciona a las empresas la habilidad para[16]:

• *Alinear el apetito de riesgo[17] con la estrategia:*

El apetito de riesgo, es el grado de riesgo que una empresa tiene voluntad de aceptar en la persecución de sus metas; puede ser establecido con relación a la organización como un todo, para diferentes grupos de riesgos o en un nivel de riesgo individual.

Hablamos de apetito de riesgo de una empresa en primer lugar cuando evalúa alternativas estratégicas, después cuando establece los objetivos alineados con la estrategia seleccionada y finalmente cuando desarrolla mecanismos para manejar los riesgos relacionados.

Por tanto la empresa debe de establecer los riesgos por los cuales tiene interés, cuál va a ser su tolerancia a los mismos, y cómo va a administrarlos para proveer una razonable seguridad acerca del cumplimiento de los objetivos establecidos. Se considera el interés por asumir riesgos al evaluar las alternativas estratégicas, al establecer los objetivos (alineándolos con la estrategia seleccionada) y al desarrollar mecanismos para gestionar los riesgos correspondientes.

La tolerancia por el riesgo es el nivel aceptable de variación relativa al logro de los objetivos. Al establecer la misma, se considera la importancia de los objetivos relacionados y alinea las tolerancias de riesgo con su interés por el riesgo. Operar dentro de la tolerancia al riesgo, provee mayor seguridad de que la empresa permanecerá dentro de su interés por el mismo y mayor seguridad de que la empresa logrará sus objetivos.

• *Vincular crecimiento, riesgo y retorno:*

Las empresas aceptan el riesgo como parte de la creación y conservación del valor, y esperan retornos en proporción a los riesgos. El ERM aumenta la capacidad de las empresas para identificar y valorar al riesgo, establecer niveles aceptables de riesgos relativos al crecimiento y las ganancias objetivo.

[16] www.ccee.edu.uy, **Administración del riesgo empresarial**, material publicado por la cátedra de Control Interno, año 2005
[17] Risk Appetite

• *Mejorar las decisiones de respuesta a los riesgos:*

Aporta la precisión para identificar y seleccionar entre las distintas alternativas de respuestas al riesgo tales como: evitar, reducir, compartir o aceptar el riesgo; proporcionando metodología y técnicas para tomar estas decisiones.

• *Reducir sorpresas y pérdidas operativas:*

En la medida que las empresas aumentan su capacidad de identificar potenciales eventos, estimando los riesgos y estableciendo respuestas, estas irán reduciendo las sorpresas y los costos o pérdidas derivados.

• *Identificar y administrar los riesgos para toda la entidad:*

Todas las empresas enfrentan múltiples riesgos que afectan a las distintas partes de la organización. No solo se necesita gestionar riesgos individuales, sino también comprender los impactos interrelacionados, y los eventos potenciales; y al considerar una amplitud de eventos se gana en la comprensión de cómo ciertos eventos representan oportunidades. El ERM facilita la respuesta efectiva e integrada a los múltiples riesgos e impactos relacionados, y permite soluciones para administrar los riesgos.

• *Proporcionar respuesta integradas para múltiples riesgos:*

Los procedimientos de negocios tienen muchos riesgos inherentes, el ERM posibilita soluciones integradas para manejar esos riesgos.

• *Aprovechar las oportunidades:*

Al considerar una amplia gama de eventos potenciales, una organización no solo debe limitarse a considerar exclusivamente los riesgos, sino también debe identificar los eventos que representen oportunidades.

• *Potenciar el uso de los recursos:*

La obtención de información sólida sobre riesgos permite evaluar eficazmente las necesidades globales de capital y mejorar su asignación.

Estas capacidades están implícitas en la administración de riesgos corporativos, que ayuda a la dirección a lograr los objetivos de rendimiento y rentabilidad de la entidad e impedir la pérdida de recursos. La administración de riesgos corporativos ayuda a asegurar la efectividad de reporte y ayuda a asegurar que las entidades cumplan las leyes y regulaciones, evitando daños a su reputación y consecuencias derivadas.

ERM no es un fin en sí mismo, sino que es un medio importante para alcanzar los objetivos de la organización. No puede operar aisladamente en una entidad, sino que es más bien un medio facilitador del proceso de gestión.

ERM está asociado al Gobierno Corporativo[18] en la medida que provee información a la dirección superior con respecto a los riesgos más significativos y a la forma como los mismos están siendo administrados. También está asociada a la administración del desempeño al proveer medidas ajustadas al riesgo y al control interno, el que es parte integrante de la ERM.

Definición de ERM: [19]

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

Esta definición refleja ciertos conceptos fundamentales:

-ERM es un *proceso,* un conjunto de acciones, es un medio para lograr un fin y no un fin en sí mismo.

-ERM es *realizado por personas* en cada nivel de una organización. No son meramente políticas, encuestas y formularios sino que es un proceso que involucra a la gente en todos los niveles de una organización.

-ERM *es aplicado en la definición de la estrategia.*

[18] Corporate Governance
[19] ERM Resumen Ejecutivo Marco

-ERM es *aplicado en toda la empresa*, en todos los niveles y en todas las unidades e incluye una visión del riesgo a nivel de la entidad.

-ERM está destinada a identificar acontecimientos potenciales que afecten a la entidad y a gestionar los riesgos dentro del nivel de *riesgo aceptado*.

-ERM *proporciona seguridad razonable* a la gerencia y al directorio de una entidad.

-ERM está orientada a la *consecución de objetivos* en una o más categorías separadas pero superpuestas de objetivos.

Proceso

ERM no se define como una situación particular o acontecimiento, sino más bien como una serie de acciones que interactúan con las actividades de una empresa. Dichas acciones están implícitas y fluyen en la forma como la dirección maneja el negocio.

Realizado por personas

Es un proceso realizado por el directorio, la Gerencia y el resto del personal. Es logrado por lo que ellos hacen y dicen. El Comité Ejecutivo lo decide, lo aprueba, y da los grandes lineamientos; la Gerencia da un paso más para aplicarlo, y finalmente, todo el personal, lo lleva adelante.

El ERM afecta las acciones de las personas, reconoce que las mismas no siempre se entienden, comunican o actúan consistentemente. Cada individuo trae a su lugar de trabajo su experiencia pasada y su habilidad técnica, y tiene distintas necesidades y prioridades. Estas realidades afectan y son afectadas por el ERM.

Con el ERM cada persona tiene un único punto de referencia que influye en la forma en cómo identifican, evalúan y responden a los riesgos.

Es aplicado en la definición de la estrategia

Una entidad fija su misión o visión y establece los objetivos estratégicos, que son las metas de alto nivel que están en línea y soporte su misión o visión. Para alcanzar los objetivos estratégicos, la entidad establece una estrategia y también fija los objetivos

conexos que desea realizar y se derivan de ella, amplificándose hacia las unidades de negocio, divisiones y procesos.

ERM se aplica durante el proceso de establecimiento de la estrategia, en la que la dirección contempla los riesgos relacionados con las estrategias alternativas.

Aplicado en toda la empresa

Para aplicar con éxito el ERM, la empresa debe de considerar todo el conjunto de actividades, desde las actividades empresariales, como la planificación estratégica y ubicación de los recursos, hasta las actividades unitarias como el marketing, recursos humanos, procedimientos de producción y estudio del crédito de un nuevo cliente. El ERM también se aplica a proyectos especiales y a nuevas iniciativas que podrían aún no tener un lugar jerárquico o en el diseño organizacional de la empresa.

La administración de riesgos corporativos requiere que una entidad adopte una perspectiva de portafolio de riesgos.

Esto puede involucrar que cada directivo responsable de una unidad de negocio, función, proceso o cualquier actividad desarrolle una evaluación de los riesgos de dicha actividad. La evaluación debe ser cuantitativa o cualitativa. Con una visión compuesta de cada nivel sucesivo de la organización, la alta dirección está en posición de determinar si el portafolio de todos los riesgos de la entidad se corresponde con su apetito de riesgo.

Riesgo aceptado[20]

El riesgo aceptado es el nivel de riesgo que una empresa está dispuesta a aceptar en su búsqueda de valor. Refleja la filosofía de administración de riesgos de la empresa, y por ende, influye en su cultura y estilo operativo. Muchas empresas consideran el riesgo aceptado de manera cualitativa, calificándolo como alto, moderado o bajo, mientras existen otras que adoptan un enfoque cuantitativo, remarcando los objetivos de crecimiento, rendimiento y riesgo.

[20] Risk Appetite

El riesgo aceptado se relaciona directamente con la estrategia de una empresa y se tiene en cuenta para establecerla, ya que diferentes estrategias exponen a una entidad a riesgos distintos. El ERM ayuda a la dirección a elegir una estrategia que alinea la creación anticipada de valor con el riesgo aceptado por la empresa.

El nivel de riesgo aceptado por una entidad orienta la asignación de recursos. La gerencia asigna recursos entre las unidades de negocios tomando en cuenta el nivel de riesgo aceptado por la entidad y la estrategia de las unidades de negocios individuales para generar el rendimiento deseado de los recursos asignados. La gerencia considera su nivel de riesgo aceptado según el mismo sea compatible con su organización, su gente y sus procesos y destina la infraestructura necesaria para responder y monitorear eficazmente los riesgos.

Las tolerancias al riesgo están relacionadas con los objetivos de la empresa. El nivel aceptable de variación con respecto al logro de objetivos determina las tolerancias al riesgo. Al definir tolerancias al riesgo específicas, la dirección considera la importancia relativa de los objetivos relacionados y pone en línea las tolerancias al riesgo con el nivel de riesgo aceptado. El operar dentro de las tolerancias al riesgo permite a la dirección una mayor seguridad de que la empresa permanecerá dentro de su nivel de riesgo aceptado y, a la vez, provee mayor grado de comodidad con respecto a que la empresa logrará sus objetivos.

Proporciona seguridad razonable

Un ERM bien diseñado y operando eficazmente puede proveer a la dirección, razonable seguridad con respecto al logro de los objetivos de la empresa.

A través de la aplicación del ERM en forma eficiente, se puede proveer una razonable seguridad de que: -Los objetivos estratégicos y operacionales están siendo logrados, -Los informes de la empresa son confiables, -Las leyes y regulaciones vigentes están siendo cumplidas.

Consecución de objetivos

El marco de Administración de Riesgos Empresariales está orientado a alcanzar los objetivos de la empresa, a los cuales clasifica en cuatro categorías:

- Estratégicos: objetivos de alto nivel, que están alineados con la misión de la empresa brindándole apoyo.

- Operacionales: vinculados al uso eficaz y eficiente de sus recursos, los que varían en función de las elecciones de una empresa sobre la estructura y desempeño.

- De Reporte: relacionados a la confiabilidad de la información de la empresa, que incluye desde la información interna como la externa, financiera o no financiera.

- De Cumplimiento: objetivos relativos al cumplimiento de la legislación y regulaciones aplicables.

Otra categoría utilizada por otras empresas, es la salvaguarda de los activos. Trata sobre la prevención de pérdidas de activos o recursos de una empresa por robos, despilfarro, ineficiencia o simplemente por decisiones financieras equivocadas.

Componentes de la ERM: [21]

Se plantea en el documento que la ERM consta de ocho componentes interrelacionados, derivados de la manera como la dirección lleva el negocio, que se integran en el proceso de administración. Estos componentes son:

1) Ambiente interno:

El ámbito interno de la entidad, al proveer disciplina y estructura, es el fundamento para todos los demás componentes de la ERM. El ámbito interno influye en la forma como se establecen la estrategia y los objetivos, como se estructuran las actividades de negocios y como se identifican, aprecian y tratan los riesgos, tanto así como influye en el diseño y funcionamiento de las actividades de control, los sistemas de información y comunicación y en el monitoreo de las actividades.

[21] www.ccee.edu.uy, **Administración del riesgo empresarial**, material publicado por la cátedra de Control Interno, año 2005

El ámbito interno comprende muchos elementos, incluyendo valores éticos de la entidad, competencia y desarrollo del personal, estilo operativo de la gerencia y en la forma como ésta asigna responsabilidad y autoridad. El directorio es una parte crítica del ámbito interno e influye significativamente en los otros elementos. Como parte del ambiente interno, la gerencia establece una filosofía gerencial del riesgo, establece el nivel de riesgo aceptado, desarrolla una cultura de riesgo e integra ERM con iniciativas relacionadas.

Una filosofía de ERM que es comprendida por todo el personal aumenta la capacidad de los empleados de reconocer y administrar eficazmente el riesgo. La filosofía – conjunto de creencias y actitudes compartidas de la empresa que caracterizan como se contempla el riesgo y cómo la misma escoge conducir sus actividades y tratar el riesgo – refleja el valor que la entidad procura de la ERM e influye en la forma como los elementos de la ERM serán aplicados. La gerencia comunica su filosofía de ERM a los empleados a través de las declaraciones de políticas y otras comunicaciones. En gran medida, la gerencia refuerza la filosofía no simplemente con palabras, sino también con acciones cotidianas.

El nivel de riesgo aceptado, establecido por la gerencia y revisado por el directorio, es un punto de referencia en la definición de la estrategia ya que el rendimiento deseado de la estrategia debe estar alineado con el riesgo aceptado de la empresa. Generalmente alguna (de entre una cantidad de estrategias diferentes) puede estar destinada a lograr las metas deseadas en cuanto a crecimiento y rendimiento, teniendo cada una diferentes riesgos asociados.

La aplicación de ERM en la definición de la estrategia ayuda a los administradores a seleccionar una estrategia compatible con el nivel de riesgo aceptado. La gerencia procura alinear la organización, la gente, los procesos y la infraestructura para facilitar la implantación de una estrategia exitosa y permitir a la entidad permanecer dentro de su nivel de riesgo aceptado.

La cultura de riesgo es el conjunto de actitudes, valores y prácticas compartidos que delinean la manera como una entidad considera el riesgo en sus actividades cotidianas.

Para muchas compañías, la cultura de riesgo fluye de la filosofía de riesgo y del nivel de riesgo aceptado de la entidad. Para aquellas compañías que no definen explícitamente su filosofía de riesgo, la cultura de riesgo puede construirse al azar, dando lugar a culturas de riesgo significativamente diferentes dentro de una empresa o aún dentro de una unidad operativa, función o departamento en particular.

2) Establecimiento de objetivos:

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

En el contexto de la misión o visión establecidas, la gerencia establece los objetivos estratégicos, selecciona la estrategia y establece los objetivos relacionados fluyendo a través de la empresa y alineados con y ligados a la estrategia. Los objetivos deben existir antes de que la gerencia pueda identificar acontecimientos que eventualmente puedan afectar el logro de los mismos.

Como vimos anteriormente los objetivos de la entidad pueden ser vistos en el contexto de cuatro categorías:

- *Estratégicos*
- *Referidos a las operaciones*
- *Referidos a la elaboración de información*
- *Referidos al cumplimiento*

Esta categorización de los objetivos de la entidad le permite a la gerencia y al directorio centrarse en distintos aspectos de ERM. Estas categorías diferentes pero trasladables – un objetivo particular puede estar comprendido en más de una categoría – abordan diferentes necesidades de la entidad y pueden estar bajo la responsabilidad directa de distintos ejecutivos. Esta categorización también permite distinguir qué es posible esperar para cada una de las categorías de objetivos.

3) Identificación de acontecimientos

Como parte de la identificación de acontecimientos, los administradores consideran factores internos y externos que afectan la ocurrencia de un acontecimiento. Los factores externos incluyen factores *económicos*, *empresariales*, *ambientales*, *políticos*, *sociales* y *tecnológicos*. Los factores internos reflejan las opciones tomadas por la gerencia e incluyen asuntos tales como *infraestructura*, *personal*, *procesos* y *tecnología*.

La identificación de factores internos y externos que impactan en los eventos es útil, a su vez, para una identificación efectiva del evento. Una vez que se han identificado los principales factores contribuyentes, la dirección puede considerar su relevancia y centrarse en los eventos que puedan afectar el logro de los objetivos.

La metodología de identificación de acontecimientos de una entidad puede comprender una combinación de técnicas y herramientas de respaldo. Las técnicas de identificación de acontecimientos están pendientes tanto del pasado como del futuro. Las técnicas que se centran en acontecimientos y tendencias pasados consideran asuntos tales como historias de cesación de pagos, cambios en los precios de los productos comercializables[22] y pérdidas de tiempo provocadas por accidentes. Las técnicas que se centran en futuros posibles escenarios consideran asuntos tales como cambios demográficos, nuevos mercados y acciones de los competidores.

Puede ser útil agrupar los eventuales acontecimientos en categorías. Agrupando los acontecimientos horizontalmente a través de una entidad y verticalmente entre unidades operativas, la gerencia puede comprender las interrelaciones entre los acontecimientos, obteniendo mayor y mejor información como base para la apreciación de riesgos.

Los acontecimientos pueden tener eventualmente un impacto positivo, uno negativo o ambos. Los acontecimientos que tienen un impacto eventualmente negativo representan riesgos que requieren apreciación y respuesta de la gerencia. En función de ello, riesgo es definido como la posibilidad de que ocurra un acontecimiento y que afecte adversamente el logro de objetivos.

[22] Commodities

Los acontecimientos con un impacto eventualmente positivo representan oportunidades o reducción del impacto negativo de riesgos. Los acontecimientos que representan oportunidades son canalizados hacia los procesos gerenciales de definición de la estrategia o de los objetivos, a efectos de que puedan formularse acciones para aprovechar las oportunidades. Los acontecimientos que eventualmente reduzcan el impacto negativo de los riesgos son considerados en la apreciación de y respuesta a los riesgos por parte de la gerencia.

4) Apreciación de riesgos

La apreciación de riesgos permite a una entidad considerar cómo los acontecimientos eventuales podrían afectar el logro de los objetivos. La gerencia aprecia los acontecimientos desde dos perspectivas: probabilidad e impacto.

La probabilidad representa la posibilidad de que un acontecimiento dado ocurra, mientras que el impacto representa su efecto en caso de que ocurriera. Las estimaciones de probabilidad e impacto de riesgo a menudo son determinados usando datos sobre acontecimientos pasados observables, los que pueden proveer una base más objetiva que las estimaciones exclusivamente subjetivas. Los datos generados internamente basados en la propia experiencia de una entidad pueden reflejar menos prejuicios personales subjetivos y proveer mejores resultados que datos de procedencia externa.

Sin embargo, aún cuando los datos generados internamente son un insumo importante, los datos externos pueden ser útiles como un punto de control o para fortalecer el análisis. Los usuarios deben ser cautelosos cuando utilizan acontecimientos pasados para hacer predicciones sobre el futuro ya que los factores que influyen en los acontecimientos cambian con el transcurso del tiempo.

La metodología de apreciación del riesgo de una entidad normalmente comprende una combinación de técnicas cuantitativas y cualitativas. La gerencia a menudo utiliza técnicas de apreciación cualitativa cuando los riesgos no se prestan a la cuantificación o cuando los datos confiables y en cantidad suficiente requeridos para la apreciación cuantitativa no están en la práctica disponibles o cuando el proceso de obtención y análisis de datos no es costo-beneficioso. Las técnicas cuantitativas normalmente tienen más precisión y son utilizadas en actividades más complejas y sofisticadas para

complementar las técnicas cualitativas. No es necesario que una entidad utilice técnicas de apreciación comunes en todas las unidades de negocios. Por el contrario, la elección de técnicas debe reflejar la necesidad de precisión y la cultura de la unidad de negocios.

En cualquier caso, los métodos utilizados por las unidades de negocios individuales deben facilitar la apreciación global de los riesgos de la entidad.

La gerencia a menudo utiliza medidas de desempeño para determinar el grado en que los objetivos están siendo alcanzados. Puede ser útil utilizar la misma unidad de medida al considerar el impacto eventual de un riesgo en el logro de un objetivo específico.

Cuando existen cadenas de acontecimientos que se combinan e interactúan dando lugar a probabilidades e impactos significativamente distintos, la gerencia puede apreciar cómo se relacionan los acontecimientos. Mientras que el impacto de un acontecimiento aislado podría ser leve, una secuencia de acontecimientos podría tener un impacto más significativo. En caso que los acontecimientos eventuales no estén directamente relacionados, la gerencia los aprecia individualmente; en caso que la ocurrencia de riesgos sea probable en múltiples unidades de negocios, la gerencia puede apreciar y agrupar los acontecimientos identificados en categorías comunes.

Existe normalmente un rango de posibles resultados asociados a un acontecimiento eventual y la gerencia los considera como una base para desarrollar una respuesta al riesgo. A través de la apreciación del riesgo, la gerencia considera las consecuencias positivas y negativas de los acontecimientos eventuales, individualmente o por categoría, a través de la entidad.

La apreciación de riesgos es aplicada en primera instancia al riesgo inherente – el riesgo para la entidad en ausencia de cualesquiera acciones que la gerencia podría tomar para modificar la probabilidad del riesgo o su impacto. Una vez que se han desarrollado las respuestas al riesgo, la gerencia utiliza técnicas de apreciación de riesgo para determinar el riesgo residual – el riesgo remanente luego de la acción de la gerencia para modificar la probabilidad o impacto del riesgo.

5) Respuesta al riesgo

La gerencia identifica opciones de respuesta al riesgo y considera su efecto sobre la probabilidad y el impacto del acontecimiento, con relación a las tolerancias al riesgo y a la relación costo-beneficio y diseña e implanta opciones de respuesta. La consideración de respuestas al riesgo y la selección e implantación de una respuesta al riesgo integran la ERM. Una ERM eficaz requiere que la gerencia seleccione una respuesta de la que pueda esperarse que coloque a la probabilidad del riesgo y a su impacto dentro de la tolerancia al riesgo de la entidad.

Las respuestas al riesgo corresponden a las categorías de evitar, reducir, compartir y aceptar el riesgo. Las respuestas "evitar" actúan para abandonar las actividades que generan riesgos. Las respuestas "reducir" reducen la probabilidad del riesgo, el impacto del mismo o ambos. Las respuestas "compartir" reducen la probabilidad o el impacto del riesgo transfiriendo o compartiendo de otro modo una porción del riesgo. Las respuestas "aceptar" no actúan de forma alguna para modificar la probabilidad o el impacto del riesgo. Como parte de la ERM, una entidad considera las eventuales respuestas para cada riesgo significativo a partir de un rango de categorías de respuestas. Esto le otorga suficiente profundidad a la selección de respuestas y también desafía el "status quo".

Luego de haber seleccionado una respuesta al riesgo, la gerencia vuelve a medir el riesgo sobre una base residual. El riesgo es considerado desde una perspectiva conjunta.

La gerencia puede adoptar un enfoque en el cual el gerente responsable de cada departamento, función o unidad operativa desarrolle una apreciación compuesta de riesgos y respuestas al riesgo para esa unidad. Esta visión refleja el perfil de riesgo de la unidad con relación a sus objetivos y a sus tolerancias al riesgo. Con una visión del riesgo para unidades individuales, se designa al gerente con mayor experiencia en la empresa para que adopte una visión conjunta, para determinar si el perfil de riesgo de la entidad está en consonancia con su nivel global de riesgo aceptado en relación con sus objetivos.

La gerencia debe reconocer que siempre existe algún nivel de riesgo residual, no sólo porque los recursos son limitados sino también por la incertidumbre sobre el futuro y las limitaciones inherentes a todas las actividades.

6) Actividades de control

Las actividades de control son las políticas y procedimientos que ayudan a asegurar que las respuestas al riesgo sean ejecutadas adecuadamente. Las actividades de control tienen lugar en toda la organización, a todos los niveles y en todas las funciones. Las actividades de control son parte del proceso a través del cual una empresa procura lograr sus objetivos de negocios. Generalmente involucran dos elementos: una política estableciendo qué debe hacerse y los procedimientos para ejecutar la política.

La confianza generalizada en los sistemas informáticos hace necesarios los controles sobre los sistemas significativos. Se pueden utilizar dos grandes grupos de actividades de control sobre los sistemas informáticos. El primero se refiere a controles generales, los que se aplican a muchos sino a todos los sistemas de aplicación y ayudan a asegurar su continua y adecuada operación. El segundo se refiere a los controles sobre aplicaciones, los que incluyen pasos computarizados dentro de los programas informáticos de la aplicación para controlar la tecnología de la misma. Combinados con otros controles procesados en forma manual, en caso de ser necesarios, estos controles aseguran la integridad, exactitud y validez de la información.

Debido a que cada entidad posee su propio conjunto de objetivos y enfoques de implantación, existirán diferencias en objetivos, estructura y actividades de control relacionadas. Aunque dos entidades tuvieran objetivos y estructuras idénticos, sus actividades de control probablemente serían diferentes. Cada entidad es gestionada por personas diferentes que en el momento de efectuar control interno, utilizan sus juicios individuales. Además, los controles reflejan el entorno y el ramo de actividad en los cuales las entidades operan así como la complejidad de su organización, su historia y su cultura.

7) Información y comunicación

La información apropiada debe ser identificada, capturada y comunicada de un modo y en un marco temporal que le permita al personal cumplir con sus cometidos. La comunicación eficaz también se realiza en un amplio sentido, fluyendo hacia abajo, hacia arriba y hacia los costados en la entidad. También existe comunicación eficaz e intercambio de información importante con terceros, tales como consumidores, proveedores, reguladores y "grupos de interés".

Se necesita información en todos los niveles de una organización para identificar, apreciar y responder a los riesgos y para administrar la entidad y lograr sus objetivos. Se utiliza una variedad de información, importante para una o más categorías de objetivos.

La información proviene de varias fuentes – externa e interna y en forma cuantitativa y cualitativa – y permite respuestas de ERM a condiciones cambiantes en tiempo real. El desafío para la gerencia consiste en procesar y refinar grandes volúmenes de datos en información utilizable. Se cumple este desafío mediante el establecimiento de infraestructuras de sistemas de información para que determinen la fuente, capturen, procesen, analicen y comuniquen la información relevante. Estos sistemas de información – generalmente computarizados pero que también involucran procesos manuales e interfaces – a menudo son vistos en el contexto del procesamiento de datos generados internamente y relacionados con las transacciones.

Para respaldar una ERM eficaz, una entidad captura y utiliza datos históricos y actuales. Los datos históricos le permiten a la entidad comparar el desempeño real con metas, planes y expectativas. Revela cómo se desempeñó la entidad bajo condiciones variantes, permitiendo a la gerencia identificar correlaciones y tendencias y proyectar el desempeño futuro. Los datos históricos también pueden proveer advertencias oportunas sobre acontecimientos eventuales que ameriten la atención de la gerencia.

Los datos actuales le permiten a una entidad apreciar sus riesgos en un momento específico y permanecer dentro de las tolerancias al riesgo establecidas. Los datos actuales permiten a la gerencia observar en tiempo real los riesgos inherentes existentes en un proceso, función o unidad e identificar variaciones con respecto a las expectativas. Esto otorga una visión del perfil de riesgo de la entidad, permitiendo a la

gerencia modificar las actividades como sea necesario para adaptarlas a su nivel de riesgo aceptado.

La información constituye una base para la comunicación que debe satisfacer las expectativas de grupos e individuos, permitiéndoles cumplir eficazmente con sus cometidos. Entre los canales de comunicación más críticos se encuentra el que conecta a la alta gerencia con el directorio. La gerencia debe mantener al directorio al tanto del desempeño, desarrollos, riesgos y operación de la ERM y otros acontecimientos y asuntos importantes. Cuanto mejor sea la comunicación, más eficazmente podrá cumplir el directorio con sus responsabilidades de supervisión, actuar como una caja de resonancia en asuntos críticos y proveer asesoramiento, consejo y orientación. Del mismo modo, el directorio debe comunicar a la gerencia qué información necesita y proveer retroalimentación[23] y orientación.

La gerencia provee comunicación específica y direccionada abordando expectativas de comportamiento y las responsabilidades del personal. Esto incluye una clara declaración con respecto a la filosofía y el enfoque de ERM de la entidad y a la delegación de autoridad. La comunicación con relación a procesos y procedimientos debe estar alineada con y respaldar la cultura de riesgo deseada. Adicionalmente, la comunicación debe ser apropiadamente formulada – la presentación de información puede afectar significativamente la manera como es interpretada y cómo son visualizados los riesgos y oportunidades asociados.

La comunicación debe concientizar sobre la importancia y relevancia de una ERM eficaz, comunicar el nivel de riesgo aceptado por la entidad y las tolerancias al riesgo, implantar y respaldar un lenguaje común sobre riesgo y asesorar al personal sobre sus roles y responsabilidades con relación a la ejecución y soporte de los componentes de la

ERM.

Los canales de comunicación deben también asegurar que el personal pueda comunicar la información sobre riesgos a través de las unidades operativas, procesos o áreas funcionales. En la mayoría de los casos, los canales apropiados de comunicación en una organización son las líneas normales de autoridad. En algunas circunstancias, sin

[23] Feedback

embargo, se necesitan líneas de comunicación diferentes a efectos de servir como un mecanismo libre de fallas en caso que los canales normales no estén operativos. En todos los casos, es importante que el personal comprenda que no se tomarán represalias por la comunicación de información relevante.

Los canales de comunicación externa pueden proveer insumos altamente significativos con relación al diseño o calidad de los productos o servicios. La gerencia considera cómo su nivel de riesgo aceptado y sus tolerancias al riesgo se alinean con los de sus consumidores, proveedores y socios, asegurándose de no tomar inadvertidamente demasiado riesgo a través de sus interacciones comerciales. La comunicación por parte de terceros externos a menudo provee información importante sobre el funcionamiento de la ERM.

8) Monitoreo

La ERM es monitoreada en un proceso que aprecia tanto la presencia como el funcionamiento de sus componentes y la calidad de su desempeño a lo largo del tiempo. El monitoreo puede ser realizado de dos formas: a través de actividades continuas o de evaluaciones independientes. El monitoreo continuo e independiente aseguran que la ERM continúe siendo aplicada a todos los niveles y a través de toda la entidad.

El monitoreo continuo se construye sobre la base de las actividades operativas normales y recurrentes de una entidad. El monitoreo continuo es ejecutado sobre la base de tiempo real, reacciona dinámicamente a los cambios en las condiciones y está arraigado en la entidad. Consecuentemente, es más eficaz que las evaluaciones independientes.

Mientras que las evaluaciones independientes tienen lugar luego de ocurridos los hechos, a menudo los problemas serán identificados más rápidamente por las rutinas de monitoreo continuo. No obstante, muchas entidades con sólidas actividades de monitoreo continuo, realizan evaluaciones independientes de la ERM.

La frecuencia de las evaluaciones independientes es un asunto de juicio de la gerencia. Al hacer esta determinación, se considera: (a) la naturaleza y el alcance de los cambios en los acontecimientos tanto internos como externos y sus riesgos asociados; (b) la competencia y experiencia del personal que implanta las respuestas a los riesgos y los

correspondientes controles y (c) los resultados del monitoreo continuo. Generalmente, algún tipo de combinación de monitoreo continuo y evaluaciones independientes asegurará que la ERM mantenga su eficacia a lo largo del tiempo.

La magnitud de la documentación de la ERM de una entidad varía según su dimensión, complejidad y otros factores similERMs. El hecho de que los elementos de la ERM no estén documentados no significa que no sean eficaces o que no puedan ser evaluados.

Sin embargo, un nivel apropiado de documentación generalmente hace que el monitoreo sea más eficaz y eficiente. En caso que la gerencia desee hacer una declaración a terceros en relación a la eficacia de la ERM, debe considerarse el desarrollo y mantenimiento de documentación que respalde dicha declaración.

Todas las deficiencias de la ERM que afecten la capacidad de una entidad de desarrollar e implantar su estrategia y lograr sus objetivos establecidos deben ser informadas a quienes tengan la autoridad para tomar las acciones necesarias. La naturaleza de los asuntos a ser comunicados variará dependiendo de la autoridad de los individuos para abordar las circunstancias que surjan y de las actividades de supervisión de los superiores. El término “deficiencia” alude a una condición del proceso de ERM que amerite ser atendido. Por lo tanto, una deficiencia puede representar un defecto percibido, eventual o real o una oportunidad de fortalecer el proceso para aumentar la probabilidad de que los objetivos de la entidad sean alcanzados. La información generada en el curso de las actividades operativas generalmente es elevada a través de canales normales. También deben existir canales de comunicación alternativos para trasmitir información sensible como actos ilegales o incorrectos.

Resulta crítico proporcionar, exactamente a quien corresponda, la información necesaria sobre las deficiencias de la ERM. Deben establecerse protocolos para definir qué información es necesaria a un nivel particular para que la toma de decisiones sea eficaz.

Dichos protocolos reflejan la regla general que un gerente debe recibir la información que afecte las acciones o el comportamiento del personal bajo su responsabilidad así como la información necesaria para lograr sus objetivos específicos.

Limitaciones de la ERM[24]

Una ERM efectiva, sin importar su alto grado de diseño y ejecución, sólo proporciona una seguridad razonable a la dirección y al consejo de administración respecto a la consecución de objetivos de la empresa.

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

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

Al considerar las limitaciones que presenta la ERM debemos reconocer tres conceptos distintos:

a) el riesgo está relacionado con el futuro, que es inherentemente incierto.

b) ERM opera a distintos niveles con respecto a objetivos diferentes. Respecto a los objetivos estratégicos y operativos; dicha gestión puede llegar a asegurar que la dirección, y el consejo en su rol supervisor, sean conscientes en forma oportuna sólo del grado de progreso de la empresa hacia la consecución de dichos objetivos. Sin embargo, no puede proporcionar ni siquiera una seguridad razonable de que los objetivos en sí mismos sean alcanzados.

c) ERM no puede facilitar una seguridad absoluta respecto a ninguna de las categorías de objetivos.

[24] ERM Resumen Ejecutivo Marco

Roles y responsabilidades[25]

Todos los integrantes de la organización tienen responsabilidades respecto a la ERM. El mismo es tarea de todos, y los roles y responsabilidades de todos los integrantes de la empresa deben estar bien definidos y comunicados adecuadamente.

Directorio

La gerencia debe rendir cuentas al directorio, el que provee gobierno, orientación y supervisión. Al seleccionar a la gerencia, el mayor rol corresponde al directorio al definir sus expectativas en cuanto a integridad moral y valores éticos y puede confirmar sus expectativas a través de las actividades de supervisión. Igualmente, al reservar para sí la autoridad para ciertas decisiones clave, el directorio juega un rol al establecer la estrategia, al formular los objetivos de alto nivel y los lineamientos generales en relación a la asignación de recursos.

El directorio provee supervisión con respecto a ERM:

– Conociendo la medida en que la gerencia ha establecido una ERM eficaz en la organización.

– Estando enterado y de acuerdo con el nivel de riesgo aceptado de la entidad.

– Revisando la visión conjunta de riesgos de la entidad y considerándola en relación con el nivel de riesgo aceptado por la entidad.

–Estando al tanto de los riesgos más importantes y si la gerencia está respondiendo apropiadamente a los mismos.

El directorio es una parte del componente ámbito interno y para que ERM sea eficaz, debe satisfacer requisitos en cuanto a composición y enfoque.

Gerencia

El gerente general es en última instancia el responsable y debe asumir la propiedad de la ERM. Más que cualquier otra persona, el gerente general da la tónica al máximo nivel que afecta la honestidad y los valores éticos y los otros factores del ámbito interno. En una empresa grande, el gerente general cumple este cometido liderando y orientando a

[25] ERM Técnicas de Aplicación

los gerentes veteranos y revisando la manera como ellos manejan el negocio. Los gerentes veteranos, a su vez, asignan responsabilidad por el establecimiento de políticas y procedimientos de administración de riesgos más específicos al personal responsable de las funciones individuales de las unidades. En una empresa más chica, la influencia del gerente general, con frecuencia un propietario-gerente, es usualmente más directa.

En cualquier caso, en un marco de responsabilidades decrecientes, un gerente es efectivamente un gerente general de su esfera de responsabilidad. También son importantes los líderes de funciones de apoyo como cumplimiento, finanzas, recursos humanos y tecnología de la información, cuyas actividades de monitoreo y control atraviesan horizontal y verticalmente las unidades operativas y de otro tipo de una empresa.

Oficial de riesgo[26]

Un oficial de riesgo trabaja con otros gerentes estableciendo y manteniendo una eficaz administración de riesgos en sus áreas de responsabilidad. El gerente de riesgo también puede tener la responsabilidad de monitorear el progreso y de dar asistencia a otros gerentes en trasmitir información importante sobre riesgos hacia arriba, abajo y horizontalmente y puede ser un miembro de un comité interno de administración de riesgos.

Auditores internos

Los auditores internos juegan un rol importante en el monitoreo de la ERM y de la calidad del desempeño como parte de sus cometidos regulares o respondiendo a especiales requerimientos de la alta gerencia o ejecutivos de divisiones o subsidiarias. Pueden dar asistencia tanto a la gerencia como al directorio o comité de auditoría monitoreando, examinando, evaluando, informando al respecto y recomendando mejoras con relación a la adecuación y eficacia de los procesos gerenciales de ERM.

[26] Risk officer

Otros miembros del personal

ERM es, en alguna medida, responsabilidad de todos los integrantes de una entidad y en consecuencia debe ser una parte explícita o implícita de la descripción del trabajo de cada uno de ellos. Virtualmente todo el personal produce información usada en ERM o realiza otras acciones necesarias para administrar riesgos. Además, todo el personal es responsable por comunicar hacia arriba con respecto a riesgos, como problemas en las operaciones, incumplimientos del código de conducta, violaciones de otras políticas o acciones ilegales.

Una cantidad de terceras partes contribuyen a menudo al logro de los objetivos de una entidad. Los auditores externos, aportando un visión independiente y objetiva, contribuyen directamente a través de la auditoría de los estados contables y de las revisiones del control interno e indirectamente proveyendo información adicional útil para el cumplimiento de sus cometidos por parte de la gerencia y el directorio. Otros que proveen información útil a la entidad para realizar la ERM son las agencias reguladoras, consumidores y otros que realizan transacciones comerciales con la entidad, analistas financieros, calificadores de bonos y los medios de difusión. Los terceros externos, sin embargo, no son responsables por la ERM de la entidad.

CAPITULO III: OTROS DOCUMENTOS DE ADMINISTRACIÓN DE RIESGO EMPRESARIAL

Toda vez que ocurre un escándalo empresarial – ya sea por fraudes, pérdidas inesperadas, prácticas indebidas de venta, graves accidentes laborales o fallas en la seguridad – el dedo acusador apunta de forma inevitable hacia la gestión de la empresa. Por lo tanto, no es sorprendente que como consecuencia de estos hechos, se haya despertado la necesidad de desarrollar estándares que den lineamiento sobre cómo medir y evaluar los riesgos de la empresa, para posibilitar la toma de acciones que mitiguen la exposición de la misma a riesgos mayores.

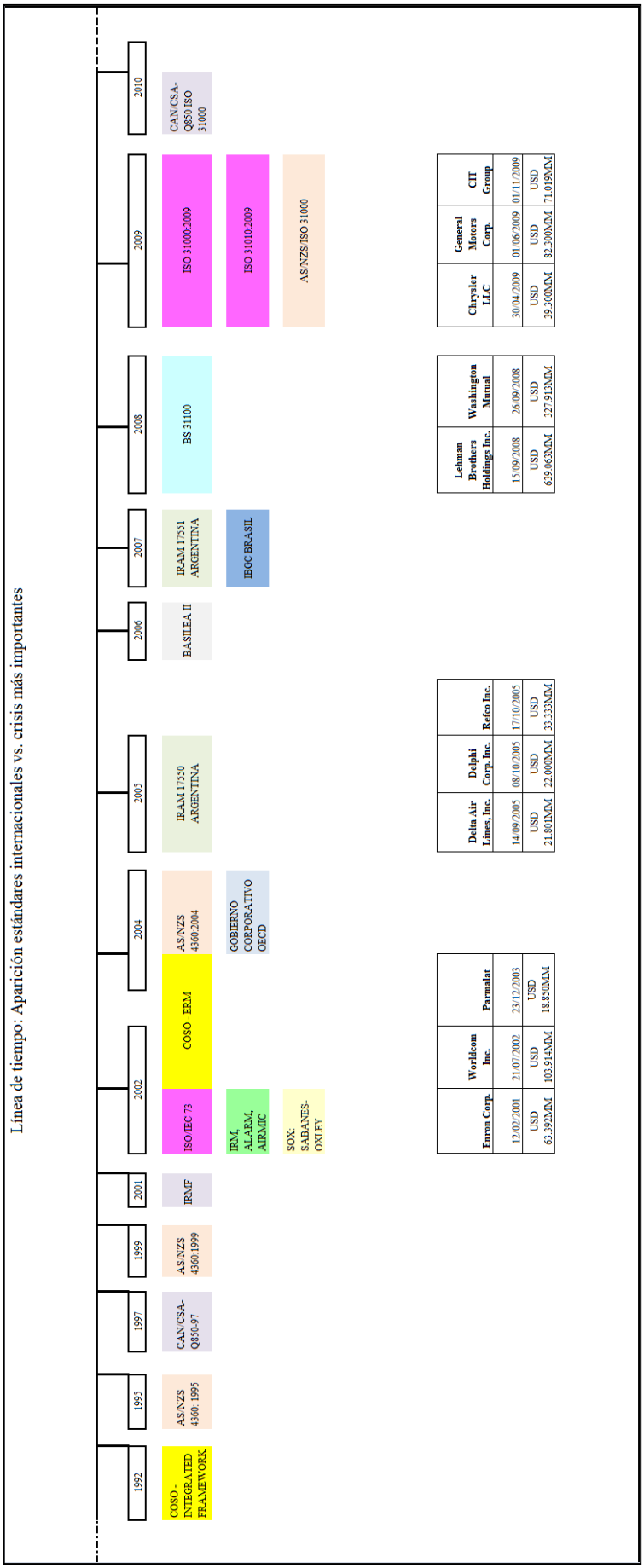
Como parte de este paradigma, se ha reformulado la cultura del riesgo y se ha avanzado muy rápidamente hacia la construcción de una nueva base conceptual, teórica y técnica para asegurar la supervivencia de las organizaciones más aptas en este ambiente de riesgo global.

Como se puede apreciar en la línea de tiempo de la hoja siguiente, en los últimos 20 años, existió y existe un paralelismo singular entre las crisis económicas y los escándalos empresariales con la aparición de marcos teóricos que tratan sobre la gestión de riesgos.

La concepción del tema ha ido evolucionando y creando una disciplina sofisticada y compleja en continuo cambio.

Los estándares que vamos a ver son genéricos y dejan claramente establecido que no tienen como objetivo estandarizar especificaciones concretas ni la implementación de un sistema a una organización en particular. Por el contrario, el llamado es a poder proveer una guía universal y válida.

Todavía no existe un estándar con un consenso internacional, un estándar global de consenso mundial. Como consecuencia veremos en el desarrollo del capítulo que existen diversas percepciones y discusiones para decidir cuál de los existentes es el mejor o más aplicable.


Línea de tiempo: Aparición estándares internacionales vs. crisis más importantes
1992
1995
1997
1999
2001
2002
2004
2005
2006
2007
2008
2009
2010
COSO - INTEGRATED FRAMEWORK
AS/NZS 4360: 1995
CAN/CSA-Q850-97
AS/NZS 4360:1999
IRMF
ISO/IEC 73
COSO - ERM
IRM, ALARM, AIRMIC
SOX: SABANES-OXLEY
AS/NZS 4360:2004
GOBIERNO CORPORATIVO OECD
IRAM 17550 ARGENTINA
BASILEA II
IRAM 17551 ARGENTINA
IBGC BRASIL
BS 31100
ISO 31000:2009
ISO 31010:2009
AS/NZS ISO 31000
CAN/CSA-Q850 ISO 31000
Enron Corp.
12/02/2001
USD 63.392MM
Worldcom Inc.
21/07/2002
USD 103.914MM
Parmalat
23/12/2003
USD 18.850MM
Delta Air Lines, Inc.
14/09/2005
USD 21.801MM
Delphi Corp. Inc.
08/10/2005
USD 22.000MM
Refco Inc.
17/10/2005
USD 33.333MM
Lehman Brothers Holdings Inc.
15/09/2008
USD 639.063MM
Washington Mutual
26/09/2008
USD 327.913MM
Chrysler LLC
30/04/2009
USD 39.300MM
General Motors Corp.
01/06/2009
USD 82.300MM
CIT Group
01/11/2009
USD 71.019MM

MARCO DE ADMINISTRACIÓN INTEGRADA DE RIESGO[27]

Introducción

El estándar canadiense surge como consecuencia de la necesidad de reforzar las prácticas de administración de riesgos en el sector público de Canadá. Tomado como prioridad dentro de la agenda del Gobierno en los años 1999 y 2000, el Consejo del Tesoro de Canadá[28] desarrolló este marco en colaboración con organizaciones federales académicas y privadas.

El estándar responde a las recomendaciones contenidas en el reporte de Gobierno de Canadá de 1997. En el mismo, el Panel de Revisión Independiente[29] subraya una nueva filosofía de contralor, que combina un fuerte compromiso en 4 componentes:

- Performance de reportes
- Administración del riesgo
- Aplicación de un adecuado sistema de control
- Valores y ética

De esta manera el marco fue diseñado para avanzar en el desarrollo y la implementación de nuevas y modernas prácticas de administración y para soportar innovaciones dentro del servicio público federal de dicho país.

Los objetivos de este documento según se mencionan en su introducción son:

- Proveer una guía para avanzar en un enfoque más corporativo y sistemático de administración de riesgos

- Contribuir en el desarrollo de un equipo de trabajo de riesgo inteligente que permita la innovación y sea responsable de tomar los riesgos mientras se asegura las precauciones adoptadas son legítimas y son tomadas para proteger el interés público, mantener la confianza pública y asegurar la debida diligencia

- Proponer un set de prácticas de administración de riesgos para que los departamentos puedan adoptar y adaptar si es necesario a sus circunstancias y ejecutar.

[27] Integrated Risk Management Framework (2001). Treasury Board of Canada Secretariat.
[28] www.tbs-sct.gc.ca Treasury Board of Canada Secretariart
[29] Report of the Independent Review Panel on Modernization of Comptrollership in the Government of Canada

Estructura

Sin dejar de respetar la estructura original del documento, plantearemos los siguientes puntos a destacar:

1. Alcance y ámbito de aplicación
2. Conceptos fundamentales
3. Marco integrado para la administración de riesgos
   3.1. Desarrollar un perfil de riesgo corporativo
   3.2. Establecer una función de IRM
   3.3. Practicar la administración de riesgos – el proceso
   3.4. Asegurar un continuo aprendizaje y comunicación

1. Alcance y ámbito de aplicación

Desde el inicio del documento se plantea que el desarrollo del estándar será para mejorar el funcionamiento de los servicios públicos. Sin embargo menciona que el marco puede proveer a cualquier organización un mecanismo para desarrollar una visión global de cómo manejar estratégicamente los riesgos al crear mecanismos de discusión, comparación y evaluación de los diferentes riesgos. Según se menciona, el documento es aplicable a toda la organización y cubre todo tipo de riesgos ya sea operacionales, financieros, legales, medioambientales, reputacionales, etc.

Enfatiza que el desafío del servicio público es lograr una administración de riesgos más integrada y sistemática que incluya dentro del proceso la comunicación y consulta con las partes interesadas[30] y el público en general para generar un cambio cultural que seguramente llevará varios años de práctica.

[30] Stakeholders. Público relevante con intereses en la empresa o incluso, individuos o entidades que asumen algún tipo de riesgo en ella, directa o indirectamente. Son entre otros, los accionistas, funcionarios, clientes, proveedores, gobierno, reguladores, entre otros.

2. Conceptos fundamentales

Dentro de los conceptos fundamentales se destacan las siguientes definiciones:

- Riesgo: como concepto general se tiene dentro de las definiciones de riesgo la incertidumbre en los resultados. Se expresa claramente que algunos pueden tomar como consecuencias de esta incertidumbre sólo los efectos negativos mientras otros son neutrales o incluso pueden existir efectos positivos. El documento plantea como definición de riesgo a la incertidumbre que rodea eventos futuros y resultados. Es la expresión probabilidad e impacto de un evento con el potencial de influenciar el logro de los objetivos de una organización. La frase "probabilidad e impacto de un evento" implica que, como mínimo, un análisis cualitativo o cuantitativo es necesario para tomar una decisión teniendo en cuenta los riesgos mayores o las amenazas que puedan existir para lograr los objetivos de una organización.

- Administración de riesgo: Para el desarrollo de este marco se define la administración de riesgos como el enfoque sistemático de disponer el mejor curso de acción bajo incertidumbre para identificar, tratar, entender y comunicar los riesgos. Para aplicarlo de manera efectiva, es vital que una cultura de administración de riesgo sea desarrollada. Ésta es quien soporta la visión, misión y objetivos globales de la organización así como los límites y fronteras establecidos para aceptar los riesgos.

- Administración integrada del riesgo: La diferencia con la definición antes dicha es que ya no es suficiente tratar los riesgos sobre un determinado nivel o para una determinada actividad, sino que se busca que el alcance de este proceso sea más exhaustivo y global. Queda definido en base a este enfoque que la administración integrada de riesgo es el proceso continuo, proactivo y sistemático de entender, administrar y comunicar los riesgos a través de decisiones estratégicas que contribuyan al logro de los objetivos. No se enfoca solo en la minimización o mitigación de los riesgos sino que soporta actividades que fomenten la innovación para que mejores retornos sean

alcanzados tanto en los resultados, los costos y los riesgos. La administración integrada de riesgos trata de lograr el balance óptimo de la empresa.

3. Marco integrado para administrar los riesgos

El estándar plantea cuatro elementos y sus resultados esperados para administrar los riesgos. El orden en el que son presentados, debería ser también el orden de aplicación, pensando en la organización a lo largo y a lo ancho de su estructura así como en las actividades individuales. Los elementos a continuación desarrollados son un paso para establecer las bases de lo que sería la administración de riesgos en el sector público:

1.1. Desarrollar un perfil de riego corporativo

Para desarrollar un perfil de riesgo a nivel corporativo se deben examinar tanto las amenazas como las oportunidades. Se debe recolectar información tanto de los niveles altos de la organización como de los operacionales para asistir a los departamentos a entender los riesgos que deben enfrentar, ya sean internos como externos.

Una organización puede esperar tres resultados del desarrollo de su perfil de riesgo:

- Las amenazas y oportunidades son identificadas en el monitoreo y análisis continuo tanto del ambiente interno como externo.
- Se logra conformar un status actual sobre lo que tiene la empresa para administrar los riesgos
- Se identifican las áreas claves a tratar, la tolerancia de riesgo, habilidades y conocimientos disponibles, así como los recursos necesarios.

El monitoreo propuesto para el análisis de factores externos considera como potenciales los factores: políticos, económicos, sociales y tecnológicos. Respecto a los factores internos se subrayan: gobierno corporativo, valores y ética, ambiente operacional, cultura y tolerancia existente, prácticas y expertise[31] existentes, políticas y procedimientos, etc.

[31] Expertise: Habilidad

La Guía de Implementación[32] de este estándar plantea diversas técnicas para realizarlo: tormenta de ideas, planificación de distintos escenarios, encuestas, reportes de auditoría y de desempeño. También detalla algunas fuentes internas que ayudan a determinar el estado de la organización en materia de riesgo. Algunos ejemplos son:

- Chequeo de la capacidad de control y su correspondiente plan de acción, que provee información sobre la percepción de los gerentes del estado de la organización en diversas áreas.
- Documentos departamentales de planificación estratégica.
- Reportes de administración del desempeño, que permiten determinar si la organización está logrando sus expectativas y objetivos.

Para los factores externos, las técnicas planteadas para realizarlo son: monitoreo de los medios, benchmarking, opinión pública, grupos de opinión, asambleas, consejos, asociaciones, grupos de consumidores.

Cómo último punto clave -pero no menos importante- a la hora de desarrollar el perfil de riesgo, está definido lo que se conoce como tolerancia al riesgo. Ésta varía con la cultura y con las condiciones cambiantes del ambiente interno y externo. El conocimiento y entendimiento del nivel de tolerancia que tienen las partes interesadas[33] es un ingrediente clave dentro de este perfil. También se debe considerar que influencian y guían los procesos de decisión. Determinar y comunicar la tolerancia de la organización permite identificar los niveles mínimos de riesgo permitidos o considerados razonables así como los riesgos que deben ser atendidos más profundamente.

1.2. Establecer una función de IRM[34]

Esto implica crear una infraestructura integrada dentro de la organización. Esta estructura corporativa sobre administración de riesgos debe ser diseñada para reforzar el entendimiento y la comunicación de los temas relacionados, para proveer una clara dirección de cómo manejarlos y demostrar el soporte de la alta dirección.

[32] Integrated Risk Management – Implementation Guide, 2002. Treasury Board of Canada Secretariat
[33] Stakeholders
[34] IRM: Integrated Risk Management

La guía de implementación en este capítulo sostiene que integrar la administración del riesgo a las existentes estructuras y procesos de decisión requiere que:

- la administración del riesgo esté anclada al nivel de la subdirección con compromiso de la dirección administrativa
- se identifique a un ejecutivo de riesgo[35] o a una unidad
- se haya desarrollado un perfil de riesgo corporativo[36], siendo clave la evaluación del grado de preparación y estructuras y procesos existentes

Continúa mencionando que para asegurarse se integra de manera racional, sistemática y proactiva, la organización debe tratar de conseguir los siguientes resultados:

- Las directivas han sido comunicadas, entendidas y aplicadas según la visión, las políticas y los principios de la empresa.
- El alcance de la operativa de esta integración es implementado a través de una estructura existente de toma de decisiones: existe gobierno corporativo, roles y responsabilidades claros, reportes de performance.
- Existen planes y herramientas para desarrollar una capacidad de aprendizaje a lo largo de la organización.

Independientemente que cada organización puede tener sus propios métodos para integrarla, existen factores que deben ser considerados en todos los casos:

- Alinearla con los objetivos en todos los niveles de la organización
- Introducir los componentes de administración de riesgo dentro de los planes estratégicos y procesos operacionales existentes
- Comunicar las directrices corporativas sobre el nivel de riesgo aceptado
- Mejorar controles y sistemas contables y procesos para que tengan en cuenta la gestión de riesgos y sus resultados.

Otro aspecto fundamental para lograr un buen resultado del proceso dentro de la empresa es el desarrollo de una capacidad organizacional para administrar los riesgos. Para construir esta capacidad, existen dos áreas claves que se deben considerar:

a) Recursos Humanos: se identifican 4 áreas principales a las que se debe prestar atención:

[35] Risk Champion
[36] Ver punto 3.1.

i. Crear conciencia de iniciativa de administración de riesgo y cultura
ii. Desarrollar habilidades a través del entrenamiento formal
iii. Aumentar la base de conocimiento, compartiendo las mejores prácticas y experiencias
iv. Construir capacidad, habilidades, facultades de trabajo en equipo

b) Herramientas y procesos: en este caso se entiende se eleva dicha capacidad:

i. Desarrollando y adoptando herramientas, técnicas, prácticas y procesos de administración de riesgo corporativo
ii. Brindando una guía para la aplicación de las mismas
iii. Permitiendo el desarrollo de métodos y técnicas alternativas
iv. Adoptando procesos que aseguren la administración de riesgos es integrada a lo largo de toda la organización

1.3.Practicar la administración de riesgos – el proceso

Una administración de riesgos integrada requiere el compromiso y la decisión de la gerencia. Para ser implementada, los siguientes resultados deben esperarse al practicarla:

- El proceso de administración de riesgos es aplicado consistentemente en todos los niveles, donde los riesgos son entendidos, manejados y comunicados
- Los resultados de las prácticas de administración de riesgos son informadas adecuadamente y priorizadas de acuerdo a las necesidades
- Las herramientas y métodos son aplicados para ayudar en la toma de decisiones
- La consulta y comunicación con las partes interesadas es continua – ya sean internas o externas.

La Guía de Implementación menciona que la implementación de IRM[37] involucra plantear objetivos y resultados y hacer un ranking de los riesgos. Se estará pronto para hacerlo cuando la cultura corporativa haya logrado:

- establecer un amplio énfasis en la administración de riegos
- la dirección se haya comunicado con todos los niveles

[37] IRM: Integrated Risk Management Framework, habla de la "función de IRM" vista en el punto 3.2. del presente capítulo

- los procesos y estructuras hayan incorporado el concepto
- se haya logrado cierta capacidad, resultado del desarrollo de guías, herramientas y entrenamiento del personal.

1.3.1. Esquema de Administración de riesgos

La figura 1 muestra el esquema del proceso reflejando en forma de círculo la idea de continuidad:

El proceso continuo de administración de riesgos consta de varias etapas detalladas a continuación:

Identificación de riesgos

1.3.1.1. Identificar y establecer el contexto: definiendo los problemas y oportunidades, el alcance, el contexto (social, cultural, etc.) y sus riesgos asociados; decidiendo qué recursos son necesarios (tanto en concepto de herramientas como personas y conocimientos)

Análisis de riesgos

1.3.1.2. Evaluar las áreas de riesgo: analizar el contexto y determinar los distintos tipos o categorías de riesgos a ser identificados, a cuáles deberá prestarle más atención por considerarse significativas o fundamentales.

1.3.1.3. Medir la probabilidad e impacto: determinar el grado de exposición y definir la probabilidad e impacto de las áreas de riesgos determinadas

1.3.1.4. Hacer un ranking de los riesgos: considerando la tolerancia al riesgo establecida por la empresa.

Respuesta al riesgo

1.3.1.5. Definir los resultados esperados para los riesgos según el ranking, en el corto y o largo plazo.

1.3.1.6. Desarrollar las opciones de tratamiento para minimizar las amenazas y maximizar las oportunidades.

1.3.1.7. Seleccionar la estrategia de tratamiento de riesgos

1.3.1.8. Implementar la estrategia elegida

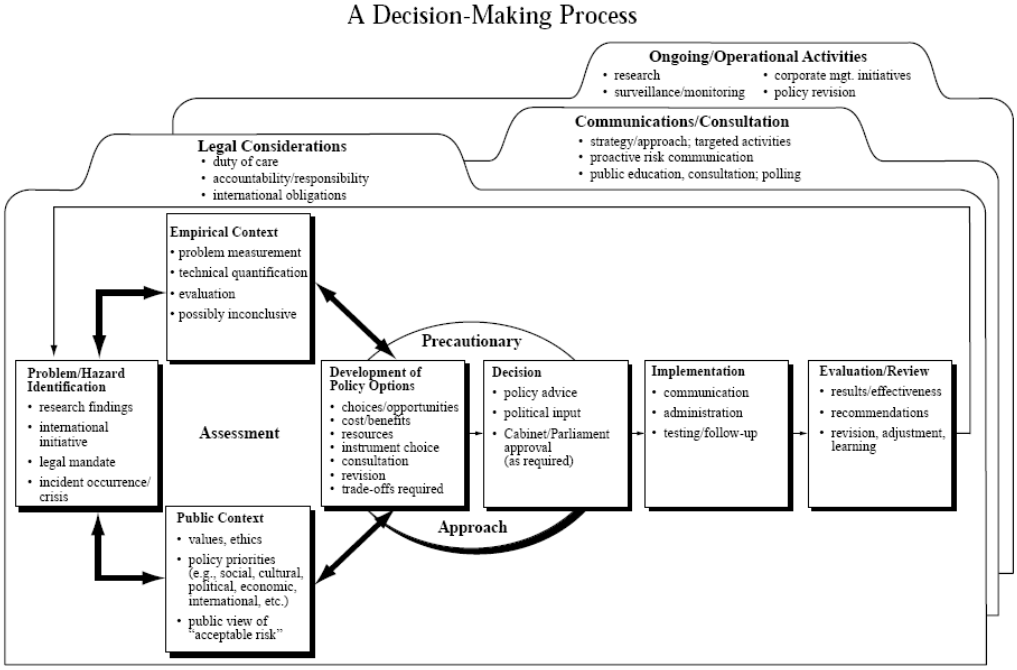
Monitoreo y evaluación

1.3.1.9. Monitorear, evaluar y ajustar

Además de estas etapas listadas, aparece en el esquema otro elemento en el centro del círculo: aprendizaje continuo y comunicación. Este aspecto lo veremos aparte en la sección 3.4.

1.3.2. El proceso de toma de decisiones:

La figura 2 muestra el proceso desde otra óptica: el proceso de toma de decisiones en el contexto del desarrollo de políticas públicas. Esta figura presenta las bases para explorar temas de interés para los creadores de políticas gubernamentales.



Se destacan algunos elementos claves que vale la pena detallar:

- La incertidumbre planteada lleva a aumentar el foco en la precaución.
- El proceso no ocurre aislado – se deben tomar en cuenta todos los factores en cada etapa del proceso.

1.3.3. Herramientas y métodos:

Algunos ejemplos de técnicas y herramientas planteadas que pueden ser utilizadas para administrar los riesgos son:

- Mapeos de riesgos: gráficos y diagramas que permitan a la empresa identificar, discutir, entender y evaluar riesgos.
- Herramientas modelo: como análisis de escenarios y pronósticos para analizar las posibilidades y desarrollar distintos escenarios según los planes de contingencia
- Esquema de administración de riesgos preventivo: con un alcance preventivo que sirva como guía para mejorar la credibilidad, predicción y consistencia en su aplicación
- Técnicas cuantitativas: como cuestionarios, talleres, auto-evaluaciones para identificar y valuar los riesgos

- Internet e Intranet: utilizarlas como medios de comunicación para promocionar la conciencia de administración de riesgos y compartir información relevante tanto interna como externa.

1.3.4. Modelo de Administración de riesgos:

La figura 3 muestra un ejemplo del modelo. En el mismo uno podría evaluar los riesgos a nivel particular, midiendo su probabilidad e impacto y la respuesta o estrategia de respuesta de la organización:

Impact	Risk Management Actions		
Significant	Considerable management required	Must manage and monitor risks	Extensive management essential
Moderate	Risks may be worth accepting with monitoring	Management effort worthwhile	Management effort required
Minor	Accept risks	Accept, but monitor risks	Manage and monitor risks
	Low	Medium	High
	Likelihood		

Este método de medición debe servir no sólo como guía para la administración de riesgos en los distintos niveles de la empresa sino también para reconocer las necesidades de cada uno.

1.4.Asegurar un continuo aprendizaje y comunicación

1.4.1. Comunicación y consulta:

La comunicación acerca de los riesgos y la consulta de las partes interesadas son un parte esencial para las decisiones en la gestión de riesgos. De hecho, la comunicación y consulta puede ser considerada en todos los niveles del proceso.

La Guía de Implementación propone desarrollar e implementar una estrategia de comunicación, monitoreo de resultados y ajustes, estableciendo circuitos de retroalimentación con todas las unidades. También establece que se deben promover oportunidades para compartir información a través de las distintas funciones, y establecer herramientas de información para compartir técnicas de administración de riesgos. Otra forma es realizando encuestas periódicas para determinar si todo el

personal es consciente de los riesgos clave, de los procedimientos sobre riesgos y de los planes de contingencia.

1.4.2. Aprendizaje continuo:

Este aspecto es fundamental para estar bien informado y para la toma de decisiones proactivas. Contribuye a una mejor administración de riesgos, refuerza la capacidad organizacional y facilita la interacción en la estructura de la organización.

Para lograr el aprendizaje continuo se deben tener en cuenta los siguientes pasos:

- Crear un ambiente de soporte dentro de la empresa: con esto se debería promover el aprendizaje, aprender de la experiencia y demostrar liderazgo en la administración de riesgos. Se crea un ambiente valorando los resultados de las lecciones, compartiendo mejores prácticas y adoptando una actitud responsable frente a los riesgos.

- Construir planes de aprendizaje: debe existir una unidad de capacitación que provea planes de entrenamiento y desarrollo según las necesidades de cada empleado. La inclusión de los planes de capacitación dentro de los objetivos de performance de los individuos es una manera útil de asegurarnos este desarrollo.

- Fomentar el continuo aprendizaje y la innovación: para fomentar el aprendizaje es importante primero reconocer que no todos los riesgos pueden ser totalmente mitigados o evitados. Lo principal es tratar de aprender de las experiencias pasadas y generar iniciativas para tratar los riesgos. El aprendizaje es fundamental para progresar.

La Guía de implementación plantea que para lograrlo es necesario:

- entusiasmar al aprendizaje y enfoque en la construcción de capacidad de administrar riesgos
- concentrarse en un incremento de la conciencia de riesgo, conocimientos y habilidades a niveles individuales, de equipo y organizacionales
- monitorear y aprender de situaciones donde la administración de riesgos se ha convertido en una herramienta de decisión.

ESTÁNDARES DE GERENCIA DE RIESGOS[38]

Introducción

Los estándares de gerencia de riesgos surgen del trabajo de un equipo de distintas organizaciones de Reino Unido: Institute of Risk Management (IRM) [39], Association of Insurance and Risk Managers (AIRMIC) [40] y el National Forum for Risk Management in the Public Sector (ALARM).[41]

Considerando que la gerencia de riesgos es una disciplina que se está desarrollando rápidamente, entendieron se necesitan estándares para consensuar: el significado del vocabulario utilizado, la estructura organizativa necesaria, el proceso de gerencia de riesgos y sus objetivos.

El estándar plantea que hay muchos modos de conseguir los objetivos de la gerencia de riesgos y que no puede recogerse en un solo documento. Por eso, el objetivo de este marco no es crear una norma imperativa, enfoque rígido o proceso certificable. Solo trata de representar una mejor práctica con la que la empresa pueda autoevaluarse.

Estructura

Siguiendo con el hilo conductor planteado anteriormente se puede plantear el siguiente esquema del contenido del documento:

1. Definiciones
    a. Definición de riesgo
    b. Definición de Gestión de riesgos
2. El proceso de gestión de riesgos
    3.1. Objetivos estratégicos y estructura organizacional
    3.2. Valoración de riesgos
        3.2.1. Análisis de riesgos
        3.2.2. Evaluación de riesgos
    3.3. Tratamiento de riesgos
    3.4. Informe y comunicación
    3.5. Supervisión y revisión del proceso de gestión de riesgos

[38] ESTÁNDARES DE GERENCIA DE RIESGOS - AIRMIC, ALARM, IRM: 2002
[39] www.theirm.org
[40] www.**airmic**.com
[41] www.alarm-uk.org

1. Definiciones

a. Definición de Riesgo

Se define como una combinación de la probabilidad y consecuencias de un suceso. Esta definición la toman de la Guía ISO/IEC 73. Se menciona que se toma como base para respetar la terminología mundialmente aceptara.

Se destaca que los riesgos constituyen oportunidades o amenazas para el éxito, considerándolo desde 2 perspectivas. Es importante a la vez reconocer que los riesgos tienen un lado positivo y otro negativo, y que las oportunidades que surgen no sólo deben considerarse en el marco de la actividad empresarial, sino también en relación con las partes interesadas[42].

b. Definición de Gestión de Riesgos

Es el proceso en el que se tratan los riesgos, para obtener un beneficio. Se centra en identificar y tratar riesgos, con el fin de añadir valor, aumentando la probabilidad de éxito o reduciendo la de fallo o incertidumbre. Debe ser un proceso continuo y de constante desarrollo, que se lleve a cabo en toda la estrategia, tratando los riesgos de actividades pasadas, presentes y futuras. Debe estar integrado en la cultura de la empresa, con políticas y programas dirigidos por la alta dirección. Debe convertir la estrategia en objetivos tácticos, asignando responsabilidades a los empleados por la gestión del riesgo, promoviendo así la eficiencia operacional.

Los riesgos pueden verse afectados por factores internos o externos. El documento los clasifica agrupándolos en factores financieros, de azar, operacionales y estratégicos.

2. Proceso de gestión de riesgos

El estándar plantea que el proceso de gerencia de riesgos protege y añade valor a la empresa y sus interesados, mediante el apoyo a los objetivos de la empresa, a través de diversas actividades. El esquema de la figura siguiente muestra las etapas de este proceso:

[42] Stakeholders

2.2 El proceso de gerencia de riesgos

Los pasos dentro del proceso de gerencia de riesgos que se destacan y se podrían identificar son los siguientes:

2.1. Objetivos estratégicos y estructura organizacional

2.2. Valoración de riesgos

3.2.1. Análisis de riesgos

3.2.2. Evaluación de riesgos

2.3. Tratamiento de riesgos

2.4. Informe y comunicación

1.5.Supervisión y revisión del proceso de gestión de riesgos

2.1. Objetivos estratégicos y estructura organizacional

El estándar desarrolla al final del documento la estructura necesaria de la empresa y la administración que detallando lo en el gráfico como la etapa de "objetivos estratégicos de la organización". Por tanto decidimos traer este desarrollo a continuación.

En una primera parte se define la política de gestión de riesgos necesaria para el proceso. En ella se debe definir su enfoque y apetito de riesgo y establecer las responsabilidades de gestión, como también un conjunto integrado de herramientas y técnicas. Para que sea efectivo, el proceso de gestión de riesgos requiere el compromiso del presidente y altos ejecutivos, la asignación de responsabilidades y la asignación de recursos apropiados.

Luego se desarrollan los diferentes roles dentro del la empresa y el papel que cada parte tiene en el proceso.

- *Papel del Consejo de Administración*

Tiene la responsabilidad de determinar la dirección estratégica y de crear el entorno y las estructuras necesarias para una eficaz gestión del riesgo. Puede hacerse por medio de una dirección ejecutiva, comisión no ejecutiva, comité de auditoria.

- *Papel de las Unidades de negocio*

Tienen como responsabilidad primaria de gestionar los riesgos día a día. La dirección de las unidades es responsable de promover la conciencia del riesgo y delinear objetivos de gestión de riesgos y fijar nuevas prioridades en el trabajo luego de analizar los riesgos.

- *Papel de la función de Gestión de Riesgos*

Dependiendo del tamaño de la empresa puede ser una persona o una unidad. La función tiene a cargo: establecer la política y estrategia de gestión de riesgos, crear cultura consciente de riesgos, establecer política y estructuras de riesgos internas para las unidades de negocios, diseñar y revisar los procesos de gestión de riesgos, desarrollar procesos de respuesta al riesgo (planes de contingencia y continuidad), preparar informes de riesgos para el consejo e interesados

- *Papel de la Auditoría Interna*

Auditoría Interna debe enfocar el trabajo de auditoria interna sobre riesgos importantes y revisar los procesos de gestión. También está dentro de su rol apoyar activamente y participar del proceso de gestión de riesgos y facilitar la identificación y valoración de

riesgos y formar al personal en la gestión de riesgos y control interno. Debe generar confianza en la gestión de riesgos.

Independientemente de estos roles explicitados, se menciona que los recursos deben establecerse a todos los niveles de gestión y en cada unidad de negocios. Las personas involucradas en la gestión de riesgos deben tener definidos sus papeles, al igual que los involucrados en la auditoria y en la revisión de los controles internos. La gestión de riesgos debe estar integrada en la empresa a través de procesos estratégicos y presupuestarios.

2.2. Valoración de riesgos

Está definida en la guía ISO/IEC 73 como el proceso general de análisis y evaluación de riesgos. La misma se compone de dos sub-etapas: análisis de riesgos y evaluación de riesgos.

2.2.1. Análisis de riesgos

Esta sub-etapa consta de tres pasos que contemplan el proceso de análisis:

A – Identificación

Se propone identificar la exposición a la incertidumbre, lo que requiere un conocimiento de la empresa, el mercado, entorno social, legal, político y cultural, y el desarrollo de una visión coherente con la estrategia y objetivos y factores claves de éxito. Debe ser un proceso metódico para asegurarse de identificar todas las actividades y decisiones importantes, que pueden clasificarse en:

- Estratégicas: objetivos a largo plazo
- Operacionales: problemas cotidianos
- Financieras: gestión efectiva y control de las finanzas
- Gestión de conocimiento: producción, protección, comunicación y control de recursos del conocimiento
- Conformidad: salud y seguridad, medio ambiente, protección del consumidor, prácticas de empleo, regulación.

B – Descripción

El objetivo de esta etapa es mostrar los riesgos identificados en forma estructurada, que facilita su valoración. Como toma en cuenta la consecuencia y probabilidad, es posible dar prioridad a los riesgos clave que deberán ser analizados. Es importante incorporar la gestión de riesgos tanto en la concepción de los proyectos así como a lo largo de la vida del mismo.

El documento propone una tabla de descripción de riesgos, que incluye: nombre del riesgo, alcance, naturaleza, interesados, cuantificación, tolerancia (apetito), tratamiento, acción de mejora, política y estrategia:

4.2.1 Tabla - Descripción de riesgos

1. Nombre del riesgo	
2. Alcance del riesgo	Descripción cualitativa de los sucesos, su tamaño, tipo, número y dependencias.
3. Naturaleza del riesgo	Ej. Estratégicos, operacionales, financieros, de gestión del conocimiento y de conformidad.
4. Interesados	Interesados y sus expectativas
5. Cuantificación del riesgo	Importancia y probabilidad
6. Tolerancia del riesgo / Apetito	Potencial de pérdida e impacto financiero del riesgo Valor en riesgo Probabilidad y tamaño de las pérdidas/ganancias potenciales Objetivo(s) del control de riesgo y nivel deseado de rendimiento
7. Tratamiento del riesgo y mecanismos de control	Medios primarios por los que se gestiona el riesgo actualmente Niveles de confianza en el control existente Identificación de protocolos de supervisión y revisión
8. Acción potencial de mejora	Recomendaciones para reducir riesgos
9. Política y estrategia a desarrollar	Identificación del responsable de la función de desarrollo de la política y la estrategia.

C- Estimación

Puede ser cuantitativa, semi-cuantitativa o cualitativa en términos de probabilidad de ocurrencia y consecuencias. Las consecuencias en términos de amenazas y oportunidades pueden dividirse en altas, medias, bajas, al igual que la probabilidad, pudiendo presentarse en una matriz de 3 x 3 (o hasta de 5 x 5).

Los métodos y técnicas de análisis de riesgos pueden ser específicos para riesgos positivos o negativos, o capaces de tratar ambos riesgos. El Apéndice[43] del estándar lista las técnicas para identificar y analizarlos dejando una guía al usuario para su aplicación.

El resultado del análisis crea un perfil de riesgos que muestra la valoración de la importancia de cada uno y aporta una herramienta para priorizar los esfuerzos de tratamiento. Clasifica los riesgos de acuerdo a su importancia relativa, permitiendo situar a cada riesgo en un mapa de la zona afectada, describir los procedimientos primarios de control e indicar en qué zonas aumentar, disminuir o reajustar los mismos.

2.2.2. Evaluación de riesgos

Es el proceso de comparar los riesgos estimados con los criterios de riesgo establecidos, para tomar decisiones sobre la importancia y sobre si se deben aceptar o tratar.

2.3. Tratamiento de riesgos

Consiste en seleccionar y aplicar medidas para modificar el riesgo. Puede ser a través del control o mitigación, elusión, transferencia, financiación, etc. El documento plantea que cualquier sistema de tratamiento debe proporcionar:

- un funcionamiento efectivo y eficiente: asistido por el análisis de riesgos, al identificar los riesgos que requieren más atención.

- controles internos efectivos: grado en que el riesgo será eliminado o reducido mediante las medidas de control. Su "rentabilidad" significa vincular sus costos con los beneficios esperados

- conformidad con leyes y reglamentos: no es opcional

2.4. Informe y Comunicación

Aquí se separa lo que sería las unidades internas de las externas, refiriéndose a "Informe" cuando se refieren a la información distribuida en los distintos sectores de la propia empresa y "Comunicación" cuando refiere al diálogo con las unidades externas.

[43] ANEXO V de la monografía, pág. 131

Respecto al informe interno sostiene que los diferentes niveles necesitan distintos tipos de información. Por ejemplo, el Consejo de Administración requerirá información sobre cómo se están manejando los riesgos en cambio las Unidades de Negocios o los Individuos deben saber sus áreas de responsabilidad, qué indicios deben tenerlos alertas, las vías de comunicación existente, etc.

Para las partes externas, en la comunicación externa se debe tratar de informar las políticas de gestión de riesgos y la efectividad en la consecución de los objetivos. Los interesados esperan que las empresas den muestras de eficiencia y responsabilidad social. Un buen Gobierno Corporativo requiere que adopten un enfoque metódico de la gestión de riesgos que proteja el interés de los interesados y asegure que el consejo de administración dirige la estrategia, crea valor y supervisa el rendimiento y asegure que los controles de gestión existen y son efectivos.

2.5. Supervisión y revisión del proceso de gestión de riesgos

Se requiere una estructura de informe y revisión para asegurar que los riesgos están identificados y evaluados eficazmente y que se llevan a cabo los controles. Con regularidad deben hacerse auditorias de la política y conformidad con los estándares, y revisiones de su rendimiento para identificar oportunidades de mejora, ya que la empresa y el entorno son dinámicos. El proceso de supervisión debe asegurar que existen controles apropiados, se entienden y se siguen los procedimientos establecidos. Debe determinar si:

- las medidas y procedimientos adoptados dan el resultado previsto
- son apropiados los procesos adoptados y la información recogida para la valoración de riesgos
- un mayor conocimiento habría ayudado a tomar mejores decisiones

AS/NZS 4360:2004 – ADMINISTRACIÓN DE RIESGOS [44]

Introducción

El estándar AS/NZS 4360 fue el primero en salir en 1995. Hoy existe una tercera versión de 2004 la cual es reconocida mundialmente y ha sido adoptada en un gran número de empresas multinacionales traduciéndose al francés, español, chino, japonés y coreano.

ISO lo aprobó como estándar nacional. Más aún, los conceptos básicos del documento de AS/NZ fueron una base importante para la primera discusión del estándar internacional que trataremos más adelante: ISO 31000.

El objetivo de este estándar es proveer una guía que permita tanto a empresas públicas o privadas como a individuos, grupos o comunidades lograr:

- una base más confiable y rigurosa para la toma de decisiones y planificación
- mejor identificación de oportunidades y amenazas
- generar valor desde la incertidumbre y variabilidad
- una gestión proactiva más que reactiva
- asignación y utilización de recursos más afectiva
- mejorar la confianza de los stakeholders[45]
- mejorar el cumplimiento con legislaciones relevantes
- tener un mejor gobierno corporativo

Estructura

La estructura del estándar es la siguiente:

1. Alcance , ámbito de aplicación y definiciones
2. Requerimientos de administración de riesgos
3. Vista general de la administración de riesgos
4. Proceso de administración de riesgos
5. Documentación

[44] AS/NZS 4360:2004: Estándar Australiano - Administración de Riesgos
[45] Stakeholders: Partes interesadas

1. Alcance, ámbito de aplicación y definiciones

Las naciones de Australia y Nueva Zelanda crearon un estándar para uso genérico en toda de la sociedad. El documento plantea como área de riesgo a todos los riesgos. Es un marco teórico genérico, que establece el contexto, plantea la identificación, análisis, tratamientos, monitoreo y comunicación. El Libro de Guía[46] tiene como alcance una variedad de actividades, incluidas las actividades del sector público, comerciales, organizaciones voluntarias y sin fines de lucro.

Definiciones: El estándar plantea en este primer capítulo una serie de definiciones que se aplican en el documento. Dentro de las más destacables están:

- Riesgo: la posibilidad de que suceda algo que tendrá un impacto sobre los objetivos. Se lo mide en términos de consecuencias y probabilidades.
- Administración de riesgos: la cultura, procesos y estructuras que están dirigidas hacia la administración efectiva de oportunidades potenciales y efectos adversos.
- Proceso de administración de riesgos: la aplicación sistemática de políticas, procedimientos y prácticas de administración a las tareas de establecer el contexto, identificar, analizar, evaluar, tratar, monitorear y comunicar riesgos.

2. Requerimientos de administración de riesgos

En esta sección se plantea que la organización debe tener "un programa sistemático de administración de riesgos". Para ello la dirección debe:

- Desarrollar una política de administración de riesgo
- Definir y planificar los recursos: "La organización debe identificar los requerimientos de recursos y proveer recursos adecuados". También debe definir los roles y responsabilidades de las personas que llevan a cabo este proceso.
- Programar la implementación: el desarrollo de esta etapa está en el Apéndice B del documento. Plantea seis pasos para el desarrollo e implementación de un programa:
    - Respaldo de la alta gerencia
    - Desarrollar la política organizacional
    - Comunicar la política

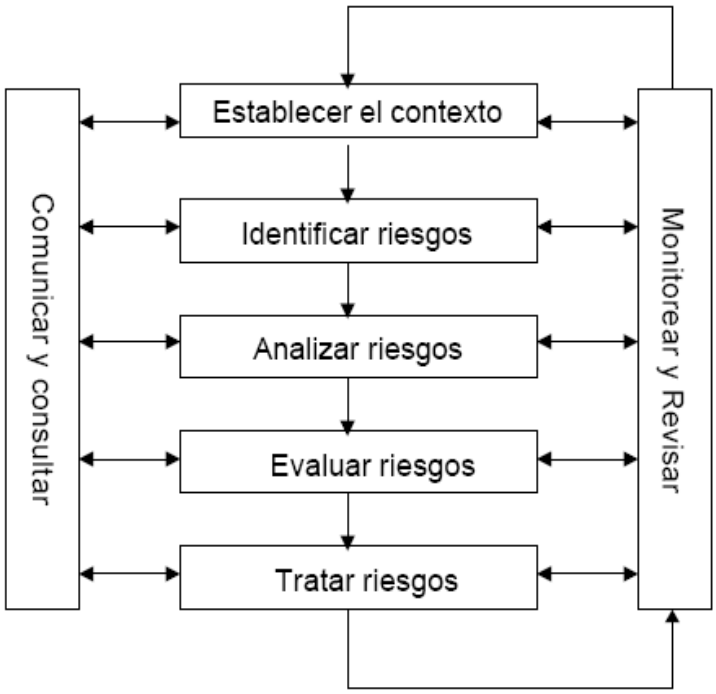
[46] Libro de Guía: Risk Management Guidelines Companion to AS/NZS 4360:2004 Standards Australia/Standards New Zealand

- Administrar riesgos a nivel organizacional
- Administrar riesgos a nivel de programa, proyecto y equipo
- Monitorear y revisar

- Revisión gerencial: el ejecutivo "debe asegurar que se lleve a cabo una revisión del sistema de administración de riesgos a intervalos especificados, suficiente para asegurar su continua conformidad y efectividad"

3. Vista general de la administración de riesgos

Se enfatiza que la administración de riesgos es un proceso multifacético, que tiene aspectos que generalmente son mejor manejados por un equipo multifacético. Es un proceso iterativo de continua evolución. La vista general, o dicho en otras palabras, el esquema de los elementos principales del proceso de administración de riesgos queda reflejado en la siguiente figura:



4. Proceso de administración de riesgos

Como vimos en el esquema de arriba, el proceso de administración de riesgos planteado tiene siete etapas.

4.1. *Establecer del contexto*: El marco define con gran detalle tres tipos de contextos que deben tomarse en cuenta para la administración de riesgos (organizacional, estratégico y para la administración de riesgo). Es importante porque define los parámetros básicos dentro de los cuales deben administrarse los riesgos y provee una guía para las decisiones dentro del estudio. Además, establece el alcance para el resto del proceso de administración de riesgos. De esta manera en esta etapa se identifican 5 aspectos:

- El contexto estratégico: definiendo la relación entre la organización y el ambiente, ya sea interno o externo. El estándar además agrega en el Anexo C un listado con una guía de cuáles pueden ser los potenciales interesados que influyen en el contexto estratégico.
- El contexto organizacional: entendiendo a la empresa y sus capacidades, así como sus metas y objetivos y estrategias para alcanzarlos.
- El contexto para la administración de riesgos: estableciendo el alcance y las fronteras para la aplicación del proceso de administración de riesgos. Por ejemplo: definiendo el proyecto o la actividad, incluyendo la extensión de tiempo y espacio, estableciendo las metas y objetivos.
- Desarrollar un criterio para la evaluación del riesgo: decidiendo qué criterios se van a utilizar para cada riesgo a la hora de ser evaluados. Esto envuelve decisiones sobre la aceptación de riesgo, su tratamiento y puede estar basado en aspectos: operacionales, técnicos, financieros, legales, sociales, humanitarios, etc.
- Definir la estructura: separando la actividad o el proyecto en un conjunto de elementos para proveer una guía lógica para la identificación y análisis del riesgo.

4.2. *Identificación de riesgo*: La segunda etapa significa identificar los riesgos para ser administrados. Esto incluye un proceso sistemático bien estructurado que debe contener: qué puede ocurrir, cómo puede ocurrir, herramientas y técnicas para la identificación. (Algunos ejemplos citados son: checklists, identificación basada en la experiencia y la historia, gráficos de evolución, tormenta de ideas).

El documento hace una mención importante y es que "la identificación debería incluir todos los riesgos, estén o no bajo control de la organización".

En su Anexo D enumera las fuentes genéricas de riesgo y sus áreas de impacto para que sirvan como guía a quienes quieran aplicarlo. La plantilla planteada como ejemplo para la identificación de riesgos se muestra en la siguiente figura:

Fuentes de Riesgo	Areas de Impacto				
	Seleccionar del Párrafo D3 según sea aplicable				
	*	*	*	*	*
Relaciones comerciales y legales					
Económicas					
Comportamiento humano					
Eventos naturales					
Circunstancias políticas					
Aspectos tecnológicos/técnicos					
Actividades y controles gerenciales					
Actividades individuales					

Las fuentes de riesgo y las áreas de impacto deberían adaptarse para la organización o actividad particular

Las áreas de impacto mencionadas como D3 en el gráfico pueden ser entre otras: Base de activos y recursos de la organización, incluyendo al personal; Ingresos y derechos; Costos de las actividades, tanto directos como indirectos; Comunidad; Desempeño; El ambiente; Intangibles tales como la reputación, gestos de buena voluntad, calidad de vida; Comportamiento organizacional, etc.

4.3. *Análisis de riesgo*: El objetivo es separar los riesgos con mayor aceptación de los riesgos con menos aceptación y proveer datos para asistir en la evolución y tratamiento de los riesgos.

Los pasos en el análisis de riesgo son:

- Determinar controles existentes: "Identificar la administración, sistemas técnicos y procedimientos existentes para controlar los riesgos y evaluar sus fortalezas y debilidades".
- Determinar consecuencias y probabilidad de ocurrencia: asegurar esto en el contexto de los controles existentes y luego cambiar las consecuencias y probabilidades para producir el nivel de riesgo.

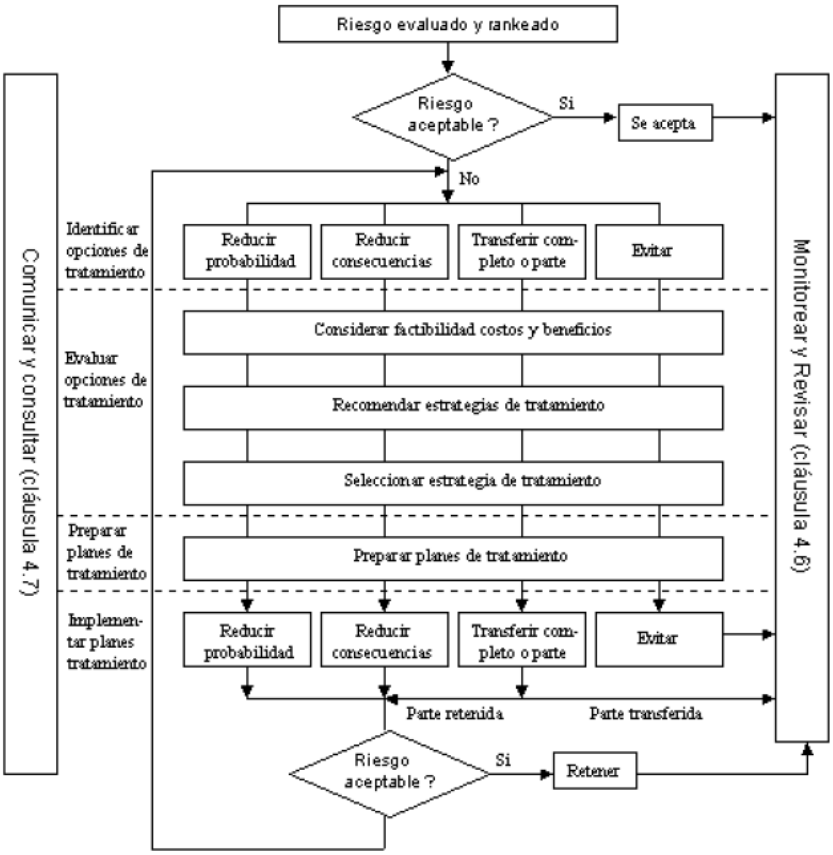
El documento sugiere que para evitar efectos negativos se deberían utilizar las mejores técnicas y fuentes de información disponibles. Algunas de las fuentes de

información planteadas son: Registros anteriores; Experiencia relevante; Prácticas y experiencia de la industria; Literatura relevante publicada; Comprobaciones de *marketing* e investigaciones de mercado; Experimentos y prototipos; Modelos económicos, de ingeniería u otros; Opiniones y juicios de especialistas y expertos. Las técnicas incluyen: entrevistas estructuradas con expertos en el área de interés; utilización de grupos multidisciplinarios de expertos; evaluaciones individuales utilizando cuestionarios; uso de modelos de computador u otros; y uso de árboles de fallas y árboles de eventos.

Tipos de análisis: El grado de refinamiento puede depender de la información de riesgo y los datos disponibles. El análisis puede ser cualitativo, semi-cualitativo o cuantitativo. El análisis cualitativo utiliza formatos de palabras o escalas descriptivas para describir la magnitud de las consecuencias potenciales y la probabilidad de que esas consecuencias ocurran. En el análisis semi-cuantitativo, a las escalas cualitativas, tales como las descriptas arriba, se les asignan valores. El objetivo es producir un ordenamiento de prioridades más detallado que el que se logra normalmente en el análisis cualitativo. El análisis cuantitativo utiliza valores numéricos para las consecuencias y probabilidades utilizando datos de distintas fuentes.

4.4. *Evaluación de riesgo*: implica comparar el nivel de riesgo durante el proceso de análisis previo a establecer el criterio de riesgo. El producto de la evaluación de riesgo es tener una lista de los riesgos con prioridades para tomar acciones posteriores. Si los riesgos caen en categorías de bajo riesgo o de riesgo aceptable, pueden ser aceptados con el mínimo de tratamiento y ser monitoreados regularmente para asegurarse se mantienen en este nivel.
Si no, deben ser tratados usando una o más de las opciones de la etapa siguiente.

4.5. *Tratamiento de riesgo*: Esta última etapa del proceso implica identificar las opciones, evaluarlas, preparar el plan de tratamiento de los riesgos e implementarlo. El proceso de tratamiento de riesgos se resume en la siguiente figura:

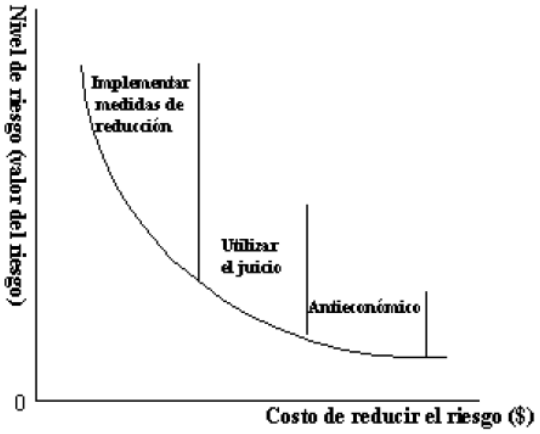


4.2 Proceso de Tratamiento de Riesgos

4.5.1. Identificar las opciones de tratamiento de riesgos. Pueden ser

- Evitar el riesgo al no proceder con la actividad
- Reducir la probabilidad de ocurrencia
- Reducir las consecuencias
- Transferir el riesgo
- Retener el riesgo

4.5.2. Evaluar las opciones de tratamiento que se van a utilizar: seleccionar las opciones más apropiadas implica balancear costos contra beneficios. El documento hace una fuerte mención a la consideración de los beneficios y las oportunidades. En particular, en la Guía de aplicación (Guidelines) se muestra en la figura 6.5 la medición de las oportunidades de insignificantes a para tener en cuenta. El estándar plantea que en general, el impacto más adverso puede generarse en el más bajo nivel. Esta idea se ilustra con la siguiente gráfica:



Bajo este esquema se plantea que es necesario priorizar cuando los costos de todos los tratamientos del riesgo están por encima del presupuesto.

4.5.3. Preparar el plan de tratamiento: en este paso deben identificar responsabilidades, cronogramas, la expectativa del resultado, presupuestos, medición de performances y un proceso de revisión continua.

4.5.4. Implementar los planes: La implementación idealmente debería llevarse a cabo por aquellos más capacitados para controlar los riesgos. "La implementación exitosa del plan de tratamiento del riesgo requiere un sistema efectivo de administración que especifique los métodos seleccionados, asigne responsabilidades y compromisos individuales por las acciones, y los monitoree respecto de criterios especificados".

4.6. *Monitoreo y revisión*: monitorear los riesgos, la efectividad del tratamiento, etc. "Los riesgos y la efectividad de las medidas de control necesitan ser monitoreadas para asegurar que las circunstancias cambiantes no alteren las prioridades de los riesgos. Pocos riesgos permanecen estáticos". Debe hacerse una revisión continua para asegurar que el plan inicial se mantiene.

4.7. *Comunicación y consulta*: importante en cada etapa del proceso. Este marco da gran importancia a desarrollar planes de comunicación tanto para los stakeholders[47] internos como externos. Enfatiza que el diálogo debe ser de ida y vuelta[48] con los esfuerzos enfocados en la consulta. Menciona que es

[47] Stakeholders: Partes interesadas
[48] Two Way Dialogue

importante que esta etapa se desarrolle desde el inicio del proceso de gestión de riesgos. Por eso en el esquema se ubica al costado de las etapas a lo largo de todo el proceso.

5. Documentación

El estándar plantea que debería documentarse cada etapa del proceso de administración de riesgos. Da una serie de razones por las cuales es apropiado documentar que consideramos importante detallar:

a) demostrar que el proceso es conducido apropiadamente;
b) proveer evidencia de un enfoque sistemático de identificación y análisis de riesgos;
c) proveer un registro de los riesgos y desarrollar la base de datos de conocimientos de la organización;
d) proveer a los tomadores de decisión relevantes de un plan de administración de riesgos para aprobación y subsiguiente implementación;
e) proveer un mecanismo y herramienta de responsabilidad;
f) facilitar el continuo monitoreo y revisión;
g) proveer una pista de auditoria; y
h) compartir y comunicar información.

BS 31100 – CÓDIGO DE PRÁCTICA PARA LA GESTIÓN DE RIESGOS [49]

Introducción

La norma internacional sobre gestión de riesgos BS 31100: Código de prácticas para la administración de riesgos (en adelante BS 31100) es un estándar internacional publicado en octubre 2008 por el BSI Group.

El estándar provee definiciones sobre riesgos y administración de riesgos y una guía sobre los principios, modelos, procesos que se podrían seguir para aplicarlos.

Define al riesgo como algo que puede ocurrir y afectar el cumplimiento de los objetivos. Con una nota a la misma que afirma que los impactos pueden ser tanto positivos como negativos (amenazas y oportunidades)

Respecto a la definición de Administración de riesgos, lo establece como el desarrollo estructurado y aplicación de la gerencia de: la cultura, los procedimientos, las políticas y las prácticas para identificar, evaluar y responder a los riesgos.

El objetivo planteado es asistir a las organizaciones a alcanzar los objetivos a través de una administración de riesgos efectiva.

Estructura

BS 31100 está estructurado de la siguiente manera:

1. Alcance
2. Principios
3. Modelo de gestión de riesgos
4. Esquema de gestión de riesgos
5. Proceso
6. Implementación

[49] Draft BS 31100 Code of practice for risk management

1. Alcance

El documento menciona que las recomendaciones son genéricas y están definidas para ser aplicadas en todo tipo de organizaciones y en cualquier parte de la organización, sean del sector público o privado, sin importar el tipo de empresa tamaño o naturaleza. Define además que el estándar puede ser utilizado por cualquiera responsable de:

- Asegurarse la empresa alcance sus objetivos
- Asegurarse los riesgos están siendo manejados en determinadas áreas o actividades
- Está encargado de supervisar la gestión de riesgos en una organización
- Está encargado de evaluar la gestión de riesgos de determinada empresa.

2. Principios

Uno de los puntos a destacar en este estándar es el planteo que establece que la organización debería basar sus prácticas de gestión en una serie de principios bien definidos. Éstos deberían derivar entre otras cosas de: la experiencia, las buenas prácticas, el gobierno corporativo, etc. El objetivo de definirlos es, entre otras cosas, proveer una base, un fundamento de lo que se entiende es una efectiva gestión de riesgos que contribuye a mejorar la performance de la organización. Se plantean 10 principios:

2.1. *La gestión de riesgos debe ser sistemática y estructurada*: esto asegura que los resultados sean confiables, robustos y comparables en el tiempo y que la toma de decisiones se realiza con confianza.

2.2. *La gestión de riesgos debe estar basada en la experiencia pasada:* debe estar basada en datos históricos, experiencia, conocimiento del tema, juicios de expertos, proyecciones, etc.

2.3. *La gestión de riesgos debe definir la incertidumbre y sus causas:* es necesario que quede claramente definida la diferencia entre riesgo, causa y efecto.

2.4. *La gestión de riesgos es parte de la toma de decisiones:* al hacer que los riesgos sean explícitos, conocidos y comunicados oportunamente, pueden ayudar en la elección de la mejor alternativa sobre qué acción o medida se va a tomar.

2.5. *La gestión de riesgos tiene en cuenta los factores humanos y comportamientos:* los factores humanos pueden afectar o influenciar la efectividad de las prácticas

de gestión de riesgos, por eso deben ser tomados en cuanta al momento de la implementación.

2.6. *La gestión de riesgos agrega valor y genera beneficios:* la optimización de este proceso y de los planes de respuesta a los riesgos deberían contribuir en una demostrable y clara maximización de valor de la organización y del alcance de los objetivos. Esto se puede ver por ejemplo en: la eficiencia de los procesos, la performance financiera, el cumplimiento legal y regulatorio, el buen gobierno corporativo, la buena reputación, aceptación del público, etc.

2.7. *La gestión de riesgos es hecha a medida:* El proceso de administración de riesgos no puede ser aplicado de una sola y determinada manera ni para un solo tipo de organización. Cada empresa debe ajustarla como a sus circunstancias reflejando como mínimo: su estructura, su contexto legal y regulatorio, sus procesos, las expectativas de sus accionistas, etc.

2.8. *La gestión de riesgos da transparencia y toma en cuenta a los accionistas*[50]*:* Un aspecto fundamental es el interés sobre los accionistas y cómo éstos podrían influenciar o modificar los resultados. Para esto es necesario entonces: identificarlos, tener en cuenta sus objetivos, su grado de influencia y el deseo de estar involucrado o no en el proceso, desarrollando un plan de comunicación para mantenerlos informados e involucrados y asegurarse la toma de decisiones sobre los puntos clave de la organización están siendo tomadas por ellos.

2.9. *La gestión de riesgos está atenta y responde al cambio:* toda empresa para sobrevivir y subsistir debe constantemente reinventarse a través del proceso de innovación y cambio ya que el ambiente está cambiando constantemente ya sea en aspectos legales, regulatorios, competitivos, comunicacionales, tecnológicos, etc.

2.10. *La gestión de riesgos es aplicada a lo largo de la empresa:* se toman en cuenta todos los aspectos de la organización: el gobierno corporativo, la cultura, los procesos, la estructura y asegura que se aplique en todos los niveles coordinados para lograr el cumplimiento de los objetivos.

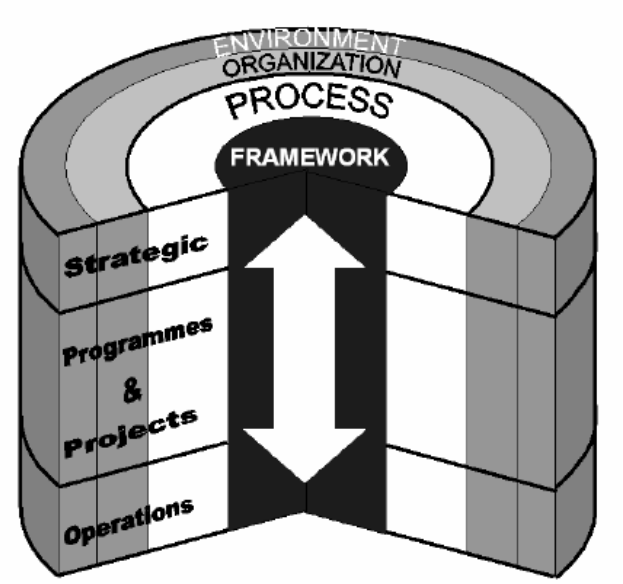
[50] Stakeholders

3. Modelo de gestión de riesgos

Éste es un modelo tridimensional en el que se ve la gestión de riesgos como un componente que recorre toda la estructura y los diferentes niveles de la organización. Los componentes son:

- El entorno
- La organización
- Los procesos
- El marco para la gestión de riesgo.

Figure 1 — Risk management model



La aplicación de los componentes puede darse en diferentes niveles los cuales se sintetizan en: estratégico, programas y proceso y operacionales.

4. Esquema de Gestión de riesgos

Mientras el modelo planteaba una visión más general de la gestión de riesgos en este capítulo se desagrega detalladamente los aspectos que se deben tener en cuenta para llevar a cabo el proceso.

Se define un esquema tipo de gestión de riesgos para proveer las bases, los fundamentos y una estructura común para desarrollar, mantener y administrar los riesgos a través de la empresa.

El esquema tiene las siguientes características:

- Define claramente el alcance y los parámetros para la gestión de riesgos

- Da un entendimiento común de lo que es y define conceptos y terminologías claves
- Asegura la gestión de riesgo es aplicada de una manera consistente, disciplinada y controlada.
- Permite el uso eficaz de capital y recursos

Los componentes del esquema están ilustrados en la siguiente figura:

Figure 2 – Risk management framework

Desarrollaremos cada uno de los componentes:

4.1. La cultura

El objetivo de este componente es asegurar que el pensamiento de gestión de riesgos está embebido en los procesos y prácticas de todos los niveles de la empresa y se convierte en una parte integral de la operativa diaria; existe conciencia; el personal tiene suficientes habilidades, conocimientos y competencias para desarrollar la gestión de riesgos.

La cultura de riesgos debe exhibir los siguientes elementos:

- Dar clara evidencia de soporte desde los altos niveles
- Dar un claro entendimiento de los roles de cada uno para enfrentar el riesgo
- Considerar que la Gestión de Riesgos es automática
- Generar discusiones claras y honestas
- Asegurarse que la información es compartida a través de la organización

- Debe considerarse como parte de la empresa
- Debe ser reforzada dentro de los proceso de la empresa.

4.2. Gobierno Corporativo

El estándar lo define como la estructura, los procesos, el tono en el cual la gestión de riesgos es llevada a cabo y las responsabilidades y autoridades están definidas y asignadas. El objetivo de la gestión del Gobierno Corporativo es asegurar que las estructuras y mecanismos son creados y especificados para:

- Permitir al ejecutarlo recibir feedback de los riesgos principales regularmente y en tiempo
- Proveer una visión independientemente de todos los aspectos de la gestión de riesgos en la organización y asegurar la integridad y aplicabilidad del marco y sus componentes.

El documento hace un paralelismo con los componentes vistos en el modelo planteando donde el Gobierno Corporativo es el resultado de unificar varios componentes del marco de gestión de riesgos, por ejemplo: estrategia, apetito de riesgo, políticas, roles, reportes, cultura, etc.

4.3. Estrategia para la Administración de riesgos

El objetivo de este componente es asegurar que las prioridades y actividades definidas en la administración de riesgos están alineadas con los objetivos generales de la organización y que el ejecutivo tiene un entendimiento claro y consistente sobre dichas prioridades y actividades que se van a realizar. Es necesario que esta estrategia permita:

- Desarrollarse de la mano de las estrategias de la organización
- Tener en cuenta la empresa y el contexto
- Ser documentada y aprobada por el ejecutivo
- Ser comunicada por todos los niveles
- Ser revisada regularmente para asegurarse está alineada con los objetivos y desafíos que tiene la organización.

4.4. Nivel de riesgo aceptado[51]

Es la cantidad de riesgo que una organización está preparada a aceptar, tolerar, o verse expuesta en cualquier momento del tiempo. Es la actitud de la organización frente al riesgo.

[51] Risk Appetite

4.5. Política de Administración de Riesgos

Es el documento que provee los lineamientos claros y concisos de la organización sobre la administración de riesgos; define acciones necesarias que deben ser llevados a cabo y las consecuencias por no adherirse a esto.

La política debe establecer un marco para la gestión de riesgos, definir los requerimientos mínimos y los puntos clave a ser tenidos en cuenta, definir el tono del proceso y comunicar cómo la administración va a ser implementada.

4.6. Categorías de riesgos y medición de impacto

Este paso tiene dos objetivos:

a) lograr consistencia en la clasificación, medición y reporte de los riesgos lo que permitirá comparar perfiles de riesgo;

b) crear una base para desarrollar metodologías de medición más avanzadas.

El documento lista, las categorías de riesgos más comunes así como las categorías de impacto, que difieren según el tipo de organización.

Para medir los riesgos, el criterio planteado tiene dos dimensiones. Estas dimensiones tienen un alcance básico y es el más aceptado: probabilidad e impacto. Las mismas pueden variar usando escalas por ejemplo: alto medio bajo, o de 1 a 5.

4.7. Roles y responsabilidades

El documento hace un fuerte hincapié en los roles y responsabilidades, mencionando que la organización debe tener claramente identificados los roles y responsabilidades que son requeridos para desarrollar la gestión de riesgos. El documento deja detalladamente planteadas las responsabilidades:

El Ejecutivo

La responsabilidad última de la administración de riesgos está en el Ejecutivo y esto se debe ver reflejado y documentado.

El equipo de gestión de riesgos

Es el encargado de monitorear el desarrollo, implementación y mantenimiento de la gestión de riesgos a lo largo de la organización.

El director o gerente de riesgos

Dependiendo del tamaño de la empresa el gerente de riesgo puede ser una sola persona dedicándose al tema o puede ser un individuo que trabaja parte del tiempo según las directrices dadas por el comité de riesgo.

Las unidades o departamentos

Son los primeros responsables de la administración de riesgos ya que están en el día a día. También son responsables de crear la conciencia de riesgo.

De los individuos

Cada individuo tiene como responsabilidad contribuir a la administración de riesgo y la incertidumbre al realizar sus tareas diarias.

Del dueño de riesgo

Se define "dueño de riesgo" al rol o el individuo responsable por la administración de todos los aspectos de un riesgo específico. Es el encargado de identificar los riesgos que necesitan ser activamente tratados.

De auditores internos y externos

Es probable que en organizaciones grandes exista la figura de la auditoría interna. Las pequeñas empresas posiblemente sólo reciban input de los auditores externos. En caso de tener auditoria interna, la misma debiera informar a la alta gerencia cómo está la administración de riesgos, si se está actuando sobre los riesgos claves y cuán confiable está siendo el proceso. Los auditores externos tendrían similares roles enfocado es su trabajo de auditoría.

4.8. Herramientas para la Administración de riesgo

Las herramientas a las que hace referencia son las prácticas, técnicas, documentos, sistemas, consejos, sugerencias, modelos, que debe tener la empresa para la gestión de riesgos. Cada organización debería tener un conjunto de herramientas alineadas al marco de administración de riesgo de la organización en particular, de los procesos, escala, complejidad, etc.

Como existe una gran variedad para seleccionar y no todas se adecuan a los requerimientos de la empresa en un determinado momento o sobre un tema específico, se plantea que las mismas deben ser elegidas en base a:

- Para quién y para qué está dirigido y cuál es el resultado deseado
- Cuál es el objetivo de llevar a cabo de la actividad
- El nivel de actividad a ser llevada a cabo
- Que tan o cuan familiar está el usuario con la herramienta para aplicarla
- Cuan familiarizados están todos los participantes con la herramienta
- La disponibilidad de la información
- La capacidad del usuario de entrever
- Su facilidad de uso, aplicabilidad, adecuación

En el Anexo A del documento[52] se detalla un listado bastante extenso de las posibles herramientas que se podrían utilizar.

4.9. Entrenamiento

El entrenamiento es una ayuda fundamental en el tema para asegurar los conceptos y la mentalidad de gestión de riesgos está incorporada a través de toda la organización y para lograr lo que se llama madurez de riesgo[53].

Dependiendo del propósito, naturaleza y extensión del entrenamiento puede proveerse conocimiento sobre por ejemplo: gobierno corporativo, cumplimiento legal, políticas y procedimientos, modelo de madurez, procesos de administración de riesgos: roles, responsabilidades, reportes, cómo identificarlos, etc.

4.10. Reporte

Los reportes y el flujo de información sobre la gestión de riesgos son claves para:

- Monitorear y manejar efectivamente los riesgos
- Satisfacer los requerimientos y las expectativas de los accionistas y asegurarse que la organización está manejando los riesgos de una forma completa y diligentemente.

Existen dos tipos de reportes: interno y externos. Los reportes internos deben estar mapeados sobre la estructura organizacional y seguir el flujo de información establecido

[52] Anexo IX de la monografía, pág. 135

[53] Se define madurez de riesgo como la extensión a través de la cual ha sido adoptado y aplicado un enfoque robusto de gestión de riesgo, planificado por la dirección a través de la organización para identificar, evaluar, decidir la respuesta y reportar oportunidades y amenazas que afectan el alcanzar los objetivos de la organización. Definición tomada del Instituto de Auditores internos, www.theiia.org

a través de ella. Estos reportes deben permitir entre otras cosas: monitorear el trabajo, escalar temas importantes, identificar cambios significativos, resaltar las áreas que tiene problemas o gaps, etc.

Los reportes externos son esenciales para los accionistas ya que muestra la gestión de riesgos, los resultados y su efectividad.

4.11. Revisión

Dado que una empresa está en continuo cambio fruto del ambiente dinámico en el que se desarrolla, se plantea como necesario el paso de revisión. Una gestión de riesgos efectiva y eficiente requiere una estructura de revisión que asegure los cambios de la organización y el ambiente son tomados en cuenta y encajan o siguen los objetivos planteados.

El tiempo en el cual el plan se debe revisar depende de cada tipo de organización. Sin embargo, se recomienda que al menos se realice una revisión una vez al año que permita por lo menos determinar si:

- El plan está alineado
- Los resultados son los esperados
- Las partes interesadas[54] están recibiendo adecuadamente los reportes y la información
- El personal tiene habilidades y conocimiento suficientes para desarrollar el proceso
- Adecuar las actividades y prioridades para el futuro.

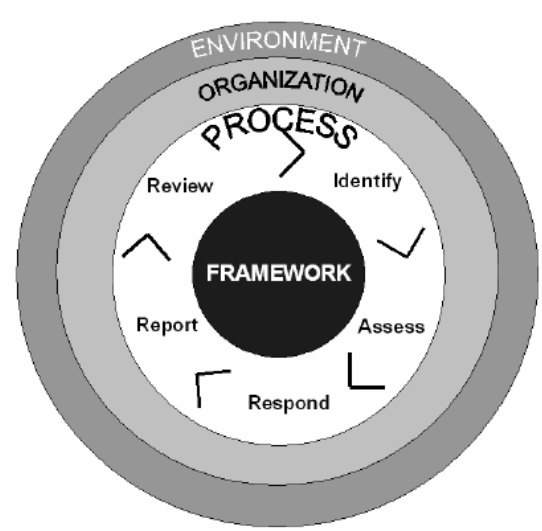
5. El proceso de Administración de riesgos

La definición del proceso permite puntualizar de manera efectiva, eficiente y sistemática el modo en el que los riesgos deben ser manejados a través de una organización. Es un proceso cíclico que debe ser adaptado para cada organización.

El esquema está definido por cinco pasos a través de la siguiente figura:

[54] Stakeholders

Figure 3 – The risk management process



5.1. Identificación de riesgos

La primera etapa es la identificación de riesgos la cual debiera hacerse metódicamente (cuando sea posible) para asegurarse entre otras cosas que:

- Todas las fuentes de incertidumbre son identificadas
- Tanto las oportunidades como las amenazas están planteadas como parte del proceso
- Las causas están determinadas
- La validez de los supuestos y las limitaciones están testeados
- Están identificados los posibles conflictos entre ahorristas y los objetivos del proceso.

El proceso de identificación de riesgos debe ser iterativo y redefinirse constantemente hasta lograr que los riesgos estén adecuada y apropiadamente reflejados. La identificación no solo debe ser apropiada sino también debe tener en cuenta el costo-beneficio del proceso. El proceso es tanto para identificar riesgos existentes como emergentes.

5.2. Evaluación de riesgos

La siguiente etapa es la evaluación de riesgos. En esta etapa se destacan dos pasos fundamentales: el análisis de riesgos y priorización, y la evaluación. La parte de análisis implica definir la probabilidad de ocurrencia y el impacto teniendo en cuenta los controles existentes y su efectividad.

Esta actividad debe estar en concordancia con el criterio de medición de riesgos.

El análisis se debe desagregar en distintos grados de detalle dependiendo del tipo de riesgo, el propósito del análisis, la información y los recursos disponibles. Debe ser un proceso iterativo que se repita cada vez que aparezca más información. El impacto debe ser medido planteando modelos de resultados según un evento o un set de eventos.
Luego que los riesgos son analizados y se ha establecido un nivel o categoría de riesgo a cada uno es necesario priorizarlos.
La segunda parte de la evaluación de riesgo debe compilar y calcular los perfiles de riesgo combinando: el análisis de riesgos, el nivel de riesgo establecido, el apetito de riesgo aceptado.
Esta información debe luego ser utilizada para informar y facilitar las decisiones sobre si responder al riesgo o no o si es necesario revisar las prioridades.
Se debe tener en cuenta que a veces de la misma evaluación de riesgos puede surgir decidir que es necesario mayor análisis o incluso que pueden surgir nuevos riesgos a ser identificados.

5.3. Respuesta al riesgo

El objetivo de esta etapa es administrar la respuesta a los riesgos según la aceptación y la tolerancia de riesgo que tenga la empresa. Una o más de las opciones de evitar, modificar, transferir o aceptar pueden ser consideradas y aplicadas a un riesgo específico.

Cuando se está analizando el método de respuesta a adoptar se debe tener en cuenta el neto de los beneficios comparados con los costos y el retorno costo-beneficio si se aplicaran otras respuestas. Como la empresa no tiene fondos ilimitados para responder a todos los riesgos, es imprescindible priorizar para definir la implementación.

5.4. Reporte

Es el proceso de comunicar los puntos y resultados claves del proceso de gestión de riesgo. El reporte debe respetar la jerarquía de la empresa. El objetivo de esta etapa es proveer seguridad que la gestión de riesgos está operando y se hace efectivamente y que los riesgos están siendo manejados. Esto genera confianza en la toma de decisiones y en el cumplimiento de los objetivos.

5.5. Revisión

La revisión del proceso permite que la empresa monitoree:

- Si los riesgos fundamentales se manejan en función del apetito y la tolerancia de riesgo en las áreas responsables.
- Si los perfiles de riesgos son adecuados y los posibles cambios que pudieren tener a lo largo del tiempo
- El progreso de los mitigantes planteados y las acciones tomadas para tratar los riesgos.

El proceso de revisión también permite entre otras cosas: escalar temas, repriorizar recursos, generar mejor información y cómo consecuencia mejores toma de decisiones.

La revisión y el reporte regular de los riesgos identificados y tratados y el proceso general de administración de riesgos es fundamental para que la empresa sea capaz de administrar los riesgos activamente, agruparlos, revisar y responder ante los cambios de los perfiles de riesgos a lo largo de todos los niveles de la organización.

ISO 31000:2009 GESTIÓN DE RIESGOS – PRINCIPIOS Y DIRECTRICES [55]

Introducción

La norma internacional sobre gestión de riesgos ISO 31000 es un estándar internacional sobre la administración de riesgo empresarial que fue adoptada por el Comité Técnico de ISO[56] y publicada en octubre de 2009. El desarrollo del marco teórico empezó en el 2005 cuando Australia y Nueva Zelanda propusieron mejorar su estándar existente (AZ/NZS 4360) y llevarlo a un nivel de estándar internacional. ISO entendió era necesario este estándar pero no en base a la adaptación del antes mencionado sino en base al desarrollo de uno nuevo que incorporara los conceptos y componentes de los mayores estándares existentes. El objetivo principal es poder crear un documento que provea una guía de principios y prácticas para el proceso de administración de riesgos.

En la introducción del documento se justifican los beneficios de utilizarlo. Se plantea que la administración de riesgos manejada de acuerdo a este estándar puede permitir:

- Aumentar la probabilidad de lograr los objetivos
- Fomentar una administración proactiva
- Estar consciente de la necesidad de identificar y tratar los riesgos a lo largo de la organización
- Mejorar la identificación de oportunidades y amenazas
- Cumplir con las leyes y regulaciones así como con las normas internacionales
- Mejorar los reportes financieros
- Mejorar el Gobierno Corporativo
- Mejorar la confianza de las partes interesadas[57]
- Establecer una base cierta para la toma de decisiones y la planificación
- Mejorar los controles
- Utilizar recursos de manera efectiva para el tratamiento de riesgos
- Mejorar la eficacia y eficiencia de las operaciones
- Asegurar una performance segura y saludable, tomando también en cuenta el ambiente
- Mejorar las predicciones de pérdidas e incidentes
- Minimizar las pérdidas
- Fomentar el aprendizaje de la organización
- Mejorar la capacidad de la organización

[55] ISO/IEC 31000: ISO/FDIS 31000:2009 Risk management — Principles and guidelines
[56] ISO Risk Management Technical Committee
[57] Stakeholders

Estructura

ISO 31000 está estructurado de la siguiente manera:

1. Alcance y ámbito de aplicación
2. Referencias normativas. Términos y definiciones
3. Principios para la administración de riesgos
4. Marco integrado
5. Proceso

1. Alcance y ámbito de aplicación

En esta primera parte del documento se describe el alcance global y su aplicabilidad universal por estar dirigido a "cualquier asociación, grupo, empresa y persona pública, privada o comunitaria" y "a través de toda la vida de una organización y de los variados rangos de actividades, procesos, funciones, proyectos, productos, servicios, activos, operaciones y decisiones". Es un estándar genérico no especificado para ninguna industria o sector particular. Aunque los lineamientos son genéricos, la idea del documento no es impartir uniformidad o un modo de operar ideal en todas las empresas sino que pueda ser adaptable a cada caso específico.

2. Referencias normativas. Términos y definiciones

Principalmente hace referencia a la Guía 73[58], como documento indispensable para la aplicación del ISO 31000. Respeta los términos y definiciones; más aún las definiciones del documento son traídas de la Guía 73, mencionada anteriormente.
El objetivo de incluir estas referencias de un documento separado en vez de incluir dentro del estándar todos los términos y definiciones es que el vocabulario manejado sobre todos los puntos de riesgos y administración de riesgos sean el mismo ya que existen varios estándares internacionales que utilizaron esta guía para sus definiciones. Para asegurar la consistencia del uso de términos y definiciones en todos los estándares, pareciera que hace sentido definir el vocabulario en un documento separado.

3. Principios para el manejo de riesgos

La tercera sección define once principios básicos para la gestión de riesgos:
3.1. La administración de riesgos crea y protege valor

[58] ISO/IEC Guide 73, Risk Management – Vocabulary (ISO 73)

3.2. La administración de riesgos es una parte integrada de toda la organización

3.3. La administración de riesgos es parte de la toma de decisiones

3.4. La administración de riesgos explícitamente define la incertidumbre

3.5. La administración de riesgos es sistemática, estructurada y oportuna

3.6. La administración de riesgos está basada en la mejor información disponible

3.7. La administración de riesgos se hace a medida, alineada con el contexto interno y externo.

3.8. La administración de riesgos toma en cuenta factores humanos y culturales

3.9. La administración de riesgos es transparente e inclusiva

3.10. La administración de riesgos es dinámica, iterativa y responde al cambio

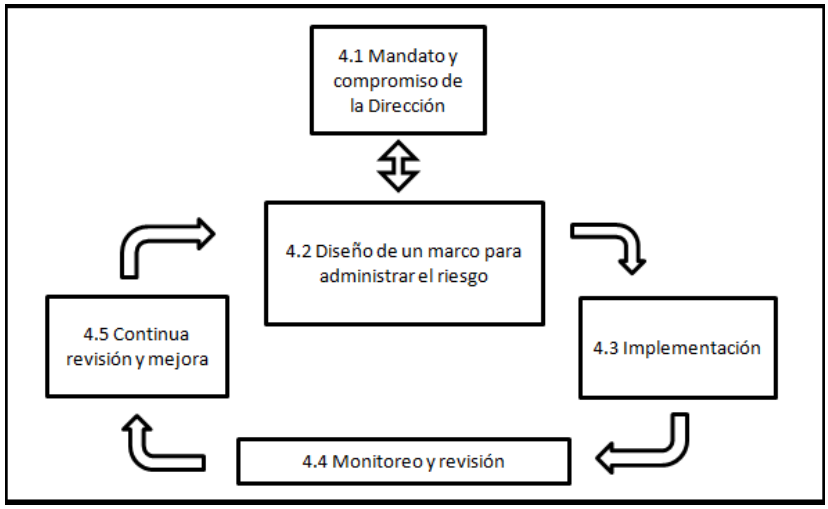
3.11. La administración de riesgos facilita la mejora continua y el mejor valor de una organización

4. Marco integrado

La cuarta sección describe el esquema del proceso de administración de riesgos, dando los lineamentos y las disposiciones que la organización debe impartir en todos los niveles de la empresa. Establece claramente que la idea de este marco no es imponer un sistema de gestión de riesgos sino que cada organización debe adaptarlo.

El objetivo del marco es asegurar que la información sobre los riesgos derivada de los procesos es adecuadamente reportada y utilizada como una base para la toma de decisiones en todos los niveles de la organización.

Los componentes necesarios para la gestión de riesgos serían los siguientes:



4.1. *Mandato y compromiso de la Dirección*: para asegurar la efectividad del plan es necesario que la dirección esté fuertemente comprometida. Para eso debe, entre otras cosas: definir y reforzar las políticas, asegurarse la cultura, políticas, procedimientos y objetivos organizacionales y de gestión de riesgo están alineados, asegurarse se tienen los recursos necesarios, comunicar los beneficios de la gestión de riesgos.

4.2. *Diseño un marco para administrar el riesgo*: Debería tener como mínimo los siguientes pasos:

- Entender la organización y su contexto (tanto interno como externo)
- Establecer las políticas de gestión de riesgos
- Definir responsabilidades
- Integrar el plan dentro de los procesos de la organización
- Identificar recursos
- Establecer las vías de comunicación interna y reportes
- Establecer las vías de comunicación externa y reportes

4.3. *Implementación*: la implementación del marco de gestión de riesgos consiste entre otras cosas: definición de estrategias de implementación y un apropiado timing; estar acorde con los requerimientos legales y regulatorios y con las políticas y procedimientos de la organización, tener buena comunicación con los interesados para asegurarse el plan es apropiado.

4.4. *Monitoreo y revisión*: Para asegurar la efectividad y continuidad se debe revisar periódicamente la performance del plan. La revisión consiste entre otras cosas en: comparaciones contra indicadores preestablecidos, mediciones del progreso y las desviaciones del plan, adecuación del proceso a lo largo del tiempo, efectividad.

4.5. *Revisión continua y mejora*: basados en los resultados del monitoreo, las decisiones deben ser tomadas en función de cómo se puede mejorar la gestión de riesgos.

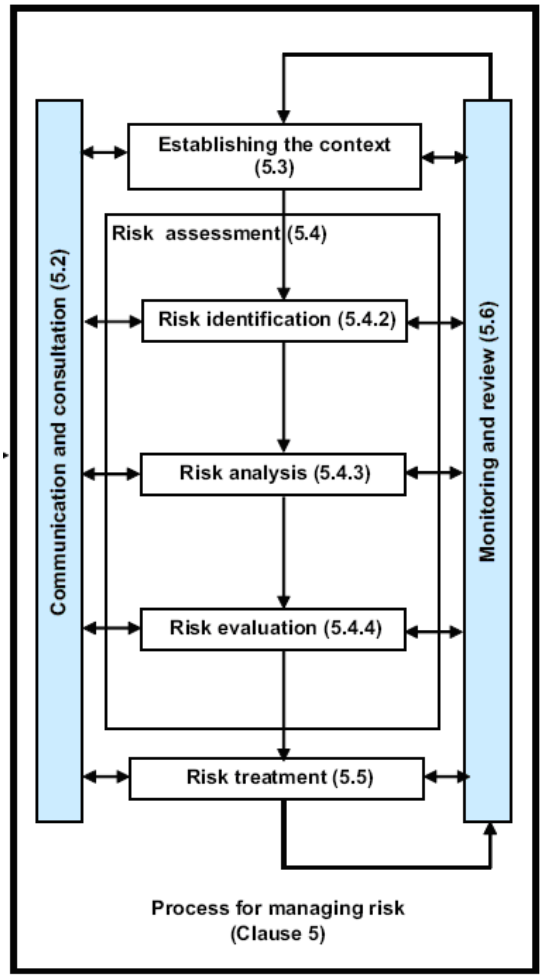
5. Proceso

Este capítulo es el más extenso. Al haber tomado como base el documento AS/NZS 4360:2004 de Australia y Nueva Zelanda, veremos las etapas del proceso son iguales y la diferencia está en la información proporcionada.

El proceso de administración de riesgos debe ser:

- Una parte integral de la gestión de la empresa
- Incorporado a la cultura y las prácticas organizacionales
- Adaptado al proceso de negocios que se tenga.

Considera las siguientes seis principales actividades:



5.1. *Establecer el contexto*: en este paso, la empresa define los parámetros internos y externos que serán tomados en cuenta para la administración de riesgos. El contexto puede incluir tanto parámetros internos como externos, relevantes para la organización (know-how, sistemas de información o políticas

económicas, ambiente competitivos, percepción de valores, etc.). Además, el contexto debe ser desarrollado (al definir roles y responsabilidades, metodologías, etc.). Por último, es importante en este proceso establecer el criterio para evaluar riesgos. Este criterio debería ser consistente con las políticas de administración de riesgos, reflejando los objetivos, valores y recursos. Debe quedar definido al principio del proceso y ser continuamente revisado. Este punto, puede ser considerado un paso similar al marco teórico visto en el punto 4. Sin embargo, en esta etapa el establecimiento debe ser más detallado que en la etapa vista anteriormente.

5.2. *Análisis y evaluación de riesgos*: Esta etapa es el proceso total de identificación, análisis y evaluación de riesgos. El objetivo de la primera actividad – identificación de riesgos - es crear una lista exhaustiva de los riesgos que podrían afectar el cumplimiento de los objetivos de la organización. En este contexto, está definida la importancia de identificar todos los riesgos, independientemente de que estén o no asociados a la búsqueda de una oportunidad.

La segunda actividad – análisis de riesgos – da los conceptos para la evaluación de riesgos así como para las decisiones de las medidas más apropiadas a tomar para tratarlos. Un riesgo en particular es analizado determinando sus consecuencias y su probabilidad de ocurrencia. En el texto se enfatiza que la confianza en la determinación de riesgos y su sensibilidad en las precondiciones y supuestos deben ser consideradas en el análisis y comunicadas efectivamente.

El tercer paso – evaluación de riesgos – implica comparar el nivel de riesgo determinado durante el análisis con el criterio definido anteriormente para priorizar la implementación de medidas adecuadas de tratamiento y mitigación.

El estándar hace referencia al IEC 31010 – técnicas para evaluar riesgos para la aplicación práctica de esta etapa.

5.3. *Tratamiento de riesgos*: Este paso envuelve la selección de una o más opciones para evitar, reducir, transferir, compartir, aceptar, asumir los riesgos identificados así como la implementación de las mejores medidas a tomar. La elección de estas mejores medidas implica balancear costos del esfuerzo con sus

beneficios (que no necesariamente tienen que ser exclusivamente monetarios). Se enfatiza que cuando se seleccionan los tratamientos de riesgos, la organización debe considerar los valores y percepciones de los accionistas y los mejores medios para estar comunicados con ellos. Otro aspecto importante es que se debe tener en cuenta que el tratamiento de riesgos en sí mismo, puede generar nuevos riesgos, como la falla o inefectividad de las medidas elegidas. Además un monitoreo adecuados debe ser parte integral del plan de tratamiento. Finalmente, se menciona que el plan debe establecer claramente la lista de prioridades y debe quedar documentado con las razones por las que se eligió, las responsabilidades, acciones propuestas, los recursos necesarios, medidas o limitaciones para llevarlo a cabo, planificación de tiempos, etc.

5.4. *Supervisión - monitoreo y revisión*: El monitoreo puede ser regular y ad hoc y la revisión de actividades deben acompañar todos los aspectos del proceso de administración de riesgos y referirse a todos los pasos descriptos anteriormente. El objetivo de este proceso es entre otras cosas: analizar y aprender lecciones de los eventos, detectando cambios en el contexto interno y externo, asegurándose que el tratamiento ha sido efectivo e identificando riesgos emergentes, obteniendo así más información para mejorar. Los resultados de esta etapa deben ser registrados y reportados también pudiendo utilizarse de input a la hora de revisar el marco

5.5. *Diálogo - comunicación y consulta*: La comunicación y la consulta son vistas como una parte integrada de las actividades de administración de riesgos y por tanto deben ser aplicadas en todas las etapas del proceso, incluyendo todas las partes interesadas[59] relevantes sean internas como externas. Es recomendado que el plan de comunicación y consulta sea desarrollado en la primera etapa, fijando temas relacionados con el riesgo en sí mismo, así como con las consecuencias y las medidas que se deben tomar para administrarlo. El marco sugiere un equipo de consulta para mantener la fluida comunicación. Además se hace un fuerte énfasis en el hecho que la comunicación y consulta es muy importante ya que los accionistas hacen juicios de valor basados en sus

[59] Stakeholders

percepciones de riesgo, las que pueden variar en gran medida por las diferencias que tengan en los valores, sus necesidades, sus supuestos, conceptos e inquietudes.

5.6. *Registro del proceso*: Las actividades de la administración de riesgos deben ser fáciles de ubicar y estar disponible para todos; los documentos deben proveer información que sirva de ayuda para reforzar métodos y herramientas, así como todo el proceso de administración.

CAPITULO IV: ANÁLISIS COMPARATIVO

En este capítulo, realizaremos el análisis comparativo de los enfoques desarrollados en los capítulos anteriores con relación a los siguientes puntos:

i) Evolución de la definición de Riesgo

ii) Evolución de la concepción de la Administración de Riesgos

iii) Comparación del alcance de los distintos documentos

iv) Análisis del proceso de Administración de Riesgos

v) Documentación

vi) Mejora Continua y Aprendizaje

vii) Roles y Responsabilidades

viii) Principios

ix) Vinculación con los principios básicos de Basilea y Basilea II

x) Vinculación con los principios de Gobierno Corporativo

i) Evolución de la definición de Riesgo

La primera definición de riesgo surge en 1921 cuando se publica el libro del economista norteamericano **Frank H. Knight** "Riesgo, Incertidumbre y Beneficio". Frank Night hace la distinción entre "riesgo" e "incertidumbre", definiendo al "riesgo" como aleatoriedad con probabilidades conocidas, y a la "incertidumbre" como aleatoriedad sin probabilidades conocidas.

En 1983, **The Royal Society** publicó en su libro "Risk assessment: report of a Royal Society study group" un nuevo enfoque de la definición de riesgos: la combinación de la frecuencia o probabilidad de los acontecimientos de un peligro definido, y la magnitud de la consecuencia de lo sucedido.

En 1995 el Estándar de Australia y Nueva Zelanda (**AS/NZS 4360:1995**) estableció que el riesgo es la posibilidad de que suceda algo que tendrá un impacto sobre los objetivos.

En el 2002 **ISO** publicó una Guía -número 73- con un listado de términos y definiciones para unificar la terminología utilizada respecto al tema. En la Guía ISO/IEC 73:2002 definió "riesgo" como la combinación de la probabilidad y de las consecuencias de un suceso.

COSO-ERM, definió en el 2004 al riesgo como "la posibilidad de que un evento ocurra y afecte desfavorablemente al logro de los objetivos".

La definición más reciente cuando también fue publicada por ISO, en su nuevo estándar internacional **ISO 31000:2009**. Toma como base la definición de la Guía ISO 73 y modifica la definición de riesgo entendiéndolo como el efecto de la incertidumbre sobre los objetivos.

A través de estas definiciones podemos apreciar la evolución que ha tenido del concepto de "riesgo" en los distintos estándares profesionales y de negocios que se han ocupado del tema.

En la concepción moderna, el riesgo tiene -entre otras- las siguientes características:

- El riesgo no trata sólo de eventos, también puede estar asociado a situaciones y/o circunstancias
- Está vinculado a la incertidumbre en tanto está referido a algo que se desea lograr o evitar
- El riesgo no es negativo ni positivo
- Las consecuencias pueden ser positivas y/o negativas. Depende principalmente del punto de vista desde el que se lo mire.

ii) Evolución de la concepción de Administración de Riesgos

Respecto a la definición de Administración de riesgo queda claro que debemos partir del enfoque de **COSO-ERM**, ya que su documento "Enterprise Risk Management – Integrated Framework" fue uno de los primeros en introducir el tema. En el mismo se define ERM como "un proceso, efectuado por el consejo de administración de una entidad, su dirección y restante personal, aplicado en la definición de la estrategia y en toda la entidad, diseñado para identificar eventos potenciales que puedan afectar a la organización y administrar sus riesgos dentro del riesgo aceptado, proporcionando una seguridad razonable sobre la consecución de los objetivos de la entidad".

Anteriormente el **CAS** (Casualty Actuarial Society) había desarrollado en el 2003 la siguiente definición: "ERM es un proceso por el cual la organización en todas las industrias, evalúa, controla, explota, costea y monitorea los riesgos desde todos los recursos con el propósito de incrementar el valor de la organización en el corto y largo plazo para todas las partes interesadas. Aquí se enfatiza el tema de creación de valor de la empresa

Por su parte, el estándar **AS/NZS 4360:2004** introdujo a una de las primeras definiciones que trata el tema de las oportunidades y no ve la administración de riesgos sólo como el tratamiento de amenazas, sino que define ERM como "la cultura, procesos y estructuras que están dirigidas hacia la administración efectiva de oportunidades potenciales y efectos adversos".

Esta consideración de beneficios y factores adversos está implícita en todo el documento, pero no explícitamente mencionada. Constituye una diferencia con varios de los otros documentos que no enfatizan en los beneficios con la misma extensión y sino que se limitan a señalar que éstos surgen de las decisiones claves que se toman en la etapa de "evaluación de riesgo".

En la misma línea, **RIMS** (Risk and Insurance Management Society) define ERM como "la cultura, los procesos y herramientas para identificar oportunidades estratégicas y reducir la incertidumbre. ERM es una visión comprensiva tanto desde el punto de vista

de las operaciones como del punto de vista estratégico. Es un proceso que soporta la reducción de la incertidumbre y promueve la explotación de oportunidades".

En el caso de **BSI Group**, su definición se limita a establecer que el propósito de la gestión de riesgo es proporcionar un proceso sistemático, eficaz y eficiente por el cual los riesgos puedan ser gerenciados en diferentes niveles de la organización.

De la lectura de estas definiciones podemos concluir que el conocimiento intuitivo sobre la existencia de algunos riesgos ya no alcanza, sino que hace falta reconocerlos expresamente y administrarlos, eficaz e integralmente a través de una estrategia y metodología de acción concreta y exitosa para la organización.

La visión moderna viene dada por el estándar **ISO 31000:2009** en el que se plantea un nuevo concepto.

Considera ERM como el conjunto de actividades coordinadas para dirigir y controlar una organización con respecto al riesgo, siendo el riesgo la combinación de la probabilidad de un evento y sus consecuencias.

Sin duda el estándar ISO 31000:2009 busca simplificar la definición de riesgo y bajarla a tierra.

Las interpretaciones de qué es ERM pueden variar ampliamente por industria y entre organizaciones. Por consiguiente, las definiciones de ERM también varían ampliamente, pero muchas coinciden en que es un enfoque desde arriba hacia abajo, basado en y soportado por una estrategia organizacional, que se centra en nuevas formas de administración y optimización de riesgos; una nueva forma de administración estratégica de negocios, relacionando la estrategia del negocio con los riesgos cotidianos de la empresa.

iii) Comparación del alcance de los distintos documentos

Respecto a su alcance, el documento COSO ERM deja entrever que los conceptos son aplicables a todas las entidades sin importar su tamaño y niveles de formalidad, pero queda claro que el desarrollo está enfocado hacia la gerencia de las típicas empresas privadas. COSO comenzó siendo aplicado en las empresas de servicios financieros, seguros, servicios públicos, petróleo, gas, e industrias manufactureras químicas ya que los riesgos en estas industrias estaban bien documentados y medidos.

Creemos el enfoque hacia la gerencia de empresas privadas es principalmente producto de haber sido desarrollado por un grupo de contadores (mayormente auditores), lo que nos lleva a concluir que su alcance no es tan amplio como se plantea o tan fácilmente aplicable en otro tipo de empresas. Sin embargo, podemos concluir que consideramos el enfoque de COSO ERM está principalmente relacionado al plan estratégico así como a la gestión de los controles internos de la empresa.

A diferencia del documento COSO ERM, el estándar canadiense tiene su aplicación en el desarrollo de mejoras en el funcionamiento de los servicios públicos. Enfatiza que el desafío del servicio público es lograr una administración de riesgos más integrada y sistemática. A pesar de que su atención es al sector público, menciona que el marco puede proveer a cualquier organización un mecanismo para desarrollar una visión global de cómo manejar estratégicamente los riesgos al crear mecanismos de discusión, comparación y evaluación de los diferentes riesgos. Es aplicable a toda organización pero está mayormente enfocado a la infraestructura de empresas públicas y poco o nada a los riesgos financieros y operacionales.

El alcance de los Estándares de gerencia de riesgos está teñido de la esencia de la pluralidad del equipo. Surgen del trabajo de un equipo de distintas organizaciones de Reino Unido: Institute of Risk Management (IRM), Association of Insurance and Risk Managers (AIRMIC) y el National Forum for Risk Management in the Public Sector (ALARM). Es una asociación de gerentes de riesgos del sector público (ALARM) como del sector privado (IRM - AIRMIC).

El documento tiene un alcance amplio pero esencialmente enfocado al sector de los negocios y a que las organizaciones agreguen valor a sus actividades. Se dirige

principalmente a los controles internos y la administración, reforzando el concepto de gobierno corporativo.

Reconociendo la existencia de este documento, y en línea con el enfoque de los negocios, el documento del BS 31100 amplía el enfoque hacia cómo los riesgos pueden ser empleados para ayudar a las organizaciones a mejorar su modelo de negocio e incrementar los beneficios.

En su primer capítulo deja claramente establecido que las recomendaciones son genéricas y que pueden ser aplicadas en todo tipo de organizaciones y en cualquier parte de la organización, sean del sector público o privado, sin importar el tipo de empresa tamaño o naturaleza. Un ejemplo de la intención de lograr este alcance genérico es el hecho del lenguaje utilizado: se trata de un lenguaje claro y llano para que lo entienda tanto la gerencia de una empresa pequeña como la gerencia de una empresa a multinacional; un experto en riesgos o un individuo que por primera vez lee del tema. En el caso de los gobiernos de Australia y Nueva Zelanda, lograron crear un estándar respetable internacionalmente debido a su amplitud.

En efecto, el marco que crea ha ganado aceptación en varios países a pesar de haber sido concebido y escrito en el contexto de sus países específicos. Así, AS/NZS 4360 constituye un marco teórico genérico, que establece el contexto, plantea la identificación, análisis, tratamientos, monitoreo y comunicación. Además, el libro de guía (Guidelines) tiene como alcance una variedad de actividades, incluidas las actividades del sector público, comerciales, organizaciones voluntarias y sin fines de lucro por lo que cualquier organización podría aplicar este esquema.

Finalmente, el estándar que se ha destacado por su universalidad, es ISO 31000. En el primer capítulo se describe su alcance global. Está dirigido a “cualquier asociación, grupo, empresa y persona pública, privada o comunitaria” y “a través de toda la vida de una organización y de los variados rangos de actividades, procesos, funciones, proyectos, productos, servicios, activos, operaciones y decisiones”. Enfatiza el nexo entre el sistema de administración de riesgos y la parte operativa de la empresa. A su vez, en la primera figura del estándar presenta las relaciones entre el marco, los

principios y el proceso para mostrar lo comprensivo del sistema de administración de riesgos.

Por otra parte, hace hincapié en que, aunque el objetivo es ser un estándar mundial, no busca impartir uniformidad o un modo de operar ideal en todas las empresas sino que pueda ser adaptable a cada caso específico. También es cierto que aunque existe preocupación sobre su utilidad universal para su éxito, han desarrollado sub-estándares que van a proveer información más en detalle sobre aspectos prácticos de cómo implementarlo como ser el estándar ISO/ IEC 31030.

En resumen, podemos concluir que todos los textos analizados tienden a buscar la generalidad, siendo los documentos más recientes los que logran o lograrán mayor aplicabilidad dentro de las diferentes empresas. Este logro del ISO 31000 y BS 31100 también es producto de que su enfoque los diferencia del enfoque de algunos otros estándares que cubren principalmente y casi exclusivamente el proceso de administración de riesgos en sí mismo – por ejemplo el estándar australiano- ignorando aspectos como el de establecer la estructura necesaria para aplicar el proceso.
Sin embargo, en nuestra opinión constituye una desventaja el hecho de que la tendencia al consenso universal puede llevar a un relativo alto nivel de abstracción, disminuyendo los niveles de detalle requeridos para la implementación y principalmente el monitoreo necesario en las organizaciones para poner en práctica el proceso.

[60]

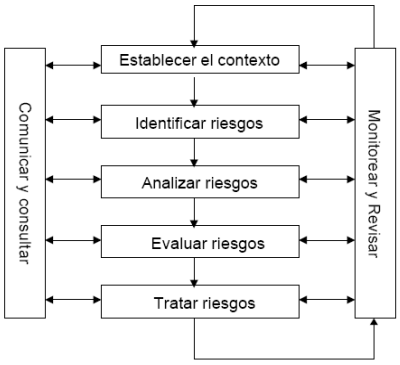
[60] Elaboración propia. Idea tomada del gráfico "Raising Standards Worldwide" de BSI Group

iv) El proceso de Administración de Riesgos

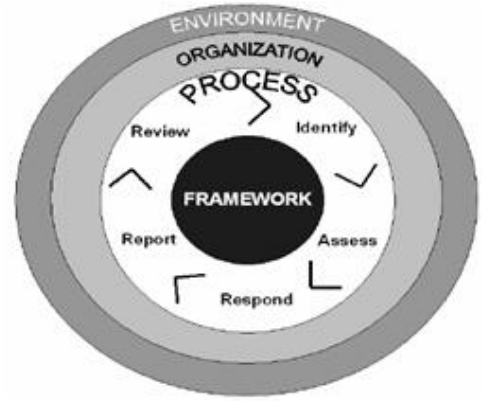
A continuación se presentan los distintos esquemas del proceso de Administración de Riesgos de los documentos desarrollados anteriormente:

IRMF

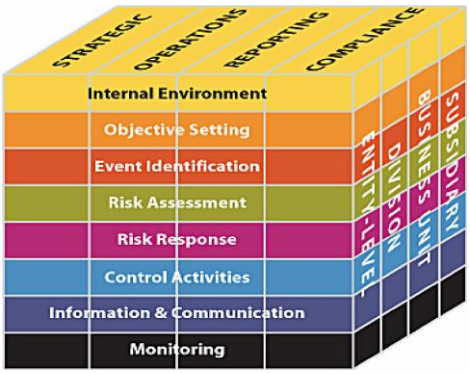
AS/NZS



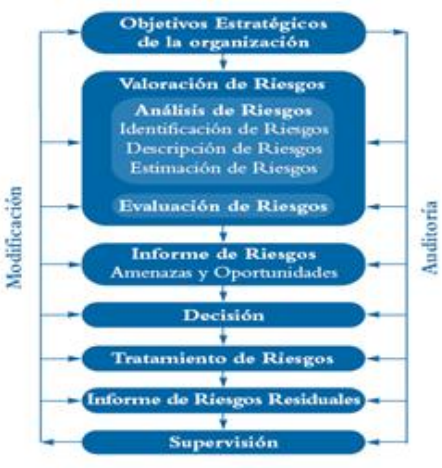
BS 31100



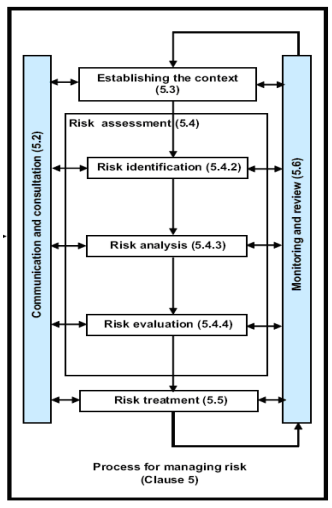
COSO-ERM



Estándares de Gerencia de Riesgo



ISO 31000



Antes de introducirnos de lleno en la comparación del alcance, etapas, duración y priorización del proceso de administración del riesgo de los documentos expuestos en el capitulo anterior, nos parece importante señalar que al tratarse de estándares contemporáneos entre sí, y emitidos en un mundo cada vez más globalizado, existen entre ellos muchas similitudes, y explícita o implícitamente se debe a que se nutren entre si, en un proceso que visualizamos como de mejora continua.
A efectos de la comparación que efectuaremos, consideramos que es fundamental comprender, en cada caso, la diferencia entre el "Proceso" y el "Marco Integrado" que de diversas formas plantean los documentos, ya que puede resultar confusa dependiendo del documento en cuestión..

El estándar **canadiense** se define a sí mismo como un Marco Integrado, en el que una de sus etapas es denominada "Practicar IRM" y refiere al proceso de administración de riesgos, que, en consecuencia, estaría contenido en dicho Marco.

No sucede lo mismo en el caso del documento **BS 31100**, en el que dentro del "Esquema de gestión de riesgos" no incluye al proceso de administración de riesgos en sí, sino una serie de conceptos a tener en cuenta a la hora de diseñar el proceso mismo.

En el estándar **AS/NZS**, previo a la exposición del proceso, se abordan los "Requerimientos de administración del riesgo", con el objetivo de describir un proceso formal para establecer un programa sistemático de administración de riesgos. En su Apéndice B, se enumeran los pasos que debe seguir dicho programa, abarcando al proceso en cuestión.

Por su parte, en los **Estándares de Gerencia de Riesgo**, luego de desarrollar todo el proceso, se hace referencia a "La estructura y la administración de la gestión de riesgos", y se explicitan los roles y responsabilidades de los diferentes actores del proceso lo que no constituiría un marco integrado sino una función de "soporte" al proceso central.

El documento más reciente, **ISO 31000,** dedica un capítulo a la preparación del proceso central de Administración de Riesgos. Plantea al "Marco Integrado" como la etapa

central de un proceso aún más genérico, que servirá de soporte para la correcta administración de los riesgos. En nuestra opinión, este estándar provee una base teórica más sólida y genérica para que todo tipo de organización pueda adaptar su proceso de administración de los riesgos.

Finalmente, en el documento **COSO-ERM**, no encontramos distinción explícita entre Marco Integrado y Proceso, con la salvedad de que el propio documento se llama Marco Integrado y podría llevar a la misma interpretación que realizamos para el documento canadiense.

A fin de parametrizar la comparación que realizaremos seguidamente, hemos entendido oportuno tomar como hilo conductor, las etapas más comunes a todos los documentos, a saber:

Etapa I: Establecer el contexto
Etapa II: Identificar riesgos
Etapa III: Analizar Riesgos
Etapa IV: Evaluar riesgos
Etapa V: Tratar riesgos
Etapa VI: Monitoreo y revisión
Etapa VII: Información, Comunicación y Consulta

Etapa I: Establecer el contexto

Para el documento **COSO-ERM**, la etapa de establecer el contexto comprende, a su vez, las etapas de "Ambiente Interno" y "Establecimiento de objetivos", centrándose en el contexto interno de la organización.

El Ambiente Interno es considerado el soporte de las demás etapas, donde se terminan definiendo el nivel de riesgo aceptado y la filosofía y cultura de riesgo, a través del análisis de los componentes: valores, competencias, estilo gerencial, responsabilidad y autoridad.

A modo de evaluación crítica, podemos señalar que, a diferencia de lo que sucede con otros documentos, el **COSO-ERM** no enfatiza la especial consideración que debería otorgársele a los stakeholders, en tanto son actores fundamentales en el proceso.

Si bien en esta etapa tampoco considera el contexto externo, lo define en la etapa siguiente denominada "Identificación de eventos".

El estándar **australiano** hace mucho hincapié en la etapa que nos ocupa, y, en sus "Guías de aplicación" amplía los conceptos. Así es que hace referencia a tres contextos: el estratégico (interno, externo), el organizacional (capacidades, metas, objetivos, estrategias) y el de administración de riesgos. En esta etapa define un concepto fundamental para el futuro: el criterio de riesgo (nivel de aceptación), que servirá para comparar con el nivel de riesgo resultante del análisis. Aquí enfatiza la importancia de la opinión de los stakeholders[61], que no todos los documentos realizan, y la limitante de los requerimientos regulatorios.

En **Estándares de gerencia de riesgo**, apenas enumera como primera etapa del proceso el "Establecimiento de objetivos estratégicos", sin hacer mención explícita al establecimiento del contexto, pero implícitamente, a través de la definición de factores internos y externos está haciendo referencia al contexto de la organización.

El documento **canadiense** lo incluye dentro de la identificación de riesgos, mencionando al igual que AS/NZS la necesidad de realizar un análisis de los Stakeholders, y determinando los recursos humanos necesarios para afrontar el proceso.

Dentro del esquema del estándar **BS 31100**, el Ambiente[62] no es una etapa, sino un concepto presente a lo largo de todo el proceso, no es definido por el documento.

El documento **ISO 31000** se acerca más al enfoque del AS/NZS, ya que plantea los contextos externo, interno y de administración de riesgos y el criterio de evaluación de

[61] Stakeholders: Partes interesadas
[62] Enviroment

riesgo de forma similar a éste. Agrega que todo el proceso debe estar alineado a la cultura organizacional, procesos, estructura y estrategia de la empresa.

Etapa II: Identificar riesgos

COSO-ERM los denomina "acontecimientos", que impactan en la estrategia de forma positiva, negativa o ambas. La metodología comprende un conjunto de herramientas y técnicas, que son desarrolladas en las Técnicas de Aplicación, donde se destacan el "Análisis de flujo de procesos"[63] y "Clasificación de eventos por categoría"[64].

Este apartado resulta ser mucho más detallado que la simple lista de ejemplos presentada por el estándar **ALARM** en su Apéndice[65]. Este documento ubica a la Identificación, junto con la Descripción y Estimación, dentro de la etapa "Valoración de Riesgo", y enfatiza en considerar el entorno, la estrategia y objetivos, los factores claves de éxito, con el fin de determinar la exposición a la incertidumbre.

AS/NZS lo enfoca más como un proceso sistemático y estructurado, donde se deben incluir todos los riesgos, estén o no bajo el control de la organización. Al igual que los anteriores, identifica una serie de técnicas e informaciones útiles para identificar riesgos, con el agregado de que condiciona la aplicabilidad de las mismas al contexto establecido en la etapa anterior. Este hecho le da más continuidad al proceso, ya que según sus "Guidelines" un buen punto de partida para esta etapa podría ser un documento denominado "establecimiento del contexto"[66]. En su Anexo D[67] presenta un cuadro de doble entrada, que relaciona las fuentes de riesgo con las áreas de impacto. Cabe destacar que este estándar va más allá de la identificación planteada en los otros estándares y desglosa los componentes del riesgo en: fuentes, incidentes, consecuencias, causas y controles.

El documento **ISO 31000** también realiza este planteo, que resulta provechoso para que el proceso de identificación sea exhaustivo. De forma similar al estándar ALARM, esta

[63] Anexo XV de la monografía, pág. 141
[64] Anexo XIII de la monografía, pág. 139
[65] Anexo V de la monografía, pág. 131
[66] Statement of context
[67] Ver página 59 de la monografía

etapa forma parte del componente Valoración[68]. Al igual que el AS/NZS, recomienda identificar aquellos riesgos que no están en un principio bajo el control de la organización, y tener la flexibilidad suficiente para discriminar diferentes escenarios y efectos acumulativos o "cascada". En su documento de soporte, el ISO/IEC 31010 clasifica los métodos de identificación en: métodos basados en evidencia, enfoques sistemáticos de equipo y razonamientos inductivos, y en su Anexo A[69] provee una tabla con todas las técnicas específicas de identificación y análisis de riesgos, que son desarrolladas luego en su Anexo B.

En el estándar **IRMF** esta etapa vendría a estar comprendida en parte en la primera etapa ya analizada, pero también es en este segundo paso "Valorar áreas clave de riesgo", donde se determinan tipos y categorías de riesgo a ser reconocidos. Los Anexos complementan lo establecido en el documento incluyendo una serie de aplicaciones prácticas a tener en cuenta. En particular, el Anexo E[70] presenta una pirámide de categorización de riesgos mostrando la jerarquía de los mismos.

Por último, el documento **BS 31100** acentúa la importancia de la revisión constante de esta etapa, dándole una perspectiva dinámica, de constante cambio, y es el único en recordar que debe ser costo-beneficioso. También en su apéndice provee una lista de ejemplos de técnicas de investigación.

Podemos observar que el producto final de esta etapa es, para todos los documentos, una lista de riesgos identificados, que servirá de insumo para la etapa siguiente. Lo que los diferencia son las formas de llegar a esa lista y el grado de profundidad de los mecanismos recomendados, y, a nuestro criterio, sobresale el estándar AS/NZS 4360:2004 por ser el más completo para esta etapa.

Etapa III: Analizar Riesgos

En primer lugar cabe destacar el consenso que existe en todos los documentos de que el eje central de esta etapa es determinar la probabilidad de ocurrencia y los impactos o consecuencias de los riesgos identificados en la etapa anterior. De eso se trata el

[68] Assessment
[69] Anexo XI de la monografía, pág. 135
[70] Anexo IV de la monografía, pág. 130

análisis: estimar el nivel de riesgo al que está expuesta la organización, a través de la interacción de estos dos conceptos. Es la esencia pura, los distintos documentos agregan sus propios condimentos.

Objetivo de esta etapa:

Expresado en diferentes palabras, todos los documentos plantean el mismo objetivo para esta etapa: transformar datos en información, proveer un input para la confrontación con el criterio u apetito de riesgo previamente establecido, y para el futuro tratamiento, y crear un perfil de riesgos de la organización. La visión de todos los estándares refuerza la idea de dinamismo de todo el proceso, ya que constantemente son referenciadas etapas anteriores y posteriores.

Controles existentes:

Tanto el documento **BS 31100** como el **AS/NZS** y el **ISO 31000** mencionan que antes de analizar se deben determinar los controles existentes y su efectividad y eficiencia, influyentes a la hora de determinar el nivel de riesgo actual. El resto de los documentos no hace mención explícita al respecto.

Diversos enfoques:

A partir de los distintos tipos de análisis que efectúan, todos los documentos, de forma más o menos explícita, consideran que existen tres clases de enfoque: cualitativo, semi-cuantitativo y cuantitativo. Difieren en el grado de profundidad que proponen y en la ejemplificación de esta clasificación.

En las Guías de Aplicación del documento **AS/NZS**, se detallan las situaciones en las que se debe tomar un camino u otro, enriqueciendo el análisis con múltiples tablas y matrices de análisis de riesgo.

De modo similar, el estándar **ERM-COSO** en sus Técnicas de Aplicación, resalta que la metodología de la evaluación de riesgos consta de una combinación de técnicas cualitativas y cuantitativas, definiendo -al igual que el documento anterior- las escalas de medición posibles. Dentro de las técnicas cuantitativas, distingue las probabilísticas

(ej.: valor en riesgo[71]) de las no probabilísticas (ej.: análisis de sensibilidad). A través de un ejemplo práctico nos muestra un "Mapa de riesgo"[72] afectado por la variabilidad de la probabilidad e impacto.

Por su parte, **BS 31100** propone un camino útil que combina los enfoques, partiendo de técnicas cualitativas para llegar a un mayor grado de detalle y por ende de certeza, con un enfoque cuantitativo.

El documento **IRMF** hace referencia a estas técnicas en sus Anexos de la Guía de Implementación. Mientras que en uno de ellos apenas lista las técnicas, en el otro provee plantillas de ejemplo[73] sobre análisis de riesgo, destacándose el "Mapa de riesgos"[74] (similar al de COSO-ERM y a los cuadros de AS/NZS).

El estándar **ALARM**, dentro de la sección "estimación de riesgos" refiere a los tres enfoques mencionados, y en su Apéndice[75] distingue las técnicas, pero no por el tipo de análisis, sino por el tipo de riesgo al que serán aplicadas: positivo, negativo, o ambos.

Por último, documento ISO/IEC 31010 desarrolla lo expuesto en **ISO 31000** respecto de los tres tipos de análisis mencionados, pero también plantea otra clasificación de técnicas de análisis de consecuencias, análisis y estimación de probabilidad y análisis de nivel de riesgos. En su Anexo A[76] muestra una tabla determinando la aplicabilidad de las técnicas a los procesos de Identificación y de Análisis, y para cada una de ellas plantea en el Anexo B su utilidad, insumos, proceso, productos y fortalezas y limitaciones.

Según los documentos ISO 31000 y AS/NZS, la utilización de un enfoque u otro depende del tipo de riesgo, el propósito del análisis, la información y recursos disponibles y la necesidad de toma de decisiones.

COSO-ERM recomienda aplicar técnicas cualitativas cuando los riesgos no son cuantificables, los datos no son los suficientemente creíbles o la obtención y análisis de

[71] Value at risk
[72] Anexo XIV de la monografía, pág. 140
[73] Templates
[74] Anexo III de la monografía, pág. 129
[75] Anexo V de la monografía, pág. 131
[76] Anexo XI de la monografía, pág. 135

ellos es excesivamente costoso. Las técnicas cuantitativas aportan más precisión y se usan en actividades más complejas, para complementar las anteriores, y son altamente dependientes de la calidad de los datos e hipótesis de soporte.

Otras consideraciones:

El documento **AS/NZS**, en sus Guías de apoyo, profundiza determinados conceptos. Señala que las consecuencias y probabilidades pueden ser estimadas mediante análisis estadístico o estimaciones subjetivas. También recuerda que la presencia de incertidumbre nos obliga a analizar el costo-beneficio de obtener información adicional, y que para lidiar mejor con ella, la "comunicación y consulta" ayudan a enfocar los esfuerzos. Por último, provee una lista detallada de hechos a documentar, para robustecer el proceso.

BS 31100 hace hincapié en que el análisis es un proceso sistemático, que se repite a medida que se obtiene mayor información, y que de esta etapa pueden surgir nuevos riesgos.

Por otro lado el estándar **ISO 31000** menciona la importancia de comunicar tanto a los tomadores de decisión como a las partes interesadas[77] el grado de confianza en la determinación del nivel de riesgo y su sensibilidad a supuestos y condiciones previas. Agrega en el ISO/IEC 31010 la necesidad de realizar un análisis preliminar y de comprender las incertidumbres y sensibilidades para interpretar y comunicar los resultados. Propone la técnica de análisis de sensibilidad para identificar aquellos datos que requieren ser precisos e íntegros.

COSO-ERM resalta la importancia de que la gerencia distinga el impacto de un acontecimiento aislado, del impacto de una combinación de acontecimientos, el que puede resultar más o menos severo. Al igual que BS 31100, la considera una etapa dinámica, ya que luego de las acciones tomadas por la gerencia sobre el "riesgo inherente", puede volver a repetirse el proceso mediante técnicas de apreciación que determinen el "riesgo residual". Estos dos conceptos introducidos por el documento

[77] Stakeholders

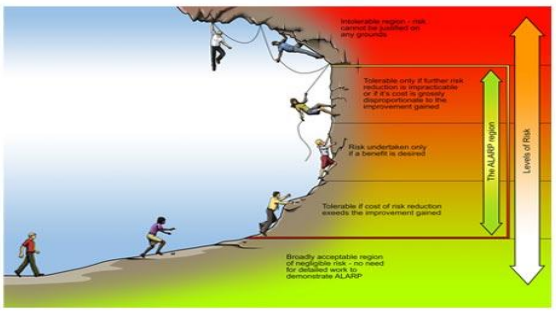
COSO-ERM (riesgo inherente y residual) son una clara evidencia de que este estándar fue creado – entre otros - por Auditores.

Etapa IV: Evaluar riesgos

Todos los nuevos documentos visualizan a esta etapa como una "bisagra" entre el análisis y el tratamiento o respuesta al riesgo. Salvo por el documento COSO-ERM, que no reserva un espacio concreto para esta etapa, el resto coincide en líneas generales en que se trata de comparar el nivel de riesgo obtenido, con el criterio de riesgo establecido o la tolerancia al riesgo de la organización. El producto de esta evaluación será una lista de riesgos ordenada, para luego tratarlos o aceptarlos.

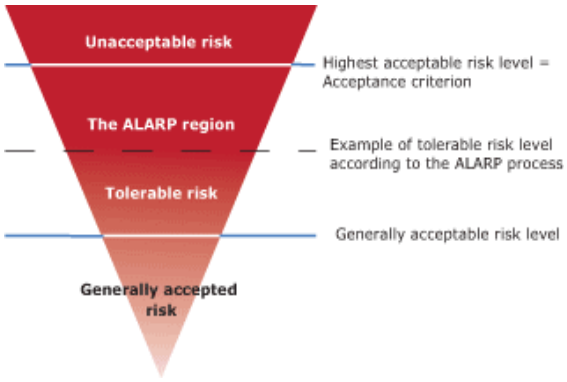
El documento **BS 31000** hace referencia a que de la misma evaluación puede surgir la necesidad de mayor análisis, o incluso pueden surgir nuevos riesgos.

En sus respectivas Guías de aplicación, tanto **ISO 31000** como **AS/NZS** y el **estándar IRMF**, plantean un esquema que divide a los riesgos analizados en tres zonas, en forma de cono, e introducen el concepto de ALARP ("As low as reasonably practicable"), o zona gris, donde deberá realizarse un análisis costo-beneficio para determinar su tratamiento o no. Cada zona determina la necesidad de un futuro tratamiento o no. Las siguientes imágenes facilitan la comprensión de dicho concepto:



78

[78] Imagen tomada de: www.tjrossin.com/images/portfolio/10.jpg



[79]

Etapa V: Tratar riesgos

Ya sea bajo el nombre de "respuesta" o de "tratamiento", la idea central de lo que implica esta etapa es compartida por todos los documentos, que, con mayor o menor grado de detalle, la desglosan en los siguientes pasos:

i. identificar opciones de tratamiento
ii. evaluar opciones
iii. estrategia o plan de tratamiento
iv. implementación

Las opciones de tratamiento de riesgo también son similares, e incluyen: evitar, reducir (probabilidad o consecuencia), transferir, compartir, retener, aceptar.

Es una etapa en la que se realizan las acciones más tangibles, y por ende una de las que implica más costos, ya que el tratamiento demanda múltiples recursos. Es por eso que los documentos AS/NZS, ISO 31000, BS 31100 y COSO-ERM y sugieren considerar la relación Costo-Beneficio del conjunto de opciones a implementar.

Estos últimos dos documentos, también hacen hincapié en que la consideración del efecto de las opciones sobre el nivel del riesgo debe hacerse mirando la tolerancia al mismo, definida al principio del proceso.

El estándar **AS/NZS** en sus Guías de aplicación y los documentos **ISO 31000 y BS 31100** introducen recomendaciones interesantes:

- al seleccionar los posibles tratamientos se deben considerar los valores y percepciones de los stakeholders[80],

[79] Imagen tomada de: www.ens.dk/.../HTML/dogp08_uk/images/s043.gif

- el tratamiento puede generar nuevos riesgos, por la falla o inefectividad de las medidas,
- debe documentarse todo el plan de tratamiento.

El **documento australiano** se extiende un poco más en las mencionadas Guías, introduciendo, además de los aspectos vistos, otros elementos a considerar en la selección de opciones (combinaciones de riesgos, análisis de sensibilidad, presupuesto, etc.). Separa los tipos de opciones de tratamiento según se trate de riesgos positivos o negativos. Introduce el concepto de "root cause" o causa raíz: factores subyacentes que influencian la efectividad del tratamiento (mencionado también en BS 31000). Por último, enumera una serie de factores que determinan la decisión por uno u otro tipo de opción.

Salvo en el caso de los documentos **IRMF y ALARM**, el resto define al riesgo residual como parte de esta etapa, lo que en la mayoría de los casos trae como consecuencia que se convierta en una etapa cíclica, ya que una vez determinado el riesgo residual, éste puede aceptarse o se puede volver a realizar todo el proceso de tratamiento.

El documento **COSO-ERM** en sus Técnicas de Aplicación ejemplifica el efecto de la respuesta al riesgo en el riesgo residual, mediante varios cuadros, e introduce una perspectiva de portafolio de dicho riesgo.

Etapa VI: Monitoreo y revisión

Esta etapa se caracteriza por nutrirse de las anteriores, y por recordar que el proceso no termina luego de tratar el riesgo, ya que lo único constante es el cambio, por lo que es fundamental seguir de cerca el proceso.

Este concepto está presente en todos los documentos, y como suele suceder, lo abordan con diferente profundidad, aunque **COSO-ERM** y el estándar **IRMF**, aportan un enfoque un tanto diferente.

El documento **AS/NZS** hace hincapié en la importancia de esta actividad para que las prioridades de los riesgos no sean alteradas. El objetivo de esta etapa es proveer vigilancia del desempeño actual versus el estimado, mediante investigación periódica.

[80] Stakeholders: Partes interesadas

En sus guías de aplicación, justifica la actividad diciendo que los cambios organizacionales planeados y los externos detectados, generan modificaciones en el contexto, en los riesgos y en la efectividad de los tratamientos, por ende el proceso debe ser revisado constantemente. Distingue tres tipos de monitoreo: continuo, revisiones de gerentes de línea y auditorias (internas y externas)[81]. Hace referencia a los indicadores de desempeño como una buena herramienta, destacando al Cuadro de Mando Integral[82].

El estándar **ALARM** no profundiza en esta etapa, pero menciona la importancia de realizar regularmente auditorias de la política y de la conformidad con los estándares, y revisiones de rendimiento para identificar oportunidades de mejora.

Por otra parte, el documento **BS 31100** destaca la importancia de la revisión y el reporte para mantener el perfil de riesgo, es decir mantener los riesgos dentro del apetito y tolerancia al riesgo definidos al principio del proceso. También le da otros usos como obtención de información, mejora en la toma de decisiones, repriorización de los recursos, etc.

ISO 31000 sigue la línea de los documentos mencionados, y agrega en su documento de apoyo IEC 31010 que esta etapa sirve para verificar:

- Validez de asunciones y suposiciones
- Logro de resultados esperados
- Resultados en línea con experiencia actual
- Técnicas de valoración aplicadas adecuadamente
- Tratamientos de riesgos efectivos

Los últimos documentos COSO-ERM y IRMF, si bien expresan conceptos similares, encaran esta etapa de otra forma:

El documento **COSO-ERM**, plantea dos etapas que podrían encuadrar dentro del monitoreo y revisión. La primera es "Actividades de Control" definidas como las políticas y procedimientos que ayudan a asegurar que las respuestas al riesgo sean ejecutadas adecuadamente. Se trata de controles generales o sobre aplicaciones, dándole un enfoque de Control Interno. En sus Técnicas de aplicación aclara que estas actividades pueden también constituir por sí mismas una respuesta al riesgo, y provee

[81] Anexo VIII de la monografía, pág. 134
[82] Balanced Scorecard

una lista con ejemplos. La segunda se denomina "Monitoreo", y se divide en actividades continuas o evaluaciones independientes. Una combinación de estas dos técnicas asegurará que la ERM conserve su eficacia. En su documento de respaldo se proveen ejemplos de estas dos formas de monitoreo, y de metodologías puntuales de evaluación.

Por último, el **documento canadiense** en esta etapa dentro del proceso, llamada "Monitoreo, evaluación y ajuste", señala que mejora el proceso de toma de decisiones y que debe complementarse con el reporte. Además, dentro de su Guía de Implementación, dedica un capítulo especial al Aprendizaje Continuo en Administración de Riesgos En ella pone el énfasis en la necesidad de monitorear y aprender de situaciones donde la administración de riesgos se ha convertido en una herramienta para la toma de decisiones. Para lograr esto se necesita crear un ambiente de trabajo de apoyo, construir capacidades, proveer incentivos para reconocer los comportamientos deseados y alentar y recompensar actitudes proactivas hacia el riesgo.

Etapa VII: Información, Comunicación y Consulta

Esta etapa se denomina de diferentes formas según sea el documento que estemos analizando, sin perjuicio de lo cual existen muchas similitudes en su enfoque y en los conceptos que aportan.

Todos los estándares con excepción del **BS 31100** indican que esta etapa debe tener lugar dentro de la empresa, y también proyectarse hacia afuera, ya que existen diversos terceros interesados en la administración de nuestros riesgos.

Los documentos **AS/NZS, IRMF, ISO 31000 y COSO-ERM** mencionan con diferente énfasis que esta actividad debe estar presente a lo largo de todo el proceso de administración de riesgos, los primeros tres recomiendan, incluso, crear planes o estrategias de comunicación.

En esta etapa es donde quizás más se evidencia la similitud que tiene el **documento australiano** con el estándar ISO 31000. Son los únicos que plantean que el plan de comunicación y consulta debe definirse al inicio del proceso de gestión de riesgos, y

otorgan un rol fundamental a los stakeholders[83], rol que los otros documentos omiten o no enfatizan.

El documento **COSO-ERM** califica a la Información como insumo para la Comunicación. El gran desafío de la organización es procesar grandes volúmenes de datos en información utilizable, para lo cual es fundamental la estructura de sistemas de información. Cuanto mejor sea la comunicación, el directorio podrá cumplir más eficazmente su función de supervisión. En sus "técnicas de aplicación" provee un diagrama de flujos de información a lo largo de todo el proceso de gestión de riesgos y destaca a la tecnología como un gran contribuyente a la efectividad y eficiencia de los procesos de información (sistemas integrados, cuadros de mando, diagramas de flujos de datos). Adicionalmente plantea varios ejemplos de vehículos para una comunicación efectiva.

Desde un abordaje diferente, el estándar **ALARM** dentro de la sub-sección "Informe Interno" hace hincapié en que diferentes niveles de una empresa requieren distintos tipos de información, y aporta ejemplos para el Consejo de Administración, las Unidades de Negocios y para los propios Individuos.

Por último, el **estándar canadiense** da relevancia a la promoción de oportunidades y para compartir información y al establecimiento de técnicas para compartir métodos de administración de riesgos. Generar conciencia sobre los riesgos clave, sobre los procedimientos y sobre los planes de contingencia es fundamental para la efectividad de esta etapa, pudiendo llevarse a cabo, entre otros, mediante encuestas periódicas al personal. Este documento comparte con el COSO-ERM y el AS/NZS la importancia que hay que prestarle al entendimiento del personal sobre el riesgo al que se enfrenta día a día. Dado que se trata de un documento orientado a las organizaciones públicas, agrega la importancia de la comunicación con el parlamento, los medios de prensa y otros actores desestimados en los otros estándares. Al tratarse de agencias del estado, el concepto de stakeholder puede ampliarse, al punto que toda la población pueda estar interesada en sus acciones, ya que en muchos casos se está sujeto al control social.

[83] Stakeholders: Partes interesadas

v) Documentación

En todo tipo de organización, sean cuales sean sus características, los empleados no estarán para siempre desempeñando sus cargos, ya que existe una rotación natural del personal, que puede verse acentuada por otros factores. Es por esto que la documentación de los aspectos relevantes es clave para poder conservar o no perder totalmente el "capital intelectual" de la empresa.

En lo que respecta al análisis de la documentación, vemos que hay dos enfoques distintos:

El primer enfoque está integrado por los documentos AS/NZS, IRMF, COSO-ERM e ISO 31000 que hacen mención explícita de la relevancia de la documentación. El estándar Australiano enfatiza que todas las etapas deben ser documentadas y que sus registros deben contener: supuestos, métodos, fuentes de datos, objetivos, involucrados, decisiones y resultados. Señala que nunca se debe desestimar el costo versus el beneficio de documentar, ni tampoco las necesidades legales de la organización. En su Anexo H provee una lista de reportes relevantes, y en las Guías de Aplicación indica que constituye un insumo para un buen Gobierno Corporativo, destacando la importancia de sus diferentes aspectos. Complementa los ejemplos del Apéndice antedicho y provee tablas de registro.

El documento canadiense plantea esta actividad de forma menos ortodoxa, ya que va señalando aisladamente cuándo y por qué es importante documentar. Menciona la importancia de documentar la primera etapa de su proceso: "Desarrollar un perfil corporativo de riesgo". Luego agrega que deben documentarse los riesgos, procesos, decisiones, planes, acciones y resultados; como también lecciones aprendidas, estudios de casos y mejores prácticas. Los objetivos van desde promover el aprendizaje continuo de la experiencia hasta reforzar las responsabilidades y demostrar Debida Diligencia[84]. En su Apéndice D expone ejemplos de cómo documentar diversas etapas del proceso de administración de riesgos.

El estándar ISO sostiene que todas las actividades de ERM deben ser trazables y que los registros son el fundamento para la mejora de métodos y herramientas. En su apartado

[84] Due Diligence

IEC 31010 sugiere varios conceptos para documentar dentro del proceso de valoración del riesgo.

En el documento COSO-ERM se dedican unas líneas a la documentación dentro de la etapa de Monitoreo. Se destaca que el alcance de esta tarea depende del tamaño y de la complejidad de las entidades y que si los componentes de administración de riesgos corporativos no están documentados, no significa que no sean efectivos. No obstante, la documentación ayuda a que las evaluaciones sean más efectivas y eficientes.

Por otra parte, los documentos BS 31000 y ALARM no realizan mención explícita a la necesidad de documentar pero, por el desarrollo de las diversas etapas del proceso de administración de riesgos, resulta evidente que toman en consideración su documentación.

vi) Mejora continua del proceso

Si bien no se trata de una etapa dentro del esquema del proceso de administración de riesgos, es una práctica que aporta mucho e influencia el futuro proceso de las organizaciones. Es considerado con diversos enfoques en los distintos documentos, excepto en los **Estándares de gerencia de riesg**o, que nada mencionan al respecto.

En las Guías de Aplicación del **documento australiano**, se plantea una última etapa denominada "Estableciendo una eficaz administración del riesgo", integrada por la planificación, las políticas y los compromisos de los diferentes actores de este proceso. El objetivo es mantener una administración de riesgos sistemática.

El estándar **ISO 31000** desarrolla en su Anexo A los "Atributos de una administración de riesgos mejorada", destacando y unificando alguno de los conceptos vistos en el documento.

El documento **BS 31000** dedica su último capítulo a este tema, bajo el nombre de "Implementando la administración de riesgos". En este capítulo se resalta la importancia de crear capacidades, medir la madurez, planificar escenarios y realizar pruebas de estrés. La mejor forma de mejorar el conocimiento, la capacidad y el futuro desempeño en administración de riesgos es que la organización aprenda de riesgos que se han materializado en pérdidas propias o de organizaciones externas relevantes.

Para el estándar **IRMF** el aprendizaje continuo es uno de los cuatro pilares que sostienen su desarrollo. Expresa que contribuye a una mejor toma de decisiones, mejor administración del riesgo, refuerza la capacidad organizacional y facilita la integración de este proceso a la estructura de la entidad. Esto se alcanza a través de la creación de una ambiente de trabajo de apoyo y planes y prácticas de aprendizaje. Es importante reconocer que no todos los riesgos pueden ser previstos o evitados, y que el desafío crítico es mostrar que el riesgo está bien administrado, se rinden cuentas y que se actúa con transparencia y debida diligencia[85]. Agrega a la documentación adecuada como otra herramienta de soporte a esta etapa.

Por último, el documento **COSO-ERM** si bien no lo manifiesta explícitamente, podemos ver que en su capítulo "Limitaciones de la administración de riesgos corporativos", de alguna forma nos está hablando de continuo aprendizaje. Es el único documento que realiza una breve autocrítica de su proceso, basándose en la premisa de que solo proporciona una seguridad razonable en la consecución de objetivos. Esto se deba a que el logro de estos se ve afectado por las limitaciones inherentes a cualquier proceso de administración: juicio humano defectuoso, errores o equivocaciones. Además, los controles pueden evadirse por la colusión de dos o más personas y por negligencia de la dirección. Por último deben considerarse los costos y beneficios de este proceso para no realizar esfuerzos desmesurados sin resultado alguno.

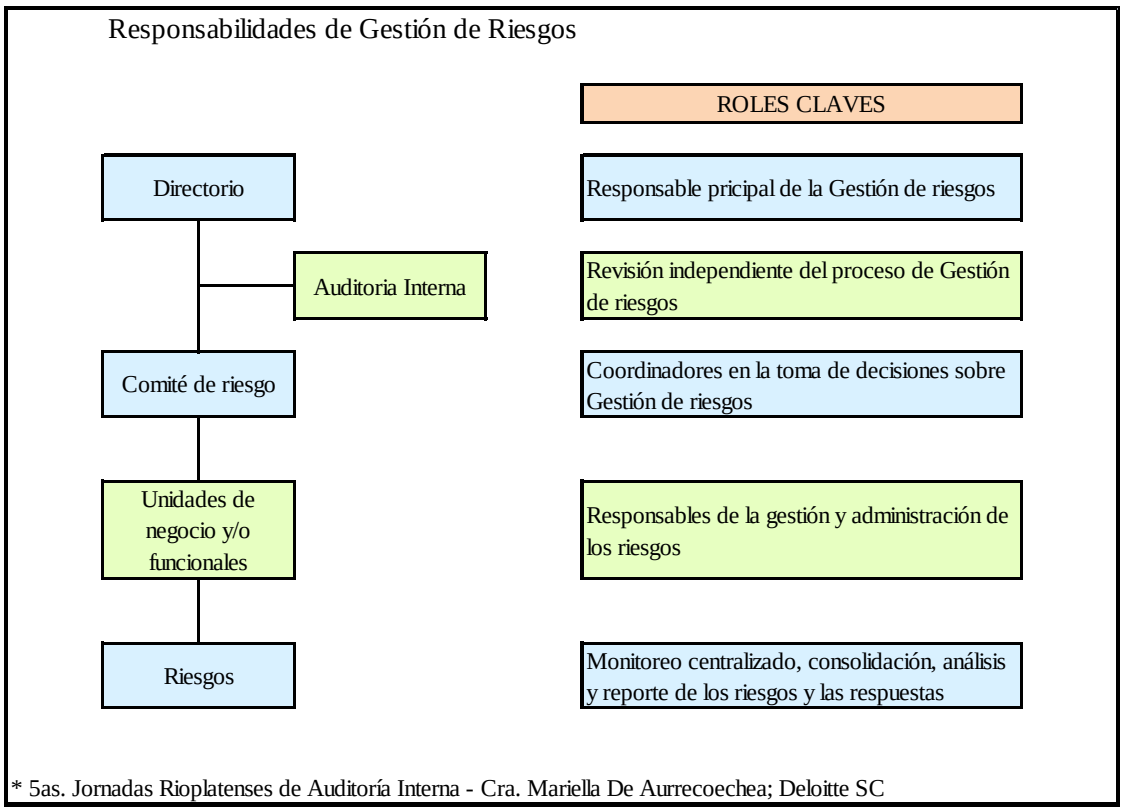
vii) Roles y responsabilidades

Como punto adicional a la comparación del proceso propiamente dicho, es importante destacar cómo establecieron los distintos documentos los papeles de las unidades de la organización dentro del proceso de administración de riesgos. Tener definidos los roles y responsabilidades de las partes interesadas en la administración de riesgos es de vital importancia para la aplicación de la misma. En algunos documentos se tratan implícitamente; en otros se detalla claramente en apartados específicos. Éstos son COSO-ERM, ALARM y BS 31000.

[85] Due Diligence

También en el apéndice del documento Guidelines de Canadá se desarrollan algunos roles y responsabilidades pero está más enfocado a las unidades del propio sector público de Canadá y no al organigrama típico que tendría una empresa estándar.

Tomando en cuenta el gráfico siguiente, vemos un esquema de las responsabilidades de gestión de riesgos de una empresa estándar que en las Quintas Jornadas Rioplatenses de Auditoría Interna, la Cra. Mariella de Aurrecoechea presentó como las más importantes:



A continuación veremos las semejanzas y diferencias que surgen de la comparación de los distintos documentos antes desarrollados.

Ejecutivo – Alta gerencia

En todos los estándares vistos, se establece que el último responsable de la ERM es el ejecutivo, la alta gerencia o el directorio – distinta terminología pero refiriéndose a lo mismo.

En el caso de **ALARM**, tiene la particularidad, que definen la figura del Consejo de Administración y no del ejecutivo en sí mismo. Sin embargo, podría estar integrado por

la dirección ejecutiva. Pero también plantean otras posibilidades como una comisión no ejecutiva, o incluso un comité de auditoria.

En caso del documento **ISO 31000**, las responsabilidades del ejecutivo están implícitamente detalladas en el componente "mandato y compromiso de la dirección" cuando define el marco para la administración de riesgos.

Oficial de riesgo[86]

Los tres documentos que dedican un capítulo a los roles y responsabilidades definen, de una manera u otra lo que conocemos como Oficial de riesgo según el documento **COSO – ERM.**

En **BS 31100** se definen tres figuras que en los otros textos se engloban en una:

1. el director o gerente de riesgos, cuando el tamaño de la empresa permite que sea un individuo;
2. el equipo de gestión de riesgos, encargado de monitorear el desarrollo, implementación y mantenimiento de la gestión de riesgos y
3. el dueño de riesgo, el cual lo define como el rol o el individuo responsable por la administración de todos los aspectos de un riesgo específico.

En el caso de **ISO 31000** también trae el concepto de dueño de riesgo según la definición que se estableció en la nueva versión de ISO 73. Define con el nombre dueño de riesgo[87] a la persona o entidad con la responsabilidad y autoridad para manejar los riesgos pero no desarrolla el concepto ni detalla las tareas específicas para el mismo.

Por otra parte, **ALARM** habla de la "función de gestión de riesgo" como una tarea a cargo de un individuo o una unidad en un concepto genérico. Por el contrario, el documento canadiense define al "risk champion", describiendo detalladamente sus cualidades y tareas.

Auditores internos

El papel de los auditores internos está visto en los tres documentos mencionados. Todos coinciden en que tienen un rol fundamental dentro de la ERM. Se entiende que pueden,

[86] Risk officer
[87] Risk owner

desde una perspectiva más independiente, lograr identificar mejoras necesarias al proceso de gestión, generar confianza del proceso e identificar riesgos importantes que se están tratando o que debieran ser tratados. En el caso de Canadá, se mencionan simplemente como encargados de reportar la performance del proceso pero no habla de otros aspectos. Los otros documentos desarrollados no hacen hincapié en el papel de los auditores.

Otros miembros del personal

Todos los textos hacen énfasis en la siguiente premisa: La administración de riesgos debe ser responsabilidad de todos los integrantes de la empresa.

Las unidades de negocios deben tener la responsabilidad primaria de gestionar los riesgos día a día y cada individuo debe ser consciente que implícita o explícitamente la administración de riesgos está en su trabajo diario.

También hacen énfasis en crear una conciencia de riesgo dentro de toda la organización, remarcando la importancia que tiene para la comunicación en todos los niveles.

Partes interesadas

El documento **COSO – ERM** es el único que dedica parte del capítulo Roles y Responsabilidades a mencionar el rol que juegan terceras partes interesadas dentro de la organización. No sólo refiere a los accionistas que los otros estándares también los mencionan, sino también: los clientes, proveedores, reguladores etc. En él se establece que podrían contribuir en el logro de los objetivos de la empresa, pero claramente no son responsables por el ERM de la misma.

En definitiva, los roles y responsabilidades detallados pueden servir para dejar claramente establecido quién está a cargo de qué. Sin embargo, entendemos que las tareas de cada uno van a depender de la organización y es la propia empresa quién debe definirlas específicamente según su estructura, capacidades y recursos.

En resumen, aunque puede haber diferencias en la terminología, existe consenso en los documentos de que debe existir un encargado, con cargo de gerente o director y con determinado conocimiento y nivel ejecutivo por ser un rol crucial dentro del proceso.

viii) Principios

Los estándares más recientes, han dedicado un capítulo aparte para definir los "principios para administrar los riesgos". Según Fernando Gaziano - Socio Risk Consulting Deloitte Chile - los principios son una serie de declaraciones que deberían ser seguidas y respetadas por las organizaciones para lograr una gestión de riegos efectiva.

La necesidad de definir principios que sirvan como base para desarrollar la administración de riesgos se fundamenta en el establecimiento de directrices sobre las mejores prácticas.

Al observar los principios establecidos en BS 31100 e ISO 31000, podemos concluir que son casi idénticos. Las diferencias pueden estar principalmente en la terminología o el desarrollo de cada uno, pero el lineamiento es similar en ambos.

El otro documento que trata el tema, aunque implícitamente, es el de Australia Nueva Zelanda. En el apartado Guidelines, no se definen explícitamente los principios pero cuando establece que debemos definir las bases para administrar los riesgos, lista seis conceptos claves que se asemejan a los establecidos en los otros documentos.

Entendemos por lo tanto que los conceptos de este estándar son comparables con los principios de BS e ISO. De hecho, son totalmente coincidentes en las siguientes premisas sobre la administración de riesgos.

- La administración de riesgos identifica las amenazas y oportunidades y define la incertidumbre. La definición explícita de la incertidumbre es un factor clave para actuar frente a los riesgos.
- Es un proceso sistemático. (Nota: En realidad, el concepto de proceso sistemático se menciona en todos los estándares vistos. Es una premisa universal que trata de reflejar la dinámica del proceso en sí mismo).
- Es dinámica, responde al cambio y debe manejarse proactivamente.
- Es transparente. La transparencia la enfocan principalmente a la información proporcionada a los stakeholders[88]. En el caso de BS 31100 desarrolla más este concepto mencionando que debemos: identificarlos, tener en cuenta sus

[88] Stakeholders: Partes interesadas

objetivos, su grado de influencia y asegurarnos las decisiones claves son tomadas por ellos. El documento AS/NZS lo trata desde la importancia en la efectiva comunicación a lo largo de la empresa.

- Es parte de la toma de decisiones. En el caso del documento AS/NZS no lo establece exactamente así pero menciona que se requiere responsabilidad en la toma de decisiones y no se debe perder el balance entre las responsabilidades por los riesgos y las habilidades en controlarlos.

Si comparamos el resto de los principios desarrollados en los documentos BS e ISO, no reflejan grandes diferencias. Se enfocan principalmente en: la creación de valor y los beneficios de aplicar la administración de riesgos en la empresa; la consideración de la organización en su conjunto para la aplicación de la misma tomando en cuenta factores humanos y comportamientos; la necesidad de realizarse según las características de cada empresa; y la consideración de los factores históricos, la experiencia pasada, el conocimiento entre otros como la mejor información disponible.

En el caso del documento COSO – ERM, se establecen principios generales de los ocho componentes de ERM en el Anexo B de las Técnicas de Aplicación. Sin embargo, los mismos tienen objetivos diferentes. COSO – ERM establece claramente que el anexo no pretende facilitar una relación completa de los principios establecidos en el Marco, ni precisarlos o describirlos totalmente. Busca simplemente aclarar y ejemplificar los conceptos claves inherentes a cada componente. Entendemos entonces en este caso no se adecuaría al concepto de principio propiamente dicho como sí lo logran los otros documentos.

ix) Vinculación con los principios básicos de Basilea y Basilea II

En 1997, el Comité de Supervisión Bancaria de Basilea[89] presentó sus 25 Principios para una Supervisión Bancaria Efectiva (Core Principles: CP). El fundamento principal de dicho documento planteaba que si un organismo de supervisión cumplía con dichos principios ejercería un mejor control sobre sus bancos y, por lo tanto, el sistema bancario sería menos vulnerable a una crisis. En 1999, emitió la Metodología para llevar

[89] El Comité de Supervisión Bancaria de Basilea, creado en 1975 por los Gobernadores de los bancos centrales del Grupo de los Diez (G10), está compuesto por altos representantes de autoridades de supervisión bancaria y de bancos centrales de Alemania, Bélgica, Canadá, España, Estados Unidos, Francia, Italia, Japón, Luxemburgo, Suecia, Suiza, los Países Bajos y el Reino Unido.

a cabo la evaluación de los CP: un listado de criterios para evaluar el cumplimiento de cada país con los CP.

En el año 2004 el Comité de Basilea decidió revisar los CP y su metodología debido a que existían importantes novedades en materia de regulación y supervisión, por ejemplo, entre ellas, las áreas específicas para la administración del riesgo. En ese sentido, el Comité de Basilea ha emitido varios documentos donde se establecen "las mejores prácticas" para diferentes tipos de riesgos materiales generalmente comunes a los sistemas financieros.

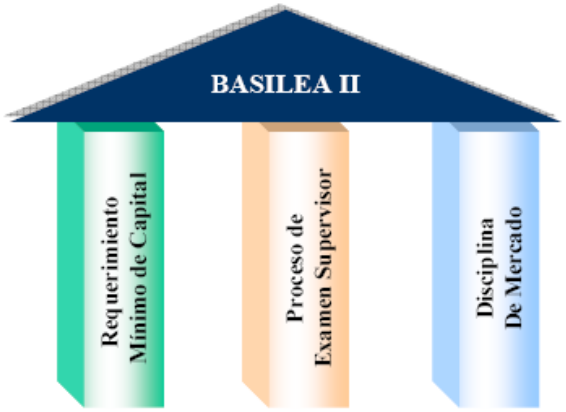
En la última versión de los CP (2006) se introdujo un nuevo principio, unificando el tratamiento general (a modo de paraguas) el cual se refiere a todos los tipos de riesgos y establece requerimientos para una adecuada administración integral de los mismos en todo el grupo bancario.

El principio que se incorporó fue el 7 y establece:
"Principio 7 – Proceso de Administración de riesgo: Los supervisores bancarios deben satisfacerse de que los bancos y grupos bancarios establezcan un proceso global de administración del riesgo (incluyendo una supervisión apropiada del Directorio y la Alta Gerencia) para identificar, evaluar, monitorear y controlar o mitigar todos los riesgos y juzgar si posee el capital adecuado de acuerdo al perfil de riesgo asumido. Estos procesos deberían ser acordes al tamaño, naturaleza y complejidad de las actividades que las instituciones llevan a cabo." [90]

Si observamos los procesos planteados en los diferentes estándares con este principio encontramos que lista casi todas las etapas del proceso de administración de riesgos. Incluso las etapas no mencionadas – Establecer el contexto y Comunicación y Consulta- están implícitamente tratadas en el desarrollo de los pilares de Basilea II. En el Pilar II: proceso de examen supervisor, exige que la alta dirección del banco se involucre activamente en el control de riesgos y en la planificación futura de las necesidades de capital. Esta supervisión, en definitiva puede implicar en cierto modo involucrarse en el establecimiento de contexto y en la comunicación de lo que entiende es tolerable.

[90] Hacia una cultura de Risk Management

Basilea II en particular, propone entre otras medidas regulatorias, mecanismos de evaluación de riesgos a adoptar por los reguladores de las entidades financieras y se basa en los siguientes tres pilares:



La propuesta se orienta a la aplicación de modelos más sofisticados de medición del riesgo. Con Basilea II se pasa de un enfoque de tipo contable a otro que propicia un manejo dinámico de los riesgos.

Adicionalmente propone un tratamiento explícito de otros tipos de riesgos presentes en la actividad financiera, introduciendo el riesgo operacional, obligando por primera vez a los bancos a aplicar un enfoque riguroso y cuantitativo a fin de controlar y mitigar este tipo de riesgo.

Según el Comité de Basilea: "el objetivo que persigue la mejora del marco de suficiencia de capital es poner más énfasis en la gestión de riesgo y fomentar mejoras continuas en la capacidad de los bancos para evaluar riesgos." Dicho objetivo "se traslada a las prácticas supervisoras y a la disciplina de mercado mediante la mejora en la divulgación de la información referida al riesgo y al capital."

En Basilea II, las decisiones acerca del riesgo y la suficiencia de capital van más allá de evaluar que el banco mantenga el nivel de capital mínimo requerido; en este sentido la normativa insta a los organismos supervisores a avanzar hacia un esquema de supervisión más orientado al riesgo. Al plantear este nuevo concepto el proceso de administración de riesgos cambia su enfoque hacia una mirada integral tal como lo plantean los estándares vistos anteriormente.

Las instituciones no debieran ver los riesgos de mercado, de crédito, operacional, individualmente sino de manera integrada. Aunque entendemos esta normativa se enfoca y tiene como alcance las instituciones financieras, creemos podemos hacer un paralelismo ya que aquí también se tiene como objetivo último lograr una administración de riesgos integral, efectiva y eficiente que permita bajar los requerimientos mínimos de capital.

Basilea II tiene una visión de gestión de riesgos moderna que ya que implica entre otras cosas:
- La utilización de sistemas integrados de gestión de riesgos de crédito, mercado y operacional;
- La utilización de indicadores que permitan gestión de riesgos en el día a día;
- Herramientas de estimación de pérdidas futuras;
- El compromiso de la Alta Dirección con la gestión de Riesgos; y
- La figura del oficial de riesgo[91] exigiendo una oficina de riesgos totalmente independiente de la gestión operativa.

Todos estos aspectos están entrevistos en los estándares de administración de riesgo planteados en el capítulo 3. Incluso, existen instituciones financieras en el mundo, que toman el proceso genérico visto en los documentos como base para cumplir con Basilea II.

x) Vinculación con principios de Gobierno Corporativo

El concepto de Gobierno Corporativo[92] apareció hace algunas décadas en los países más desarrollados del oeste de Europa, en Canadá, los Estados Unidos y Australia, como consecuencia de la necesidad que tenían los accionistas minoritarios de una empresa de conocer el estado que guardaba su inversión; esto es, querían saber qué se estaba haciendo con su dinero y cuáles eran las expectativas futuras. Esto hizo que los accionistas mayoritarios de un negocio y sus administradores, iniciaran un proceso de

[91] Risk Officer
[92] Corporate Governance

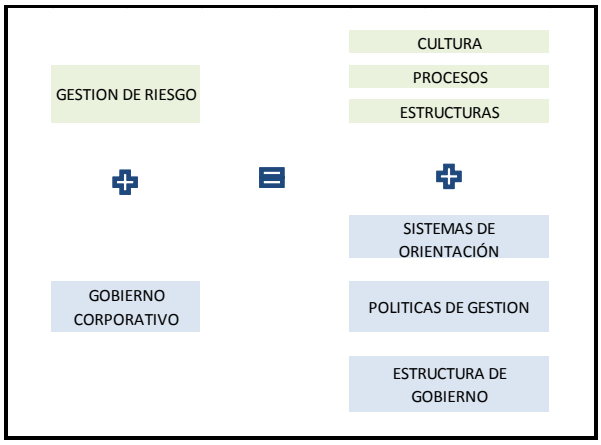
apertura de la información, al mismo tiempo de profesionalización y transparencia en el manejo del mismo.[93]

La Organización para la Cooperación y el Desarrollo Económicos[94] (OECD), emitió en mayo de 1999 sus "Principios de Gobierno Corporativo"[95] en los que se encuentran las ideas básicas que dan forma al concepto que es utilizado no sólo por los países miembros sino también por algunos otros en proceso de serlo. Su última versión del 2004 es por excelencia la más aceptada mundialmente y los lineamientos básicos en ella son:

- Los derechos de los accionistas.
- Tratamiento equitativo de los accionistas
- La función de los grupos de interés social en el gobierno de las sociedades
- Comunicación y transparencia informativa
- Las responsabilidades del consejo

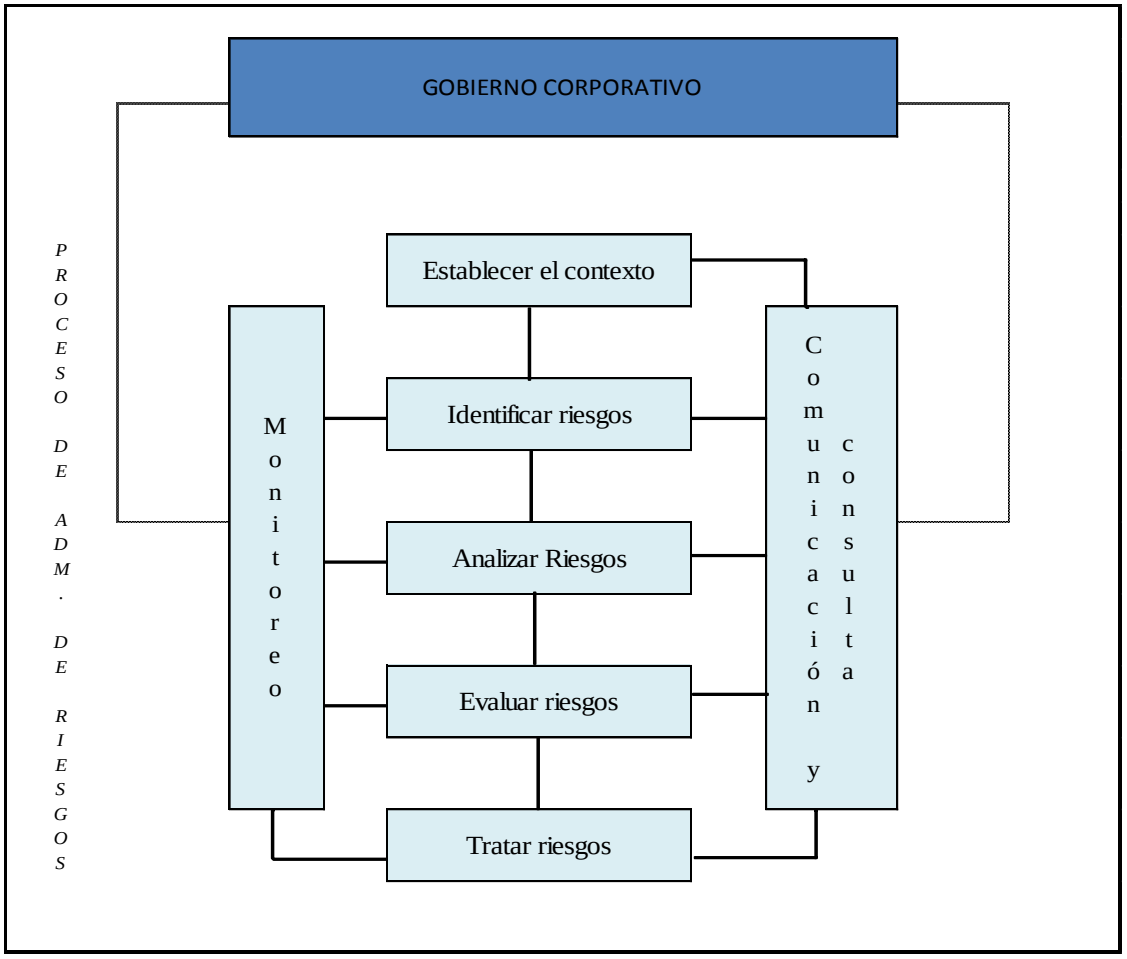
Según Alfonso Parias[96], mediante prácticas adecuadas de Gobierno Corporativo se adoptan sistemas de orientación y gestión, cultura, procesos y estructuras para obtener oportunidades potenciales y manejar los eventos adversos. La Gestión de riesgos entonces es vista como una respuesta estratégica de la organización al riesgo.

Parias resume la relación entre los dos con el siguiente esquema:



[93] es.**wikipedia**.org/wiki/**Gobierno_corporativo**
[94] www.**oecd**.org Organisation for Economic Co-operation and Development, en adelante OECD
[95] www.**oecd**.org/data**oecd**/47/25/37191543.pdf
[96] Alfonso Parias, Risk Control Manager de DECEVAL, www.deceval.com en su presentación "La Gestión de riesgos apoyada en el Gobierno Corporativo"

Luego, lo relaciona con el proceso de gestión de riesgos en sí tomando como base el esquema de AS/NZS 4360:2004:



Observamos existe principalmente vinculación entre los principios cuatro y cinco de Buen Gobierno Corporativo establecidos por la OECD y las etapas de Monitoreo y Comunicación y consulta en el proceso de Administración de riesgos.

El principio cuatro habla de la transparencia de la información y entre otras cosas establece que "El marco del gobierno de las sociedades debe asegurar que se presenta la información de manera precisa y de modo regular acerca de todas las cuestiones materiales referentes a la sociedad, incluidos los resultados, la situación financiera, la propiedad y el gobierno de la sociedad." En particular luego menciona los factores de riesgo material previsibles y la información necesaria. Este es el enfoque que le dan los estándares a la etapa de Comunicación y consulta, enfatizando el diálogo de ida y vuelta.

En cuanto al Monitoreo, existe relación respecto a las responsabilidades del Consejo en la supervisión. Así es que una de las funciones que debe realizar el consejo es: "La revisión y dirección de la estrategia corporativa, los planes de acción principales, la política de riesgo, los presupuestos anuales y los planes de negocio; el establecimiento de los objetivos sobre los resultados; el control y seguimiento de la implantación de los resultados corporativos; y la supervisión de los principales gastos, adquisiciones y enajenaciones de capital".

Si miramos los documentos desarrollados en los capítulos anteriores, evidenciamos que algunos de ellos traen el concepto de Gobierno Corporativo. En el caso de COSO: ERM, se establece que está asociado en la medida que provee información a la dirección superior con respecto a los riesgos más significativos y a la forma como los mismos están siendo administrados.

En el caso de los Estándares de Gerencia de Riesgo enfatiza que un buen Gobierno Corporativo requiere que adopten un enfoque metódico de la gestión de riesgos que proteja el interés de los interesados y asegure que el consejo de administración dirige la estrategia, crea valor y supervisa el rendimiento y asegure que los controles de gestión existen y son efectivos.

Por otra parte, el estándar BS 31100 define claramente su concepto estableciendo que es la estructura, los procesos, el tono en el cual la gestión de riesgos es llevada a cabo y las responsabilidades y autoridades están definidas y asignadas. El documento hace un paralelismo con los componentes vistos en el modelo planteando donde el Gobierno Corporativo es el resultado de unificar varios componentes del marco de gestión de riesgos, por ejemplo: estrategia, apetito de riesgo, políticas, roles, reportes, cultura, etc.

Por último cabe mencionar que ISO 31000 establece como uno de los objetivos generales el de mejorar el Gobierno Corporativo.

CAPITULO V: CONCLUSIONES

Es claro que el objetivo fundamental de todo negocio es maximizar el valor para sus accionistas (dueños/stakeholders) y que ningún proceso de administración de riesgos puede crear un ambiente libre de riesgos. Sin perjuicio de ello, es necesario contar con un sistema de administración de riesgos para reducir al mínimo las pérdidas que puedan derivarse de ellos y potenciar al máximo las ganancias.

Como hemos visto en los Capítulos II y III, existen numerosos marcos teóricos que tratan sobre la forma más eficaz de realizarlo. En líneas generales, independientemente del marco que se tome como referencia, cualquiera de ellos pueden resultar en varios aspectos una herramienta útil para todo tipo de organización (público o privada):

- ✓ Al proveer definiciones claras, inequívocas y consistentes, ayudan a establecer un entendimiento general sobre los temas importantes dentro de toda la organización. Además pueden contribuir a una mejor comunicación entre diferentes entidades y sus stakeholders[97] (ya sean accionistas propiamente dichos, clientes, proveedores, reguladores, etc.). Este aspecto puede ser de especial importancia en empresas grandes, diversificadas y más complejas, por ejemplo las multinacionales que tienen distintas subsidiarias en varios países y con una gran variedad de actividades.
- ✓ Al describir los componentes, procesos y estructuras esenciales dentro de una organización para tener un sistema de administración de riesgo eficiente y eficaz, permite definir un proyecto sobre el cual debe trabajar para diseñar e implementar dicho sistema.
- ✓ Al definir cómo sería un sistema tipo, da pautas de lo que se conoce como "buenas prácticas" y sirve como un punto de referencia sobre el cual las organizaciones pueden compararse. Además sirve para identificar potenciales deficiencias en sus sistemas existentes al comparar el status actual con el que se debiera tener.
- ✓ Al diseñar e implementar un sistema de acuerdo a un estándar internacional que ha sido trabajado, discutido y testeado por varias organizaciones, la empresa puede asegurarse la transparencia de su propia herramienta. El sistema también

[97] Partes interesadas

puede ser de apoyo para el cumplimiento de las normas y la reglamentación establecidas en cada contexto, garantizando a la organización una base sólida para la aplicación de cualquier otra norma o metodología de gestión de riesgos específica para un determinado segmento.

Además de servir como soporte, la aplicación de un estándar internacional trae varios beneficios, en especial:

- ✓ Puede contribuir a mejorar la confianza de las partes interesadas –ya sean internas y/o externas- sobre las habilidades que tiene la empresa para manejarse en un ambiente de riesgos.
- ✓ Reduce los riesgos para los procesos corporativos y los costos provenientes de dichos riesgos.
- ✓ Crea mecanismos de evaluación de riesgos, revisión de los procesos y en definitiva mejora los mecanismos de control y tratamiento.
- ✓ Mejora el Gobierno Corporativo.

Es cierto también que la aplicación de un estándar internacional traerá problemas y desafíos, principalmente vinculados a los objetivos de la empresa, como ser: asignación ineficaz de los recursos, problemas en la conducción del Gobierno Corporativo, inseguridad o falta de confianza en las partes involucradas, gestión de riesgos reactiva en vez de proactiva, entre otros.

El desafío principal de la aplicación de los estándares es demostrar a priori la rentabilidad de las medidas orientadas a mejorar la administración de riesgos empresariales, y obtener los resultados previstos. Es verdad que implica un costo pero también conlleva un beneficio. Por lo tanto, gestionar eficazmente estos riesgos para garantizar resultados económicos que concuerden con los objetivos estratégicos de la organización, quizás sea uno de los mayores retos de los administradores. Algunos podrán lograrlo en el corto plazo, otros deberán esperar más tiempo para obtener incremento y sostenibilidad en sus ganancias.

Para esto, es necesario un cambio en la cultura organizacional, lo que puede resultar difícil principalmente en empresas donde la alta gerencia es de corte tradicional y

burocrática con fuerte impronta de generaciones pasadas. Se debe generar una conciencia de riesgo y abrir la mente para percibir que estos procesos llevan a mejorar los beneficios de la empresa.

La realidad muestra que los dos factores de resistencia de las empresas para gestionar riesgos son: su costo y el cambio cultural que implicaría en la alta dirección. En el primer caso, los costos de infraestructura, capacitación continua y sistemas de información pueden a veces parecer elevados si se toman en cuenta los costos ocultos de la no medición de riesgos y que los beneficios económico-financieros, tangibles e intangibles, no siempre son inmediatos. En segundo lugar está la resistencia generacional de la alta dirección, deriva de que posiblemente no hayan tenido la oportunidad de formarse dentro de una cultura de riesgos, debiendo actualizarse para poder ser el motor del cambio y promover este nuevo enfoque. Por más que los empleados estén convencidos de lo provechoso que puede resultar la administración empresarial del riesgo, si desde los altos niveles no se la promueve y se la estimula, a la larga culmina resultando en un requisito administrativo más.

A nuestro entender, el surgimiento de la norma ISO 31000 en el 2009 con el agregado de la norma ISO 31010 (que detalla numerosos instrumentos para aplicar el sistema de administración integral de riesgos), llevará a una aceptación y aplicación universal y las organizaciones empezarán a utilizarla como modelo de gestión, incluso algunas de ellas, sustituyendo el modelo de COSO- ERM existente.

Mas allá de esto y como fue mencionado en el análisis del alcance, la utilización de un estándar genérico como el ISO 31000, deriva en la necesidad de complementarlo, ya sea con un estándar regional o nacional, o con un documento aplicado a la industria o a la propia empresa. Esto se debe a que cada vez las realidades empresariales son más complejas y con regulaciones más especializadas, requiriendo una atención más particularizada.

Hemos visualizado esta tendencia en el análisis comparativo de la información relevada que abarca desde los desarrollos iniciales hasta los más recientes, a lo largo y ancho del mundo.

Estándares de naciones como Australia y Nueva Zelanda (AS/NZS 4360) y Canadá (CAN/CSA-Q850) ya han adaptado sus lineamientos con la nueva norma ISO 31000.

En el caso de AS/NZS 4630:2004 al haber sido el esquema fundamental para la creación del documento ISO 31000, la adaptación al nuevo estándar internacional simplemente consiste en modificar la Introducción y el Prefacio, creando así el nuevo estándar AS/NZS ISO 31000.

Por su parte, actualmente Canadá está desarrollando la actualización de su estándar de Administración de Riesgos. En enero 2010 apareció el primer borrador del documento CAN/CSA-ISO 31000 para comentario del público.

En la región, tanto en Argentina como en Brasil, se han publicado normas de gerencia de riesgos. En el caso de Argentina el Instituto Argentino de Normalización y Certificación[98] emitió las normas IRAM 17550 (2005) e IRAM 17551 (2007) que tratan el tema siendo éstas casi idénticas al estándar de Australia y Nueva Zelanda del 2004. En Brasil, el Instituto Brasilero de Gobernanza Corporativa [99] emitió en el 2007 una Guía de Orientación para el Gerenciamiento de Riesgos Corporativos que toma como base el modelo de COSO – ERM.

Por más que estos países son notoriamente más influyentes y con escalas mucho mayores que el nuestro, Uruguay, a pesar de ser un país en vías de desarrollo, está cada vez más inmerso en el contexto globalizado. Por este motivo es que la creciente relevancia a nivel mundial de la institucionalización de una función de administración de riesgos no puede quedar ajena a nuestra realidad. Uruguay desde hace más de una década y fuertemente en el último período ha profundizado las medidas de estimulo al ingreso de inversiones extranjeras y uno de los aspectos que mide un inversor cuando va a comprar una empresa son los riesgos que están involucrados en su gestión (las contingencias, incertidumbre y probabilidad de efectos adverso). En la medida que las

[98] http://www.iram.org.ar/
[99] IBGC Instituto Brasileiro de Governança Corporativa, www.**ibgc**.org.br

empresas reconozcan la bondad de administración de riesgos, permitirá la transparencia del mercado y ofrecerá un producto de mejor calidad para el inversor.

La administración de riesgos surge en economías que tienen un grado de madurez mayor a la nuestra, tanto a nivel de las entidades privadas como de las públicas.
En cuanto a las empresas públicas, uno de los principales objetivos del próximo gobierno es avanzar y profundizar la modernización del Estado; y para hacerlo, debe abordar una serie de aspectos de la administración en los cuales se encuentra la administración de riesgos propiamente dicha. Modelos como los del gobierno de Canadá se podrían tomar como ejemplo para realizarlo.

En consecuencia sería recomendable comenzar a investigar y profundizar más en el tema, ajustándose a los avances del resto del mundo que sean aplicables y convenientes para nuestro país, adaptando estos estándares "macro" a ámbitos de aplicación de menor escala (por ejemplo, las PYMES).

Finalmente, entendemos sería conveniente que desde el ámbito académico (Universidades) y desde el ámbito profesional (Colegio de Profesionales) se aborde la tarea de difundir los estándares, las ventajas de utilizar esta herramienta por parte de las empresas, enfatizando que la ecuación costo beneficio en el corto o largo plazo es favorable porque la administración integral de riesgos permite a los empresarios evitar o mitigar erogaciones extraordinarias originadas por el surgimiento de circunstancias o situaciones adversas que ellos pueden gestionar.

ANEXOS:

ANEXO I:

Ejemplo de tablas de valoración de riesgos

Elaboración propia en base a los distintos estándares estudiados

Escala de Probabilidad

Casi cierto	Se espera que ocurra en la mayoría de las circunstancias
Probable	Probablemente ocurrirá en la mayoría de las circunstancias
Posible	Podría ocurrir en algún momento
Improbable	Pudo ocurrir en algún momento
Excepcional	Puede ocurrir sólo en circunstancias excepcionales

Escala de Impacto

Insignificante	Efectos insignificantes sobre los objetivos
Leve	Efectos menores que pueden fácilmente remediarse
Moderada	Algunos objetivos se pueden ver afectados
Grave	Algunos de los objetivos no pueden alcanzados
Catastrófica	La mayoría de los objetivos no pueden ser alcanzados

Nivel de riesgo

Extremo	Se deben tomar acciones inmediatas
Alto	Constante administación y monitoreo
Medio	Monitoreo y evaluación periódica
Bajo	Administrar mediante procedimientos de rutina

ANEXO II:

Ejemplo de Matriz de riesgos

Elaboración propia en base a los distintos estándares estudiados

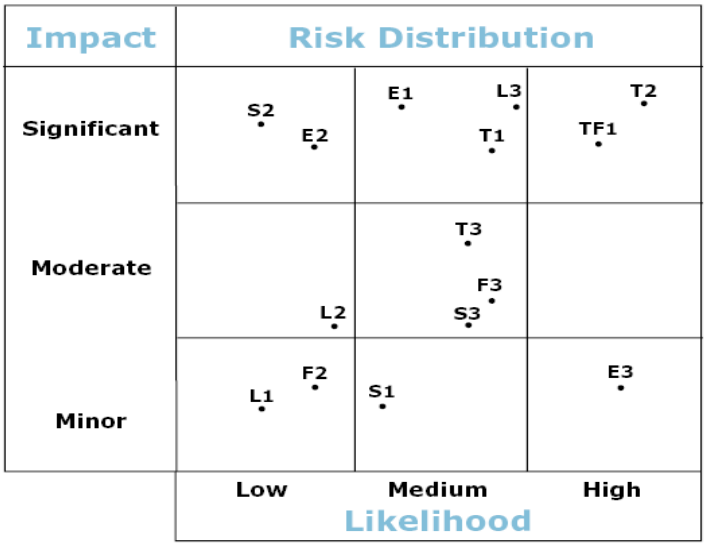
Probabilidad	Consecuencias				
	Insignificante	Leve	Moderada	Grave	Catastrófica
Casi cierto	Monitoreo y evaluación periódica	Constante adminsitración y monitoreo	Acciones inmediatas	Acciones inmediatas	Acciones inmediatas
Probable	Monitoreo y evaluación periódica	Monitoreo y evaluación periódica	Constante adminsitración y monitoreo	Acciones inmediatas	Acciones inmediatas
Posible	Administrar mediante procedimientos de rutina	Monitoreo y evaluación periódica	Monitoreo y evaluación periódica	Constante adminsitración y monitoreo	Acciones inmediatas
Improbable	Administrar mediante procedimientos de rutina	Administrar mediante procedimientos de rutina	Monitoreo y evaluación periódica	Constante adminsitración y monitoreo	Acciones inmediatas
Excepcional	Aceptar	Administrar mediante procedimientos de rutina	Administrar mediante procedimientos de rutina	Monitoreo y evaluación periódica	Constante adminsitración y monitoreo

ANEXO III:

Ejemplo de matriz de mapeo de riesgos

Documento Canadiense

Exhibit 3: A Risk Map



Risks identified:

Economic and Financial
- F1 Interest rate
- F2 Securities
- F3 Cost of insurance

Environmental
- E1 Climate change
- E2 Pollution
- E3 Ozone depletion

Legal
- L1 Liabilities
- L2 Human rights
- L3 International agreements

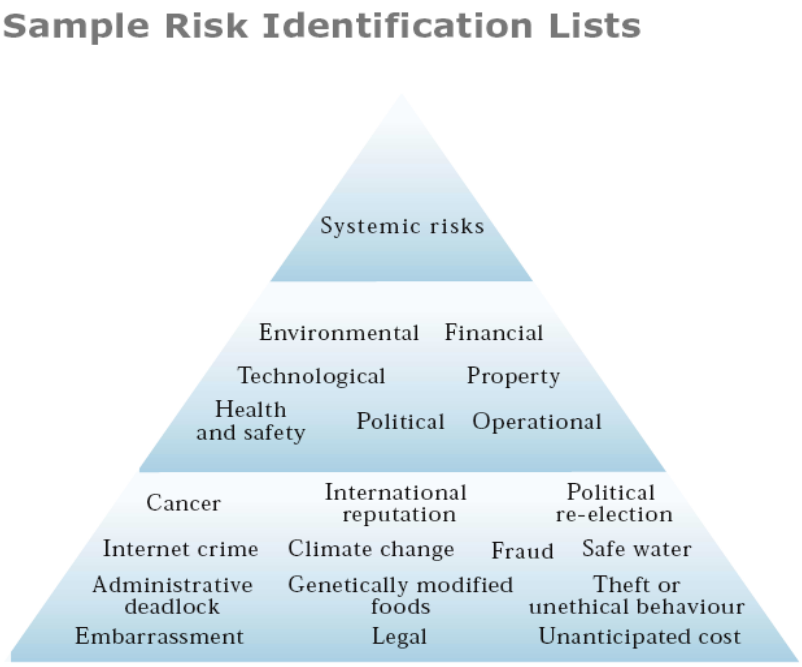
Technological
- T1 Nuclear power
- T2 Biotechnology
- T3 Genetic engineering

Safety and Security
- S1 Invasion
- S2 Terrorism
- S3 Organized crime

ANEXO IV:

Pirámide de categorización de riesgos

Documento Canadiense



ANEXO V:

Apéndice Estándares de Gerencia de Riesgo

10. Apéndice

Técnicas de identificación de riesgos - ejemplos

- *Tormenta de ideas*
- *Cuestionarios*
- *Estudios empresariales que se centren en cada proceso de negocio y describan tanto los procesos internos como los factores externos que puedan influir en estos procesos.*
- *Establecimiento de criterios de competencia comparativa ("benchmarking") en la industria.*
- *Análisis de distintos escenarios*
- *Talleres de valoración de riesgos*
- *Investigación de incidentes*
- *Auditoría e inspección*
- *Método HAZOP (Hazard & Operability Studies -Estudios de Azar y Operatividad-)*

Métodos y técnicas de análisis de riesgos - ejemplos

Riesgo positivo

- *Estudios de mercado*
- *Prospección*
- *Pruebas de mercado*
- *Investigación y desarrollo*
- *Análisis de impacto en el negocio*

Ambos

- *Establecimiento de modelos de dependencia*
- *Análisis SWOT (Strengths, Weaknesses, Opportunities, Threats -puntos fuertes, puntos flacos, oportunidades y amenazas-)*
- *Análisis del árbol de sucesos*
- *Planes de continuidad del negocio*
- *Análisis BPEST (Business, Political, Economic, Social, Technological -de negocio, político, económico, social, tecnológico-)*
- *Establecimiento de modelos de opción real.*
- *Toma de decisiones en condiciones de riesgo e incertidumbre*
- *Inferencia estadística*
- *Medidas de tendencia central y dispersión*
- *PESTLE (Political, Economic, Social, Technical, Legal, Environmental - político, económico, social, técnico, legal, medioambiental-)*

Riesgos negativos

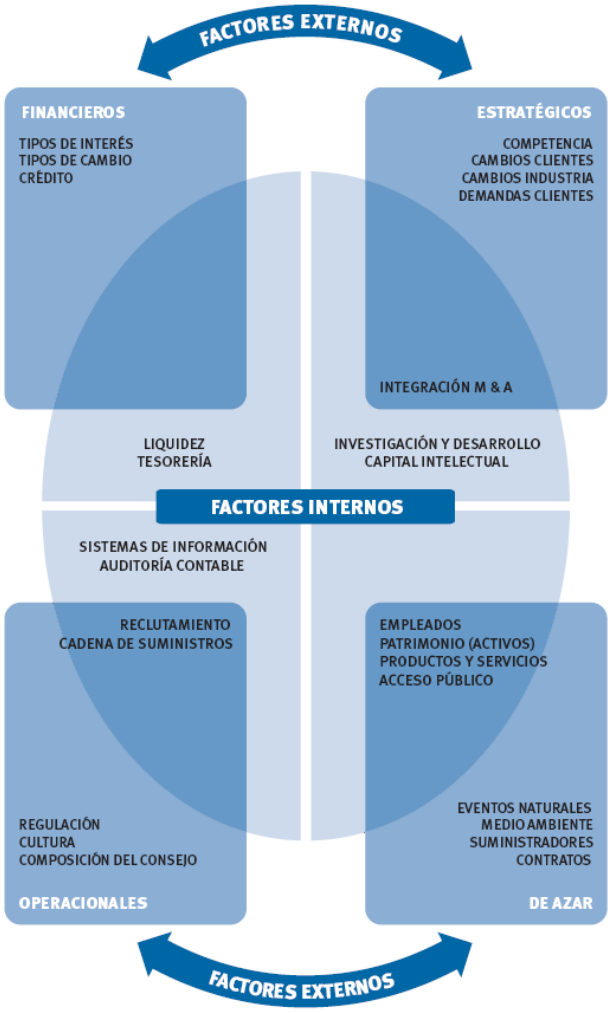
- *Análisis de amenazas*
- *Análisis del árbol de fallos*
- *Análisis FMEA (Failure Mode & Effects Análisis -análisis de los modos de fallos y sus efectos-)*

ANEXO VI:

Análisis de factores externos o Internos del documento

Estándares de Gerencia de Riesgo

2.1 Ejemplos de Factores Externos e Internos



ANEXO VII:

Ejemplo de valoración de oportunidades

Estándar australiano AS/NZS 4360:2004

Example of detailed description for positive consequence

Level	Descriptor	Description
1	Insignificant	Small benefit, low financial gain
2	Minor	Minor improvement to image, some financial gain
3	Moderate	Some enhancement to reputation, high financial gain
4	Major	Enhanced reputation, major financial gain
5	Outstanding	Significantly enhanced reputation, huge financial gain

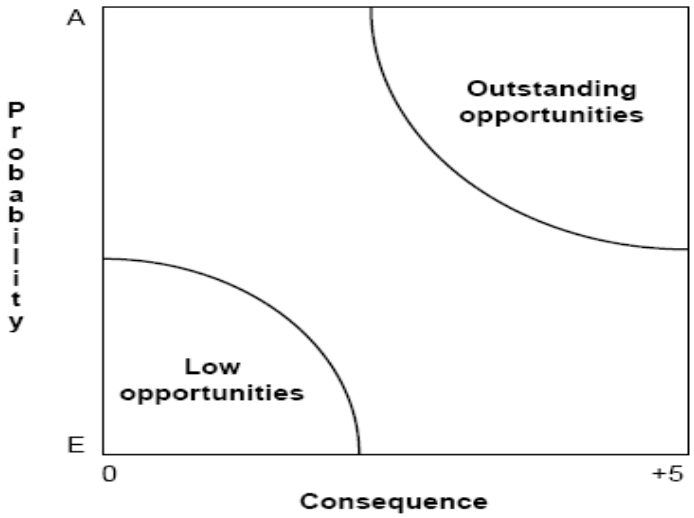


FIGURE 6.5 OPPORTUNITIES

ANEXO VIII:

Jerarquía de actividades para monitorear los riesgos

Estándar australiano AS/NZS 4360:2004

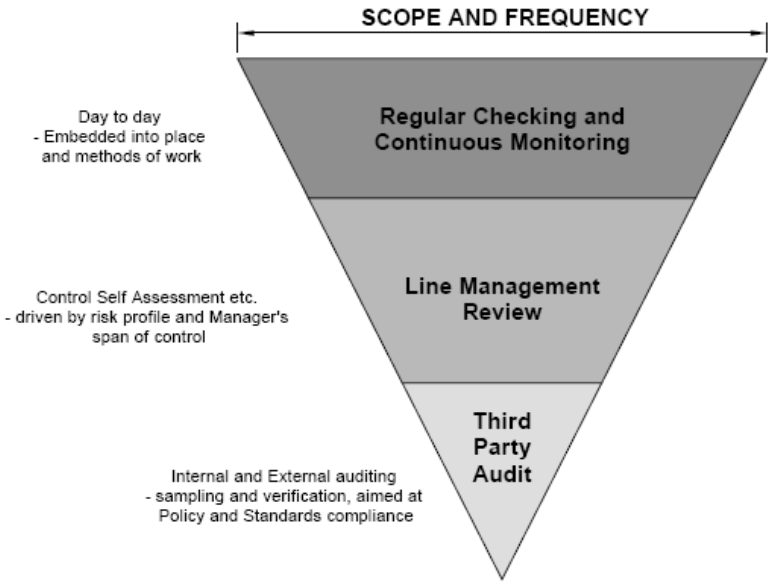


FIGURE 9.1 HIERARCHY OF ASSURANCE ACTIVITIES

ANEXO IX:

Técnicas de identificación y análisis de riesgos

Documento BS 31100

Tool	Identification	Assessment	Response
Risk Questionnaires	✓		
Risk Checklists/ Prompt Lists	✓		
Risk Identification Workshop	✓	✓	
Nominal Group Technique	✓	✓	
Risk Breakdown Structure	✓	✓	
Delphi Technique	✓	✓	
Process Mapping	✓	✓	
Cause-and-Effect Diagrams	✓	✓	
Risk Mapping/ Risk Profiling	✓	✓	
Risk Indicators	✓		
Brainstorming/ "thought shower" events;	✓		
Interviews and focus groups;	✓		
"What if?" workshops;	✓		
Scenario analysis/ scenario planning/ horizon scanning;	✓	✓	✓
Hazard and Operability Study (HAZOPs),:	✓	✓	
PEST (Political, Economic, Sociological, Technological) Analysis	✓	✓	
SWOT (Strengths, Weaknesses, Opportunities, Threats) Analysis	✓	✓	
Stakeholder Engagement/ Matrices	✓		
Risk Register/ Database	✓	✓	✓
Project Profile Model (PPM)	✓		
Risk Taxonomy	✓		
Gap Analysis: Pareto Analysis	✓	✓	
Probability and Impact Grid/ Diagrams (PIDs)/ Boston Grid	✓	✓	
CRAMM	✓	✓	✓
Probability Trees		✓	
Expected Value Method		✓	
Risk Modelling/ Risk Simulation (Monte Carlo/ Latin Hypercube):		✓	
Flow charts, process maps and documentation;		✓	
Fault and event tree modelling; Failure Mode Effects Analysis (FMEA)		✓	
Stress Testing	✓	✓	
Critical Path Analysis (CPA) or Critical Path Method (CPM)		✓	
Sensitivity Analysis		✓	
Cash Flow Analysis		✓	
Portfolio Analysis		✓	
Cost-Benefit Analysis		✓	✓
Utility theory		✓	
Visualization techniques heat maps, RAG status reports, Waterfall charts, Profile graphs, 3D Graphs, Radar chart, Scatter diagram;		✓	✓

ANEXO X:

Relación entre los principios, el marco y el proceso de administración de riesgos

Documento ISO 31000

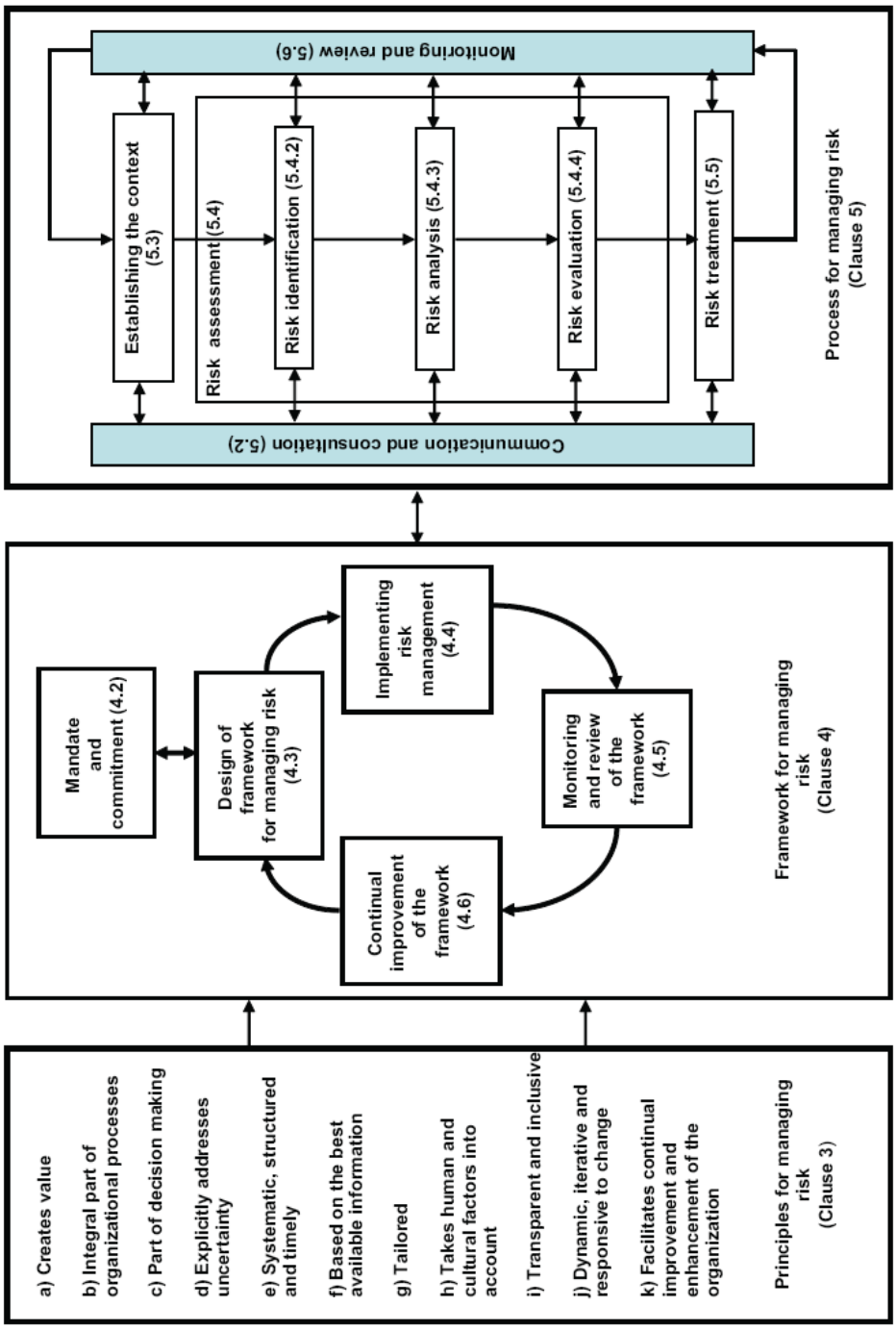


Figure 1 — Relationships between the risk management principles, framework and process

ANEXO XI:

Tabla con posibles técnicas para evaluar riesgos

Documento ISO 31010

Table A.1 – Applicability of tools used for risk assessment

Tools and techniques	Risk assessment process					See Annex
	Risk Identification	Risk analysis			Risk evaluation	
		Consequence	Probability	Level of risk		
Brainstorming	SA[1)]	NA[2)]	NA	NA	NA	B 01
Structured or semi-structured interviews	SA	NA	NA	NA	NA	B 02
Delphi	SA	NA	NA	NA	NA	B 03
Check-lists	SA	NA	NA	NA	NA	B 04
Primary hazard analysis	SA	NA	NA	NA	NA	B 05
Hazard and operability studies (HAZOP)	SA	SA	A[3)]	A	A	B 06
Hazard Analysis and Critical Control Points (HACCP)	SA	SA	NA	NA	SA	B 07
Environmental risk assessment	SA	SA	SA	SA	SA	B 08
Structure « What if? » (SWIFT)	SA	SA	SA	SA	SA	B 09
Scenario analysis	SA	SA	A	A	A	B 10
Business impact analysis	A	SA	A	A	A	B 11
Root cause analysis	NA	SA	SA	SA	SA	B 12
Failure mode effect analysis	SA	SA	SA	SA	SA	B 13
Fault tree analysis	A	NA	SA	A	A	B 14
Event tree analysis	A	SA	A	A	NA	B 15
Cause and consequence analysis	A	SA	SA	A	A	B 16
Cause-and-effect analysis	SA	SA	NA	NA	NA	B 17
Layer protection analysis (LOPA)	A	SA	A	A	NA	B 18
Decision tree	NA	SA	SA	A	A	B 19
Human reliability analysis	SA	SA	SA	SA	A	B 20
Bow tie analysis	NA	A	SA	SA	A	B 21
Reliability centred maintenance	SA	SA	SA	SA	SA	B 22
Sneak circuit analysis	A	NA	NA	NA	NA	B 23
Markov analysis	A	SA	NA	NA	NA	B 24
Monte Carlo simulation	NA	NA	NA	NA	SA	B 25
Bayesian statistics and Bayes Nets	NA	SA	NA	NA	SA	B 26
FN curves	A	SA	SA	A	SA	B 27
Risk indices	A	SA	SA	A	SA	B 28
Consequence/probability matrix	SA	SA	SA	SA	A	B 29
Cost/benefit analysis	A	SA	A	A	A	B 30
Multi-criteria decision analysis (MCDA)	A	SA	A	SA	A	B 31

[1)] Strongly applicable.

[2)] Not applicable.

[3)] Applicable.

ANEXO XII:

ALARP

Documento ISO 31010

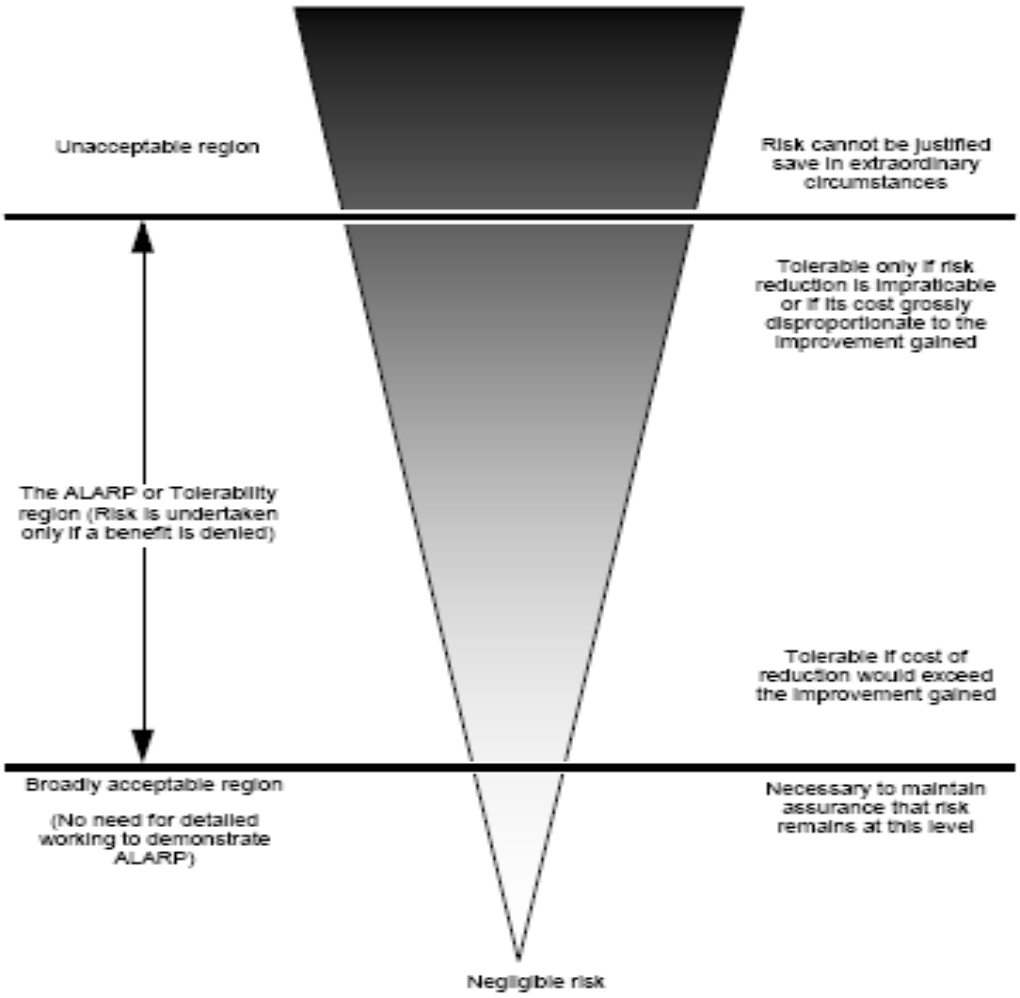


Figure B.12 – The ALARP concept

ANEXO XIII

Clasificación de eventos por categorías

Documento COSO - ERM

Figura 4.12
Clasificación de eventos por categorías

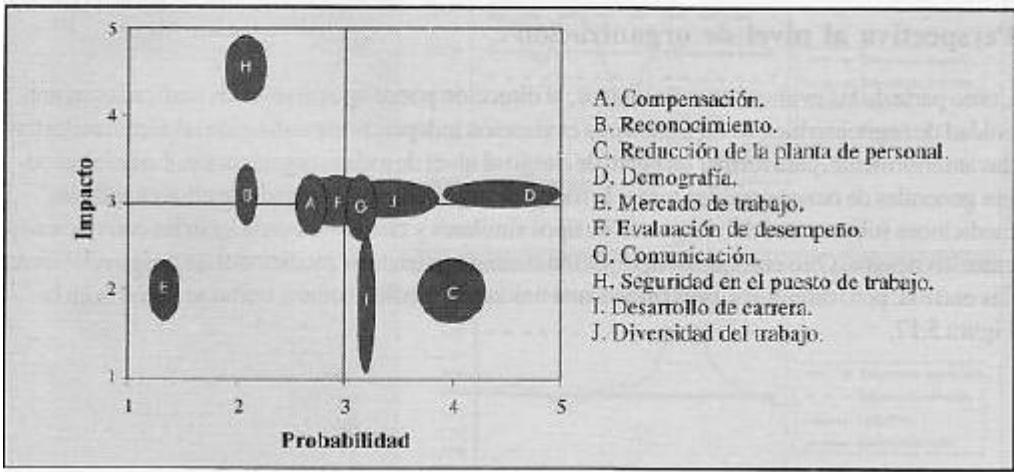
Factores	Económicos	Salud pública	Prestación de servicios	Recursos humanos	Tecnología	Medio ambientales
Eventos	Cambios en:					
	• Financiación. • Tasas de cambio. • Tasas de interés. • Impagos de crédito. • Disponibilidad de capital a largo plazo.	• Decisiones de estilo de vida. • Comportamientos sociales. • Estándares de la industria.	• Guías de intervención aguda. • Prácticas ambulatorias. • Prácticas de cuidados continuos. • Procedimientos de diagnóstico. • Prevención de enfermedades. • Prácticas de servicios de emergencia. • Prácticas de cuidados palintivos.	• Oportunidades de empleo. • Tasas de retención de empleados. • Niveles de planta del personal médico y de enfermería. • Procedimientos de evaluación. • Prácticas de seguridad e higiene.	• Protocolos de acceso a sistemas / datos. • Disponibilidad de sistemas y datos. • Tecnologías disponibles. • Sistemas (implantados o abandonados). • Requisitos de registros sanitarios.	• Emisiones / Productos de desecho generados. • Catástrofes naturales.

ANEXO XIV

Mapa de riesgo

Documento COSO - ERM

Figura 5.15
Mapa de riesgo con la variabilidad de probabilidad e impacto

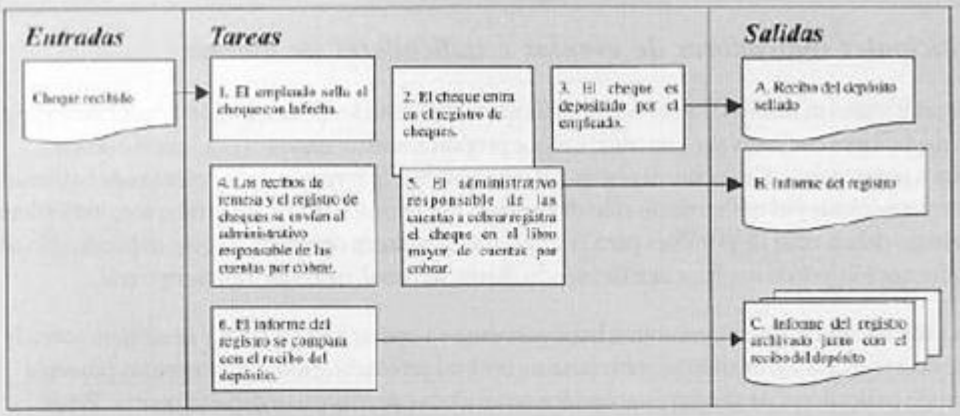


ANEXO XV

Análisis del flujo de procesos

Documento COSO - ERM

Figura 4.6
Análisis del flujo de procesos



Tareas	Posibles eventos
1. El empleado sella el cheque con la fecha.	• El administrativo olvida sellar el cheque.
2. El cheque entra en el registro de cheques.	• El administrativo olvida registrar los detalles del cheque. • El administrativo registra detalles incorrectos del cheque. • El administrativo malversa los fondos del cheque.
3. El cheque es depositado por el empleado.	• El cheque se pierde de camino al banco. • El cheque se ingresa en la cuenta bancaria incorrecta. • El banco registra una cantidad incorrecta. • El recibo sellado del depósito se pierde.
4. Los recibos de remesa y el registro de cheques se envían al administrativo responsable de las cuentas por cobrar.	• Los recibos de la remesa o el registro de cheques se extravían o se pierden.
5. El administrativo responsable de las cuentas a cobrar registra el cheque en el libro mayor de cuentas por cobrar.	• Los cheques se aplican en cuentas incorrectas. • Se registra una cantidad incorrecta en la cuenta del cliente. • El administrativo responsable de las cuentas a cobrar no registra los cheques.
6. El informe del registro se compara con el recibo del depósito.	• Los detalles no cruzan.

BIBLIOGRAFIA Y SITIOS WEB

BIBLIOGRAFÍA

- Administración de Riesgos Corporativos - Marco Integrado - Resumen Ejecutivo Marco (2005). Pricewaterhouse Coopers. 135 pág.
- Administración de Riesgos Corporativos - Marco Integrado - Técnicas de Aplicación Marco (2005). Pricewaterhouse Coopers. 113 pág.

SITIOS WEB

- Administración del riesgo empresarial, material publicado por la cátedra de Control Interno (2005). www.ccee.edu.uy
- AIRMIC - An overview comparison of the AIRMIC/ALARM/ IRM Risk Management Standard with: the Australia/New Zealand Standard AS/NZS 4360:2004 and the COSO Enterprise Risk Management - Integrated Framework (2005) www.airmic.com 14 pág.
- A Risk Management Standard (2002), Institute of Risk Management (IRM), Association of Insurance and Risk Managers (AIRMIC), and National Forum for Risk Management in the Public Sector (ALARM). Traducción de FERMA (Federation of European Risk Management Associations) al español (2003) www.ferma-asso.org 16 pág.
- AS/NZS 4360:1999 Estándar Australiano Administración de Riesgos. Traducción tomada de http://www.netconsul.com/riesgos/ar.pdf 36 pág.
- AS/NZS 4360:2004, Risk Management (2006) Standards Australia/Standards New Zealand 39 pág. http://www.ucop.edu/riskmgt/erm/documents/as_stdrds4360_2004.pdf
- A simple guide to risk and its management. (2009) Broadleaf Capital International Pty Ltd. www.broadleaf.com.au 9 pág.
- A ‘Standards Based’ approach to Operational Risk Management under Basel II (2005) Patrick Mc Connell www.continuitycentral.com/feature0168.htm 17 pág.

- Basilea: Metodología de los Principios Básicos. (2006) Versión en español. Bank for International Settlements (BIS) http://www.bis.org/publ/bcbs130esp.pdf 53 pág.
- CAN/CSA-Q850-97 R2002, Risk management: Guidelines for decision-makers. (2002) Canadian Standards Association. www.csa.ca 46 pág.
- COSO (2004) Enterprise Risk Management – Integrated Framework. The Committee of Sponsoring Organisations of the Treadway Commission. www.coso.org
- Draft ISO/FDIS 31000:2009 Risk management — Principles and guidelines (2009) www.iso.org 34 pág.
- Draft IEC/FDIS 31010 Risk management — Risk assessment techniques, (2009) International Electrotechnical Commission, www.iec.org 92 pág.
- Draft BS 31100:2009 Code of practice for risk management, DPC: 07/30153955 DC. (2007) British Standards Institution. www.bsi-global.com 44 pág.
- Draft AS/NZS ISO 31000:2009 Risk management— Principles and guidelines. Standards Australia/Standards New Zealand www.standards.org.au 10 pág.
- Draft Standard CAN/CSA-Q850 Risk management: Implementation of CAN/CSA-ISO-31000. (2010) Canadian Standards Association. www.csa.ca 37 pág.
- ¿Es posible situar al riesgo en un área confortable? Nueve principios para construir una Empresa Inteligente en Riesgos. (2009) Quintas Jornadas Rioplatenses de Auditoría Interna – Instituto Uruguayo de Auditoría interna, Cra. Mariella de Aurrecoechea, Deloitte S.C. www.deloitte.com
- Guia de Orientação para Gerenciamento de Riscos Corporativos (2007) Instituto Brasileiro de Governança Corporativa www.ibgc.org.br 50 pág.
- Hacia una cultura de Risk Management (2008) *www.asbaweb.org/E-News/enws-8/PDF.../0708_TC_01_ES.pdf*

- Information Brief on International Risk Management Standards (2005) Marc Saner, Institute On Governance www.iog.ca 37 pág.
- Integrated Risk Management Framework (2001). Treasury Board of Canada Secretariat http://www.tbs-sct.gc.ca/rm-gr 42 pág.
- Integrated Risk Management Implementation Guide (2002). Treasury Board of Canada Secretariat http://www.tbs-sct.gc.ca 102 pág.
- IRAM 17550 (2005) Instituto Argentino de Normalización y Certificación www.**iram**.org.ar/ (documentos en estudio) 27 pág.
- IRAM 17551 (2007) Instituto Argentino de Normalización y Certificación www.**iram**.org.ar/ (documentos en estudio) 27 pág.
- ISO/IEC Guide 73:2002, Risk management – Vocabulary – Guidelines for use in standards (2002) www.iso.org 3 pág.
- La Administración de Riesgos Empresarial en el contexto actual del Control Interno (2006). Dra. Aleida González-Cueto Longres, Msc. Manuel Pando Franco. www.nodo50.org/cubasigloXXI/economia/gcueto_311206.pdf 17 pág.
- La gestión de riesgos apoyada en el Gobierno Corporativo (2007) Alfonso Parias www.deceval.com
- Modelo de Identificación de los riesgos de Control Interno para la actividad empresarial (2009). Lic.Yadira Rodriguez Carrazana, MSc. Manuel Guerra Garcés, Ing. Francisco E. Reyes Santos. http://www.eumed.net/ce/2009a/cgs.htm 56 pág.
- Principios del Buen Gobierno Corporativo (1999) Organisation for Economic Co-operation and Development (OECD) Traducción al español. www.oecd.org/ 54 pág.
- Raising the standard – The new ISO Risk Management Standard, Willington Meeting (2009) Broadleaf Capital International Pty Ltd. www.broadleaf.com.au 5 pág.

- Raz, T & Hillson, D A (2005) A comparative review of risk management standards. Risk Management: An International Journal. www.jstor.org/stable/3867797 14 pág.
- Revista: A Wake-up Call for Enterprise Risk Management, 2009 Risk and Insurance Management Society, Inc. (RIMS) www.RIMS.org 10 pág.
- Risk Governance towards an integrative approach. International Risk Governance Council, Ortwin Renn www.irgc.com 157 pág.
- Risk Management Guidelines Companion to AS/NZS 4360:2004 Standards Australia/Standards New Zealand www.standards.org.au 131 pág.
- Roland Franz, Risk Management Standards – role, benefits & applicability (2008) 2nd European Risk Conference Università Bocconi. www.nottingham.ac.uk/.../PC24_erben.20080828.112817.pdf 34 pág.
- Sample pages: The Risk Management Universe. (2007) David Hillson, British Standards Institution www.BSIgroup.com 10 pág.
- Tutorial: Risk Management Standard, AS/NZS 4360:2004 (2007) Broadleaf Capital International Pty Ltd. www.broadleaf.com.au 6 pág.

Sitios Web recomendados

www.coso.org Committee for Sponsoring Organizations (COSO)

www.theirm.org Institute of Risk Management (IRM)

www.airmic.com Association of Insurance and Risk Managers (AIRMIC)

www.alarm-uk.com National Forum for Risk Management in the Public Sector (ALARM)

www.standards.org.au Standards Australia

www.standards.co.nz Standards New Zealand

www.BSIgroup.com British Standards Institution

http://www.tbs-sct.gc.ca Treasury Board of Canada Secretariat

www.csa.ca Canadian Standards Association

www.**iram**.org.ar Instituto Argentino de Normalización y Certificación

www.theiia.org The Institute of Internal Auditors

www.iso.org International Standarization Organization