



12 JUN 14 AM 10:52

## NORMAS Y PROCEDIMIENTOS DE LA EVALUACION DE GESTION DE RIESGO

### INTRODUCCIÓN

Estas normas tienen el propósito de establecer una evaluación de control de gestión de riesgo (*Enterprise Risk Management, ERM*) para el establecimiento de un sistema de control interno adecuado. Todas las entidades existen con el fin de generar valor a sus grupos de interés y nuestro reto es determinar cuánta incertidumbre se puede aceptar mientras nos esforzamos en incrementar el valor y la calidad de nuestros servicios a los lesionados y patronos. La incertidumbre implica riesgos y oportunidades y posee el potencial de erosionar o aumentar el valor. Esta evaluación de gestión de riesgo nos permitirá tratar eficazmente la incertidumbre, sus riesgos y las oportunidades asociadas, mejorando así la capacidad de generar una mejor calidad de servicio.

La gestión de riesgo<sup>1</sup>, se define como "... un proceso, efectuado por la Junta de Directores de la entidad, la administración y otro personal, aplicables en establecer la estrategia en toda la empresa y diseñado para identificar eventos potenciales que puedan afectar a la entidad, gestionar sus riesgos dentro del riesgo aceptado y proporcionar una seguridad razonable sobre el logro de los objetivos de la entidad." Esta definición recoge los siguientes conceptos básicos:

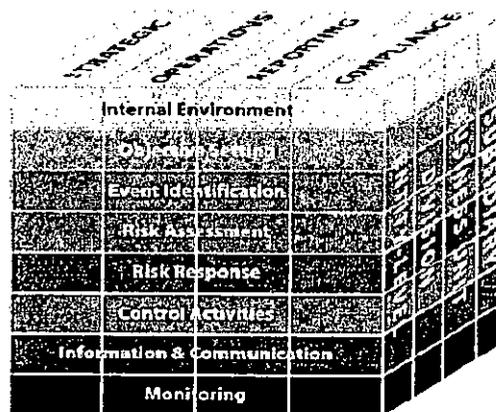
- Es un proceso continuo que fluye por toda la entidad.
- Es realizado por su personal en todos los niveles de la organización.
- Se aplica en el establecimiento de la estrategia.

<sup>1</sup> Definición según: COSO Enterprise Risk Management – Integrated Framework. 2004. COSO.

- Se aplica en toda la entidad, en cada nivel y unidad e incluye adoptar una perspectiva del riesgo a nivel conjunto de la entidad.
- Está diseñado para identificar acontecimientos potenciales que, de ocurrir, afectarían a la entidad y para gestionar los riesgos dentro del nivel de riesgo aceptado.
- Es capaz de proporcionar una seguridad razonable al consejo de administración y a la dirección de una entidad.
- Esta orientada al logro de objetivos dentro de unas categorías diferenciadas, aunque susceptibles de solaparse.

## COMPONENTES DE LA GESTIÓN DE RIESGO

La gestión de riesgo consta de ocho componentes relacionados entre sí, que se derivan de la manera en que la dirección conduce la empresa y como están integraos en el proceso de gestión. Los componentes son los siguientes:



- *Ambiente interno* - Abarca el talante de una organización y establece la base de cómo el personal de la entidad percibe y trata los riesgos, incluyendo la filosofía para su gestión, el riesgo aceptado, la integridad y valores éticos y el entorno en que se actúa.

- *Establecimiento de objetivos* - Los objetivos deben existir antes de que la dirección pueda identificar potenciales eventos que afecten a su consecución. La gestión de riesgos asegura que la dirección ha establecido un proceso para fijar objetivos y que los objetivos seleccionados apoyan la misión de la entidad y están en línea con ella, además de ser consecuentes con el riesgo aceptado.
- *Identificación de eventos* - Los acontecimientos internos y externos que afectan a los objetivos de la entidad deben ser identificados, diferenciando entre riesgos y oportunidades. Estas últimas revierten hacia la estrategia de la dirección o los procesos para fijar objetivos.
- *Evaluación de riesgos* - Los riesgos se analizan considerando su probabilidad e impacto como base para determinar cómo deben ser gestionados y se evalúan desde una doble perspectiva, inherente y residual.
- *Respuesta al riesgo* - La dirección selecciona las posibles respuestas - evitar, aceptar, reducir o compartir los riesgos - desarrollando una serie de acciones para alinearlos con el riesgo aceptado y las tolerancias al riesgo de la entidad.
- *Actividades de control* - Las políticas y procedimientos se establecen e implantan para ayudar a asegurar que las respuestas a los riesgos se llevan a cabo eficazmente.
- *Información y comunicación* - La información relevante se identifica, capta y comunica en forma y plazo adecuado para permitir al personal afrontar sus responsabilidades. Una comunicación eficaz debe producirse en un sentido amplio, fluyendo en todas direcciones dentro de la entidad.

- *Supervisión* - La totalidad de la gestión de riesgos corporativos se supervisa, realizando modificaciones oportunas cuando se necesiten. Esta supervisión se lleva a cabo mediante actividades permanentes de la dirección, evaluaciones independientes o ambas actuaciones a la vez.

## ROLES Y RESPONSABILIDADES

Todas las personas que integran una entidad tienen alguna responsabilidad en la gestión de riesgos. Hay una obligación específica para los ejecutivos, los directores y jefes de unidades para establecer el tono para la eficaz administración de riesgos. El mismo es como sigue:

- Presidente, asistido por el Director Ejecutivo es responsable de la aplicación de procesos de gestión de riesgo. Ella o él es, en consecuencia, responsable de la aplicación de la política *ERM*, incluidos el establecimiento y mantenimiento de controles clave y procesos de aprobación o todos los procesos de negocios más importantes y funciones. El Presidente también es responsable de revisar los riesgos subyacentes de forma sistemática y la asignación adecuada de rendición de cuentas. El Director Ejecutivo trabaja con otros directores y supervisores para establecer y mantener una administración eficaz de los riesgos en sus áreas de responsabilidad, comprometiéndose con las políticas de *ERM* en toda la organización.
- El Comité de gestión del riesgo ayuda a la Administración a orientar el desarrollo de la *ERM* en el CIPR, la coordinación de su aplicación y la revisión y supervisión de procesos *ERM* y salidas sobre una base regular. Asiste en la educación y capacitación del personal, revisa la elaboración y actualización del perfil de riesgos y presenta informes periódicamente a la administración.

- Los Directores fomentan una cultura de gestión de riesgos y garantiza la aplicación adecuada de las políticas y procedimientos para salvaguardar los activos. Deben adoptar medidas apropiadas para controlar los riesgos de forma coherente y proactiva.
- Auditoría Interna desempeña un papel importante en la supervisión de *ERM* y la calidad de rendimiento como parte de sus actividades normales. Sin embargo, no, tienen responsabilidad principal de la aplicación de *ERM* o su mantenimiento. Juega un rol clave en la continuidad del funcionamiento del *ERM*, monitoreando objetivamente su aplicación y efectividad. En su rol apoya a la Gerencia proveyendo seguridad sobre:
  - El proceso de *ERM* – su diseño y su funcionamiento
  - La efectividad y eficiencia de la respuesta al riesgo y las actividades de control relacionadas
  - Integridad y exactitud en reportar *ERM*

En algunos casos también actúan en un rol de consultores:

- Promover el desarrollo de un entendimiento del *ERM*
  - Facilitador en talleres
  - Proveer herramientas y técnicas para ayudar a la gerencia en el análisis de riesgos y diseño de actividades de control
- Todo el personal contribuye y es responsable de la gestión de los riesgos y los procesos de control interno. En particular, apoyar el desarrollo y la actualización de la documentación de riesgos, identificar y evaluar los riesgos en sus áreas y contribuir a la mitigación de los mismos.

## PROCEDIMIENTOS

La evaluación se realizara anualmente y solo comprenderá las etapas de identificación de eventos, evaluación de riesgos y la respuesta al riesgo de al menos uno de los objetivos incluidos en el Plan Estratégico. Se utilizara la tabla adjunto para recopilar los resultados de la evaluación, ver anejo A. Las etapas para la realización de la evaluación es la siguiente:

### 1. Clasificar el objetivo a evaluar

Dentro del contexto de misión o visión establecida en la entidad, su dirección establece los objetivos estratégicos, selecciona la estrategia y fija objetivos alineados que fluyen en toda la entidad. Los objetivos se pueden clasificar en cuatro categorías:

Estratégicos:	Objetivos a alto nivel, alineados con la misión de la entidad y dándole apoyo
Operacionales:	Objetivos vinculados al uso eficaz y eficiente de recursos
Reporte (Financiero):	Objetivos de fiabilidad de la información suministrada
Cumplimiento:	Objetivos relativos al cumplimiento de leyes y normas aplicables

Esta clasificación de los objetivos de una entidad permite centrarse en aspectos diferenciados de la gestión de riesgos. Estas categorías distintas, aunque solapables - un objetivo individual puede incidir en más de una categoría- se dirigen a necesidades diferentes de la entidad y pueden ser de responsabilidad directa de

diferentes ejecutivos. También permiten establecer diferencias entre lo que cabe esperar de cada una de ellas. Otra categoría utilizada por algunas entidades es la salvaguarda de activos.

Dado que los objetivos relacionados con la confiabilidad de la información y el cumplimiento de leyes y normas están integrados en el control de la entidad, puede esperarse que la gestión de riesgos facilite una seguridad razonable de su consecución. El logro de los objetivos estratégicos y operativos, sin embargo, está sujeto a acontecimientos externos no siempre bajo control de la entidad; por tanto, respecto a ellos, la gestión de riesgos puede proporcionar una seguridad razonable de que la dirección, y el consejo de administración en su papel de supervisión, estén siendo informados oportunamente del progreso de la entidad hacia su consecución

## 2. Describir el evento o riesgo

Un evento es un suceso o fenómeno natural, tecnológico o provocado por el hombre que se describe en términos de sus características, su severidad, ubicación y área de influencia. Es el registro en el tiempo y el espacio de un fenómeno que caracteriza una amenaza. Es importante diferenciar entre un evento potencial y el evento mismo, una vez éste se presenta.

Un riesgo es la probabilidad que se presente un nivel de consecuencias económicas, sociales o ambientales en un sitio particular y durante un período de tiempo definido. Se obtiene de relacionar la amenaza con la vulnerabilidad de los elementos expuestos.

Los administradores reconocen que existen incertidumbres – que no se puede conocer con certeza si un acontecimiento ocurrirá y cuándo y cuáles serán sus resultados en caso de ocurrir. 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 las decisiones que

toman la Corporación del Fondo del Seguro del Estado y factores tecnológicos. Los factores internos reflejan las opciones tomadas por la gerencia e incluyen asuntos tales como infraestructura, personal, procesos y tecnología.

Por lo tanto, dentro de este renglón se desglosaran los eventos o riesgos que ocurrirían para evitar el logro del objetivo bajo evaluación.

### 3. Clasificar la probabilidad de la ocurrencia del evento o riesgo

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. Las estimaciones de probabilidad e impacto de riesgo a menudo son determinadas 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.

De acuerdo a los eventos o riesgos identificados que probabilidad existe de que ocurran. Esto se clasificara de la siguiente manera:

Alta	Mucha	Probable	3
Mediana	Poca	Razonablemente Posible	2
Baja	Ninguna	Remota	1

#### 4. Clasificar el impacto

El impacto representa el efecto en caso de que ocurriera el evento o riesgo. Se determinara al igual que las probabilidades usando datos sobre acontecimientos pasados observables. 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.

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. 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.

Por lo tanto, el impacto se clarificara de la siguiente manera:

Alto	Mucho	Muy Significativo	3
Mediano	Poco	Significativo	2
Bajo	Ninguno	Inmaterial	1

5. Calcular el nivel de riesgo

Es la cantidad de riesgo que una entidad está dispuesta a aceptar en la búsqueda de valor. Las entidades a menudo consideran el nivel de riesgo aceptado en forma cualitativa, con categorías tales como alta, moderada o baja o pueden aplicar un enfoque cuantitativo reflejando y buscando un equilibrio entre las metas de crecimiento, rendimiento y riesgo.

El nivel de riesgo máximo aceptable debe tener una tolerancia ya que en caso contrario limitaría las decisiones, o se eludiría el nivel máximo en forma arbitraria. La tolerancia al riesgo es el nivel aceptable de desviación en relación con el logro de los objetivos.

a. Evaluación cualitativa:

PROBABILIDAD	Alta	AB	AM	AA
	Media	MB	MM	MA
	Baja	BB	BM	BA
		Bajo	Medio	Alto
		IMPACTO		

Nivel de riesgo:

Bajo – sombreado color verde

Medio – sombreado color amarillo

Alto – sombreado color rojo

b. Evaluación cuantitativa:

$$\text{Nivel de riesgo} = \text{Probabilidad de ocurrencia} \times \text{Impacto en el objetivo afectado}$$

Donde:

Probabilidad = alta (3), media (2) y baja (1)

Impacto = alto (3), medio (2) y bajo (1)

Nivel de riesgo:

Bajo = de 1 al 3 (1x1), (1x2), (2x1), (1x3), (3x1)

Medio = 4 ó 6 (2x2), (2x3) (3x2)

Alto = 9 (3x3)

## 6. Identificar las 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. 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.

Existen distintos tipos de actividades de control: preventivas, detectivas, manuales, computarizadas y controles gerenciales. Identifique aquellas políticas o procedimientos establecidos que estén relacionadas al objetivo y al riesgo bajo evaluación.

## 7. Concluir sobre las actividades de control y establecer recomendaciones

*ERM* identifica cuatro categorías de respuestas al riesgo – evitar, reducir, compartir y aceptar. Como parte de la *ERM*, 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. Luego de haber considerado respuestas al riesgo sobre una base individual o grupal, la gerencia considera el efecto total de sus respuestas al riesgo en relación a la entidad en toda su extensión.

Las respuestas al riesgo:

Evitar – actúan para abandonar las actividades que generan riesgos. Asociado a rediseñar o eliminar la actividad de control.

Reducir – reducen la probabilidad del riesgo, el impacto del mismo o ambos. Se deben implantar controles internos.

Compartir – reducen la probabilidad o el impacto del riesgo transfiriendo o compartiendo de otro modo una porción del riesgo. Como por ejemplo transferir el riesgo a través de una póliza de seguro.

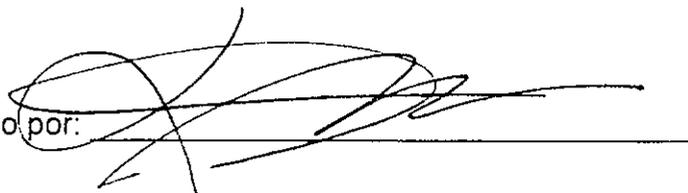
Aceptar – no actúan de forma alguna para modificar la probabilidad o el impacto del riesgo. O sea, no se toma ninguna acción sobre las actividades de control establecidas.

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. 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.

Por lo tanto, se desglosaran recomendaciones sobre las actividades de control detalladas anteriormente. Estableciendo si son suficientes, adecuadas o están funcionando para evitar o mitigar el riesgo.

Aprobado por:

A handwritten signature in black ink, consisting of several overlapping loops and a long horizontal stroke extending to the right. The signature is written over a horizontal line.

Fecha: 30 dic 2010