

AS/NZS 4360:1999  
Estándar Australiano  
Administración de Riesgos

# Administración de Riesgos

# Contenido

1 Alcance , aplicación y definiciones	3
1.1 Alcance	3
1.2 Aplicación	3
1.3 Definiciones	3
2 Requerimientos de administración de riesgos	6
2.1 Propósito	6
2.2 Política de administración de riesgos	6
2.3 Planeamiento y recursos	6
2.4 Programa de implementación	7
2.5 Revisión gerencial	7
3 Vista general de la administración de riesgos	8
3.1 General	8
3.2 Elementos principales	8
4 Proceso de administración de riesgos	10
4.1 Establecer el contexto	10
4.2 Identificación de riesgos	12
4.3 Análisis de riesgos	13
4.4 Evaluación de riesgos	15
4.5 Tratamiento de los riesgos	16
4.6 Monitoreo y revisión	19
4.7 Comunicación y consulta	19
5 Documentación	20
5.1 General	20
5.2 Razones para documentar	20
Apéndices	
A Aplicaciones de administración de riesgos	21
B Pasos en el desarrollo e implementación de un programa de administración de riesgos	22
C Interesados	24
D Fuentes genéricas de riesgo y sus áreas de impacto	25
E Ejemplos de definición y clasificación de riesgos	28
F Ejemplos de expresiones cuantitativas de riesgos	30
G Identificar opciones para tratamiento de los riesgos	31
H Administración y documentación de riesgos	32

# 1 Alcance, aplicación y definiciones

## 1.1 Alcance

Este Estándar provee una guía genérica para el establecimiento e implementación del proceso de administración de riesgos involucrando el establecimiento del contexto y la identificación, análisis, evaluación, tratamiento, comunicación y el monitoreo en curso de los riesgos.

## 1.2 Aplicación

La administración de riesgos es reconocida como una parte integral de las buenas prácticas gerenciales. Es un proceso iterativo que consta de pasos, los cuales, cuando son ejecutados en secuencia, posibilitan una mejora continua en el proceso de toma de decisiones.

Administración de riesgos es el término aplicado a un método lógico y sistemático de establecer el contexto, identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos asociados con una actividad, función o proceso de una forma que permita a las organizaciones minimizar pérdidas y maximizar oportunidades. Administración de riesgos es tanto identificar oportunidades como evitar o mitigar pérdidas.

Este Estándar puede ser aplicado a todas las etapas de la vida de una actividad, función, proyecto, producto o activo. El beneficio máximo se obtiene generalmente aplicando el proceso de administración de riesgos desde el principio.

A menudo se llevan a cabo una cantidad de estudios diferentes en las diferentes etapas de un proyecto.

**nota:** Este Estándar se puede aplicar a un amplio rango de actividades u operaciones de cualquier empresa pública, privada o comunitaria, o grupo.

Se brindan ejemplos en el Apéndice A.

## 1.3 Definiciones

Para el propósito de este Estándar se aplican las definiciones de abajo.

- 1.3.1 **Aceptación de riesgo:** una decisión informada de aceptar las consecuencias y probabilidad de un riesgo en particular.
- 1.3.2 **Administración de riesgos:** la cultura, procesos y estructuras que están dirigidas hacia la administración efectiva de oportunidades potenciales y efectos adversos.
- 1.3.3 **Análisis árbol de eventos:** una técnica que describe el rango y secuencia posibles de los productos que podrían surgir de un evento iniciado.
- 1.3.4 **Análisis árbol de fallas:** un método de ingeniería de sistemas para representar las combinaciones lógicas de varios estados del sistema y causas posibles que pueden contribuir a un evento especificado (denominado evento superior o "top event").
- 1.3.5 **Análisis de modos y efectos de fallas (FMEA):** un procedimiento por el cual se analizan modos de fallas potenciales en un sistema técnico. Se puede extender un FMEA para realizar lo que se denomina análisis de modo, efecto y criticidad de fallas (FMECA). En un FMECA, cada modo de falla identificado es ordenado de acuerdo a la influencia combinada de su probabilidad de ocurrencia y severidad de sus consecuencias.
- 1.3.6 **Análisis de riesgo:** un uso sistemático de la información disponible para determinar cuan frecuentemente pueden ocurrir eventos especificados y la magnitud de sus consecuencias.

- 1.3.7 Análisis de sensibilidad: examina cómo varían los resultados de un cálculo o modelo a medida que se cambian los supuestos o hipótesis individuales.
- 1.3.8 Azar de riesgo: una fuente de daño potencial o una situación con potencial para causar pérdidas.
- 1.3.9 Consecuencia: el producto de un evento expresado cualitativa o cuantitativamente, sea este una pérdida, perjuicio, desventaja o ganancia. Podría haber un rango de productos posibles asociados a un evento.
- 1.3.10 Control de riesgos: la parte de administración de riesgos que involucra la implementación de políticas, estándares, procedimientos y cambios físicos para eliminar o minimizar los riesgos adversos.
- 1.3.11 Costo: de las actividades, tanto directas como indirectas, involucrando cualquier impacto negativo, incluyendo pérdidas de dinero, de tiempo, de mano de obra, interrupciones, problemas de relaciones, políticas e intangibles.
- 1.3.12 Evaluación de riesgo: el proceso global de análisis de riesgo y evaluación de riesgo, ver la Figura 3.1.
- 1.3.13 Evaluación de riesgos: el proceso utilizado para determinar las prioridades de administración de riesgos comparando el nivel de riesgo respecto de estándares predeterminados, niveles de riesgo objetivos u otro criterio.
- 1.3.14 Evento: un incidente o situación, que ocurre en un lugar particular durante un intervalo de tiempo particular.
- 1.3.15 Evitar un riesgo: una decisión informada de no verse involucrado en una situación de riesgo.
- 1.3.16 Financiamiento de riesgos: los métodos aplicados para fondar el tratamiento de riesgos y las consecuencias financieras de los riesgos.  
**nota**: En algunas industrias financiamiento de riesgos se refiere sólo al fondeo de las consecuencias financieras de los riesgos.
- 1.3.17 Frecuencia: una medida del coeficiente de ocurrencia de un evento expresado como la cantidad de ocurrencias de un evento en un tiempo dado. Ver también Probabilidad.
- 1.3.18 Identificación de riesgos: el proceso de determinar qué puede suceder, por qué y cómo.
- 1.3.19 Ingeniería de riesgos: la aplicación de principios y métodos de ingeniería a la administración de riesgos.
- 1.3.20 Interesados: aquella gente y organizaciones que pueden afectar, ser afectados por, o percibir ellos mismos ser afectados, por una decisión o actividad.  
**nota**: El término puede incluir también partes interesadas tal como lo define la ISO 14050:1998 y la AS/NZS ISO 14004:1996.
- 1.3.21 Monitoreo: comprobar, supervisar, observar críticamente, o registrar el progreso de una actividad, acción o sistema en forma sistemática para identificar cambios.
- 1.3.22 Organización: una compañía, firma, empresa o asociación, u otra entidad legal o parte de ella, sea o no incorporada, pública o privada, que tiene sus propias funciones y administración.
- 1.3.23 Pérdida: cualquier consecuencia negativa, financiera o de otro tipo.
- 1.3.24 Probabilidad: la probabilidad de un evento específico o resultado, medido por el coeficiente de eventos o resultados específicos en relación a la cantidad total de posibles eventos o resultados. La probabilidad se expresa como un número entre 0 y 1, donde 0 indica un evento o resultado imposible y 1 indica un evento o resultado cierto.
- 1.3.25 Probabilidad: utilizado como una descripción cualitativa de probabilidad o frecuencia.
- 1.3.26 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.
- 1.3.27 Reducción de riesgos: una aplicación selectiva de técnicas apropiadas y principios de administración para reducir las probabilidades de una ocurrencia, o sus consecuencias, o ambas.
- 1.3.28 Retención de riesgos: intencionalmente o sin intención retener la responsabilidad por las pérdidas, o la carga financiera de las pérdidas dentro de la organización.

- 1.3.29 Riesgo residual: el nivel restante de riesgo luego de tomar medidas de tratamiento del riesgo.
- 1.3.30 Riesgo: la posibilidad de que suceda algo que tendrá un impacto sobre los objetivos. Se lo mide en términos de consecuencias y probabilidades.
- 1.3.31 Transferir riesgos: cambiar la responsabilidad o carga por las pérdidas a una tercera parte mediante legislación, contrato, seguros u otros medios. Transferir riesgos también se puede referir a cambiar un riesgo físico, o parte el mismo a otro sitio.
- 1.3.32 Tratamiento de riesgos: selección e implementación de opciones apropiadas para tratar el riesgo.

# 2 Requerimientos de administración de riesgos

## 2.1 Propósito

El propósito de esta Sección es describir un proceso formal para establecer un programa sistemático de administración de riesgos.

Se necesita el desarrollo de una política organizacional de administración de riesgos y un mecanismo de soporte con objeto de proveer una estructura para llevar a cabo un programa de administración de riesgos más detallado a nivel sub-organizacional o de proyecto.

## 2.2 Política de administración de riesgos

El ejecutivo de la organización debe definir y documentar su política para administración de riesgos, incluyendo objetivos para, y su compromiso con, la administración de riesgos. La política de administración de riesgos debe ser relevante para el contexto estratégico de la organización y para sus metas, objetivos y la naturaleza de su negocio. La gerencia asegurará que esta política es comprendida, implementada y mantenida en todos los niveles de la organización.

## 2.3 Planeamiento y recursos

### 2.3.1 Compromiso gerencial

La organización debería asegurar que:

- a) se ha establecido, implementado y mantenido un sistema de administración de riesgos, de acuerdo con este Estándar; y
- b) se reporta el desempeño del sistema de administración de riesgos a la gerencia de la organización para revisión y como base para su mejora.

### 2.3.2 Responsabilidad y autoridad

Deberá definirse y documentarse la responsabilidad, autoridad e interrelaciones del personal que realiza y verifica el trabajo que afecta la administración de riesgos, particularmente para la gente que necesita la libertad y autoridad organizacional para realizar una o más de las siguientes acciones:

- a) iniciar acciones para prevenir o reducir los efectos adversos de los riesgos;
- b) controlar el tratamiento posterior de los riesgos hasta que el nivel de riesgo se haga aceptable;
- c) identificar y registrar cualquier problema relativo a la administración de riesgos;
- d) iniciar, recomendar o proveer soluciones a través de los canales asignados;
- e) verificar la implementación de soluciones; y
- f) comunicar y consultar interna y externamente según corresponda.

### 2.3.3 Recursos

La organización debe identificar los requerimientos de recursos y proveer recursos adecuados, incluyendo la asignación de personal entrenado para las actividades de administración, desempeño del trabajo, y verificación incluyendo la revisión interna.

## 2.4 Programa de implementación

Se requiere seguir una cantidad de pasos para implementar un sistema efectivo de administración de riesgos dentro de una organización. En el Apéndice B se proveen ejemplos. Dependiendo de la filosofía, cultura y estructura general de administración de riesgos de la organización, debería ser posible combinar u omitir ciertos pasos. Sin embargo, deberían considerarse todos los pasos.

## 2.5 Revisión gerencial

El ejecutivo de la organización 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 para satisfacer los requerimientos de este Estándar, y las políticas y objetivos de administración de riesgos establecidos en la organización (ver Cláusula 2.2). Deberá llevarse un registro de tales revisiones.

# 3 Vista general de la administración de riesgos

## 3.1 General

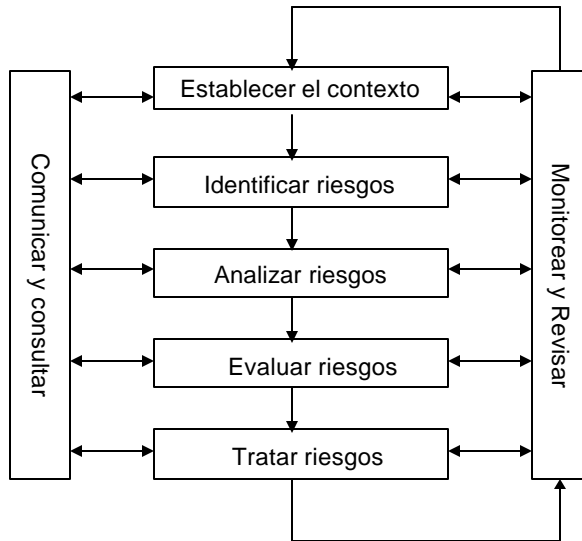
La administración de riesgos es una parte integral del proceso de administración. La administración de riesgos es un proceso multifacético, aspectos apropiados del cual son a menudo llevados a cabo mejor por un equipo multidisciplinario. Es un proceso iterativo de mejora continua.

## 3.2 Elementos principales

Los elementos principales del proceso de administración de riesgos, como se muestra en la figura Figura 3.1, son los siguientes:

- a) Establecer el contexto  
Establecer el contexto estratégico, organizacional y de administración de riesgos en el cual tendrá lugar el resto del proceso. Deberían establecerse criterios contra los cuales se evaluarán los riesgos y definirse la estructura del análisis.
- b) Identificar riesgos  
Identificar qué, por qué y cómo pueden surgir las cosas como base para análisis posterior.
- c) Analizar riesgos  
Determinar los controles existentes y analizar riesgos en términos de consecuencias y probabilidades en el contexto de esos controles. El análisis debería considerar el rango de consecuencias potenciales y cuán probable es que ocurran esas consecuencias. Consecuencias y probabilidades pueden ser combinadas para producir un nivel estimado de riesgo.
- d) Evaluar riesgos  
Comparar niveles estimados de riesgos contra los criterios preestablecidos.  
Esto posibilita que los riesgos sean ordenados como para identificar las prioridades de administración. Si los niveles de riesgo establecidos son bajos, los riesgos podrían caer en una categoría aceptable y no se requeriría un tratamiento.
- e) Tratar riesgos  
Aceptar y monitorear los riesgos de baja prioridad. Para otros riesgos, desarrollar e implementar un plan de administración específico que incluya consideraciones de fondeo.
- f) Monitorear y revisar  
Monitorear y revisar el desempeño del sistema de administración de riesgos y los cambios que podrían afectarlo.
- g) Comunicar y consultar  
Comunicar y consultar con interesados internos y externos según corresponda en cada etapa del proceso de administración de riesgos y concerniendo al proceso como un todo.  
La administración de riesgos se puede aplicar en una organización a muchos niveles. Se lo puede aplicar a nivel estratégico y a niveles operativos. Se lo puede aplicar a proyectos específicos, para asistir con decisiones específicas o para administrar áreas específicas reconocidas de riesgo.  
La administración de riesgos es un proceso iterativo que puede contribuir a la mejora organizacional. Con cada ciclo, los criterios de riesgos se pueden fortalecer para alcanzar progresivamente mejores niveles de administración de riesgos.  
Para cada etapa del proceso deberían llevarse registros adecuados, suficientes como para satisfacer a una auditoría independiente.





### 3.1 Vista General de la Administración de Riesgos

# 4 Proceso de administración de riesgos

## 4.1 Establecer el contexto

### 4.1.1 General

En la Figura 4.1 se muestran los detalles del proceso de administración de riesgos. El proceso ocurre dentro de la estructura del contexto estratégico, organizacional y de administración de riesgos de una organización. Esto necesita ser establecido para definir los parámetros básicos dentro de los cuales deben administrarse los riesgos y para proveer una guía para las decisiones dentro de estudios de administración de riesgos más detallados. Esto establece el alcance para el resto del proceso de administración de riesgos.

### 4.1.2 Establecer el contexto estratégico

Definir la relación entre la organización y su entorno, identificando las fortalezas, debilidades, oportunidades y amenazas de la organización. El contexto incluye los aspectos financieros, operativos, competitivos, políticos (percepciones públicas / imagen), sociales, de clientes, culturales y legales de las funciones de la organización.

Identificar los interesados internos y externos, y considerar sus objetivos, tomar en cuenta sus percepciones, y establecer políticas de comunicación con estas partes.

**nota:** El apéndice C establece una lista de interesados potenciales. Este paso está focalizado en el entorno en el cual opera la organización. La organización debería buscar determinar los elementos cruciales que podrían sustentar o dificultar su habilidad para administrar los riesgos que enfrenta. Puede llevarse a cabo un análisis estratégico. El mismo debería ser endosado al nivel ejecutivo, para que establezca los parámetros básicos y provea una guía en los procesos más detallados de administración de riesgos. Debería existir una estrecha relación entre la misión u objetivos estratégicos de una organización y la administración de todos los riesgos a los cuales está expuesta.

### 4.1.3 Establecer el contexto organizacional

Antes de comenzar un estudio de administración de riesgos, es necesario comprender la organización y sus capacidades, así como sus metas y objetivos y las estrategias que están vigentes para lograrlos.

Esto es importante por las siguientes razones:

- a) La administración de riesgos tiene lugar en el contexto de las amplias metas, objetivos y estrategias de la organización;
- b) La falla en lograr los objetivos de la organización, o de una actividad específica, o proyecto en consideración, es un conjunto de riesgos que debería ser administrado;
- c) La política y metas de la organización ayudan a definir los criterios mediante los cuales se decide si un riesgo es aceptable o no, y constituye la base para las opciones de tratamientos.

### 4.1.4 Establecer el contexto de administración de riesgos

Deberían establecerse las metas, objetivos, estrategias, alcance y parámetros de la actividad, o parte de la organización a la cual se está aplicando el proceso de administración de riesgos. El proceso debería ser llevado a cabo con plena consideración de la necesidad de balancear costos, beneficios y oportunidades.

También deberían especificarse los recursos requeridos y los registros que se van a llevar. Establecer el alcance y los límites de una aplicación del proceso de administración de riesgos involucra:

- a) Definir el proyecto o actividad y establecer sus metas y objetivos;
- b) Definir la extensión del proyecto en tiempo y ubicación;
- c) Identificar cualquier estudio necesario y su alcance, objetivos y recursos requeridos. Pueden proveer una guía para esto las fuentes genéricas de riesgo y las áreas de impacto.  
**nota:** Para obtener ejemplos de fuentes genéricas de riesgo y sus áreas de impacto consultar el Apéndice D.
- d) Definir el alcance y amplitud de las actividades de administración de riesgos a llevar a cabo.

Los aspectos específicos que también podrían ser discutidos incluyen lo siguiente:

- i. Los roles y responsabilidades de las distintas partes de la organización que participan en la administración de riesgos;
- ii. Las relaciones entre el proyecto y otros proyectos o partes de la organización.

#### 4.1.5 Desarrollar criterios de evaluación de riesgos

Decidir los criterios contra los cuales se va a evaluar el riesgo. Las decisiones concernientes a aceptabilidad de riesgos y tratamiento de riesgos pueden basarse en criterios operativos, técnicos, financieros, legales, sociales, humanitarios u otros. Esto a menudo depende de las políticas, metas y objetivos internos de la organización y de los intereses de las demás partes interesadas.

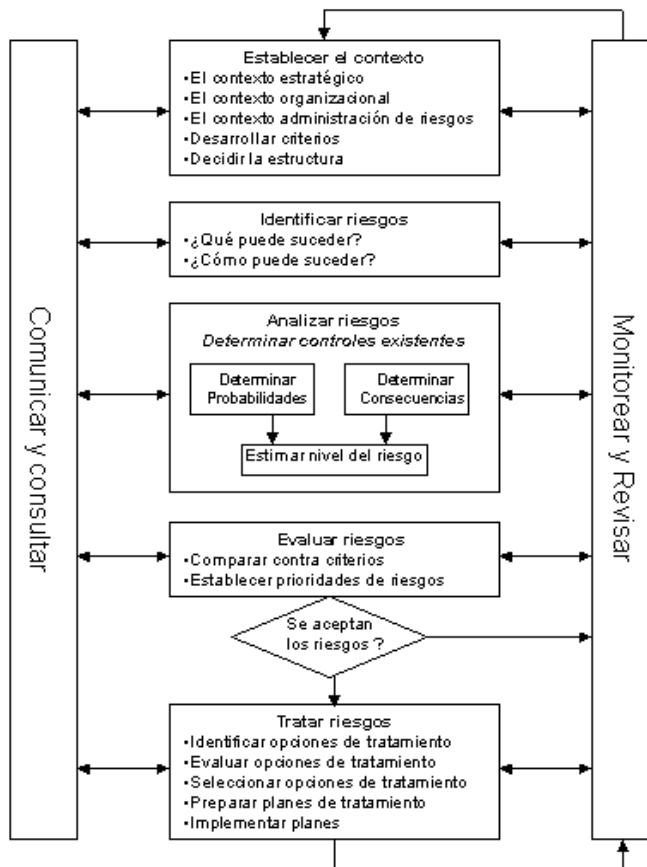
Los criterios pueden estar afectados por percepciones internas y externas y por requerimientos legales. Es importante que los criterios apropiados sean determinados al comienzo.

Aunque los criterios de riesgo son inicialmente desarrollados como parte del establecimiento del contexto de administración de riesgos, los mismos pueden ser posteriormente desarrollados y refinados a medida que se identifican riesgos particulares y se seleccionan técnicas de análisis de riesgos, ej: los criterios de riesgo deben corresponder al tipo de riesgos y a la forma en que se expresan los niveles de riesgo.

#### 4.1.6 Definir la estructura

Esto involucra separar la actividad o proyecto en un conjunto de elementos.

Estos elementos proveen una estructura lógica para identificación y análisis lo cual ayuda a asegurar que no se pasen por alto riesgos significativos. La estructura seleccionada depende de la naturaleza de los riesgos y del alcance del proyecto o actividad.



#### 4.1 Proceso de Administración de Riesgos

### 4.2 Identificación de riesgos

#### 4.2.1 General

Este paso busca identificar los riesgos a administrar. Es crítica una identificación amplia utilizando un proceso sistemático bien estructurado, porque los riesgos potenciales que no se identifican en esta etapa son excluidos de un análisis posterior. La identificación debería incluir todos los riesgos, estén o no bajo control de la organización.

#### 4.2.2 Qué puede suceder

La intención es generar una lista amplia de eventos que podrían afectar a cada elemento de la estructura referida en la Cláusula 4.1.6. Estos son luego considerados en mayor detalle para identificar lo que puede suceder.

**nota:** El apéndice D provee información sobre las fuentes genéricas de riesgo y sus áreas de impacto.

#### 4.2.3 Cómo y por qué pueden suceder

Habiendo identificado una lista de eventos, es necesario considerar causas y escenarios posibles. Hay muchas formas en que se puede iniciar un evento. Es importante que no se omitan las causas significativas.

#### 4.2.4 Herramientas y técnicas

Los enfoques utilizados para identificar riesgos incluyen “*checklists*”, juicios basados en la experiencia y en los registros, diagramas de flujo, “*brainstorming*”, análisis de sistemas, análisis de escenarios y técnicas de ingeniería de sistemas.

El enfoque utilizado dependerá de la naturaleza de las actividades bajo revisión y los tipos de riesgos.

### 4.3 Análisis de riesgos

#### 4.3.1 General

Los objetivos de análisis son separar los riesgos menores aceptables de los riesgos mayores, y proveer datos para asistir en la evaluación y tratamiento de los riesgos. El análisis de riesgos involucra prestar consideración a las fuentes de riesgos, sus consecuencias y las probabilidades de que puedan ocurrir esas consecuencias. Pueden identificarse los factores que afectan a las consecuencias y probabilidades. Se analiza el riesgo combinando estimaciones de consecuencias y probabilidades en el contexto de las medidas de control existentes.

Se puede llevar a cabo un análisis preliminar para excluir del estudio detallado los riesgos similares o de bajo impacto. De ser posible los riesgos excluidos deberían listarse para demostrar que se realizó un análisis de riesgos completo.

#### 4.3.2 Determinar los controles existentes

Identificar la administración, sistemas técnicos y procedimientos existentes para controlar los riesgos y evaluar sus fortalezas y debilidades. Pueden ser apropiadas las herramientas utilizadas en 4.2.4, como asimismo los enfoques tales como inspecciones y técnicas de auto-evaluación de controles (‘CSA’).

#### 4.3.3 Consecuencias y probabilidades

La magnitud de las consecuencias de un evento, si el mismo ocurriera, y la probabilidad del evento y sus consecuencias asociadas, se evalúan en el contexto de los controles existentes. Las consecuencias y probabilidades se combinan para producir un nivel de riesgo. Se pueden determinar las consecuencias y probabilidades utilizando análisis y cálculos estadísticos. Alternativamente cuando no se dispone de datos anteriores, se pueden realizar estimaciones subjetivas que reflejan el grado de convicción de un individuo o grupo de que podrá ocurrir un evento o resultado particular.

Para evitar prejuicios subjetivos cuando se analizan consecuencias y probabilidades, deberían utilizarse las mejores técnicas y fuentes de información disponibles.

Se pueden incluir las siguientes fuentes de información:

- a) Registros anteriores;
- b) Experiencia relevante;
- c) Prácticas y experiencia de la industria;
- d) Literatura relevante publicada;
- e) Comprobaciones de *marketing* e investigaciones de mercado;
- f) Experimentos y prototipos;
- g) Modelos económicos, de ingeniería u otros;
- h) Opiniones y juicios de especialistas y expertos.

Las técnicas incluyen:

- i) entrevistas estructuradas con expertos en el área de interés;
- ii) utilización de grupos multidisciplinarios de expertos;
- iii) evaluaciones individuales utilizando cuestionarios;
- iv) uso de modelos de computador u otros; y
- v) uso de árboles de fallas y árboles de eventos.

Siempre que sea posible, debería incluirse el nivel de confianza asignado a las estimaciones de los niveles de riesgo.

#### 4.3.4 Tipos de análisis

El análisis de riesgos pueden ser llevado con distintos grados de refinamiento dependiendo de la información de riesgos y datos disponibles. Dependiendo de las circunstancias, el análisis puede ser cualitativo, semi-cuantitativo o cuantitativo o una combinación de estos. El orden de complejidad y costos de estos análisis en orden ascendente, es cualitativo, semi-cuantitativo y cuantitativo. En la práctica, a menudo se utiliza primero el análisis cualitativo para obtener una indicación general del nivel de riesgo. Luego puede ser necesario llevar a cabo un análisis cuantitativo más específico. El detalle de los tipos de análisis es el siguiente:

##### a) Análisis cualitativo

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. Estas escalas se pueden modificar o ajustar para adaptarlas a las circunstancias, y se pueden utilizar distintas descripciones para riesgos diferentes.

**nota:** Las tablas E1 y E2 del Apéndice E muestran ejemplos de escalas simples cualitativas o descriptivas para probabilidades y consecuencias. La tabla E3 es un ejemplo de una matriz en la cual los riesgos están asignados a clases de prioridad mediante la combinación de su probabilidad y consecuencia. Se necesita adaptar estas tablas para satisfacer las necesidades de una organización individual o la materia particular de evaluación de riesgos.

El análisis cualitativo se utiliza:

- i. como una actividad inicial de tamiz, para identificar los riesgos que requieren un análisis más detallado;
- ii. cuando el nivel de riesgo no justifica el tiempo y esfuerzo requerido para un análisis más completo; o
- iii. cuando los datos numéricos son inadecuados para un análisis cuantitativo.

##### b) Análisis semi-cuantitativo

En el análisis semi-cuantitativo, a las escalas cualitativas, tales como las descritas arriba, se les asignan valores. El número asignado a cada descripción no tiene que guardar una relación precisa con la magnitud real de las consecuencias o probabilidades. Los números pueden ser combinados en cualquier rango de fórmula dado que el sistema utilizado para priorizar confronta el sistema seleccionado para asignar números y combinarlos. El objetivo es producir un ordenamiento de prioridades más detallado que el que se logra normalmente en el análisis cualitativo, y no sugerir valores realistas para los riesgos tales como los que se procuran en el análisis cuantitativo.

Se debe tener cuidado con el uso del análisis semi-cuantitativo porque los números seleccionados podrían no reflejar apropiadamente las relatividades, lo que podría conducir a resultados inconsistentes. El análisis semi-cuantitativo puede no diferenciar apropiadamente entre distintos riesgos, particularmente cuando las consecuencias o las probabilidades son extremas.

A veces es apropiado considerar la probabilidad compuesta de dos elementos, a los que se refiere generalmente como frecuencia de la exposición y probabilidad.

Frecuencia de la exposición es la extensión a la cual una fuente de riesgo existe, y probabilidad es la chance de que, cuando existe esa fuente de riesgo, le seguirán las consecuencias. Deberá ejercerse precaución en las situaciones en que las relaciones entre los dos elementos no es completamente independiente, ej. Cuando hay una fuerte relación entre frecuencia de la exposición y la probabilidad.

Este enfoque se puede aplicar en el análisis semi-cuantitativo y cuantitativo.

#### c) Análisis cuantitativo

El análisis cuantitativo utiliza valores numéricos para las consecuencias y probabilidades (en lugar de las escalas descriptivas utilizadas en los análisis cualitativos y semi-cuantitativos) utilizando datos de distintas fuentes (tales como las mencionadas en los sub-párrafos (a) a (h) de la Cláusula 4.3.3). La calidad del análisis depende de la precisión e integridad de los valores numéricos utilizados.

Las consecuencias pueden ser estimadas modelando los resultados de un evento o conjunto de eventos, o extrapolarlo a partir de estudios experimentales o datos del pasado. Las consecuencias pueden ser expresadas en términos de criterios monetarios, técnicos o humanos, o cualquier otro criterio referido en la Cláusula 4.1.5. En algunos casos se requiere más de un valor numérico para especificar las consecuencias para distintos momentos, lugares, grupos o situaciones.

La probabilidad es expresada generalmente como una probabilidad, una frecuencia, o una combinación de exposición y probabilidad.

La forma en que se expresan las probabilidades y las consecuencias y las formas en que las mismas son combinadas para proveer un nivel de riesgo variarán de acuerdo con el tipo de riesgo y el contexto en el cual se va a utilizar el nivel de riesgo.

**nota:** En el Apéndice F se brindan algunos ejemplos de expresiones de riesgo cuantitativo.

#### 4.3.5 Análisis de sensibilidad

Dado que algunas de las estimaciones realizadas en el análisis cuantitativo son imprecisas, deberá llevarse a cabo un análisis de sensibilidad para comprobar el efecto de los cambios en los supuestos y en los datos.

## 4.4 Evaluación de riesgos

La evaluación de riesgos involucra comparar el nivel de riesgo detectado durante el proceso de análisis con criterios de riesgo establecidos previamente.

El análisis de riesgo y los criterios contra los cuales se comparan los riesgos en la evaluación de riesgos deberían considerarse sobre la misma base. En consecuencia, la evaluación cualitativa involucra la comparación de un nivel cualitativo de riesgo contra criterios cualitativos, y la evaluación cuantitativa involucra la comparación de un nivel numérico de riesgo contra criterios que pueden ser expresados como un número específico, tal como, un valor de fatalidad, frecuencia o monetario.

El producto de una evaluación de riesgo es una lista de riesgos con prioridades para una acción posterior.

Deberían considerarse los objetivos de la organización y el grado de oportunidad que podrían resultar de tomar el riesgo.

Las decisiones deben tener en cuenta el amplio contexto del riesgo e incluir consideración de la tolerabilidad de los riesgos sostenidos por las partes fuera de la organización que se benefician de ellos.

Si los riesgos resultantes caen dentro de las categorías de riesgos bajos o aceptables, pueden ser aceptados con un tratamiento futuro mínimo. Los riesgos bajos y aceptados deberían ser monitoreados y revisados periódicamente para asegurar que se mantienen aceptables.

Si los riesgos no caen dentro de la categoría de riesgos bajos o aceptables, deberían ser tratados utilizando una o más de las opciones consideradas en la Cláusula 4.5.

## 4.5 Tratamiento de los riesgos

El tratamiento de los riesgos involucra identificar el rango de opciones para tratar los riesgos, evaluar esas opciones, preparar planes para tratamiento de los riesgos e implementarlos.

### 4.5.1 Identificar opciones para tratamiento de los riesgos

La Figura 4.2 ilustra el proceso de tratamiento de los riesgos. Las opciones, que no son necesariamente mutuamente exclusivas y apropiadas en todas las circunstancias, incluyen lo siguiente:

- a) Evitar el riesgo decidiendo no proceder con la actividad que probablemente generaría el riesgo (cuando esto es practicable).

Evitar riesgos puede ocurrir inadecuadamente por una actitud de aversión al riesgo, que es una tendencia en mucha gente (a menudo influenciada por el sistema interno de una organización). Evitar inadecuadamente algunos riesgos puede aumentar la significación de otros.

La aversión a riesgos tiene como resultado:

- i) decisiones de evitar o ignorar riesgos independientemente de la información disponible y de los costos incurridos en el tratamiento de esos riesgos.
- ii) fallas en tratar los riesgos;
- iii) dejar las opciones críticas y/o decisiones en otras partes;
- iv) diferir las decisiones que la organización no puede evitar; o
- v) seleccionar una opción porque representa un riesgo potencial más bajo independientemente de los beneficios.

- b) Reducir la probabilidad de la ocurrencia

**nota:** Se muestran ejemplos en el Apéndice G.

- c) Reducir las consecuencias

**nota:** Se muestran ejemplos en el Apéndice G.

- d) Transferir los riesgos

Esto involucra que otra parte soporte o comparta parte del riesgo. Los mecanismos incluyen el uso de contratos, arreglos de seguros y estructuras organizacionales tales como sociedades y "joint ventures".

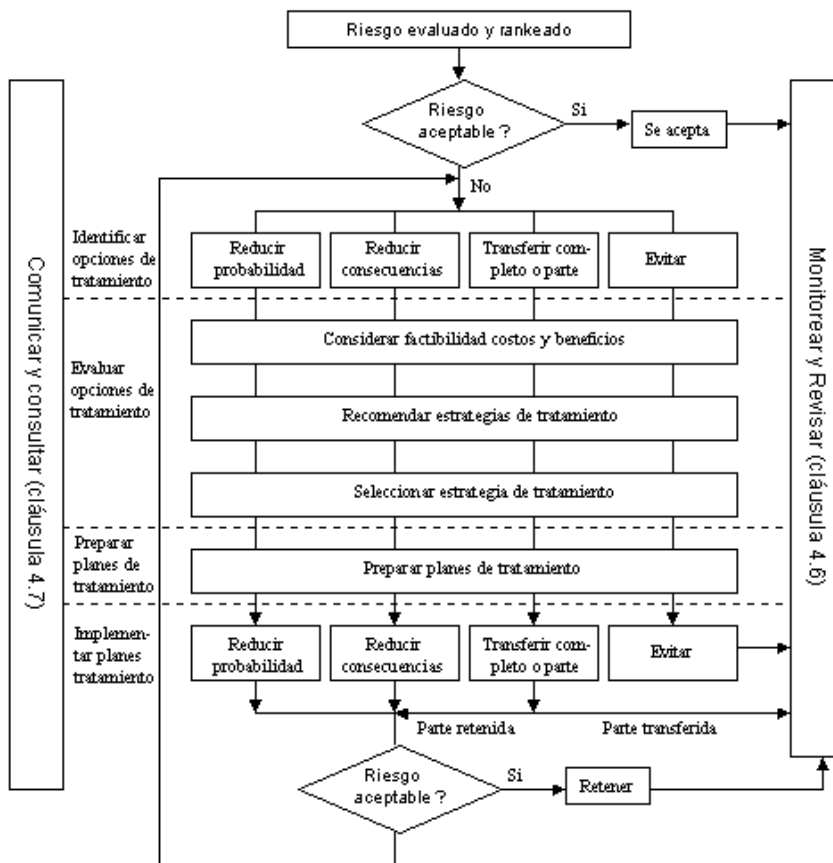
La transferencia de un riesgo a otras partes, o la transferencia física a otros lugares, reducirá el riesgo para la organización original, pero puede no disminuir el nivel general del riesgo para la sociedad.

Cuando los riesgos son total o parcialmente transferidos, la organización que transfiere los riesgos ha adquirido un nuevo riesgo, que la organización a la cual ha transferido el riesgo no pueda administrarlo efectivamente.

- e) Retener los riesgos

Luego de que los riesgos hayan sido reducidos o transferidos, podría haber riesgos residuales que sean retenidos. Deberían ponerse en práctica planes para administrar las consecuencias de esos riesgos si los mismos ocurrieran, incluyendo identificar medios de financiar dichos riesgos. Los riesgos también pueden ser retenidos en forma predeterminada, ej. cuando hay una falla para identificar y/o transferir apropiadamente o de otro modo tratar los riesgos.





#### 4.2 Proceso de Tratamiento de Riesgos

A la reducción de las consecuencias y probabilidades se las puede referir como control de riesgos. El control de riesgos involucra determinar el beneficio relativo de nuevos controles a la luz de la efectividad de los controles existentes. Los controles pueden involucrar políticas de efectividad, procedimientos o cambios físicos.

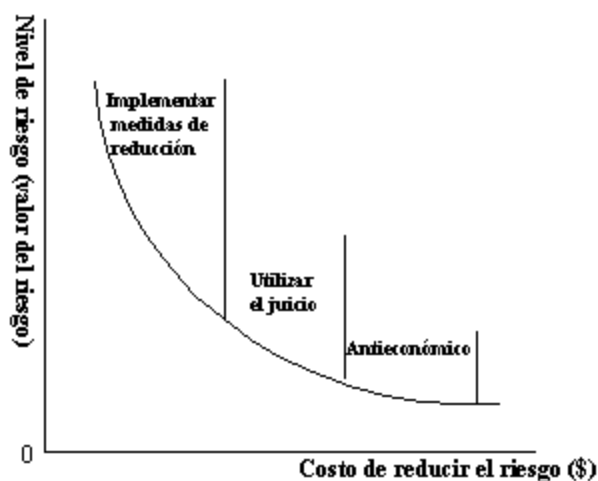
##### 4.5.2 Evaluar opciones de tratamiento de los riesgos

Las opciones deberían ser evaluadas sobre la base del alcance de la reducción del riesgo, y el alcance de cualquier beneficio u oportunidad adicional creadas, tomando en cuenta los criterios desarrollados en la Cláusula 4.1.5. Pueden considerarse y aplicarse una cantidad de opciones ya sea individualmente o combinadas.

La selección de la opción más apropiada involucra balancear el costo de implementar cada opción contra los beneficios derivados de la misma. En general, el costo de administrar los riesgos necesita ser conmensurada con los beneficios obtenidos.

Cuando se pueden obtener grandes reducciones en el riesgo con un gasto relativamente bajo, tales opciones deberían implementarse. Otras opciones de mejoras pueden ser no económicas y necesita ejercerse el juicio para establecer si son justificables. Esto se ilustra en la Figura 4.3.

Las decisiones deberían tener en cuenta la necesidad de considerar cuidadosamente los riesgos raros pero severos, que podrían justificar medidas de seguridad que no son justificables por fundamentos estrictamente económicos.



### 4.3 Costo de las Medidas de Reducción de Riesgos

En general el impacto adverso de los riesgos debería hacerse tan bajo como sea razonablemente practicable, independientemente de cualquier criterio absoluto.

Si el nivel de riesgo es alto, pero podrían resultar oportunidades considerables si se lo asume, tal como el uso de una nueva tecnología, entonces la aceptación del riesgo necesita estar basada en una evaluación de los costos de tratamiento y los costos de rectificar las consecuencias potenciales versus las oportunidades que podrían depararse de tomar el riesgo.

En muchos casos, es improbable que cualquier opción de tratamiento del riesgo sea una solución completa para un problema particular. A menudo la organización se beneficiará sustancialmente mediante una combinación de opciones tales como reducir la probabilidad de los riesgos, reducir sus consecuencias, y transferir o retener algunos riesgos residuales. Un ejemplo es el uso efectivo de contratos y la financiación de riesgos sustentados por un programa de reducción de riesgos.

Cuando el costo acumulado de implementación de todos los tratamientos de riesgos excede el presupuesto disponible, el plan debería identificar claramente el orden de prioridad bajo el cual deberían implementarse los tratamientos individuales de los riesgos. El ordenamiento de prioridad puede establecerse utilizando distintas técnicas, incluyendo análisis de "ranking" de riesgos y de costo-beneficio. Los tratamientos de riesgos que no puedan ser implementados dentro de los límites del presupuesto disponible deben esperar la disponibilidad de recursos de financiamiento adicionales, o, si por cualquier razón todos o algunos de los tratamientos restantes son considerados importantes, debe plantearse el problema para conseguir el financiamiento adicional.

Las opciones de tratamiento de los riesgos deberían considerar cómo es percibido el riesgo por las partes afectadas y las formas más apropiadas de comunicárselo a dichas partes.

#### 4.5.3 Preparar planes de tratamiento

Los planes deberían documentar cómo deben ser implementadas las opciones seleccionadas.

El plan de tratamiento debería identificar las responsabilidades, el programa, los resultados esperados de los tratamientos, el presupuesto, las medidas de desempeño y el proceso de revisión a establecer.

**nota:** Para mayores detalles consultar Parte H5, Apéndice H.

El plan también debería incluir un mecanismo para evaluar la implementación de las opciones contra criterios de desempeño, las responsabilidades individuales y otros objetivos, y para monitorear los mojonos críticos de implementación.

Figura 4.3 Costo de las medidas de reducción de riesgos.

#### 4.5.4 Implementar planes de tratamiento

Idealmente, la responsabilidad por el tratamiento del riesgo debería ser llevada a cabo por aquellos con mejor posibilidad de controlar el riesgo. Las responsabilidades deberían ser acordadas entre las partes en el momento más temprano posible.

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.

Si luego del tratamiento hay un riesgo residual, debería tomarse la decisión de si retener este riesgo o repetir el proceso de tratamiento.

## 4.6 Monitoreo y revisión

Es necesario monitorear los riesgos, la efectividad del plan de tratamiento de los riesgos, las estrategias y el sistema de administración que se establece para controlar la implementación. 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.

Es esencial una revisión sobre la marcha para asegurar que el plan de administración se mantiene relevante. Pueden cambiar los factores que podrían afectar las probabilidades y consecuencias de un resultado, como también los factores que afectan la conveniencia o costos de las distintas opciones de tratamiento. En consecuencia, es necesario repetir regularmente el ciclo de administración de riesgos. La revisión es una parte integral del plan de tratamiento de la administración de riesgos.

## 4.7 Comunicación y consulta

La comunicación y consulta son una consideración importante en cada paso del proceso de administración de riesgos. Es importante desarrollar un plan de comunicación para los interesados internos y externos en la etapa más temprana del proceso. Este plan debería encarar aspectos relativos al riesgo en sí mismo y al proceso para administrarlo.

La comunicación y consulta involucra un diálogo en ambas direcciones entre los interesados, con el esfuerzo focalizado en la consulta más que un flujo de información en un sólo sentido del tomador de decisión hacia los interesados.

Es importante la comunicación efectiva interna y externa para asegurar que aquellos responsables por implementar la administración de riesgos, y aquellos con intereses creados comprenden la base sobre la cual se toman las decisiones y por qué se requieren ciertas acciones en particular.

Las percepciones de los riesgos pueden variar debido a diferencias en los supuestos, conceptos, las necesidades, aspectos y preocupaciones de los interesados, según se relacionen con el riesgo o los aspectos bajo discusión. Los interesados probablemente harán juicios de aceptabilidad de los riesgos basados en su percepción de los mismos.

Dado que los interesados pueden tener un impacto significativo en las decisiones tomadas, es importante que sus percepciones de los riesgos, así como, sus percepciones de los beneficios, sean identificadas y documentadas y las razones subyacentes para las mismas comprendidas y tenidas en cuenta.

# 5 Documentación

## 5.1 General

Debería documentarse cada etapa del proceso de administración de riesgos.  
La documentación debería incluir los supuestos, los métodos, las fuentes de datos y los resultados.

## 5.2 Razones para la documentación

Las razones para la documentación son las siguientes:

- 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 auditoría; y
- h) compartir y comunicar información.

Las decisiones concernientes al alcance de la documentación pueden involucrar costos y beneficios y deberían tomar en consideración los factores mencionados arriba.

Guía: Para asistir y dar alguna guía acerca de la documentación apropiada, se proveen ejemplos en el Apéndice H. Estos ejemplos son indicativos más que comprensivos.

# A Aplicaciones de la administración de riesgos

## A1 Organizaciones

Este Estándar puede aplicarse a un rango muy amplio de organizaciones incluyendo:

- a) públicas:
  - nacionales, regionales, locales;
- b) comerciales:
  - compañías, "joint ventures", firmas, franquicias, prácticas exclusivas; y
- c) voluntarias:
  - de caridad, sociales, deportivas.

## A2 Aplicaciones

El Estándar tiene un amplio rango de aplicaciones incluyendo, pero no circunscrito a:

- i) administración de activos y planeamiento de recursos;
- ii) interrupción del negocio;
- iii) cambios: organizacionales, tecnológicos y políticos;
- iv) actividad de construcción;
- v) planeamiento de contingencia, para desastres y emergencias;
- vi) responsabilidades de diseño y producto;
- vii) responsabilidades de directores y funcionarios;
- viii) procedimientos, entrenamiento, discriminación y acoso en empleos;
- ix) aspectos ambientales;
- x) aspectos éticos y de probidad;
- xi) estudios de factibilidad;
- xii) detección de incendios / prevención de incendios;
- xiii) operaciones de cambio monetario;
- xiv) prevención, detección y administración de fraudes;
- xv) sanidad humana, animal y vegetal;
- xvi) sistemas de información / redes de computación;
- xvii) inversiones;
- xviii) cumplimiento legislativo;
- xix) salud y seguridad ocupacional;
- xx) sistemas de operaciones y mantenimiento;
- xxi) administración de proyectos;
- xxii) riesgo público y responsabilidad general;
- xxiii) administración de contratos de compra;
- xxiv) asesoramiento profesional;
- xxv) aspectos de reputación e imagen;
- xxvi) seguridad;
- xxvii) transporte incluyendo aire, mar, carretera, ferrocarril; y
- xxviii) tesorería y finanzas.

# B Pasos en el desarrollo e implementación de un programa de administración de riesgos

## Paso 1: Respaldo de la alta gerencia

Desarrollar una filosofía de administración de riesgos organizacional y toma de conciencia sobre 'riesgos' a nivel de la alta gerencia. Esto podría ser facilitado mediante entrenamiento, educación y síntesis a la gerencia ejecutiva.

- Es necesario el apoyo permanentemente activo del Presidente (*CEO*) de la organización.
- Se necesita que patrocine la iniciativa un gerente ejecutivo principal o un "campeón" similar (o un grupo).
- Todos los ejecutivos principales deben dar pleno apoyo.

## Paso 2: Desarrollar la política organizacional

Desarrollar y documentar una política y estructura corporativa para administrar los riesgos, a ser endosada por el ejecutivo de la organización e implementada en toda la organización. La política debe incluir información tal como:

- los objetivos de la política y explicación para administrar los riesgos;
- los vínculos entre la política y el plan estratégico / corporativo de la organización;
- el alcance, o el rango de aspectos a los cuales se aplica la política;
- guía de lo que puede ser considerado como riesgo aceptable;
- quién es responsable por administrar riesgos;
- el apoyo / capacidad disponibles para asistir a los responsables de administrar riesgos;
- el nivel de documentación requerido; y
- el plan para revisar el desempeño organizacional en relación con la política.

## Paso 3: Comunicar la política

Desarrollar, establecer e implementar una infraestructura o medidas para asegurar que la administración de riesgos se convierte en una parte integral de los procesos de planeamiento y administración y de la cultura general de la organización. Esto puede incluir:

- establecer un equipo que comprenda personal de alta gerencia para ser responsable por las comunicaciones internas acerca de la política;
- procurar la toma de conciencia acerca de la administración de riesgos;
- comunicación / diálogo en toda la organización acerca de administración de riesgos y la política de la organización;
- adquirir pericia en administración de riesgos, ej: consultores, y desarrollar destrezas en el personal a través de la educación y capacitación;
- asegurar niveles apropiados de reconocimiento, recompensas y sanciones; y
- establecer procesos de administración de desempeño.

## Paso 4: Administrar riesgos a nivel organizacional

Desarrollar y establecer un programa para administrar riesgos a nivel organizacional a través de la aplicación del sistema de administración de riesgos descrito en la Sección 2. El proceso de

administración de riesgos debería estar integrado con los procesos de planeamiento estratégico y administración de la organización. Esto involucrará documentar:

- el contexto de la organización y de la administración de riesgos;
- los riesgos identificados para la organización;
- el análisis y evaluación de estos riesgos;
- las estrategias de tratamiento;
- los mecanismos para revisar el programa; y
- las estrategias para procurar la toma de conciencia, la adquisición de pericia, la capacitación y la educación.

## Paso 5: Administrar riesgos a nivel de programa, proyecto y equipo

Desarrollar y establecer un programa para administrar los riesgos para cada área sub-organizacional, programa, proyecto o actividad de equipo a través de la aplicación del proceso de administración de riesgos descrito en la Sección 4. El proceso para administrar riesgos debería estar integrado con otras actividades de planeamiento y administración. Debería documentarse el proceso seguido, las decisiones tomadas y las acciones planeadas.

## Paso 6: Monitorear y revisar

Desarrollar y aplicar mecanismos para asegurar revisiones de los riesgos sobre la marcha. Esto asegurará que la implementación y la política de administración de riesgos se mantenga relevante, dado que las circunstancias cambian todo el tiempo y se hace vital la revisión de las decisiones anteriores. Los riesgos no son estáticos. También debería monitorearse y revisarse la efectividad del proceso de administración de riesgos.

# C Interesados

Interesados son aquellos individuos que están, o perciben estar, afectados por una decisión o actividad. Ellos pueden incluir:

- individuos dentro de la organización, tales como los empleados, la gerencia, la alta gerencia, y voluntarios;
- tomadores de decisiones;
- contrapartes de negocios o comerciales;
- grupos de empleados;
- grupos sindicales;
- instituciones financieras;
- organizaciones de seguros;
- reguladores y otras organizaciones gubernamentales que tienen autoridad sobre las actividades;
- políticos (a todos los niveles del gobierno) que pudieran tener un interés electoral o de cartera;
- organizaciones no-gubernamentales tales como grupos ambientales y grupos de interés público;
- clientes;
- proveedores, proveedores de servicios y contratistas para la actividad;
- los medios, que son interesados potenciales, como también, conductos de información a otros interesados;
- individuos o grupos que están interesados en aspectos relacionados con la propuesta;
- comunidades locales; y
- la sociedad como un todo.

La mezcla de interesados puede cambiar con el tiempo. Nuevos interesados pueden unirse y desear ser considerados, mientras que otros podrían quedar excluidos al no estar más involucrados en el proceso. Consecuentemente, el proceso de análisis de interesados debería ser continuo, y como tal, debería ser parte integrante del proceso de administración de riesgos.

El nivel de preocupación de los interesados puede cambiar en respuesta a nueva información, ya sea porque se han encarado las necesidades y preocupaciones de los interesados, o porque nueva información ha dado lugar a nuevas necesidades, aspectos o preocupaciones. Nótese también que distintos interesados podrían tener diferentes opiniones y diferentes niveles de conocimiento en relación a un aspecto en particular.



# D Fuentes genéricas de riesgo y sus áreas de impacto

## D1 General

La identificación de fuentes de riesgo y áreas de impacto provee una estructura para identificación y análisis de riesgos. A raíz de la gran cantidad potencial de fuentes e impactos, desarrollar una lista genérica focaliza las actividades de identificación de riesgos y contribuye a una administración más efectiva.

Las fuentes de riesgo y áreas de impacto genéricas son seleccionadas de acuerdo a su relevancia para la actividad bajo estudio (ver Cláusulas 4.1.4 y 4.2.2).

Los componentes de cada categoría genérica pueden formar la base para un estudio completo de riesgos.

## D2 Fuentes de riesgo

Cada fuente genérica tiene numerosos componentes, cualquier de los cuales pueden dar lugar a un riesgo. Algunos componentes estarán bajo control de la organización que realiza el estudio, mientras que otros estarán fuera de su control. Cuando se identifican los riesgos se necesita considerar a ambos tipos. Las fuentes genéricas de riesgo incluyen:

- a) Relaciones comerciales y legales  
Entre la organización y otras organizaciones, ej: proveedores, subcontratistas, arrendatarios.
- b) Circunstancias económicas  
De la organización, país, internacionales, como asimismo factores que contribuyen a esas circunstancias ej: tipos de cambio.
- c) Comportamiento humano  
Tanto de los involucrados en la organización como de los que no lo están.
- d) Eventos naturales
- e) Circunstancias políticas  
Incluyendo cambios legislativos y factores que pudieran influenciar a otras fuentes de riesgo.
- f) Aspectos tecnológicos y técnicos  
Tanto internos como externos a la organización.
- g) Actividades y controles gerenciales
- h) Actividades individuales

## D3 Áreas de impacto

El análisis de riesgo se puede concentrar en impactos en un área solamente o en varias áreas posibles de impacto.

Las áreas de impacto incluyen a las siguientes:

- a) Base de activos y recursos de la organización, incluyendo al personal.
- b) Ingresos y derechos
- c) Costos de las actividades, tanto directos como indirectos.
- d) Gente

- e) Comunidad
- f) Desempeño
- g) Cronograma y programa de actividades
- h) El ambiente
- i) Intangibles tales como la reputación, gestos de buena voluntad, calidad de vida.
- j) Comportamiento organizacional

## D4 Identificación de riesgos

Un método de resumir la forma en la cual surgen los riesgos en una organización es utilizando una plantilla de identificación de riesgos del tipo que se muestra en la Tabla D1. Las entradas pueden realizarse con marcas para mostrar donde ocurren los riesgos, o con notas descriptivas más detalladas.

## D5 Otras clasificaciones de riesgo

Distintas disciplinas a menudo categorizan las fuentes de riesgo de otra forma, utilizando términos tales como azares o exposiciones de riesgo. Estas clasificaciones pueden ser subconjuntos de las fuentes de riesgo listadas arriba en D2. Los siguientes son algunos ejemplos:

- a) Enfermedades  
ej: afectando a humanos, animales y plantas.
- b) Económicos  
ej: fluctuaciones en la moneda, tasas de interés, mercado accionario.
- c) Ambientales  
ej: ruidos, contaminación, polución.
- d) Financieros  
ej: riesgos contractuales, malversaciones de fondos, fraudes, multas.
- e) Humanos  
ej: motines, huelgas, sabotajes, errores.
- f) Desastres naturales  
ej: condiciones climáticas, terremotos, incendios de bosques, plagas, actividad volcánica.
- g) Salubridad y seguridad ocupacional  
ej: medidas de seguridad inadecuadas, administración de seguridad pobre.
- h) Responsabilidad por productos  
ej: errores de diseño, calidad bajo estándar, pruebas inadecuadas.
- i) Responsabilidad profesional  
ej: consejo equivocado, negligencia, error de diseño.
- j) Daños a la propiedad  
ej: fuego, inundaciones, terremotos, contaminación, error humano.
- k) Responsabilidad pública  
ej: acceso, egreso y seguridad públicas.
- l) Seguridad  
ej: desfalcos, vandalismo, robo, apropiación indebida de información, penetración ilegal.
- m) Tecnológicos  
ej: innovación, obsolescencia, explosiones y dependencia.

**Tabla D1 Ejemplo de plantilla de identificación de riesgos.**

<b>Fuentes de Riesgo</b>	<b>Áreas de Impacto</b>				
	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

# E Ejemplos de definición y clasificación de riesgos.

**Tabla E1 Medidas cualitativas de consecuencia o impacto.**

Nivel	Descriptor	Ejemplo de descripción detallada
1	Insignificante	Sin perjuicios, baja pérdida financiera
2	Menor	Tratamiento de primeros auxilios, liberado localmente se contuvo inmediatamente, pérdida financiera media
3	Moderado	Requiere tratamiento médico, liberado localmente contenido con asistencia externa, pérdida financiera alta
4	Mayor	Perjuicios extensivos, pérdida de capacidad de producción, liberación externa, sin efectos nocivos, pérdida financiera mayor
5	Catastrófico	Muerte, liberación tóxica externa con efectos nocivos, enorme pérdida financiera

Las medidas utilizadas deberían reflejar las necesidades y naturaleza de la organización y actividad bajo estudio

**Tabla E2 Medidas cualitativas de probabilidad.**

Nivel	Descriptor	Descripción
A	Casi certeza	Se espera que ocurra en la mayoría de las circunstancias
B	Probable	Probablemente ocurrirá en la mayoría de las circunstancias
C	Posible	Podría ocurrir en algún momento
D	Improbable	Pudo ocurrir en algún momento
E	Raro	Puede ocurrir sólo en circunstancias excepcionales

Estas tablas necesitan ser adaptadas para satisfacer las necesidades de una organización en particular

**Tabla E3 Matriz de análisis de riesgo cualitativo – nivel de riesgo.**

<b>Probabilidad</b>	<b>Consecuencias</b>				
	Insignificantes 1	Menores 2	Moderadas 3	Mayores 4	Catastróficas 5
A (casi certeza)	H	H	E	E	E
B (probable)	M	H	H	E	E
C (moderado)	L	M	H	E	E
D (improbable)	L	L	M	H	E
E (raro)	L	L	M	H	H

La cantidad de categorías deberían reflejar las necesidades del estudio.

**Leyenda**

- E: riesgo extremo; requiere acción inmediata
- H: riesgo alto; necesita atención de la alta gerencia
- M: riesgo moderado; debe especificarse responsabilidad gerencial
- L: riesgo bajo; administrar mediante procedimientos de rutina

# F Ejemplos de expresiones cuantitativas de riesgo

## F1 Riesgo de pérdida o ganancia financiera

La pérdida (o ganancia) financiera multiplicada por la frecuencia anual de la pérdida (o ganancia) da el valor esperado en dólares por año.

## F2 Riesgo de fatalidad

El riesgo de fatalidad de una actividad.

## F3 Desastres naturales o producidos por el hombre

Las consecuencias pueden ser modeladas utilizando simulaciones computarizadas y las probabilidades estimadas a partir de datos históricos, árboles de fallas u otras técnicas de ingeniería de sistemas.

## F4 Riesgos de salubridad

Los riesgos de salubridad se expresan normalmente en alguna de las siguientes formas:

- a) La cantidad de nuevos casos de enfermedad por año en una población expuesta comparado con el total de esa población, ej: 5 nuevos casos en una población expuesta de 100 000 es un riesgo de  $5 \times 10^{-5}$  por persona expuesta, por año. Cantidad de muertes por año en la población expuesta a la actividad.
- b) El coeficiente de probabilidad de muerte antes de cierta edad, con y sin exposición.
- c) La cantidad de fatalidades por edad 70 que se espera resulte de una exposición, dividida por la cantidad de gente expuesta.

Los riesgos de salubridad pueden derivarse de datos epidemiológicos (censos de población de fatalidad o enfermedad) o de datos experimentales basados en estudios sobre animales.

**nota:** En lugar de calcular el valor promedio de un riesgo, la distribución de valores posibles se puede calcular reemplazando los valores promedio de las variables, de las cuales depende el resultado, por las distribuciones apropiadas de valores.

# G Identificar opciones para tratamiento de riesgos

## G1 Acciones para reducir o controlar la probabilidad

Estos pueden incluir:

- i) programas de auditoria y cumplimiento;
- ii) condiciones contractuales;
- iii) revisiones formales de requerimientos, especificaciones, diseño, ingeniería y operaciones;
- iv) inspecciones y controles de procesos;
- v) administración de inversiones y cartera;
- vi) administración de proyectos
- vii) mantenimiento preventivo;
- viii) aseguramiento de calidad, administración y estándares;
- ix) investigación y desarrollo, desarrollo tecnológico;
- x) capacitación estructurada y otros programas;
- xi) supervisión;
- xii) comprobaciones;
- xiii) acuerdos organizacionales; y
- xiv) controles técnicos.

## G2 Procedimientos para reducir o controlar las consecuencias

Estos pueden incluir:

- i) planeamiento de contingencia;
- ii) arreglos contractuales;
- iii) condiciones contractuales;
- iv) características de diseño;
- v) planes de recupero de desastres;
- vi) barreras de ingeniería y estructurales;
- vii) planeamiento de control de fraudes;
- viii) minimizar la exposición a fuentes de riesgo;
- ix) planeamiento de cartera;
- x) política y controles de precios;
- xi) separación o reubicación de una actividad y recursos;
- xii) relaciones públicas; y
- xiii) pagos *ex gratia*.

# H Documentación de administración de riesgos

## H1 General

Para administrar correctamente el riesgo, se requiere una documentación apropiada. Esto puede necesitar ser suficiente para satisfacer a una auditoría independiente. Las decisiones concernientes al alcance de la documentación puede involucrar costos y beneficios y debería tomar en cuenta los factores listados en la Cláusula 5.2. La declaración de la política de administración de riesgos debería definir la documentación necesaria.

En cada etapa del proceso, la documentación debería incluir:

- a) objetivos;
- b) fuentes de información;
- c) supuestos; y
- d) decisiones.

El Apéndice H incluye un ejemplo de un registro de riesgo, y un programa de tratamiento y plan de acción. Los planes para las áreas de alto riesgo pueden necesitar ser más específicos y detallados.

## H2 Política

En el Apéndice B se dan ejemplos de la información que podría ser incluida en la declaración de política de una organización.

## H3 Declaración de cumplimiento y diligencia debida

En algunas circunstancias puede requerirse una declaración de cumplimiento y diligencia debida, de forma tal que los gerentes tomen conocimiento formal de su responsabilidad por el cumplimiento de las políticas y procedimientos de administración de riesgos.

## H4 Registro de riesgos \*

Por cada riesgo identificado el registro de riesgo comprende:

- a) fuente;
- b) naturaleza;
- c) controles existentes;
- d) consecuencias y probabilidad;
- e) puntaje inicial del riesgo; y
- f) vulnerabilidad a factores externos / internos.

Consultar como guía la proforma de muestra.

## H5 Programa de tratamiento de riesgos y plan de acción \*

Un tratamiento de riesgos y plan de acción documenta los controles gerenciales a adoptar y lista la siguiente información:



- a) Quién tiene responsabilidad por la implementación del plan;
- b) Qué recursos se van a utilizar;
- c) Asignación de presupuesto;
- d) Calendario de implementación;
- e) Detalles del mecanismo y frecuencia de la revisión de cumplimiento del plan de tratamiento.

## H6 Monitorear y auditar documentos

Los registros de monitoreo y auditoría deberían documentar:

- a) Detalles del mecanismo y frecuencia de la revisión de riesgos y del proceso de administración de riesgos como un todo;
- b) Los resultados de las auditorías y de otros procedimientos de monitoreo;
- c) Detalles de cómo son seguidas e implementadas las recomendaciones de las revisiones.

- Estos ejemplos son solo indicativos.

# Registro de Riesgos

Fecha de revisión de riesgo.....  
 Compilado por.....Fecha.....  
 Revisado por.....Fecha.....

Función/actividad.....

Ref	Riesgo: qué puede suceder y cómo puede suceder	Las consecuencias de suceder un evento		Aptitud de los controles existentes	Puntaje de consecuencia	Puntaje de probabilidad	Nivel del riesgo	Prioridad del riesgo
		Consecuencias	Probabilidad					

## Programa y plan de tratamiento de riesgos

Fecha de revisión de riesgo.....

Compilado por..... Fecha.....

Función/actividad.....

Revisado por..... Fecha.....

El riesgo en orden de prioridad del Registro de Riesgo	Opciones posibles de tratamiento	Opciones preferidas	Puntaje de Riesgo luego del tratamiento	Resultado del análisis de costo/beneficio A: acepta B: rechaza	Persona responsable por implementación de la opción	Calendario de implementación	Cómo será monitoreado este riesgo y las opciones de tratamiento

## Plan de acción de riesgos

Item	Ref
Riesgo	
<b>Resumen – Respuesta e impacto recomendado</b>	
<b>Plan de acción</b>	
1 Acciones propuestas	
2 Requerimientos de recursos	
3 Responsabilidades	
4 Programa de fechas	
5 Monitoreo e informes requeridos	
Compilador.....Fecha..... Revisor.....Fecha.....	