NORMA TÉCNICA COLOMBIANA

NTC 5254

2004-05-31

GESTIÓN DEL RIESGO

E: RISK MANAGEMENT

CORRESPONDENCIA:	esta norma es una adopción modificada (MOD), de la AS/NZ 4360:1999 Risk Management.
DESCRIPTORES:	gestión; riesgo; gestión del riesgo; probabilidad; posibilidad; contexto; implementación; identificar; analizar; evaluar; tratar.

I.C.S.: 03.100.01

Editada por el Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC)
Apartado 14237 Bogotá, D.C. - Tel. 6078888 - Fax 2221435

Editada 2004-06-15

PRÓLOGO

El Instituto Colombiano de Normas Técnicas y Certificación, **ICONTEC**, es el organismo nacional de normalización, según el Decreto 2269 de 1993.

El **ICONTEC** es una entidad de carácter privado, sin ánimo de lucro, cuya Misión es fundamental para brindar soporte y desarrollo al productor y protección al consumidor. Colabora con el sector gubernamental y apoya al sector privado del país, para lograr ventajas competitivas en los mercados interno y externo.

La representación de todos los sectores involucrados en el proceso de Normalización Técnica está garantizada por los Comités Técnicos y el período de Consulta Pública, este último caracterizado por la participación del público en general.

La NTC 5254 fue ratificada por el Consejo Directivo del 2004-05-31.

Esta norma está sujeta a ser actualizada permanentemente con el objeto de que responda en todo momento a las necesidades y exigencias actuales.

A continuación se relacionan las empresas que colaboraron en el estudio de esta norma a través de su participación en el Comité Técnico 32 Gestión de riesgo.

ACODRES
ALMAVIVA S.A.
ALPINA
CÁMARA DE COMERCIO DE BOGOTÁ
CENTRAL DE SEGUROS
COMESTIBLES RICOS
ECOPETROL
EMPRESA DE ACUEDUCTO DE BOGOTÁ
FIDUCOLOMBIA

Además de las anteriores, en Consulta Pública el Proyecto se puso a consideración de las siguientes empresas:

A TODA HORA S.A.
ACICAM
ACODRES
ACONTA LTDA.
ACOR PAÍS
ADUACARGA
AGRÍCOLA DE SEGUROS
AGRÍCOLA SANTAMARÍA S.A.
AGUAS DE CARTAGENA S.A.
ALCIAUTOS LTDA.
ALFAMED LTDA.
ALFONSO NIETO L Y CÍA.
ALMACENAR
ALMACENES GENERALES DE DEPÓSITO ALMAVIVA S.A.
ALPOPULAR S.A. - ALMACÉN GENERAL DE DEPÓSITOS
ALTE LTDA.
ANDICEL S.A.
ÁNIMO CREATIVO
APD DE COLOMBIA
APUESTAS LA 30
ARP ARQUIT. ING. S.A.
ARSEG
ASIS CAPÍTULO COLOMBIA
ASOHOFRUCOL
AUDILIMITED
AVE COLOMBIANA LTDA.
BANCO DE BOGOTÁ
BANCO GANADERO
BANCO SUDAMERIS
BANCOLDEX
BOLSA DE VALORES
BRINKS DE COLOMBIA S.A.
BVC
C Y C LTDA.

C&E S.A.
CAGRECAPITAL
CAMARA DE COMERCIO DE BOGOTA
CÁMARA DE COMERCIO DE CALI
CAMARA DE COMERCIO DE MEDELLÍN
CARBONES DEL CERREJÓN
CASALS & ASOCIATE
CÁMARA DE COMERCIO DE BARRANQUILLA
CEINNOVA
CELLSTAR DE COLOMBIA LTDA.
CENTRAL DE SEGUROS
CERTICÁMARA
CHALLENGER S.A.
CHICLE ADAMS S.A.
CHUBB DE COLOMBIA
CISA
CODECAV LTDA.
COLDECOM
COLMENA RIESGOS PROFESIONALES
COLMUNDO RADIO
COLPATRIA
COLSEGUROS
COLTEUNIDOS LTDA.
COMESTIBLES RICAS
CONINSA Y RAMON H S.A.
CONTRALORÍA MUNICIPAL DE BUCARAMANGA
COONALTRABRINKS
COOP CAFAM LTDA.
COOPARTES LTDA.
COOPCULTURA
COOPMUNICOL LTDA.
COOPSERVIR LTDA.
COPERAGRO
CORFINCORA
COTELCO
CREACIONES KELINDA
DANOVO COLOMBIA
DIS LTDA.
DISTRITODO
EAGLE COMERCIAL
ECOPETROL-VICEPRESIDENCIA DE TRANSPORTE
EDUCACIÓN MÉDICA
ELECTRO HIDRÁULICA S.A.
EMPRESA DE ACUEDUCTO DE BOGOTÁ
EMPRESAS PÚBLICAS DE MEDELLÍN
EMTELCO S.A.
ENERGÍA CUNDINAMARCA
EPS FAMISANAR LTDA.
ERNST & YOUNG
EXPOCAFÉ
EXXON MOBIL DE COLOMBIA S.A.
FERRELUM
FERTIQUIM LTDA.
FIDUCIARIA LA CENTRAL S.A.
FIDUCOLOMBIA S.A. SOCIEDAD
FIDUCIARIA S.A.
FIDUPREVISORA S.A.
FINAGRO
FINDETER S.A.
FLORES LA MANA LTDA.
FONDO DE EMPELADOS DE S.C. JHONSON
FONDO NACIONAL DEL AHORRO
GABRIEL FORERO Y CÍA. S.A.
GAS NATURAL ESP
GEOTEC ING. LTDA.
GESTOR COLOMBIA
GIT LTDA.
GONZALO USME Y CÍA.
GRUPO ODINSA S.A.
HERNANDO RODRÍGUEZ C.P.E.O.
HOME CENTER
IDEXCOL LTDA.
IFI LEASING S.A.
ILURAM S.A.
IMAGEN DIGITAL
INAMOO LTDA.
INDEP
INDUSTRIAS GRÁFICAS DARBEL
INGENIAR
INGENIO DEL CAUCA S.A.
INMUNOPHARMOS
INVERSIONES PIRÁMIDE
ISVI LTDA.
JAB REPRESENTACIONES
JOHN CRANE COL
KELINDA LTDA.
KPMG
LA PREVISORA VIDA S.A.
LEASING BOLIVAR S.A.
MAQUIPAN LTDA.
MERCURIO INTERNACIONAL S.A.
MINISTERIO DE COMERCIO INDUSTRIA Y TURISMO
MINISTERIO DE DEFENSA
MINISTERIO DE TRANSPORTE
MINISTRO DEL MEDIO AMBIENTE
P I A LTDA.
PARAGUERÍA DEL NORTE
PAVCO S.A.
PRICE WATER HOUSE C.
PROCESOS Y CANJE
PRODUCTIVIDAD EMPRESARIAL LTDA.
PRODUCTOS KIBORY
PRODUCTOS NISOL LTDA.

PROTELA S.A.
PVC GERFOR S.A.
QUALA S.A.
QUÍMICA INTERNACIONAL
RAISBERG LARA RODRÍGUEZ
ROJAS BAREÑO Y CÍA.
ROVIGAN LTDA.
ROYAL & SUNALLIANCE
SÁENZ RUIZ CADENA ING. CIVILES
SANICULTIVOS
SCHNEIDER ELECTRIC
SEGURIDAD ATEMPI
SEGURIDAD ELECTRICA LTDA.
SEGUROS ALFA S.A.
SEGUROS BOLIVAR
SEGUROS CONFIANZA
SEÑAL 3
SERVIS S.A.
SICUREX
SIDEIN LTDA.
SIEMENS S.A. MOTORES
SIGRA S.A.
SISTEROM LTDA.
SPN GLOBAL ASESORES LTDA.
SU TEMPORAL LTDA.
SUIZO S.A.
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO
SUPERPOLO S.A.
SURATEP S.A.
TERMINAL DE TRANSPORTE
TEXTILES FASCINA LTDA.
THOMAS GREG & SONS DE COLOMBIA S.A. IMPRESORA DE VALORES
TOTALSEGUROS LTDA.
TRO INMOBILIARIA LTDA.
UNIVERSIDAD DE LA SABANA
USTA-ICONTEC
VASELIN LTDA.
WILLIS SEGUROS
WSA ELECTRONIC DE COL.
ZONA FRANCA DE BOGOTA S.A. FREE ZONE OF BOGOTÁ

El **ICONTEC** cuenta con un Centro de Información que pone a disposición de los interesados normas internacionales, regionales y nacionales.

DIRECCIÓN DE NORMALIZACIÓN

GESTIÓN DEL RIESGO

PREFACIO A LA NORMA

Esta norma tiene como objetivo proporcionar un marco genérico para establecer el contexto, la identificación, el análisis, la evaluación, el tratamiento, el seguimiento y la comunicación del riesgo. Se debe leer en conjunto con otras normas aplicables o pertinentes.

Esta norma especifica los elementos del proceso de gestión del riesgo, pero no es su propósito obligar a la uniformidad de los sistemas de gestión del riesgo. Es genérica e independiente de cualquier sector industrial o económico específico. El diseño e implementación del sistema de gestión del riesgo se verá influenciado por las necesidades variables de una organización, sus objetivos particulares, sus productos y servicios y los procesos y prácticas específicas empleadas.

La gestión del riesgo es un proceso iterativo que consta de pasos bien definidos que, tomados en secuencia, apoyan una mejor toma de decisiones mediante su contribución a una mayor profundización en los riesgos y sus impactos. El proceso de gestión del riesgo puede aplicarse a cualquier situación donde un resultado indeseado o inesperado podría ser importante o donde se identifiquen oportunidades. Quienes toman decisiones deben conocer los posibles resultados y tomar medidas para controlar su impacto.

La gestión del riesgo se reconoce como parte integral de la buena práctica de gestión. A fin de ser lo más efectiva posible, la gestión del riesgo debe volverse parte de la cultura de una organización. Debe integrarse en las filosofías de la organización, las prácticas y planes empresariales en vez de verse o practicarse como un programa separado. Cuando esto se logra, la gestión del riesgo se vuelve asunto de cada una de las personas de la organización.

Si por alguna razón no es posible integrar la gestión del riesgo a lo largo de una organización entera, puede ser posible aplicarla exitosamente a departamentos, procesos o proyectos individuales.

La terminología empleada en esta norma se ha seleccionado para que resulte aceptable en toda una serie de riesgos y disciplinas de gestión del riesgo en la medida de lo posible. Se han evitado las palabras que tienen significados con ligeras diferencias en diferentes ramas de la gestión del riesgo y se han remplazado por palabras que pudieran definirse con un significado común. Un ejemplo es el término de *tratamiento del riesgo* que se define para cubrir más de lo que usualmente se quiere decir con el término *control del riesgo*.

El término *informativo* se ha empleado en esta norma para definir la aplicación del anexo al cual se aplica. Un anexo *informativo* sólo es para información y orientación.

GESTIÓN DEL RIESGO

INTRODUCCIÓN

El documento es modificado porque en párrafos donde la norma de referencia tiene recomendaciones, el comité de normalización 32 de gestión de riesgo consideró que estos eran requisitos de carácter mandatario, por está razón se cambio el verbo debería por debe.

1. OBJETO, APLICACIÓN Y DEFINICIONES

1.1 OBJETO

Esta norma ofrece unos requisitos generales para el establecimiento e implementación del proceso de gestión del riesgo, que involucra la determinación del contexto y la identificación, análisis, evaluación, tratamiento, comunicación y monitoreo regular de los riesgos.

1.2 APLICACIÓN

La gestión del riesgo se reconoce como una parte integral de las buenas prácticas de gestión. Es un proceso iterativo compuesto por una serie de pasos que, si se ejecutan en secuencia, permiten la mejora continua en la toma de decisiones.

La gestión del riesgo es el término aplicado a un método lógico y sistemático para el establecimiento del contexto, identificación, análisis, evaluación, tratamiento, monitoreo y comunicación de los riesgos asociados con cualquier actividad, función o proceso, de forma que posibilite que las organizaciones minimicen pérdidas y maximicen oportunidades. La gestión del riesgo tiene que ver tanto con la identificación de oportunidades como con la prevención o mitigación de pérdidas.

Esta norma puede aplicarse en todas las etapas de la vida de una actividad, función, proyecto, producto o bien. Por lo general, el máximo beneficio se obtiene mediante la aplicación del proceso de gestión del riesgo desde el inicio. Con frecuencia se realizan numerosos estudios en diferentes etapas de un proyecto.

NOTA La presente norma puede aplicarse a una gama muy amplia de actividades u operaciones de cualquier empresa pública, privada o comunitaria, o grupo. En el Anexo A se presentan ejemplos.

1.3 DEFINICIONES

Para el propósito de esta norma, se aplican las siguientes definiciones:

1.3.1
consecuencia
resultado de un evento expresado cualitativa o cuantitativamente, como por ejemplo una pérdida, lesión, desventaja o ganancia. Puede haber una serie de resultados posibles asociados con un evento.

1.3.2
costo
actividades, tanto directas como indirectas, que involucran cualquier impacto negativo, incluyendo pérdidas de dinero, tiempo, mano de obra, interrupción del trabajo, buen nombre, pérdidas políticas e intangibles.

1.3.3
evento
incidente o situación que ocurre en un lugar particular durante un intervalo de tiempo particular.

1.3.4
análisis de árbol de eventos
técnica que describe la posible gama y secuencia de los resultados que pueden provenir del inicio de un evento.

1.3.5
análisis de efectos y modo de falla (AEMF)
procedimiento mediante el cual se analizan los modos de falla potencial en un sistema técnico. Un AEMF se puede ampliar para realizar lo que se denomina análisis de modos de falla, efectos y grado de severidad (FMECA). En un FMECA, cada modo de falla identificado se clasifica de acuerdo con la influencia combinada de su probabilidad de ocurrencia y la severidad de sus consecuencias.

1.3.6
análisis de árbol de fallas
método de ingeniería de sistemas usado para representar las combinaciones lógicas de varios estados del sistema y las posibles causas que pueden contribuir a un evento específico (llamado el evento superior).

1.3.7
frecuencia
medida de la tasa de ocurrencia de un evento, expresada como el número de ocurrencias de un evento en un tiempo determinado. Véase también Posibilidad y Probabilidad.

1.3.8
peligro
fuente de daño potencial o situación con potencial para causar pérdida.

1.3.9
posibilidad
se emplea como una descripción cualitativa de la probabilidad o frecuencia.

1.3.10
pérdida
cualquier consecuencia negativa, financiera u otra.

1.3.11
monitorear
verificar, supervisar, observar de forma crítica, o registrar el progreso de una actividad, acción o sistema, en forma regular, a fin de identificar cambios.

1.3.12
organización
empresa, firma, compañía o asociación, u otra entidad legal o parte de la misma, ya sea constituida o no, pública o privada, que tiene sus propias funciones y administración.

1.3.13
probabilidad
posibilidad de que ocurra un evento o resultado específico, medida por la relación entre los eventos o resultados específicos y el número total de eventos o resultados posibles. La probabilidad se expresa como un número entre 0 y 1, en donde 0 indica un evento o resultado imposible y 1 un evento o resultado seguro.

1.3.14
riesgo residual
nivel restante de riesgo después de que se han tomado medidas de tratamiento del riesgo.

1.3.15
riesgo
posibilidad de que suceda algo que tendrá impacto en los objetivos. Se mide en términos de consecuencias y posibilidad de ocurrencia.

1.3.16
aceptación del riesgo
decisión informada de aceptar las consecuencias y posibilidad de un riesgo particular.

1.3.17
análisis del riesgo
uso sistemático de la información disponible, para determinar la frecuencia con la que pueden ocurrir eventos especificados y la magnitud de sus consecuencias.

1.3.18
valoración del riesgo
proceso general de análisis del riesgo y evaluación del riesgo. Véase la Figura 3.1.

1.3.19
evitar el riesgo
decisión informada de no involucrarse en una situación de riesgo.

1.3.20
control del riesgo
parte de la gestión del riesgo que involucra la implementación de políticas, normas, procedimientos y cambios físicos a fin de eliminar o minimizar los riesgos adversos.

1.3.21
ingeniería del riesgo
aplicación de principios de ingeniería y métodos para la gestión del riesgo.

1.3.22
evaluación del riesgo
proceso usado para determinar las prioridades de gestión del riesgo mediante la comparación del nivel de riesgo contra normas predeterminadas, niveles de riesgo objeto u otros criterios.

1.3.23
financiación del riesgo
métodos aplicados para suministrar fondos para el tratamiento del riesgo y las consecuencias financieras del riesgo.

NOTA En algunas industrias, la financiación del riesgo sólo se relaciona con el suministro de fondos para afrontar las consecuencias financieras del riesgo.

1.3.24
identificación del riesgo
proceso para determinar lo que puede suceder, por qué y cómo.

1.3.25
gestión del riesgo
cultura, procesos y estructuras que se dirigen hacia la gestión eficaz de las oportunidades potenciales y los efectos adversos.

1.3.26
proceso de gestión del riesgo
aplicación sistemática de políticas de gestión, procedimientos y prácticas, a las tareas de establecimiento del contexto, identificación, análisis, evaluación, tratamiento, monitoreo y comunicación del riesgo.

1.3.27
reducción del riesgo
aplicación selectiva de técnicas apropiadas y principios de gestión a fin de reducir la posibilidad de una ocurrencia o sus consecuencias, o ambas.

1.3.28
retención del riesgo
retención, intencional o no, de la responsabilidad por pérdida, o carga por la pérdida financiera dentro de la organización.

1.3.29
transferencia del riesgo
traslado de la responsabilidad o carga por la pérdida a otra parte, por medio de la legislación, contratos, seguros u otros medios. La transferencia del riesgo también se puede referir al traslado de un riesgo físico o parte del mismo a cualquier otra parte.

1.3.30
tratamiento del riesgo
selección e implementación de las opciones apropiadas para ocuparse del riesgo.

1.3.31
análisis de sensibilidad
análisis que examina la forma como los resultados de un cálculo o modelo varían a medida que cambian las suposiciones de los individuos.

1.3.32
partes interesadas
personas y organizaciones que pueden afectar, verse afectadas, o percibirse ellas mismas como afectadas por una decisión o actividad.

NOTA El término parte interesada también puede incluir las partes interesadas definidas en las normas ISO 14050:1998 e ISO 14004:1996.

2. REQUISITOS DE LA GESTIÓN DEL RIESGO

2.1 PROPÓSITO

El propósito de esta sección es describir un proceso formal para el establecimiento de un programa sistemático de gestión del riesgo.

Para llevar a cabo un programa de gestión del riesgo, detallado, a nivel de proyectos o suborganizacional, es necesario desarrollar una política de gestión del riesgo organizacional y un mecanismo de soporte.

2.2 POLÍTICA DE GESTIÓN DEL RIESGO

La alta dirección de la organización debe definir y documentar su política para gestión del riesgo, incluidos los objetivos para la gestión del riesgo y su compromiso con ella. La política de gestión del riesgo debe ser pertinente para el contexto estratégico de la organización y sus metas, objetivos y la naturaleza de sus negocios. La dirección debe asegurar que su política sea entendida, implementada y mantenida en todos los niveles de la organización.

2.3 PLANEACIÓN Y SUMINISTRO DE RECURSOS

2.3.1 Compromiso de la dirección

La organización debe asegurar que:

a) Se establezca, implemente y mantenga un sistema de gestión del riesgo de acuerdo con esta norma, y

b) Se reporte el desempeño del sistema de gestión del riesgo a la dirección de la organización para revisión y como base para mejora.

2.3.2 Responsabilidad y autoridad

Debe definirse y documentarse la responsabilidad, autoridad y la interrelación del personal que realiza y verifica la gestión del riesgo, en especial para las personas que requieren autonomía y autoridad organizacional para efectuar una o más de las siguientes actividades:

a) iniciar acciones a fin de evitar o reducir los efectos adversos del riesgo;

b) controlar el tratamiento posterior de los riesgos hasta que el nivel de riesgo se vuelva aceptable;

c) identificar y registrar cualquier problema relacionado con la gestión del riesgo;

d) iniciar, recomendar o proporcionar soluciones por medio de los canales designados;

e) verificar la implementación de soluciones; y

f) comunicar y consultar interna y externamente, según sea apropiado.

2.3.3 Recursos

La organización debe identificar los requerimientos en cuanto a recursos y brindar los recursos adecuados, que incluyen la asignación de personal entrenado para actividades de gestión, realización del trabajo y de verificación, incluida la verificación interna.

2.4 PROGRAMA DE IMPLEMENTACIÓN

Se requieren varios pasos para implementar un sistema eficaz de gestión del riesgo dentro de una organización. En el Anexo B se presentan algunos ejemplos. Dependiendo de la filosofía, cultura y estructura generales de la organización en cuanto a gestión del riesgo, debe ser posible combinar u omitir algunos pasos. No obstante, cuando sea aplicable s e deben tener todos en cuenta.

2.5 REVISIÓN POR LA DIRECCIÓN

La alta dirección de la organización debe garantizar que se realice una revisión del sistema de gestión del riesgo a intervalos especificados, suficiente para asegurar su continua conveniencia y eficacia para cumplir los requisitos de la presente norma y la política y objetivos de gestión del riesgo establecidos por la organización (véase el numeral 2.2). Se deben mantener registros de dichas revisiones.

3. PANORAMA DE LA GESTIÓN DEL RIESGO

3.1 GENERALIDADES

La gestión del riesgo es una parte integral del proceso de gestión. La gestión del riesgo es un proceso multifacético, cuyos aspectos apropiados los realiza, con frecuencia, un equipo multi-disciplinario. Es un proceso iterativo de mejora continua.

3.2 ELEMENTOS PRINCIPALES

Los elementos principales del proceso de gestión del riesgo, como se ilustra en la Figura 3.1, son los siguientes:

a) Establecer el contexto

Establecer el contexto estratégico, organizacional y de gestión del riesgo en el cual ocurrirá el resto del proceso. Es conveniente que se establezcan criterios contra los cuales va a de evaluar el riesgo, y se debe definir la estructura del análisis.

b) Identificar riesgos

Identificar qué, por qué y cómo pueden surgir elementos como base para análisis posterior.

c) Analizar riesgos

Determinar los controles existentes y analizar los riesgos en términos de consecuencia y posibilidad en el contexto de estos controles. El análisis debe considerar la gama de consecuencias potenciales y la posibilidad de que éstas ocurran. Se pueden combinar la consecuencia y la posibilidad para producir un nivel estimado de riesgo.

d) Evaluar los riesgos

Comparar los niveles estimados de riesgo, contra los criterios pre-establecidos. Esto posibilita que los riesgos sean clasificados de modo que se identifiquen prioridades de gestión. Si los niveles de riesgo establecido son bajos, entonces los riesgos pueden encajar en una categoría aceptable, y es posible que no se requiera tratamiento.

e) Tratar los riesgos

Aceptar y monitorear los riesgos de baja prioridad. Para los demás riesgos, desarrollar e implementar un plan de gestión específico que incluya considerar el suministro de recursos.

f) Monitorear y revisar

Monitorear y revisar el desempeño del sistema de gestión del riesgo y los cambios que pudieran afectarlo.

g) Comunicar y consultar

Comunicar y consultar con las partes interesadas, internas y externas, según sea apropiado, en cada etapa del proceso de gestión del riesgo y con relación al proceso en conjunto.

La gestión del riesgo puede aplicarse en muchos niveles de una organización. Puede aplicarse en el nivel estratégico y en niveles operacionales; puede aplicarse a proyectos específicos, para servir de ayuda en decisiones específicas o manejar áreas de riesgo específicas reconocidas.

La gestión del riesgo es un proceso iterativo que puede contribuir a la mejora organizacional. Con cada ciclo, los criterios de riesgo pueden fortalecerse para lograr progresivamente mejores niveles de gestión del riesgo.

Para cada etapa del proceso deben mantenerse registros adecuados que sean suficientes para satisfacer la auditoría independiente.

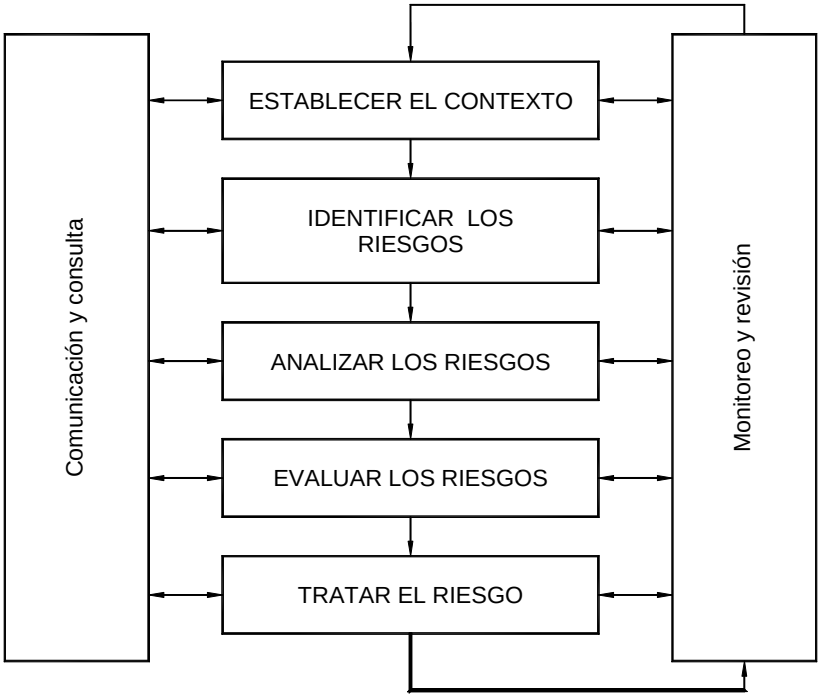

Figura 3.1. Proceso general de gestión del riesgo

4. PROCESO DE GESTIÓN DEL RIESGO

4.1 DETERMINACIÓN DEL CONTEXTO

4.1.1 Generalidades

En la Figura 4.1 se muestran los detalles del proceso de gestión del riesgo. El proceso ocurre dentro del marco de un contexto estratégico, organizacional y de gestión del riesgo de una organización. Este requiere establecerse para definir los parámetros básicos dentro de los cuales se debe manejar el riesgo, y para ofrecer orientación con relación a decisiones dentro de estudios de gestión del riesgo más detallados. Aquí se establece el alcance para el resto del proceso de gestión del riesgo.

4.1.2 Determinación del contexto estratégico

Define la relación entre la organización y su entorno, identificando las fortalezas, debilidades, oportunidades y amenazas de la organización. El contexto incluye los aspectos financieros, operacionales, competitivos, políticos (percepciones/imagen ante el público), sociales, del cliente, culturales y legales de las funciones de una organización.

Identifica las partes interesadas internas y externas, y considera sus objetivos; tiene en cuenta sus percepciones y establece políticas de comunicación con estas partes.

NOTA El Anexo C presenta una lista de partes interesadas potenciales.

Este paso se enfoca hacia el medio ambiente en el cual opera la organización. La organización debe tratar de determinar los elementos cruciales que pudieran apoyar o afectar su capacidad para manejar los riesgos que enfrenta.

Se puede emprender un análisis estratégico, el cual debe tener respaldo al nivel de la alta dirección; debe determinar los parámetros básicos y proporcionar orientación para los procesos de gestión del riesgo más detallados. Debe existir una estrecha relación entre la misión u objetivos estratégicos de una organización y su gestión de todos los riesgos a los cuales está expuesta.

4.1.3 Determinación del contexto organizacional

Antes de dar inicio a un estudio de gestión del riesgo, es necesario comprender la organización y sus capacidades, lo mismo que sus metas y objetivos, y las estrategias implementadas para lograrlos.

Esto es importante por las siguientes razones:

a) La gestión del riesgo tiene lugar en el contexto de las metas, estrategias y objetivos más amplios de la organización;

b) el no lograr los objetivos de la organización o la actividad específica, o el proyecto en consideración, representa un conjunto de riesgos que deben manejarse;

c) La política y metas organizacionales ayudan a definir los criterios por los cuales se decide si un riesgo es aceptable o no, y forma la base de opciones para su tratamiento.

4.1.4 Determinación del contexto de la gestión del riesgo

Es conveniente establecer las metas, objetivos, estrategias, alcance y parámetros de la actividad o parte de la organización a la cual se está aplicando el proceso de gestión del riesgo. El proceso se debe emprender prestando atención cuidadosa a la necesidad de equilibrar costos, beneficios y oportunidades. También deben especificarse los recursos requeridos y los registros que se deben llevar.

El establecimiento del objeto y límites de una aplicación del proceso de gestión del riesgo involucra:

a) Definición del proyecto o actividad y establecimiento de sus metas y objetivos;

b) Definición del alcance del proyecto, en cuanto a tiempo y lugar;

c) Identificación y estudios necesarios, y su alcance, objetivos y los recursos requeridos. Las fuentes genéricas de riesgo y las áreas de impacto pueden ofrecer una guía para este punto.

NOTA Para ejemplos de fuentes genéricas de riesgo y sus áreas de impacto, véase al Anexo D.

d) Definición del alcance y cobertura de las actividades de gestión del riesgo por realizar.

Entre los asuntos específicos que también pueden discutirse se encuentran:

i) Las funciones y responsabilidades de diferentes partes de la organización que participan en la gestión del riesgo;

ii) Las relaciones entre el proyecto y otros proyectos o partes de la organización.

4.1.5 Definición de los criterios de evaluación del riesgo

Decidir los criterios contra los cuales se va a evaluar el riesgo. Las decisiones relacionadas con la aceptabilidad del riesgo y su tratamiento pueden basarse en criterios operacionales, técnicos, financieros, legales, sociales, humanitarios u otros. Con frecuencia, estos dependen de la política interna de una organización, sus metas, objetivos y los intereses de las partes interesadas.

Los criterios pueden verse afectados por percepciones internas y externas y requisitos legales. Es importante que se determinen criterios apropiados desde el principio.

Aunque los criterios del riesgo se desarrollan inicialmente como parte de la determinación del contexto de gestión del riesgo, éstos pueden desarrollarse luego y refinarse posteriormente a medida que se identifican los riesgos particulares y se seleccionan técnicas de análisis, es decir, los criterios del riesgo deben corresponder al tipo de riesgos y a la forma en la que se expresan los niveles de riesgo.

4.1.6 Definición de la estructura

Esto involucra la separación de la actividad o proyecto en un conjunto de elementos. Estos elementos ofrecen una estructura lógica para la identificación y análisis que ayuda a garantizar que no se pasen por alto riesgos significativos. La selección de la estructura depende de la naturaleza de los riesgos y del alcance del proyecto o actividad.

4.2 IDENTIFICACIÓN DEL RIESGO

4.2.1 Generalidades

En este paso se busca identificar los riesgos que se van a gestionar. Es esencial realizar una identificación de conjunto usando un proceso sistemático bien estructurado, debido a que un riesgo potencial no identificado durante esta etapa será excluido del análisis posterior. La identificación debe incluir todos los riesgos, sea que estén o no bajo el control de la organización.

4.2.2 ¿Qué puede suceder?

El objetivo es generar una lista global de eventos que podrían afectar cada elemento de la estructura a la que se hace referencia en el numeral 4.1.6. Estos eventos se consideran entonces con mayor detalle, para identificar lo que puede ocurrir.

NOTA El Anexo D proporciona información acerca de fuentes genéricas de riesgo y sus áreas de impacto.

4.2.3 ¿Cómo y por qué puede suceder?

Una vez que se haya identificado una lista global de eventos, es necesario considerar sus posibles causas y escenarios. Existen muchas formas en las que se puede iniciar un evento. Es importante que no se omitan causas significativas.

4.2.4 Herramientas y técnicas

Entre los métodos empleados para identificar riesgos se encuentran las listas de chequeo, juicios basados en experiencia y registros, diagramas de flujo, lluvia de ideas, análisis de sistemas, análisis de escenarios y técnicas de ingeniería de sistemas.

El método empleado dependerá de la naturaleza de las actividades bajo revisión y los tipos de riesgo.

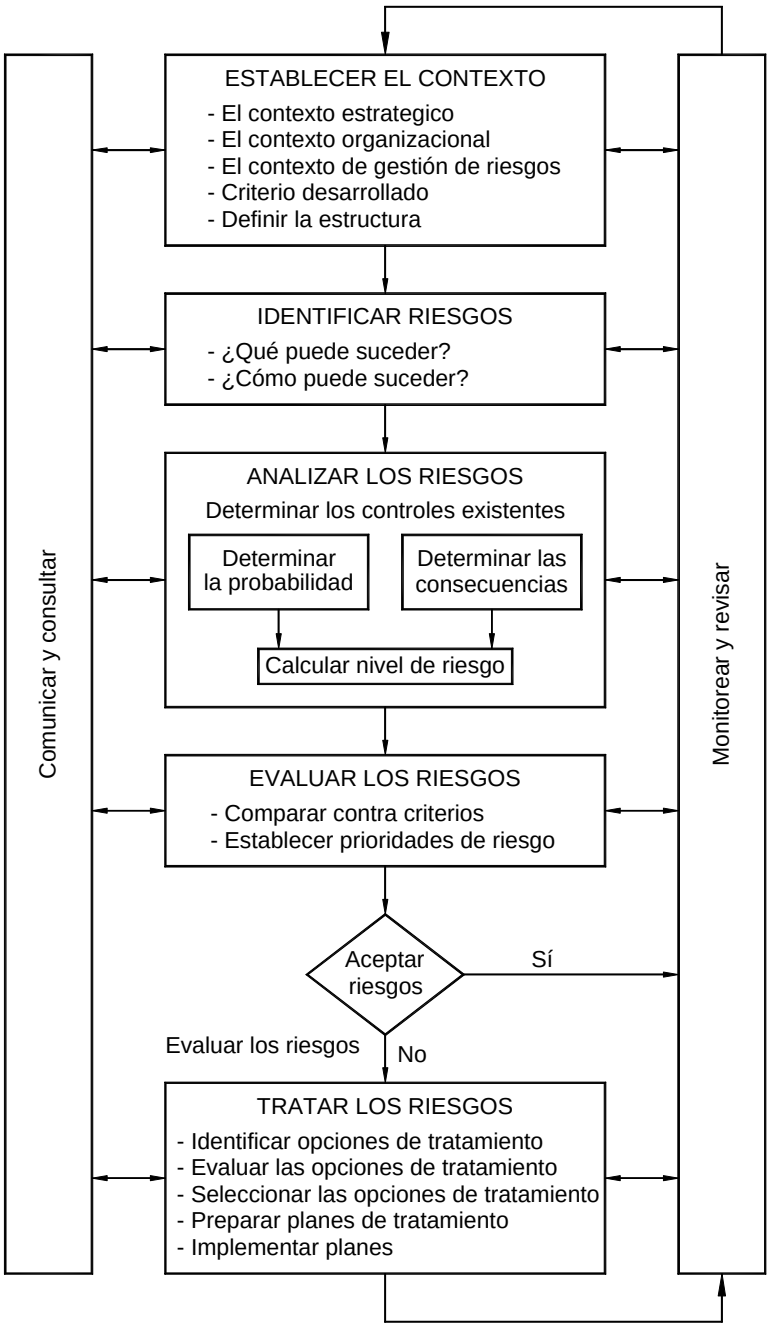

Figura 4.1. Proceso de gestión del riesgo

4.3 ANÁLISIS DEL RIESGO

4.3.1 Generalidades

Los objetivos del análisis consisten en separar los riesgos aceptables menores de los mayores, y proporcionar datos que sirvan para la evaluación y el tratamiento de riesgos. El análisis del riesgo incluye considerar las fuentes de riesgo, sus consecuencias y la posibilidad de que estas consecuencias ocurran. Se pueden identificar los factores que afectan las consecuencias y la posibilidad. El riesgo se analiza mediante la combinación de estimaciones de consecuencias y posibilidad en el contexto de las medidas de control existentes.

Se puede realizar un análisis preliminar de manera que se excluyan del estudio detallado los riesgos similares o de bajo impacto. Se deben enumerar los riesgos excluidos, siempre que sea posible, a fin de demostrar que el análisis de riesgos es completo.

4.3.2 Determinación de los controles existentes

Se deben identificar la gestión, los sistemas técnicos y procedimientos existentes para controlar el riesgo y evaluar sus fortalezas y debilidades. Las herramientas empleadas en el numeral 4.2.4 pueden resultar apropiadas, lo mismo que métodos tales como inspecciones y técnicas de control por auto-evaluación ('CAE').

4.3.3 Consecuencias y posibilidad

Se evalúa la magnitud de las consecuencias de un evento, si ocurriera, y la posibilidad del evento y sus consecuencias asociadas, en el contexto de los controles existentes. Las consecuencias y la posibilidad se combinan para producir un nivel de riesgo. Las consecuencias y la posibilidad se pueden determinar a partir de análisis y cálculos estadísticos. Como alternativa, cuando no hay a disposición datos del pasado, se pueden hacer estimaciones subjetivas que reflejen el grado de creencia de un individuo o grupo con respecto a la probabilidad de ocurrencia de un evento o resultado particular.

A fin de evitar los sesgos subjetivos, al analizar las consecuencias y la posibilidad, se recomienda emplear los mejores recursos y técnicas de información disponibles. Entre las fuentes de información se pueden incluir:

a) registros pasados;

b) experiencia pertinente;

c) práctica y experiencia industrial;

d) literatura publicada pertinente;

e) marketing de ensayo e investigación de mercado;

f) experimentos y prototipos;

g) modelos económicos, de ingeniería y otros;

h) juicios de especialistas y expertos.

Entre las técnicas, se emplean:

i) entrevistas estructuradas con expertos en el área de interés;

ii) empleo de grupos de expertos multidisciplinarios;

iii) evaluaciones individuales empleando cuestionarios;

iv) uso del computador y otros modelos;

v) uso de árboles de falla y árboles de eventos.

Siempre que sea posible, se debe incluir el grado de confianza de los cálculos de los niveles de riesgo.

4.3.4 Tipos de análisis

El análisis del riesgo se puede aplicar con diferentes grados de exactitud, dependiendo de la información del riesgo y de la disponibilidad de datos. El análisis puede ser cualitativo, semi-cuantitativo, cuantitativo, o una combinación de estos, según las circunstancias. El orden de complejidad y el costo de estos análisis, en orden ascendente, es: cualitativo, semi-cuantitativo y cuantitativo. En la práctica, con frecuencia se emplea primero el análisis cualitativo, para obtener una indicación general del nivel del riesgo. Posteriormente puede ser necesario realizar un análisis cuantitativo más específico. En detalle, los tipos de análisis son los siguientes:

a) Análisis cualitativo

El análisis cualitativo emplea palabras o escalas descriptivas para describir la magnitud de las consecuencias potenciales y la posibilidad de que estas consecuencias ocurran. Estas escalas pueden adaptarse o ajustarse según las circunstancias, y se pueden emplear diferentes descripciones para diferentes riesgos.

NOTA Las Tablas E.1 y E.2 del Anexo E muestran ejemplos de escalas cualitativas o descriptivas simples para posibilidad y consecuencias. La Tabla E.3 es un ejemplo de una matriz en la cual se asignan riesgos a clases de prioridad, mediante la combinación de su posibilidad y consecuencia. Estas tablas deben ajustarse para satisfacer las necesidades de cada organización o del tema particular de evaluación de riesgos.

El análisis cualitativo se emplea;

i) Como una actividad inicial de preselección, para identificar los riesgos que necesitan un análisis más detallado;

ii) cuando el nivel del riesgo no justifica el tiempo y esfuerzo requeridos para un análisis más completo; ó

iii) Cuando los datos numéricos disponibles son inadecuados para un análisis cuantitativo.

b) Análisis semicuantitativo

En el análisis semicuantitativo, se asignan valores a escalas cualitativas como las descritas anteriormente. No es obligatorio que el número asignado a cada descripción tenga una relación exacta con la magnitud real de las consecuencias o posibilidad. Los números se pueden combinar mediante cualquier fórmula de entre una variedad de ellas, siempre y cuando el sistema usado para priorización

sea compatible con el sistema escogido para asignar números y combinarlos. El objetivo es producir una priorización más detallada de la que se logra generalmente en el análisis cualitativo, y no sugerir cualquier valor realista del riesgo tal como se intenta en el análisis cuantitativo.

Se debe tener cuidado con el uso del análisis semicuantitativo, ya que es posible que los números seleccionados no reflejen adecuadamente los tipos de relatividad que pueden conducir a resultados inconsistentes. Puede ser que el análisis semi-cuantitativo no diferencie adecuadamente entre los riesgos, en especial cuando las consecuencias o la posibilidad son extremas.

Algunas veces resulta apropiado considerar la posibilidad como compuesta de dos elementos, a los que generalmente se les denomina frecuencia de exposición y probabilidad.

Frecuencia de exposición es el grado en el que existe una fuente de riesgo, y la probabilidad es la posibilidad de que, cuando existe una fuente de riesgo, ocurran consecuencias. Se debe tener precaución en situaciones donde la relación entre los dos elementos no es completamente independiente, es decir, donde existe una fuerte relación entre frecuencia de exposición y probabilidad.

Este método puede aplicarse en análisis semi-cuantitativo y cuantitativo.

c) Análisis cuantitativo

El análisis cuantitativo emplea valores numéricos (en lugar de las escalas descriptivas empleadas en los análisis cualitativo y semi-cuantitativo), tanto para las consecuencias como para la posibilidad a partir de datos de una variedad de fuentes (tales como aquellos a los que se hace referencia en los literales (a) a (h) del numeral 4.3.3). La calidad del análisis depende de la exactitud y de la integridad de los valores numéricos empleados.

Las consecuencias se pueden estimar mediante el modelado de los resultados de un evento o grupo de eventos, o por extrapolación de estudios experimentales o datos históricos. Las consecuencias pueden expresarse en términos de criterios monetarios, técnicos, humanos o cualquiera de los criterios a que hace referencia el numeral 4.1.5. En algunos casos, se requiere más de un valor numérico para especificar las consecuencias en diferentes tiempos, lugares, grupos o situaciones.

Por lo general, la posibilidad se expresa ya sea como probabilidad, frecuencia o una combinación de exposición y probabilidad.

La forma como se expresan la posibilidad y las consecuencias, y la formas en que se combinan para brindar un nivel de riesgo, variará de acuerdo con el tipo de riesgo y el contexto en el cual se va a emplear el nivel del riesgo.

NOTA En el Anexo F se ofrecen algunos ejemplos de expresiones de riesgo cuantitativo.

4.3.5 Análisis de sensibilidad

Puesto que algunas de las estimaciones realizadas en el análisis cuantitativo son imprecisas, debe realizarse un análisis de sensibilidad para determinar el efecto de los cambios en las hipótesis y datos.

4.4 EVALUACIÓN DEL RIESGO

La evaluación del riesgo involucra la comparación del nivel de riesgo encontrado durante el proceso de análisis contra los criterios de riesgo previamente establecidos.

El análisis del riesgo y los criterios contra los cuales se comparan los riesgos en la evaluación del riesgo se deben considerar sobre la misma base. Por tanto, la evaluación cualitativa involucra la comparación de un nivel cualitativo del riesgo contra los criterios cualitativos; y la evaluación cuantitativa involucra la comparación del nivel numérico del riesgo, contra los criterios que pueden expresarse como un número específico, como por ejemplo un valor que indique fatalidad, frecuencia o valor monetario.

El resultado de una evaluación del riesgo es una lista priorizada de riesgos, para tomar acciones posteriores.

Se deben considerar los objetivos de la organización y el grado de oportunidad que pudiera resultar de asumir el riesgo.

Las decisiones deben dar cuenta del contexto más amplio del riesgo e incluir la consideración de la tolerabilidad de los riesgos asumidos por partes diferentes de la organización que se beneficia de ella.

Si los riesgos resultantes se encuentran en las categorías de riesgo bajo o aceptable, pueden aceptarse con mínimo tratamiento posterior. Los riesgos bajos y aceptados deben monitorearse y revisarse periódicamente para garantizar que siguen siendo aceptables.

Si los riesgos no entran en la categoría de riesgo bajo o aceptable, deben tratarse empleando una o más de las opciones consideradas en el numeral 4.5.

4.5 TRATAMIENTO DEL RIESGO

El tratamiento del riesgo incluye la identificación de la gama de opciones para tratar el riesgo, la evaluación de dichas opciones, la preparación de planes para el tratamiento del riesgo y su implementación.

4.5.1 Identificación de opciones para el tratamiento del riesgo

La Figura 4.2 ilustra el proceso del tratamiento del riesgo. Entre las opciones, que no necesariamente son mutuamente excluyentes o apropiadas en todas las circunstancias, se encuentran las siguientes:

a) No afrontar el riesgo, al decidir no proceder con la actividad que tiene posibilidad de generar riesgo (siempre que esto sea aplicable).

   Puede ocurrir que el riesgo no se enfrente debido a una actitud de aversión hacia él, la cual es una tendencia de muchas personas (con frecuencia influenciadas por un sistema interno de una organización). El hecho de no afrontar el riesgo puede incrementar la importancia de otros riesgos.

   La aversión al riesgo conlleva a:

   i) decisiones para evitar o ignorar los riesgos sin importar la información disponible y los costos incurridos en el tratamiento de tales riesgos.

ii) error en el tratamiento del riesgo;

iii) dejar opciones críticas y/o decisiones en otras partes;

iv) aplazar decisiones que la organización no puede evitar; o

v) seleccionar una opción por que representa un riesgo potencial más bajo sin importar los beneficios.

b) Reducir la posibilidad de la ocurrencia

NOTA En el Anexo G se muestran algunos ejemplos.

c) Reducir las consecuencias

NOTA En el Anexo G se muestran algunos ejemplos.

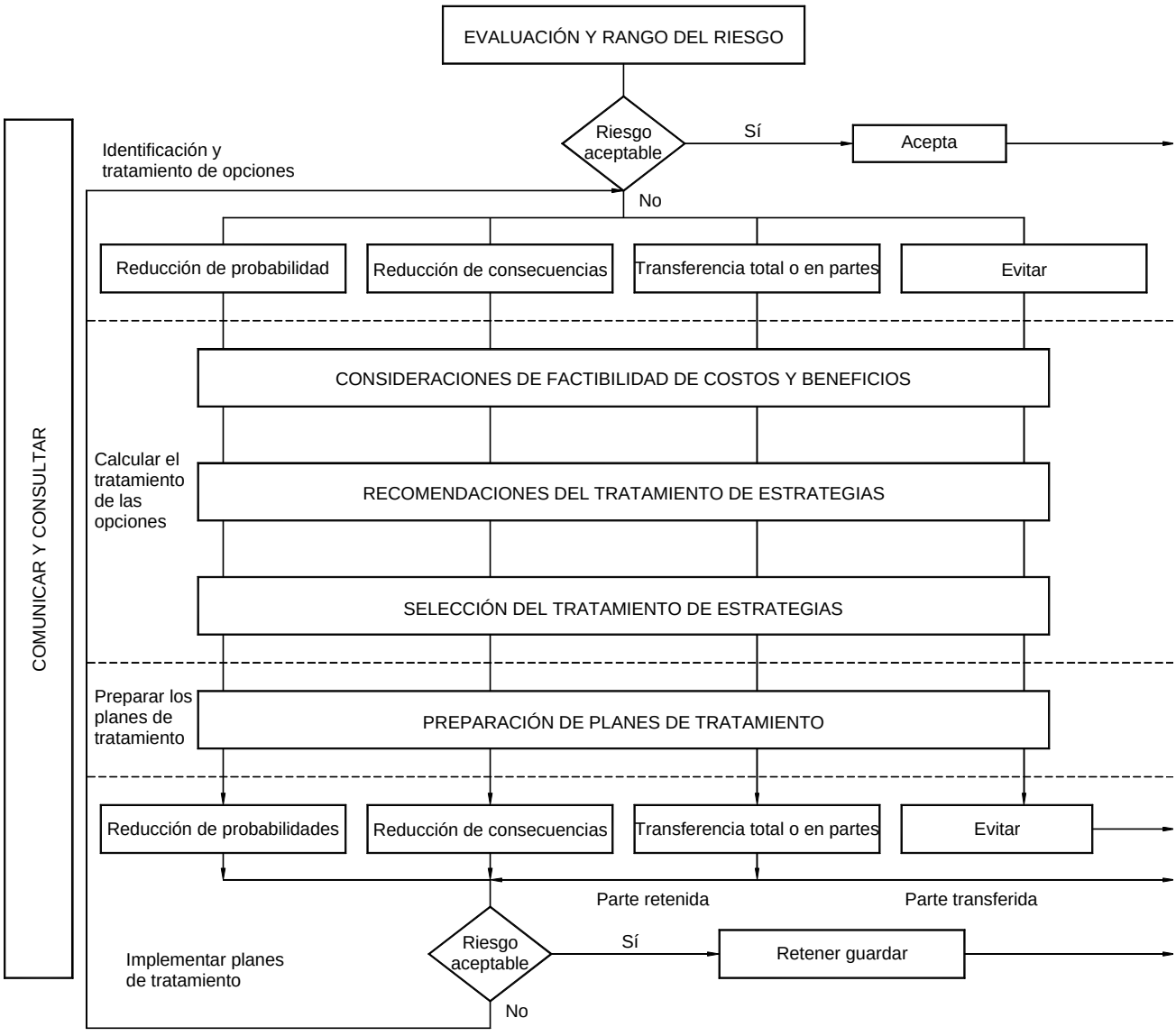

Figura 4.2. Proceso de tratamiento del riesgo

d) Transferir el riesgo

Aquí participa otra parte que asume o comparte algún porcentaje del riesgo. Entre los mecanismos para esto se encuentran el uso de contratos, acuerdos de seguros y estructuras organizacionales tales como sociedades o alianzas estratégicas (*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 es posible que no disminuya el nivel general de riesgo para la sociedad.

Cuando los riesgos se transfieren en su totalidad o parcialmente, la organización que transfiere el riesgo ha adquirido un nuevo riesgo: el de que la organización a la cual le ha transferido el riesgo no pueda manejarlo en forma efectiva.

e) Retener el riesgo

Después de haber reducido o transferido los riesgos, puede haber riesgos residuales que se han retenido. Es recomendable implementar planes para manejar las consecuencias de estos riesgos, si ocurrieran, incluida la identificación de un medio de financiación del riesgo. Los riesgos también pueden retenerse por defecto, es decir, cuando existe fracaso en la identificación y/o transferencia apropiada u otro tratamiento de estos.

Se puede hacer referencia a la reducción de las consecuencias y a la posibilidad, como control del riesgo. El control del riesgo incluye la determinación del beneficio relativo de nuevos controles a la luz de la eficacia de los controles existentes. Los controles pueden incorporar políticas sobre eficacia, procedimientos o cambios físicos.

4.5.2 Evaluación de opciones de tratamiento de riesgo

Se aconseja evaluar las opciones sobre la base del grado de reducción del riesgo y el alcance de cualquier beneficio adicional u oportunidades creadas, tomando en cuenta los criterios desarrollados en el numeral 4.1.5. Se pueden considerar varias opciones y aplicarse ya sea de forma individual o en combinación.

La selección de la opción más apropiada incluye el equilibrio del costo de la implementación de cada opción contra los beneficios derivados de ella. En general, el costo de la gestión de riesgos debe ser proporcional a los beneficios obtenidos.

Cuando exista la posibilidad de obtener grandes reducciones con gasto relativamente menor, tales opciones deben implementarse. Otras opciones de mejora pueden resultar costosas y se deben considerar con buen criterio para determinar si son justificables. En la Figura 4.3 se ilustra este aspecto.

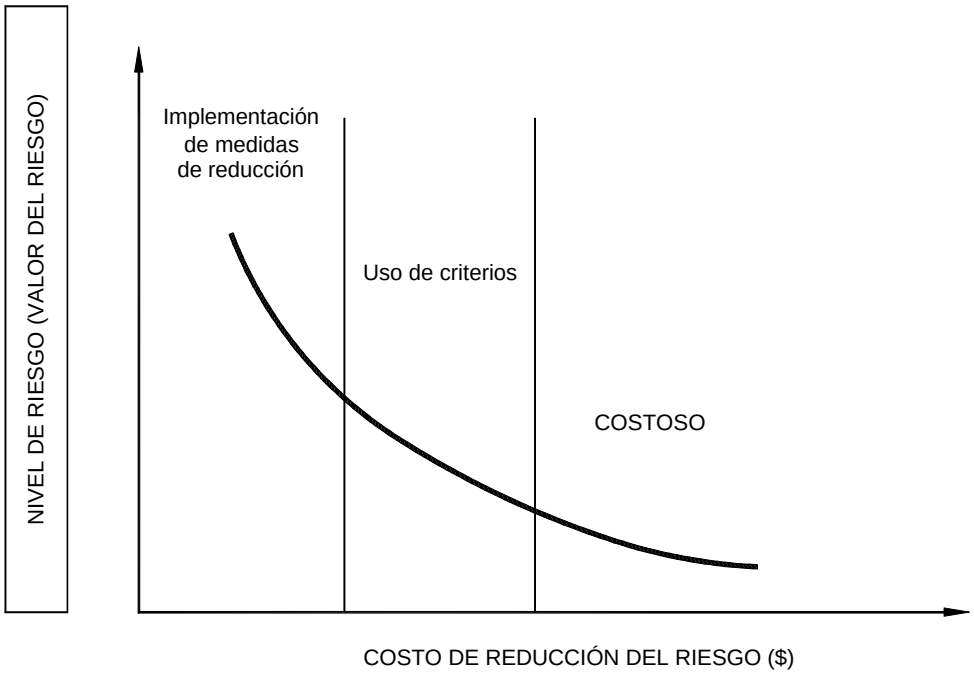

Figura 4.3. Costo de las medidas de reducción del riesgo

Al tomar decisiones se debe tener en cuenta la necesidad de considerar cuidadosamente riesgos raros pero graves, los cuales podrían ameritar medidas de reducción de riesgo que nos son justificables desde un punto de vista estrictamente económico.

En general, el impacto adverso del riesgo debe disminuirse en la medida razonablemente posible, independientemente de cualquier criterio absoluto.

Si el nivel del riesgo es alto, pero pueden surgir oportunidades considerables al asumirlo, tal como el uso de una nueva tecnología, entonces la aceptación del riesgo debe basarse en la valoración de los costos del tratamiento del riesgo y los costos de rectificación de las consecuencias potenciales contra las oportunidades que se presentan al asumir el riesgo.

En muchos casos, resulta improbable que cualquier opción de tratamiento del riesgo sea una solución completa para un problema particular. Con frecuencia, la organización se beneficiará en forma sustancial de una combinación de opciones tales como la reducción de la posibilidad de riesgos, la reducción de sus consecuencias y las transferencias o retención de cualquier riesgo residual. Un ejemplo lo constituye el uso efectivo de contratos y financiación del riesgo apoyados en un programa de reducción del riesgo.

Cuando el costo acumulativo de la implementación de los tratamientos del riesgo excede el presupuesto disponible, el plan debe identificar claramente el orden de prioridad en el cual deben implementarse los tratamientos de riesgo individuales. El orden de prioridad puede establecerse empleando varias técnicas, incluida la clasificación del riesgo y el análisis costo-beneficio. Los tratamientos de riesgo que no pueden implementarse dentro del límite del presupuesto disponible, deben esperar la disponibilidad de recursos financieros adicionales, o, si por cualquier razón, uno o todos los tratamientos restantes se consideran importantes debe realizarse alguna acción para asegurar finanzas adicionales.

En las opciones del tratamiento del riesgo se debe considerar la forma como perciben el riesgo las partes afectadas y las formas más apropiadas de comunicarlas a esas partes.

4.5.3 Preparación de planes de tratamiento

En los planes se debe documentar la forma como se deben implementar las opciones seleccionadas.

El plan de tratamiento debe identificar responsabilidades, cronogramas, el resultado esperado de los tratamientos, el presupuesto, las medidas de desempeño y el proceso de revisión por implementar.

NOTA Para tener detalles, véase la Sección H.5, Anexo H.

El plan también debe incluir un mecanismo para evaluar la implementación de las opciones contra los criterios de desempeño, responsabilidades individuales y otros objetivos, y monitorear acontecimientos importantes en donde la implementación del plan sea crítica.

4.5.4 Implementación de planes de tratamiento

De manera ideal, las partes con mayor capacidad para controlar el riesgo deben asumir la responsabilidad del tratamiento del mismo. Se deben acordar las responsabilidades entre las partes, lo más temprano posible.

La implementación exitosa del plan de tratamiento del riesgo requiere un sistema de gestión eficaz que especifique los métodos seleccionados, asigne responsabilidades y obligaciones de reporte individuales con respecto a acciones y las monitoree contra criterios especificados.

Si después del tratamiento existe un riesgo residual, debe tomarse una decisión en cuanto a retenerlo o repetir su proceso de tratamiento.

4.6 MONITOREO Y REVISIÓN

Es necesario monitorear los riesgos, la eficacia del plan de tratamiento del riesgo, las estrategias y el sistema de gestión que se establecen para controlar la implementación. Deben monitorearse los riesgos y la eficacia de las medidas de control a fin de garantizar que las circunstancias cambiantes no alteren las prioridades del riesgo. Pocos riesgos permanecen estáticos.

Resulta esencial la revisión permanente para asegurarse de que el plan de gestión continúa siendo pertinente. Los factores que pueden afectar la posibilidad y las consecuencias de un resultado pueden cambiar, al igual que los factores que afectan la conveniencia o el costo de las diferentes opciones de tratamiento. Por consiguiente, es necesario repetir regularmente el ciclo de gestión del riesgo. La revisión es una parte integral del plan de tratamiento de gestión del riesgo.

4.7 COMUNICACIÓN Y CONSULTA

La comunicación y la consulta constituyen una consideración importante en cada paso del proceso de gestión del riesgo. Resulta primordial desarrollar un plan de comunicación tanto para las partes interesadas internas como para las externas en la etapa más temprana del proceso. Este plan debe tratar asuntos relacionados tanto con el riesgo mismo como con el proceso para gestionarlo.

La comunicación y consulta incluyen un diálogo bilateral entre las partes interesadas, y los esfuerzos se deben centrar en la consulta, más que en un flujo unilateral de información proveniente de quien toma las decisiones hacia las otras partes interesadas.

La comunicación interna y externa efectiva es importante para garantizar que quienes son responsables de implementar la gestión del riesgo y quienes tienen un interés creado comprendan la base sobre la cual se toman decisiones y por qué se requieren acciones particulares.

Las percepciones del riesgo pueden variar debido a la diferencia en las creencias y conceptos y las necesidades, asuntos y preocupaciones de las partes interesadas, en la medida en que se relacionan con el riesgo u otros asuntos bajo discusión. Es probable que las partes interesadas realicen juicios acerca de la aceptabilidad de un riesgo con base en su percepción de éste. Puesto que las partes interesadas pueden tener un impacto significativo en las decisiones tomadas, resulta primordial que se identifiquen y documenten sus percepciones del riesgo, lo mismo que sus percepciones de los beneficios, y que se entiendan y traten las razones subyacentes.

5. DOCUMENTACIÓN

5.1 GENERALIDADES

Cada etapa del proceso de gestión del riesgo se debe documentar. La documentación debe incluir las creencias, métodos, fuentes de datos y resultados.

5.2 RAZONES PARA LA DOCUMENTACIÓN

Las razones para la documentación son las siguientes:

a) demostrar que el proceso se realiza en forma apropiada;

b) proporcionar evidencia de un enfoque sistemático para la identificación y análisis del riesgo;

c) ofrecer un registro de los riesgos y desarrollar la base de datos del conocimiento de la organización

d) proporcionar un plan de gestión del riesgo a las personas encargadas de la toma decisiones pertinentes, para su aprobación y posterior implementación.

e) proporcionar un mecanismo y herramienta de responsabilidad

f) facilitar el monitoreo y la revisión continuos

g) ofrecer un rastro o registro de auditoría y

h) compartir y comunicar la información.

Las decisiones concernientes al alcance de la documentación pueden incluir costos y beneficios y deben tomar en cuenta los factores arriba mencionados.

Orientación: En el Anexo H se presentan algunos ejemplos que son útiles y ofrecen orientación acerca de la documentación apropiada. Estos ejemplos son indicativos más que globales.

ANEXO A
(Informativo)

APLICACIONES DE LA GESTIÓN DEL RIESGO

A.1 ORGANIZACIONES

Esta norma puede aplicarse a una amplia gama de organizaciones, que incluyen:

a) públicas:

- nacionales, regionales, locales

b) comerciales:

- empresas, alianzas estratégicas, firmas, franquicias, prácticas aisladas y

c) voluntarias:

- entidades de beneficencia, sociales y deportivas

A.2 APLICACIONES

La norma tiene una serie de aplicaciones, que incluyen (aunque no exclusivamente):

i) gestión de activos y planeación de recursos;

ii) riesgos de continuidad de negocio;

iii) cambio: organizacional, tecnológico y político;

iv) actividad de construcción;

v) planeamiento de contingencia para emergencias y desastres.

vi) diseño y responsabilidad por el producto;

vii) responsabilidad del director y los funcionarios;

viii) procedimientos de selección de personal, entrenamiento, discriminación y hostigamiento;

ix) asuntos ambientales;

x) asuntos de ética y honradez;

xi) estudios de factibilidad;

xii) detección de incendio /prevención de incendio;

xiii) operaciones de divisas;

xiv) prevención, detección y manejo de fraude;

xv) salud humana, animal y vegetal

xvi) sistemas de información / redes de computación

xvii) inversiones;

xviii) cumplimiento legal;

xix) salud ocupacional y seguridad industrial ;

xx) operaciones y sistemas de mantenimiento;

xxi) gestión de proyectos;

xxii) riesgo público y responsabilidad general;

xxiii) gestión de contratación de compras;

xxiv) asesoría profesional;

xxv) asuntos de reputación e imagen;

xxvi) seguridad;

xxvii) transporte aéreo, marítimo, por carretera y ferrocarril;

xxviii) tesorería y finanzas.

ANEXO B
(Informativo)

PASOS EN EL DESARROLLO E IMPLEMENTACIÓN DE UN PROGRAMA DE GESTIÓN DEL RIESGO

PASO 1. RESPALDO DE LA ALTA DIRECCIÓN

Consiste en el desarrollo de una filosofía de gestión del riesgo organizacional y toma de conciencia del "riesgo" en los niveles de la alta dirección. Esto podría facilitarse mediante formación, educación e instrucciones de la dirección ejecutiva.

- Es necesario el respaldo continuo de la alta dirección
- Un director ejecutivo de alto rango o "líder" similar (o equipo) debe patrocinar la iniciativa.
- Toda la alta dirección debe brindar pleno respaldo.

PASO 2. DESARROLLO DE LA POLÍTICA DE LA ORGANIZACIÓN

Comprende el desarrollo y documentación de una política corporativa y una estructura para gestionar los riesgos, que tenga el respaldo de la alta dirección y sea implementada en toda la organización. La política puede incluir información tal como:

- Los objetivos para la política y fundamentos para la gestión del riesgo;
- los enlaces entre la política y el plan corporativo o estratégico de la organización;
- el alcance o gama de asuntos a los que se aplica la política;
- orientación sobre lo que puede ser considerado como riesgo aceptable;
- quién es el responsable de la gestión del riesgo;
- el apoyo/pericia con que se cuenta para asesorar a los responsables de la gestión del riesgo;
- el nivel de documentación requerida, y
- el plan para revisión del desempeño organizacional con respecto a la política.

PASO 3. COMUNICACIÓN DE LAS POLÍTICAS

Abarca el desarrollo, establecimiento e implementación de una infraestructura o disposiciones que aseguren que el manejo del riesgo llegue a ser una parte integral de la planeación, los procesos de gestión y, en general, de la cultura organizacional. Esto puede incluir:

- Conformación de un equipo que contenga personal de la alta dirección, que sea responsable de las comunicaciones internas acerca de la política.

- Promover la toma de conciencia acerca de la gestión del riesgo.

- Comunicación/diálogo en toda la organización sobre la gestión del riesgo y la política de la organización.

- Adquirir habilidades en gestión del riesgo, por ejemplo por medio de consultores y desarrollando experiencia mediante entrenamiento y educación.

- Asegurar niveles apropiados de reconocimiento, recompensas y sanciones, y

- Establecimiento de procesos de gestión de desempeño.

PASO 4. GESTIÓN DEL RIESGO A ESCALA ORGANIZACIONAL

Comprende el desarrollo y establecimiento de un programa de gestión del riesgo a escala organizacional, mediante la aplicación de un sistema de gestión, de acuerdo con los lineamientos del numeral 2 de la norma. El proceso para la gestión del riesgo debe estar integrado con la planeación estratégica y procesos de gestión de la organización, y debe tener la siguiente documentación:

- el contexto de la organización y de la gestión del riesgo;

- identificación de riesgos para la organización;

- el análisis y evaluación de los riesgos;

- estrategias de tratamiento;

- mecanismos de revisión del programa;

- estrategias que fomenten la toma de conciencia, adquisición de experiencia, formación y educación.

PASO 5. GESTIÓN DE RIESGOS EN LOS NIVELES DE PROGRAMA, PROYECTO Y DE EQUIPO

Comprende el desarrollo y establecimiento de un programa de gestión del riesgo en la organización, para cada subárea organizacional, programa, proyecto o actividades de equipo, por medio de la aplicación del proceso de gestión del riesgo de acuerdo con el numeral 4. El proceso de gestión del riesgo se debe integrar con otras actividades de planeación y gestión. Es conveniente documentar los procesos seguidos, las decisiones tomadas y las acciones planeadas.

PASO 6. MONITOREO Y REVISIÓN

Desarrollar y aplicar mecanismos que aseguren la revisión continua de los riesgos. Esto asegurará que la implementación y la política de gestión del riesgo mantengan su pertinencia, a medida que las circunstancias cambian con el tiempo y se hace vital revisar las decisiones previas. Los riesgos no son estáticos. La efectividad del proceso de gestión del riesgo debe ser revisada y monitoreada.

ANEXO C
(Informativo)

PARTES INTERESADAS

Las partes interesadas son los individuos que se ven o se perciben como afectados por una decisión o actividad. Entre ellos se pueden incluir:

- individuos al interior de la organización, tales como empleados, la dirección, gerentes y voluntarios.
- las personas que toman decisiones;
- empresas o contrapartes comerciales;
- grupos de empleados;
- grupos de sindicatos;
- instituciones financieras;
- organizaciones de seguros;
- reguladores y otras organizaciones gubernamentales que tienen autoridad sobre actividades;
- políticos (en todos los niveles del gobierno) que tienen un interés electoral o en el portafolio.
- organizaciones no gubernamentales, tales como grupos medioambientales y de interés público;
- clientes;
- proveedores, incluidos los de servicios, y los contratistas para la ejecución de actividades;
- los medios, quienes son partes interesadas potenciales y conductos de información para otras partes interesadas;
- individuos o grupos que estén interesados en asuntos relacionados con la propuesta;
- comunidades locales, y
- la sociedad en conjunto

Con el tiempo, la mezcla de partes interesadas puede cambiar. Se pueden unir nuevas partes interesadas y desear participar en cualquier aspecto, mientras que otras pueden interrumpir su participación en el proceso. Por consiguiente, el proceso de análisis de las partes interesadas debe ser continuo y, como tal, debe ser una parte integral del proceso de gestión del riesgo.

El nivel de interés de la parte interesada puede cambiar en respuesta a nueva información, ya sea porque se han resuelto las necesidades y preocupaciones de las partes interesadas, o porque la nueva información tiende a crear nuevas necesidades, problemas o preocupaciones. Nótese también que diferentes partes interesadas pueden tener diferentes opiniones y diferentes niveles de conocimiento con respecto a un asunto particular.

ANEXO D
(Informativo)

FUENTES GENÉRICAS DE RIESGO Y SUS ÁREAS DE IMPACTO

D.1 GENERALIDADES

La identificación de fuentes de riesgo y áreas de impacto ofrece un marco para la identificación y análisis de riesgo. El desarrollo de una lista genérica enfoca las actividades de identificación del riesgo y contribuye a hacer más efectiva la gestión, debido a la gran cantidad posible de fuentes e impactos.

Las fuentes genéricas de riesgo y áreas de impacto se seleccionan de acuerdo con su pertinencia en las actividades estudiadas (véanse los numerales 4.1.1 y 4.2.2). Los componentes de cada categoría genérica pueden formar las bases para el estudio de los riesgos.

D.2 FUENTES DE RIESGO

Cada fuente genérica tiene numerosos componentes, cualquiera de los cuales puede dar origen a un riesgo. Algunos componentes estarán bajo el control de la organización que conduce el estudio, mientras que otros pueden estar por fuera de su control. Ambos tipos deben considerarse al identificar los riesgos. Entre las fuentes genéricas de riesgo se encuentran:

a) relaciones legales y comerciales al interior de la organización y con otras organizaciones, por ejemplo proveedores, subcontratistas, arrendatarios.;

b) circunstancias económicas y de mercado, organizacionales, nacionales, e internacionales, así como factores que contribuyen a estas circunstancias, por ejemplo tasas de cambio;

c) comportamiento humano de quienes están involucrados en la organización y de quienes no lo están;

d) eventos naturales;

e) circunstancias políticas: cambios legislativos y factores sociales que pueden influenciar otras fuentes de riesgo;

f) tecnología y asuntos técnicos, tanto internos como externos, de la organización;

g) actividades de gestión y control;

h) Actividades individuales.

D.3 ÁREAS DE IMPACTO

El análisis de riesgo puede concentrarse en una sola área de impacto o en varias áreas de impacto posibles.

Las siguientes son áreas de impacto:

a) base de activos y recursos de la organización incluido el personal;

b) Ingresos y derechos;

c) costos de actividades, tanto directos como indirectos;

d) gente;

e) comunidad;

f) desempeño;

g) el momento y programación de las actividades;

g) medio ambiente;

h) intangibles: reputación, buen nombre, calidad de vida;

i) comportamiento organizacional.

D.4 IDENTIFICACIÓN DE RIESGOS

Un método para resumir la forma como surge el riesgo en una organización consiste en utilizar una plantilla de identificación del riesgo como la mostrada en la Tabla D1. Las entradas pueden hacerse con señales para mostrar en dónde ocurren los riesgos, o con notas descriptivas más detalladas.

D.5 OTRAS CLASIFICACIÓN DE RIESGOS

Las diferentes disciplinas categorizan, frecuentemente, fuentes de riesgo de otra forma a partir de términos semejantes, como peligro o exposición al riesgo. Esas clasificaciones pueden ser subconjuntos de las fuentes de riesgo de la lista D.2 anterior.

EJEMPLOS:

a) Enfermedades, afecciones humanas, de animales y plantas;

b) económicas: fluctuaciones del dinero, tasas de interés, participación en el mercado;

c) medioambientales: ruido y contaminación;

d) financiero: riesgos contractuales, fraudes, malversación de fondos y multas;

e) humanos: disturbios, ataques, sabotajes y errores

f) riesgos naturales: condiciones climáticas, terremotos, incendios forestales, inundaciones, plagas y actividad volcánica;

g) salud ocupacional y seguridad: medidas inadecuadas de seguridad, deficiente gestión de seguridad;

h) responsabilidad de un producto: error de diseño, control de calidad por debajo de la norma, ensayos inadecuados;

i) responsabilidad profesional: mala asesoría, error de diseño, negligencia;

j) daños en la propiedad: incendio, terremotos, inundaciones, contaminación, errores humanos;

k) responsabilidad pública: ingreso y egreso de publico, y seguridad;

l) seguridad: disposición del dinero, vandalismo, robo, uso ilegal de la información, entrada ilegal;

m) tecnológica: innovación, obsolescencia, explosiones y seguridad de funcionamiento.

NOTA Los literales anteriores se citan como ejemplo.

Tabla D.1. Ejemplo de formato para identificación de fuentes de riesgo

	Área de impacto					
	Seleccione según sea aplicable de acuerdo con el literal D.3					
Fuentes de riesgo	#	#	#	#	#	#
Relaciones comerciales y legales						
Económicas						
Comportamiento humano						
Eventos naturales						
Circunstancias políticas						
Tecnológicas/asuntos técnicos						
Actividades de gestión y controles						
Actividades individuales						
NOTA Las fuentes de riesgo y las áreas de impacto se deberían adaptar a cada organización o actividad.						

ANEXO E
(Informativo)

EJEMPLOS DE DEFINICIÓN DE RIESGO Y CLASIFICACIÓN

Tabla E.1. Medidas cualitativas de la consecuencia o impacto

Nivel	descriptor	Descripción detallada de ejemplo
1	Insignificante	Ningún daño, perdidas financieras pequeñas
2	Menor	Tratamiento de primeros auxilios, las descargas en el sitio son contenidas inmediatamente, medianas pérdidas financieras,
3	Moderada	Requiere tratamiento médico, las descargas en el sitio son contenidas con ayuda externa, pérdidas financieras altas.
4	Mayor	Lesiones grandes, pérdida de la capacidad de producción, descargas fuera del sitio sin efectos perjudiciales, pérdida financiera importante.
5	catastrófica	Muerte, liberación de tóxicos fuera del sitio con efecto perjudicial, enorme pérdida financiera.
NOTA Las medidas tomadas deberían reflejar las necesidades y naturaleza de la organización y actividades bajo estudio.		

Tabla E.2. Medidas cualitativas de las posibilidades

Nivel	Descriptor	Descripción
A	Casi cierto	Se espera que ocurra en la mayoría de las circunstancias.
B	Probable	Puede probablemente ocurrir en la mayoría de las circunstancias.
C	Posible	Es posible que ocurra en algunas veces.
D	Improbable	Podría ocurrir en algunas veces.
E	Raro	Puede ocurrir solamente en circunstancias excepcionales.
NOTA Las tablas necesitan ajustarse para satisfacer las necesidades individuales de la organización.		

Tabla E.3. Matriz de análisis cualitativo de riesgos. Nivel de riesgos

Probabilidad	Consecuencias				
	Insignificante 1	Menor 2	Moderada 3	Mayor 4	Catastrófica 5
A (casi cierto)	H	H	E	E	E
B (probable)	M	H	H	E	E
C (posible)	L	M	H	E	E
D (improbable)	L	L	M	M	E
E (Raro)	L	L	M	H	H

NOTA El número de categorías debe reflejar las necesidades del estudio

Convenciones:

E = Riesgo extremo, se requiere acción inmediata.

H = Alto riesgo, es necesario la atención del director.

M = Riesgo moderado, se debe especificar la responsabilidad de la dirección.

L = riesgo inferior, gestionar mediante procedimientos de rutina.

ANEXO F
(Informativo)

EJEMPLOS DE EXPRESIONES CUANTITATIVAS DE RIESGO

F.1 RIESGO DE PÉRDIDA O GANANCIA FINANCIERA

Las pérdidas (o ganancias) financieras multiplicadas por la frecuencia anual de pérdidas (o ganancias) dan el valor esperado en dólares por año.

F.2 RIESGO DE FATALIDAD

El riesgo de fatalidad de una actividad puede ser calculado como:

$$\frac{\text{Número de muertes por año en una actividad}}{\text{Población expuesta}}$$

F.3 DESASTRES NATURALES–OCASIONADOS POR EL HOMBRE

Las consecuencias se pueden modelar usando simuladores de computador y probabilidades estimadas a partir de datos históricos, árboles de fallas u otras técnicas de ingeniería de sistemas.

F.4 RIESGOS DE SALUD

Los riesgos de salud se expresan comúnmente de las siguientes maneras:

a) el número de casos de salud-enfermedad por año, en una población expuesta, comparada con el total de esa población, es decir, cinco nuevos casos en una población expuesta de 100 000, es un riesgo de 5×10^{-5} por persona expuesta, por año;

b) la proporción de la probabilidad de muertes antes una cierta edad, con y sin exposición;

c) el número de fatalidades a la edad de 70 años, que se espera como consecuencia de una exposición, dividido por el numero de personas expuestas.

Los riesgos de salud se pueden derivar de datos epidemiológicos (encuestas de población de fatalidades o enfermedad) o de una base de datos experimental basada en estudios en animales.

NOTA En vez de calcular el valor promedio de un riesgo, se puede calcular la distribución de los valores posibles remplazando los valores promedio de las variables de las que depende el resultado, por las distribuciones apropiadas de los valores.

ANEXO G
(Informativo)

IDENTIFICACIÓN DE OPCIONES PARA EL TRATAMIENTO DEL RIESGO

G.1 ACCIONES PARA REDUCIR O CONTROLAR LA POSIBILIDAD

Estas pueden incluir:

i) auditoría y programas de verificación de cumplimiento;

ii) condiciones contractuales;

iii) revisión formal de requisitos, especificaciones, diseño, ingeniería y operaciones;

iv) inspección y procesos de control;

v) inversiones y gestión de portafolios;

vi) gestión de proyectos;

vii) mantenimiento preventivo;

viii) aseguramiento de la calidad, gestión y normalización;

ix) investigación y desarrollo, desarrollo tecnológico;

x) formación estructurada y otros programas;

xi) supervisión;

xii) ensayos;

xiii) disposiciones organizacionales;

xiv) técnicas de control;

G.2 PROCEDIMIENTOS DE REDUCCIÓN O CONTROL DE CONSECUENCIAS

Estos pueden incluir:

i) planes de contingencia,

ii) arreglos contractuales,

iii) condiciones contractuales,

iv) características de diseño,

v) planes de recuperación de desastres,

vi) barreras estructurales y de ingeniería,

vii) planeación de control de fraudes,

viii) reducción de exposición a fuentes de riesgo,

ix) planeación del portafolio,

x) políticas y control de precios,

xi) separación o reubicación de una actividad y recursos,

xii) relaciones públicas,

xiii) pagos ex gratia (discrecionales).

ANEXO H
(Informativo)

DOCUMENTACIÓN DE GESTIÓN DEL RIESGO

Para gestionar el riesgo correctamente se requiere documentación apropiada, que debe ser la suficiente para satisfacer auditorías independientes. Las decisiones concernientes a la extensión de la documentación pueden involucrar costos y beneficios que deben tener en cuenta los factores relacionados en el numeral 5.2. La declaración de la política de gestión del riesgo debe definir la documentación necesaria.

En cada estado del proceso, la documentación debe incluir:

a) objetivos,

b) fuentes de información,

c) suposiciones y

d) decisiones.

Este Anexo H incluye un ejemplo de un registro del riesgo, un cronograma de tratamiento y un plan de acción. Es posible que se requieran planes más específicos y detallados para áreas de alto riesgo.

H.2 POLÍTICA

En el Anexo B se presentan ejemplos de información los cuales pueden ser incluidos en la declaración de las políticas de una organización.

H.3 CONFORMIDAD Y DECLARACIÓN DE DEBIDA DILIGENCIA

En algunas circunstancias, se puede requerir una declaración de conformidad y de debida diligencia, de modo que los gerentes reconozcan formalmente su responsabilidad en el cumplimiento de las políticas y procedimientos de gestión del riesgo

H.4 REGISTRO DEL RIESGO

Para cada riesgo identificado, se lleva un registro del riesgo que incluya:

a) fuente,

b) naturaleza,

c) controles existentes,

d) consecuencias y posibilidad,

e) clasificación del riesgo inicial, y

f) vulnerabilidad a factores internos o externos.

Véase el formato (pro forma) que se presenta a continuación, a manera de guía:

H.5 PROGRAMA DEL TRATAMIENTO DEL RIESGO Y PLANES DE ACCIÓN

Un plan de tratamiento del riesgo y de acción documenta los controles por adoptar y enuncia la siguiente información:

a) quién es el responsable de la implementación del plan;

b) qué recursos se van a utilizar;

c) distribución del presupuesto;

d) cronograma para la implementación;

e) detalles del mecanismo y frecuencia de revisión del cumplimiento con el plan de tratamiento.

H.6 DOCUMENTOS DE MONITOREO Y AUDITORÍA

Los registros de monitoreo y auditoría deben documentar:

a) detalles del mecanismo y la frecuencia de revisión de riesgos y el proceso de gestión del riesgo en conjunto;

b) los resultados de las auditorias y otros procedimientos de monitoreo;

c) detalles de cómo se siguen e implementan las recomendaciones de revisión.

REGISTRO DE RIESGO

Fecha de revisión del riesgo
Compilado por.....Fecha.....
Función/Actividad..... Revisado por.....Fecha

REF.	EL RIESGO: QUÉ PUEDE OCURRIR Y CÓMO PUEDE OCURRIR	LAS CONSECUENCIAS DE QUE OCURRA UN EVENTO		SUFICIENCIA DE LOS CONTROLES EXISTENTES	CLASIFICACIÓN DE LA CONSECUENCIA	CLASIFICACIÓN DE LA POSIBILIDAD	NIVEL DE RIESGO	PRIORIDAD DE RIESGO
		CONSECUENCIAS	POSIBILIDAD					

CRONOGRAMA Y PLAN DE TRATAMIENTO DEL RIESGO

Fecha de revisión del riesgo
Compilado por.....Fecha.....
Función/Actividad..... Revisado por.....Fecha

RIESGO EN ORDEN DE PRIORIDAD, DE ACUERDO CON EL REGISTRO DE RIESGO	POSIBLES OPCIONES DE TRATAMIENTO	OPCIONES PREFERIDAS	CLASIFICACIÓN DEL RIESGO DESPUÉS DEL TRATAMIENTO	RESULTADO DEL ANÁLISIS COSTO BENEFICIO: A: ACEPTAR B: RECHAZAR	PERSONA RESPONSABLE PARA IMPLEMENTACIÓN DE OPCIÓN	CRONOGRAMA PARA IMPLEMENTACIÓN	COMO SE MONITOREARÁN ESTE RIESGO Y LAS OPCIONES DE TRATAMIENTO

PLAN DE ACCIÓN DE RIESGO

ELEMENTO RIESGO	Ref
Resumen - Respuesta recomendada e impacto	
Plan de acción 1. Acciones propuestas 2. Recursos requeridos 3.Responsabilidades 4.Cronograma 5.Reporte y monitoreo requeridos	
Responsable.....Fecha.....Revisar.....Fecha.....	

DOCUMENTO DE REFERENCIA

AUSTRALIAN STANDARDS. Risk Management, Sydney. AS, 1999, 45 p. (AS/NZS 4360:1999)