

# NORMA TÉCNICA COLOMBIANA

NTC  
31000

2011-02-16

## GESTIÓN DEL RIESGO. PRINCIPIOS DIRECTRICES



E: RISK MANAGEMENT. PRINCIPLES AND GUIDELINES

---

CORRESPONDENCIA: esta norma es una adopción idéntica (IDT) por traducción de la norma ISO 31000:2009.

---

DESCRIPTORES: gestión; riesgo; incertidumbre.

---

I.C.S.: 03.100.01

Editada por el Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC)  
Apartado 14237 Bogotá, D.C. - Tel. (571) 6078888 - Fax (571) 2221435

---

Prohibida su reproducción

Editada 2011-02-22

GESTIÓN DEL RIESGO 7

---

**8 GESTIÓN DEL RIESGO**

## PRÓLOGO

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

**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 norma NTC-ISO 31000 fue ratificada por el Consejo Directivo de 2011-02-16.

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 del riesgo.

AON COLOMBIA  
ASEGURADORES TÉCNICOS LTDA.  
BANCO AGRARIO DE COLOMBIA  
COMPAÑÍA NACIONAL DE CHOCOLATES S.A.  
CONCRETO S.A.  
CREDIBANCO VISA  
DELIMA MARSH S.A.  
DIRECCIÓN DE PREVENCIÓN Y ATENCIÓN DE EMERGENCIAS -DPAE-  
ECOPETROL S.A.  
EMPRESA DE ACUEDUCTO DE BOGOTÁ  
ERNEST & YOUNG COLOMBIA  
GIT LTDA.  
INDUSTRIAS SPRING S.A.  
ITEAM  
MINISTERIO DE MEDIO AMBIENTE Y DESARROLLO TERRITORIAL  
REDEBAN MULTICOLOR  
SEGURIDAD ATLAS  
SIKA COLOMBIA.  
TECNICONTROL S.A.

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

ADAMS CADBURY  
AEROVIAS DEL CONTINENTE AMERICANO S.A. -AVIANCA S.A.-  
AJOVER S.A.  
ALICO COLOMBIA SEGUROS DE VIDA S.A.  
ARP SEGUROS BOLÍVAR  
ASETRANS LTDA.  
ASOCIACION COLOMBIANA DE CONTINUIDAD DEL NEGOCIO  
ATESA S.A. E.S.P.  
CAJA DE COMPENSACIÓN FAMILIAR DE FENALCO - SECCIONAL QUINDÍO  
CAJAS Y SUPLEMENTOS  
CÁMARA DE COMERCIO DE BOGOTÁ  
CENTRO COMERCIAL CHIPICHAPE  
CHAIN VARGAS  
CHALLENGER S.A.  
CJE SUPPLIES LTDA.  
COLCHONES NUEVO MILENIO  
COMPAÑIA AGRÍCOLA DE SEGUROS DE VIDA S.A.  
COMPAÑIA DE SEGUROS BOLÍVAR S.A.  
COMPAÑIA MUNDIAL DE SEGUROS S.A.  
COMPUCABLES NUGER LTDA.  
CONCALIDAD LTDA.  
COOPERATIVA DE LOS TRABAJADORES DEL INSTITUTO DE SEGUROS SOCIALES  
CRUZ ROJA SECCIONAL CUNDINAMARCA Y BOGOTÁ  
DECEVAL S.A.  
DELOTTE COLOMBIA  
EMPRESA IBAGUEREÑA DE ACUEDUCTO Y ALCANTARILLADO  
EMPRESAS PÚBLICAS DE MEDELLÍN E.S.P.  
ENCLAN S.A.  
ENLACE OPERATIVO S.A.  
ESCUELA COLOMBIANA DE INGENIERÍA  
FENALCO  
FIDUCOLOMBIA S.A. SOCIEDAD FIDUCIARIA S.A.  
FUNDACIÓN UNIVERSITARIA AGRARIA DE COLOMBIA -ESPECIALIZACIÓN EN SISTEMAS  
DE GESTIÓN DE LA CALIDAD-  
GESCOP LTDA.  
GESTIÓN & ESTRATEGIA S.A.S.  
GRUPO ATLAS DE SEGURIDAD INTEGRAL  
HOSPITAL SANTA MARGARITA E.S.E.  
ILURAM S.A.  
INDUSTRIA FARMACÉUTICA SYNTOFARMA S.A.  
INFOCOMUNICACIONES LTDA.  
JARDINE LLOYD THOMPSON VALENCIA & IRAGORRI CORREDORES DE  
SEGUROS S.A.  
JM INGENIERÍA LTDA.  
KPMG  
LA PREVISORA S.A. COMPAÑÍA DE SEGUROS  
LINALCA S.A.  
MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.  
MATPEL DE COLOMBIA S.A.

---

## 10 GESTIÓN DEL RIESGO

MAUDT  
MEGALITE LTDA.  
MERCK S.A.  
MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO  
MINISTERIO DE TRANSPORTE  
MUNICIPIO DE MEDELLÍN - SECRETARÍA DE EVALUACIÓN Y CONTROL  
OCCIDENTAL DE COLOMBIA INC  
ORGANISMO NACIONAL DE ACREDITACIÓN DE COLOMBIA  
ORGANIZACIÓN TERPEL  
OVERSIGHT S.A.S. RISK CONSULTING & RISK MANAGEMENT SERVICES  
PARQUES Y FUNERARIA S.A. JARDINES DEL RECUERDO  
PÉREZ Y VILLA S.A.  
PETROTESTING COLOMBIA S.A.  
POLIPROPILENO DEL CARIBE S.A.  
POSITIVA COMPAÑÍA DE SEGUROS S.A.  
PROCESS CONSULTANTS, INC. SUCURSAL COLOMBIA -PCIB-  
PRODUCTORES DE SEGUROS DE ANTIOQUIA ANPROSEGUROS CORREDORES DE  
SEGUROS S.A.  
PROFESIONALES EN DEPORTE -PRODEPORT LTDA.-  
PROTECCIÓN  
PROTEGIENDO BFR S.A.  
REDES HUMANAS S.A.  
SEGUROS BOLÍVAR  
SEGUROS DE VIDA ALFA S.A.  
SEGUROS DE VIDA COLPATRÍA S.A.  
SERFUNORTE  
SERVICIO OCCIDENTAL DE SALUD S.A.  
SETELCOM LTDA.  
SIS S.A. SERVICIOS INTEGRALES DE SEGUROS Y SEGURIDAD SOCIAL  
SURATEP  
SURTIDORA DE GAS DEL CARIBE S.A. E.S.P.  
TEAM FOODS COLOMBIA S.A.  
TECFIN INTERNATIONAL S.A.  
TECSEGUROS S.A. CORREDORES DE SEGUROS  
TERPEL  
TOTAL SEGUROS CÍA. ASESORES DE SEGUROS LTDA.  
TRANSPORTADORA DE VALORES ATLAS  
UNIVERSIDAD SANTIAGO DE CALI  
VICEPRESIDENCIA DE RIESGOS LABORALES DEL INSTITUTO DE SEGUROS SOCIALES  
NIVEL NACIONAL BOGOTÁ D.C.  
WILLIS COLOMBIA CORREDORES DE SEGUROS S.A.

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

#### DIRECCIÓN DE NORMALIZACIÓN

GESTIÓN DEL RIESGO **11**

---

**12 GESTIÓN DEL RIESGO**

## CONTENIDO

	Página
INTRODUCCIÓN .....	15
1.    OBJETO .....	18
2.    TÉRMINOS Y DEFINICIONES .....	18
3.    PRINCIPIOS.....	24
4.    MARCO DE REFERENCIA.....	26
4.1    GENERALIDADES.....	26
4.2    DIRECCIÓN Y COMPROMISO .....	27
4.3    DISEÑO DEL MARCO DE REFERENCIA PARA LA GESTIÓN DEL RIESGO...	27
4.4    IMPLEMENTAR LA GESTIÓN DEL RIESGO.....	31
4.5    MONITOREAR Y REVISAR EL MARCO DE REFERENCIA.....	31
4.6    MEJORA CONTINUA DEL MARCO DE REFERENCIA .....	32
5.    PROCESO .....	32
5.1    GENERALIDADES.....	32
5.2    COMUNICACIÓN Y CONSULTA.....	32
5.3    ESTABLECIMIENTO DEL CONTEXTO.....	34
5.4    VALORACIÓN DEL RIESGO.....	37
5.5    TRATAMIENTO DEL RIESGO.....	39
5.6    MONITOREO Y REVISIÓN.....	41
5.7    REGISTRO DEL PROCESO PARA LA GESTIÓN DEL RIESGO .....	42

GESTIÓN DEL RIESGO **13**

	<b>Página</b>
<b>ANEXO A (Informativo)</b>	
ATRIBUTOS DE LA GESTIÓN MEJORADA DEL RIESGO .....	43
BIBLIOGRAFÍA.....	46
DOCUMENTO DE REFERENCIA.....	47

## **FIGURAS**

Figura 1. Relaciones entre los principios, el marco de referencia y los procesos para la gestión del riesgo .....	17
Figura 2. Relación entre los componentes del marco de referencia para la gestión del riesgo .....	26
Figura 3. Proceso para la gestión del riesgo .....	33

## GESTIÓN DEL RIESGO. PRINCIPIOS Y DIRETRICES

### INTRODUCCIÓN

Las organizaciones de todo tipo y tamaño enfrentan factores e influencias, internas y externas, que crean incertidumbre sobre si ellas lograrán o no sus objetivos. El efecto que esta incertidumbre tiene en los objetivos de una organización es el "riesgo".

Todas las actividades de una organización implican riesgo. Las organizaciones gestionan el riesgo mediante su identificación y análisis y luego evaluando si el riesgo se debería modificar por medio del tratamiento del riesgo con el fin de satisfacer los criterios del riesgo. A través de este proceso, las organizaciones se comunican y consultan con las partes involucradas, monitorean y revisan el riesgo y los controles que lo están modificando con el fin de garantizar que no se requiere tratamiento adicional del riesgo. Esta norma describe este proceso sistemático y lógico en detalle.

Aunque todas las organizaciones gestionan el riesgo en algún grado, esta norma establece un número de principios que es necesario satisfacer para hacer que la gestión del riesgo sea eficaz. Esta norma recomienda que las organizaciones desarrollen, implementen y mejoren continuamente un marco de referencia cuyo propósito sea integrar el proceso para la gestión del riesgo en los procesos globales de gobierno, estrategia y planificación, gestión, procesos de presentación de informes, políticas, valores y cultura de la organización.

La gestión del riesgo se puede aplicar a toda la organización, en todas sus muchas áreas y niveles, en cualquier momento, así como a funciones, proyectos y actividades específicos.

Aunque la práctica de la gestión del riesgo se ha desarrollado con el paso del tiempo y en muchos sectores para satisfacer diversas necesidades, la adopción de procesos consistentes dentro de un marco de referencia exhaustivo puede ayudar a garantizar que el riesgo se gestiona eficaz, eficiente y coherentemente en toda la organización. El enfoque genérico que se describe en esta norma suministra los principios y las directrices para la gestión de cualquier forma de riesgo en una manera sistemática, transparente y creíble, y en cualquier alcance y contexto.

Cada sector específico o cada aplicación de la gestión del riesgo traen consigo necesidades, audiencias, percepciones y criterios individuales. Por lo tanto, una característica clave de esta norma es la inclusión del "establecimiento del contexto" como una actividad al inicio

---

**NORMA TÉCNICA COLOMBIANA NTC-ISO 31000**

---

de este proceso genérico para la gestión del riesgo. Al establecer el contexto se capturaran los objetivos de la organización, el entorno en el cual ella persigue sus objetivos, sus partes involucradas y la diversidad de criterios de riesgo; todo en conjunto ayudará a revelar y evaluar la naturaleza y la complejidad de sus riesgos.

La relación entre los principios para la gestión del riesgo, el marco de referencia en el cual ésta sucede y los procesos de gestión del riesgo descritos aquí se ilustra en la Figura 1.

Cuando la gestión del riesgo se implementa y se mantiene de acuerdo con esta norma, dicha gestión le permite a la organización, entre otros:

- aumentar la probabilidad de alcanzar los objetivos;
- fomentar la gestión proactiva;
- ser consciente de la necesidad de identificar y tratar los riesgos en toda la organización;
- cumplir con los requisitos legales y reglamentarios pertinentes y con las normas internacionales;
- mejorar la presentación de informes obligatorios y voluntarios;
- mejorar el gobierno;
- mejorar la confianza y honestidad de las partes involucradas,
- establecer una base confiable para la toma de decisiones y la planificación;
- mejorar los controles;
- asignar y usar eficazmente los recursos para el tratamiento del riesgo;
- mejorar la eficacia y la eficiencia operativa;
- incrementar el desempeño de la salud y la seguridad, así como la protección ambiental;
- mejorar la prevención de pérdidas y la gestión de incidentes;
- minimizar las pérdidas;
- mejorar el aprendizaje organizacional; y
- mejorar la flexibilidad organizacional.

Esta norma está destinada a satisfacer las necesidades de un rango amplio de partes involucradas, incluyendo:

---

**16 GESTIÓN DEL RIESGO**

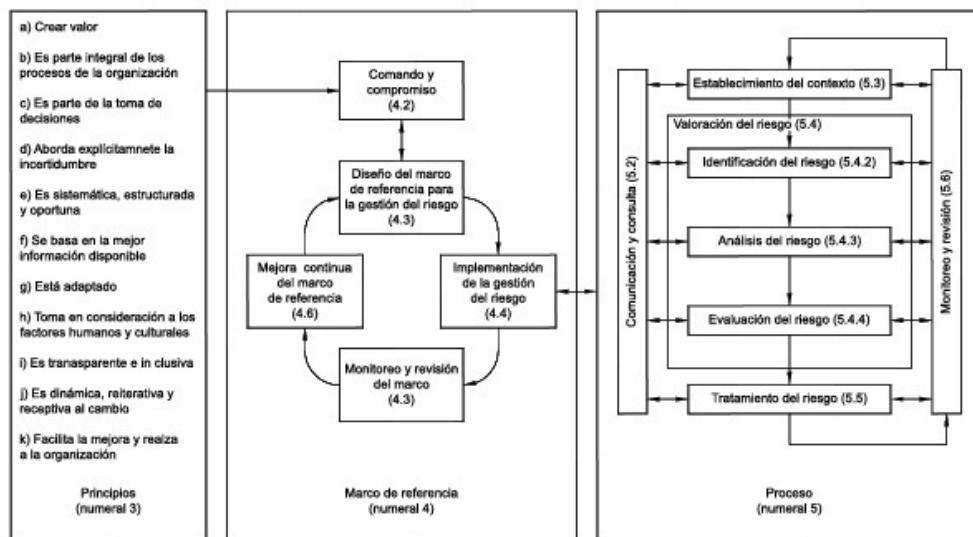
---

## NORMA TÉCNICA COLOMBIANA NTC-ISO 31000

- a) aquellos responsables del desarrollo de la política de gestión del riesgo dentro de la organización;
- b) aquellos responsables de garantizar que el riesgo se gestiona eficazmente dentro de la organización como unidad o dentro de un área, proyecto o actividad específicos;
- c) aquellos que necesitan evaluar la eficacia de una organización en cuanto a la gestión del riesgo; y
- d) aquellos que desarrollan normas, guías, procedimientos y códigos de práctica que, parcial o totalmente, establecen la manera de gestionar el riesgo dentro del contexto específico de estos documentos.

En muchas organizaciones las prácticas y procesos actuales para la gestión incluyen componentes de la gestión del riesgo y muchas organizaciones ya han adoptado un proceso formal para la gestión del riesgo para tipos particulares de riesgos o circunstancias. En tales casos, una organización puede decidir realizar una revisión crítica de sus prácticas y procesos existentes a la luz de esta norma.

En esta norma, se usan las expresiones "gestión del riesgo" y "gestionar el riesgo". En términos generales, la "gestión del riesgo" se refiere a la arquitectura (principios, marco y procesos) para la gestión eficaz del riesgo, mientras que "gestionar el riesgo" se refiere a la aplicación de esa arquitectura a riesgos particulares.



**Figura 1. Relaciones entre los principios, el marco de referencia y los procesos para la gestión del riesgo**

## NORMA TÉCNICA COLOMBIANA NTC-ISO 31000

### 1. OBJETO

Esta norma brinda los principios y las directrices genéricas sobre la gestión del riesgo.

Esta norma puede ser utilizada por cualquier empresa pública, privada o comunitaria, asociación, grupo o individuo. Por lo tanto, no es específica para ninguna industria o sector.

**NOTA** Para propósitos de conveniencia, se hace referencia a todos los diversos usuarios de esta norma con el término general de "organización".

Esta norma se puede aplicar durante toda la duración de una organización y a un amplio rango de actividades, incluyendo estrategias y decisiones, operaciones, procesos, funciones, proyectos, productos, servicios y activos.

Esta norma se puede aplicar a cualquier tipo de riesgo, cualquiera sea su naturaleza, bien sea que tenga consecuencias positivas o negativas.

Aunque esta norma suministra directrices genéricas, no se pretende promover la uniformidad de la gestión del riesgo en todas las organizaciones. Será necesario que el diseño y la implementación de planes y marcos de referencia para la gestión del riesgo tomen en consideración las diversas necesidades de una organización específica, sus objetivos particulares, contexto, estructura, operaciones, procesos, funciones, proyectos, productos, servicios o activos, y las prácticas específicas empleadas.

Se pretende que esta norma sea utilizada para armonizar los procesos de la gestión del riesgo en las normas existentes y futuras. Suministra un enfoque común en apoyo de las normas que tratan con riesgos, sectores específicos, o ambos, y no reemplaza a tales normas.

Esta norma no está destinada para fines de certificación.

### 2 TÉRMINOS Y DEFINICIONES

Para los fines de este documento, se aplican los siguientes términos y definiciones:

#### 2.1 Riesgo. Efecto de la incertidumbre sobre los objetivos.

**NOTA 1** Un efecto es una desviación de aquello que se espera, sea positivo, negativo o ambos.

**NOTA 2** Los objetivos pueden tener aspectos diferentes (por ejemplo financieros, salud y seguridad, y metas ambientales) y se pueden aplicar en niveles diferentes (estratégico, en toda la organización, en proyectos, productos y procesos).

**NOTA 3** A menudo el riesgo está caracterizado por la referencia a los **eventos** (véase el numeral 2.17) potenciales y las consecuencias (véase el numeral 2.18) o a una combinación de ellos.

**NOTA 4** Con frecuencia, el riesgo se expresa en términos de una combinación de las consecuencias de un evento (incluyendo los cambios en las circunstancias) y en la **probabilidad** (*Likelihood*) (véase el numeral 2.19) de que suceda.

**NOTA 5** Incertidumbre es el estado, incluso parcial, de deficiencia de información relacionada con la comprensión o el conocimiento de un evento, su consecuencia o probabilidad.

## 18 GESTIÓN DEL RIESGO

## NORMA TÉCNICA COLOMBIANA NTC-ISO 31000

GTC 137 (ISO Guía 73:2009, definición 1.1).

**2.2 Gestión del riesgo.** Actividades coordinadas para dirigir y controlar una organización con respecto al **riesgo** (véase el numeral 2.1).

GTC 137 (ISO Guía 73:2009, definición 2.1).

**2.3 Marco de referencia para la gestión del riesgo.** Conjunto de componentes que brindan las bases y las disposiciones de la organización para diseñar, implementar, **monitorear** (véase el numeral 2.28), revisar y mejorar continuamente la **gestión del riesgo** (véase el numeral 2.2) a través de toda la organización.

NOTA 1 Las bases incluyen la política, los objetivos, el comando y el compromiso para gestionar el **riesgo** (véase el numeral 2.1).

NOTA 2 Las disposiciones de la organización incluyen planes, relaciones, rendición de cuentas (Accountability), recursos, procesos y actividades.

NOTA 3 El marco de referencia para la gestión del riesgo está incluido en las políticas y prácticas estratégicas y operacionales globales de la organización.

GTC 137 (ISO Guía 73:2009, definición 2.1.1).

**2.4 Política para la gestión del riesgo.** Declaración de la dirección y las intenciones generales de una organización con respecto a la **gestión del riesgo** (véase el numeral 2.2).

GTC 137 (ISO Guía 73:2009, definición 2.1.2).

**2.5 Actitud hacia el riesgo.** Enfoque de la organización para evaluar y eventualmente buscar, retener, tomar o alejarse del **riesgo** (véase el numeral 2.1).

GTC 137 (ISO Guía 73:2009, definición 3.7.1.1).

**2.6 Plan para la gestión del riesgo.** Esquema dentro del **marco de referencia para la gestión del riesgo** (véase el numeral 2.3) que especifica el enfoque, los componentes y los recursos de la gestión que se van a aplicar a la **gestión del riesgo** (véase el numeral 2.1).

NOTA 1 Los componentes de la gestión comúnmente incluyen procedimientos, prácticas, asignación de responsabilidades, secuencia y oportunidad de las actividades.

NOTA 2 El plan para la gestión del riesgo se puede aplicar a productos, procesos y proyectos particulares, y a parte de la organización o su totalidad.

GTC 137 (ISO Guía 73:2009, definición 2.1.3).

**2.7 Propietario del riesgo.** Persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un **riesgo** (véase el numeral 2.1).

GTC 137 (ISO Guía 73:2009, definición 3.5.1.5).

**2.8 Proceso para la gestión del riesgo.** Aplicación sistemática de las políticas, los procedimientos y las prácticas de gestión a las actividades de comunicación, consulta, estableci-

---

## NORMA TÉCNICA COLOMBIANA NTC-ISO 31000

---

miento del contexto, y de identificación, análisis, evaluación, tratamiento, **monitoreo** (véase el numeral 2.28) y revisión del **riesgo** (véase el numeral 2.1).

GTC 137 (ISO Guía 73:2009, definición 3.1).

**2.9 Establecimiento del contexto.** Definición de los parámetros internos y externos que se han de tomar en consideración cuando se gestiona el riesgo, y establecimiento del alcance y los **criterios del riesgo** (véase el numeral 2.22) para la **política para la gestión del riesgo** (véase el numeral 2.4).

GTC 137 (ISO Guía 73:2009, definición 3.3.1).

**2.10 Contexto externo.** Ambiente externo en el cual la organización busca alcanzar sus objetivos.

NOTA El contexto externo puede incluir:

- el ambiente cultural, social, político, legal, reglamentario, financiero, tecnológico, económico, natural y competitivo, bien sea internacional, nacional, regional o local;
- impulsores clave y tendencias que tienen impacto en los objetivos de la organización; y
- relaciones con las **partes involucradas** (véase el numeral 2.13) y sus percepciones y valores.

GTC 137 (ISO Guía 73:2009, definición 3.3.1.1).

**2.11 Contexto interno.** Ambiente interno en el cual la organización busca alcanzar sus objetivos.

NOTA El contexto interno puede incluir:

- gobierno, estructura organizacional, funciones y responsabilidades;
- políticas, objetivos y estrategias implementadas para lograrlos;
- las capacidades, entendidas en términos de recursos y conocimiento (por ejemplo capital, tiempo, personas, procesos, sistemas y tecnologías);
- sistemas de información, flujos de información y procesos para la toma de decisiones (tanto formales como informales);
- relaciones con las partes involucradas internas y sus percepciones y valores;
- la cultura de la organización;
- normas, directrices y modelos adoptados por la organización; y
- forma y extensión de las relaciones contractuales.

GTC 137 (ISO Guía 73:2009, definición 3.3.1.2).

**2.12 Comunicación y consulta.** Procesos continuos y reiterativos que una organización lleva a cabo para suministrar, compartir u obtener información e involucrarse en un diálogo

---

## 20 GESTIÓN DEL RIESGO

---

## NORMA TÉCNICA COLOMBIANA NTC-ISO 31000

con las **partes involucradas** (véase el numeral 2.13) con respecto a la gestión del **riesgo** (véase el numeral 2.1).

NOTA 1 La información se puede relacionar con la existencia, la naturaleza, la forma, la probabilidad (*Likelihood*) (véase el numeral 2.19), el significado, la evaluación, la aceptabilidad y el tratamiento de la gestión del riesgo.

NOTA 2 La consulta es un proceso de doble vía de la comunicación informada entre una organización y sus partes involucradas, acerca de algún tema, antes de tomar una decisión o determinar una dirección para dicho tema. La consulta es:

- un proceso que tiene impacto en la decisión a través de la influencia más que del poder; y
- una entrada para la toma de decisiones, no para la toma conjunta de decisiones.

GTC 137 (ISO Guía 73:2009, definición 3.2.1).

**2.13 Parte involucrada.** Persona u organización que puede afectar, verse afectada o percibirse a sí misma como afectada por una decisión o una actividad.

NOTA Una persona que toma decisiones puede ser una parte involucrada.

GTC 137 (ISO Guía 73:2009, definición 3.2.1.1).

**2.14 Valoración del riesgo.** Proceso global de **identificación del riesgo** (véase el numeral 2.15), **análisis del riesgo** (véase el numeral 2.21) y **evaluación del riesgo** (véase el numeral 2.24).

GTC 137 (ISO Guía 73:2009, definición 3.4.1)

**2.15 Identificación del riesgo.** Proceso para encontrar, reconocer y describir el **riesgo** (véase el numeral 2.1).

NOTA 1 La identificación del riesgo implica la identificación de las **fuentes de riesgo** (véase el numeral 2.16), los **eventos** (véase el numeral 2.17), sus causas y sus **consecuencias** (véase el numeral 2.18) potenciales.

NOTA 2 La identificación del riesgo puede involucrar datos históricos, análisis teóricos, opiniones informadas y expertas, y las necesidades de las **partes involucradas** (véase el numeral 2.13).

GTC 137 (ISO Guía 73:2009, definición 3.5.1).

**2.16 Fuente de riesgo.** Elemento que solo o en combinación tiene el potencial intrínseco de originar un **riesgo** (véase el numeral 2.1).

NOTA Una fuente de riesgo puede ser tangible o intangible.

GTC 137 (ISO Guía 73:2009, definición 3.5.1.2).

**2.17 Evento.** Presencia o cambio de un conjunto particular de circunstancias.

NOTA 1 Un evento puede ser una o más ocurrencias y puede tener varias causas.

NOTA 2 Un evento puede consistir en algo que no está sucediendo.

## NORMA TÉCNICA COLOMBIANA NTC-ISO 31000

NOTA 3 En ocasiones, se puede hacer referencia a un evento como un "incidente" o "accidente".

NOTA 4 También se puede hacer referencia a un evento sin consecuencias (véase el numeral 2.18) como un "cuasi accidente", "incidente", "situación de peligro" o "conato de accidente".

GTC 137 (ISO Guía 73:2009, definición 3.5.1.3)

**2.18 Consecuencia.** Resultado de un **evento** (véase el numeral 2.17) que afecta a los objetivos.

NOTA 1 Un evento puede originar un rango de consecuencias.

NOTA 2 Una consecuencia puede ser cierta o incierta y puede tener efectos positivos o negativos en los objetivos.

NOTA 3 Las consecuencias se pueden expresar cualitativa o cuantitativamente.

NOTA 4 Las consecuencias iniciales pueden escalar a través de efectos secundarios.

GTC 137 (ISO Guía 73:2009, definición 3.6.1.3)

**2.19 Probabilidad** (*Likelihood*). Oportunidad de que algo suceda.

NOTA 1 En la terminología de la gestión del riesgo, la palabra "probabilidad (*Likelihood*)" se utiliza para hacer referencia a la oportunidad de que algo suceda, esté o no definido, medido o determinado objetiva o subjetivamente, cualitativa o cuantitativamente, y descrito utilizando términos generales o matemáticos (como la probabilidad numérica (*Probability*) o la frecuencia en un periodo de tiempo determinado).

NOTA 2 El término inglés "*Likelihood* (probabilidad)" no tiene un equivalente directo en algunos idiomas; en lugar de ello se utiliza el término equivalente de "*Probability* (probabilidad numérica). Sin embargo en inglés "*Probability*" con frecuencia se interpreta más estrechamente como un término matemático. Por lo tanto, en la terminología de la gestión del riesgo, "*Likelihood*" se usa con la intención de que tenga la misma interpretación amplia que el término "probabilidad" en muchos idiomas diferentes del inglés.

GTC 137 (ISO Guía 73:2009, definición 3.6.1.1).

**2.20 Perfil del riesgo.** Descripción de cualquier conjunto de **riesgos** (véase el numeral 2.1).

NOTA El conjunto de riesgos puede contener aquellos que se relacionan con la organización en su totalidad, con parte de la organización o según otra definición.

GTC 137 (ISO Guía 73:2009, definición 3.8.2.5).

**2.21 Análisis del riesgo.** Proceso para comprender la naturaleza del **riesgo** (véase el numeral 2.1) y determinar el **nivel de riesgo** (véase el numeral 2.23).

NOTA 1 El análisis del riesgo proporciona las bases para la evaluación del riesgo (véase el numeral 2.24) y las decisiones sobre el tratamiento del riesgo (véase el numeral 2.25).

NOTA 2 El análisis del riesgo incluye la estimación del riesgo.

GTC 137 (ISO Guía 73:2009, definición 3.6.1).

**2.22 Criterios del riesgo.** Términos de referencia frente a los cuales se evalúa la importancia de un **riesgo** (véase el numeral 2.1).

## 22 GESTIÓN DEL RIESGO

## NORMA TÉCNICA COLOMBIANA NTC-ISO 31000

NOTA 1 Los criterios del riesgo se basan en los objetivos y el contexto externo (véase el numeral 2.10) e interno (véase el numeral 2.11) de la organización.

NOTA 2 Los criterios del riesgo se pueden derivar de normas, leyes, políticas y otros requisitos.

GTC 137 (ISO Guía 73:2009, definición 3.3.1.3).

**2.23 Nivel de riesgo.** Magnitud de un **riesgo** (véase el numeral 2.1) o de una combinación de riesgos, expresada en términos de la combinación de las **consecuencias** (véase el numeral 2.18) y su **probabilidad** (véase el numeral 2.19).

GTC 137 (ISO Guía 73:2009, definición 3.6.1.8).

**2.24 Evaluación del riesgo.** Proceso de comparación de los resultados del **análisis del riesgo** (véase el numeral 2.21) con los **criterios del riesgo** (véase el numeral 2.22), para determinar si el **riesgo** (véase el numeral 2.1), su magnitud o ambos son aceptables o tolerables.

NOTA La evaluación del riesgo ayuda en la decisión acerca del **tratamiento del riesgo** (véase el numeral 2.25).

GTC 137 (ISO Guía 73:2009, definición 3.7.1).

**2.25 Tratamiento del riesgo.** Proceso para modificar el **riesgo** (véase el numeral 2.1).

NOTA 1 El tratamiento del riesgo puede implicar:

- evitar el riesgo decidiendo no iniciar o continuar la actividad que lo originó;
- tomar o incrementar el riesgo con el fin de perseguir una oportunidad;
- retirar la **fuente del riesgo** (véase el numeral 2.16);
- cambiar la **probabilidad** (véase el numeral 2.19);
- cambiar las **consecuencias** (véase el numeral 2.18);
- compartir el riesgo con una o varias de las partes (incluyendo los contratos y la financiación del riesgo); y
- retener el riesgo a través de la decisión informada.

NOTA 2 En ocasiones se hace referencia a los tratamientos del riesgo relacionados con consecuencias negativas como "mitigación del riesgo", "eliminación del riesgo", "prevención del riesgo" y "reducción del riesgo".

NOTA 3 El tratamiento del riesgo puede crear riesgos nuevos o modificar los existentes.

GTC 137 (ISO Guía 73:2009, definición 3.8.1).

**2.26 Control.** Medida que modifica al **riesgo** (véase el numeral 2.1)

NOTA 1 Los controles incluyen procesos, políticas, dispositivos, prácticas u otras acciones que modifican al riesgo.

NOTA 2 Los controles no siempre pueden ejercer el efecto modificador previsto o asumido.

GTC 137 (ISO Guía 73:2009, definición 3.8.1.1).

## **2.27 Riesgo residual**

**Riesgo** (véase el numeral 2.1) remanente después del **tratamiento del riesgo** (véase el numeral 2.25).

NOTA 1 El riesgo residual puede contener un riesgo no identificado.

NOTA 2 El riesgo residual también se conoce como "riesgo retenido".

GTC 137 (ISO Guía 73:2009, definición 3.8.1.6).

**2.28 Monitoreo.** Verificación, supervisión, observación crítica o determinación continua del estado con el fin de identificar cambios con respecto al nivel de desempeño exigido o esperado.

NOTA El monitoreo se puede aplicar al **marco de referencia para la gestión del riesgo** (véase el numeral 2.3), al **proceso para la gestión del riesgo** (véase el numeral 2.8), al **riesgo** (véase el numeral 2.1) o al control (véase el numeral 2.26).

GTC 137 (ISO Guía 73:2009, definición 3.8.2.1).

**2.29 Revisión.** Acción que se emprende para determinar la idoneidad, conveniencia y eficacia de la materia en cuestión para lograr los objetivos establecidos.

NOTA La revisión se puede aplicar al **marco de referencia para la gestión del riesgo** (véase el numeral 2.3), al **proceso para la gestión del riesgo** (véase el numeral 2.8), al **riesgo** (véase el numeral 2.1) o al control (véase el numeral 2.26).

GTC 137 (ISO Guía 73:2009, definición 3.8.2.2)

## **3. PRINCIPIOS**

Para que la gestión del riesgo sea eficaz, la organización debería cumplir con todos los siguientes principios en todos los niveles:

### a) **La gestión del riesgo crea y protege el valor**

La gestión del riesgo contribuye al logro demostrable de los objetivos y a la mejora del desempeño en, por ejemplo, la salud y la seguridad humana, la conformidad legal y reglamentaria, la seguridad, la aceptación pública, la protección del ambiente, la calidad del producto, la gestión de proyectos, la eficiencia en las operaciones, el gobierno y la reputación.

### b) **La gestión del riesgo es una parte integral de todos los procesos de la organización**

La gestión del riesgo no es una actividad independiente que se separa de las actividades y los procesos principales de la organización. La gestión del riesgo es parte de las responsabilidades de la dirección y una parte integral de todos los procesos de la organización, incluyendo la planificación estratégica y todos los procesos de gestión de proyectos y de cambio.

---

## **24 GESTIÓN DEL RIESGO**

c) **La gestión del riesgo es parte de la toma de decisiones**

La gestión del riesgo ayuda a quienes toman las decisiones a hacer elecciones informadas, priorizar acciones y distinguir entre cursos de acción alternativos.

d) **La gestión del riesgo aborda explícitamente la incertidumbre**

La gestión del riesgo toma en consideración explícitamente a la incertidumbre, su naturaleza y la forma en que se puede tratar.

e) **La gestión del riesgo es sistemática, estructurada y oportuna**

Un enfoque sistemático, oportuno y estructurado para la gestión del riesgo contribuye a la eficiencia y a resultados consistentes, comparables y confiables.

f) **La gestión del riesgo se basa en la mejor información disponible**

Las entradas para el proceso de gestión del riesgo se basan en fuentes de información tales como datos históricos, experiencia, retroalimentación de las partes involucradas, observación, previsiones y examen de expertos. Sin embargo, quienes toman las decisiones deberían informarse y tomar en consideración todas las limitaciones de los datos o de los modelos utilizados, o la posibilidad de divergencia entre los expertos.

g) **La gestión del riesgo está adaptada**

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

h) **La gestión del riesgo toma en consideración los factores humanos y culturales**

La gestión del riesgo reconoce las capacidades, percepciones e intenciones de individuos externos e internos, los cuales pueden facilitar o dificultar el logro de los objetivos de la organización.

i) **La gestión del riesgo es transparente e inclusiva**

La correcta y oportuna intervención de las partes involucradas y, en particular, de aquellos que toman las decisiones en todos los niveles de la organización, garantiza que la gestión del riesgo siga siendo pertinente y se actualice. Esta intervención también permite a las partes involucradas estar correctamente representadas y hacer que sus puntos de vista se tomen en consideración al determinar los criterios del riesgo.

j) **La gestión del riesgo es dinámica, reiterativa y receptiva al cambio**

La gestión del riesgo siente y responde continuamente al cambio. A medida que se presentan los eventos externos e internos, el contexto y el conocimiento cambian, tienen lugar el monitoreo y la revisión de los riesgos, emergen riesgos nuevos, algunos cambian y otros desaparecen.

k) **La gestión del riesgo facilita la mejora continua de la organización**

Las organizaciones deberían desarrollar e implementar estrategias para mejorar la madurez de su gestión de riesgos junto con todos los otros aspectos de su organización.

El Anexo A suministra asesoría adicional para las organizaciones que requieren gestionar el riesgo más eficazmente.

#### 4. MARCO DE REFERENCIA

##### 4.1 GENERALIDADES

El éxito de la gestión del riesgo dependerá de la eficacia del marco de referencia para la gestión, el cual brinda las bases y las disposiciones que se introducirán en todos los niveles de la organización. El marco ayuda a la gestión eficaz del riesgo a través de la aplicación del proceso para la gestión del riesgo (véase el numeral 5) en los diversos niveles y en contextos específicos de la organización. El marco garantiza que la información acerca del riesgo derivada del proceso para la gestión del riesgo se reporte de manera adecuada y se utilice como base para la toma de decisiones y la rendición de cuentas en todos los niveles pertinentes de la organización.

Este numeral describe los componentes necesarios del marco para gestionar el riesgo y la forma en que ellos se interrelacionan de manera reiterativa, tal como se ilustra en la Figura 2.

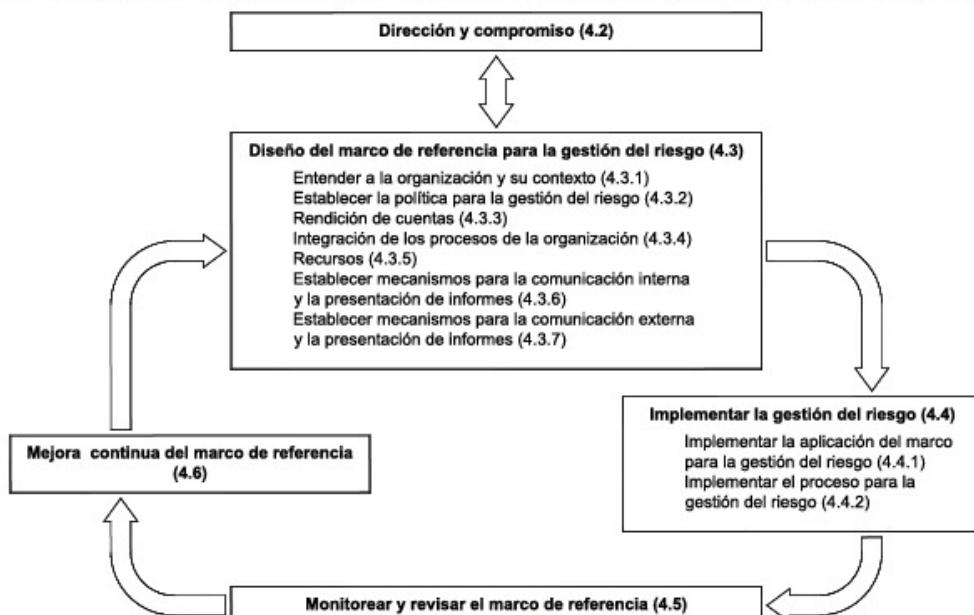


Figura 2. Relación entre los componentes del marco de referencia para la gestión del riesgo

## **NORMA TÉCNICA COLOMBIANA NTC-ISO 31000**

Este marco de referencia no tiene como finalidad prescribir un sistema de gestión sino facilitar a la organización la integración de la gestión del riesgo en su sistema de gestión global. Por lo tanto, las organizaciones deberían adaptar los componentes del marco a sus necesidades específicas.

Si las prácticas y procesos de gestión existentes de la organización incluyen componentes de la gestión del riesgo, o si la organización ya ha adoptado un proceso formal para la gestión del riesgo para tipos particulares de riesgos o situaciones, entonces éstos se deberían revisar y valorar de forma crítica frente a esta norma, incluyendo los atributos del Anexo A, con el fin de determinar su eficacia y conveniencia.

### **4.2 DIRECCIÓN Y COMPROMISO**

La introducción de la gestión del riesgo, y garantizar su eficacia continua, requiere de un compromiso fuerte y sostenido por parte de la dirección de la organización, así como de planificación estratégica y rigurosa para lograr el compromiso a todo nivel. La dirección debería:

- definir y aprobar la política para la gestión del riesgo;
- garantizar que la cultura de la organización y la política para la gestión del riesgo están alineadas;
- determinar indicadores del desempeño de la gestión para el riesgo que estén acordes con los indicadores del desempeño de la organización;
- alinear los objetivos de la gestión del riesgo con los objetivos y las estrategias de la organización;
- garantizar la conformidad legal y reglamentaria;
- asignar obligaciones y responsabilidades en los niveles respectivos dentro de la organización;
- garantizar que se asignan los recursos necesarios para la gestión del riesgo;
- comunicar los beneficios de la gestión del riesgo a todas las partes involucradas; y
- garantizar que el marco de referencia para gestionar el riesgo sigue siendo adecuado.

### **4.3 DISEÑO DEL MARCO DE REFERENCIA PARA LA GESTIÓN DEL RIESGO**

#### **4.3.1 Entender a la organización y su contexto**

Antes de empezar el diseño y la implementación del marco de referencia para la gestión del riesgo, es importante evaluar y entender el contexto, tanto externo como interno de la organización, dado que éste puede tener influencia significativa en el diseño de dicho marco.

---

**NORMA TÉCNICA COLOMBIANA NTC-ISO 31000**

---

La evaluación del contexto externo de la organización puede incluir, entre otros:

- a) el ambiente social y cultural, político, legal, reglamentario, financiero, tecnológico, económico, natural y competitivo, bien sea internacional, nacional, regional o local;
- b) impulsores clave y tendencias que tienen impacto en los objetivos de la organización; y
- c) las relaciones con las partes involucradas externas, y sus percepciones y valores.

La evaluación del contexto interno de la organización puede incluir, entre otros:

- gobierno, estructura organizacional, funciones y obligaciones;
- políticas, objetivos y estrategias que se han implementado para lograrlos;
- capacidades, entendidas en términos de recursos y conocimiento (por ejemplo capital, tiempo, personas, procesos, sistemas y tecnologías);
- sistemas de información, flujos de información y procesos de toma de decisiones (tanto formales como informales);
- relaciones con las partes involucradas internas y sus percepciones y valores;
- la cultura de la organización;
- normas, directrices y modelos adoptados por la organización; y
- forma y extensión de las relaciones contractuales.

#### **4.3.2 Establecer la política para la gestión del riesgo**

La política para la gestión del riesgo debería establecer claramente los objetivos de la organización para la gestión del riesgo y su compromiso con ella, y comúnmente debería abordar los siguientes aspectos:

- la justificación de la organización para gestionar el riesgo;
- los vínculos entre los objetivos y las políticas de la organización y la política para la gestión del riesgo;
- las obligaciones y responsabilidades para gestionar el riesgo;
- la forma de tratar los conflictos de intereses;
- el compromiso para poner a disposición los recursos necesarios con el fin de ayudar a los responsables de la gestión del riesgo y de rendir cuentas con respecto a ésta;

## **NORMA TÉCNICA COLOMBIANA NTC-ISO 31000**

- la forma en la cual se va a medir y a reportar el desempeño de la gestión del riesgo; y
- el compromiso para revisar y mejorar periódicamente la política y el marco de la gestión del riesgo y en respuesta a un evento o un cambio en las circunstancias. La política para la gestión del riesgo se debería comunicar de manera adecuada.

### **4.3.3 Rendición de cuentas**

La organización debería garantizar que existe responsabilidad, autoridad y competencia adecuada para gestionar el riesgo, incluyendo la implementación y mantenimiento del proceso para la gestión del riesgo y garantizando la idoneidad, eficacia y eficiencia de todos los controles. Esto se puede facilitar mediante:

- la identificación de los propietarios del riesgo a quienes corresponde rendir cuentas y tienen autoridad para su gestión;
- la identificación de quién debe dar cuentas por el desarrollo, la implementación y el mantenimiento del marco para la gestión del riesgo;
- la identificación de otras responsabilidades en el proceso para la gestión del riesgo de los individuos en todos los niveles de la organización;
- estableciendo la medición del desempeño y procesos de escalamiento y reporte externo, interno, o ambos; y
- garantizando niveles adecuados de reconocimiento.

### **4.3.4 Integración en los procesos de la organización**

La gestión del riesgo debería estar incluida en todas las prácticas y los procesos de la organización en una manera que sea pertinente, eficaz y eficiente. El proceso para la gestión del riesgo se debería convertir en parte, no independiente, de los procesos de la organización. En particular, la gestión del riesgo se debería incluir en el desarrollo de la política, la planificación estratégica y del negocio, la revisión y en los procesos de gestión del cambio.

Debería existir un plan para la gestión del riesgo a todo lo ancho de la organización para garantizar que se implementa la política para la gestión del riesgo y que la gestión del riesgo está incluida en todas las prácticas y los procesos de la organización. El plan para la gestión del riesgo se podría integrar en otros planes de la organización, por ejemplo en el plan estratégico.

### **4.3.5 Recursos**

La organización debería asignar los recursos adecuados para la gestión del riesgo.

## NORMA TÉCNICA COLOMBIANA NTC-ISO 31000

Se recomienda considerar los siguientes aspectos:

- personas, habilidades, experiencia y competencia;
- recursos necesarios para cada paso del proceso de gestión del riesgo;
- los procesos, métodos y herramientas de la organización que se van a utilizar para gestionar el riesgo;
- procesos y procedimientos documentados;
- sistemas de gestión de la información y el conocimiento; y
- programas de entrenamiento.

### 4.3.6 Establecer mecanismos para la comunicación interna y la presentación de informes

La organización debería establecer mecanismos para la comunicación interna y la presentación de informes con el fin de ayudar y fomentar la rendición de cuentas y la pertenencia del riesgo.

Estos mecanismos deberían garantizar que:

- los componentes clave del marco para la gestión del riesgo y todas las modificaciones posteriores se comunican de manera correcta;
- existe un reporte interno adecuado acerca del marco, su eficacia y resultados;
- la información pertinente derivada de la aplicación de la gestión del riesgo está disponible en los niveles y los momentos convenientes; y
- existen procesos para la consulta con las partes involucradas internas.

Estos mecanismos deberían incluir, cuando así corresponda, los procesos para consolidar la información del riesgo proveniente de diversas fuentes, y puede ser necesario que consideren la sensibilidad de la información.

### 4.3.7 Establecer mecanismos para la comunicación externa y la presentación de informes

La organización debería desarrollar e implementar un plan sobre la forma como se comunicará con las partes involucradas externas. El plan debería incluir:

- involucrar apropiadamente las partes interesadas externas y garantizar un intercambio efectivo de la información;

## 30 GESTIÓN DEL RIESGO

## **NORMA TÉCNICA COLOMBIANA NTC-ISO 31000**

- reporte externo para cumplir con los requisitos legales, reglamentarios y del gobierno;
- brindar retroalimentación e informes sobre la comunicación y las consultas;
- usar la comunicación para crear confianza en la organización; y
- comunicarse con las partes involucradas en el evento de una crisis o contingencia.

Estos mecanismos deberían incluir, cuando así corresponda, los procesos para consolidar la información del riesgo proveniente de diversas fuentes, y puede ser necesario que consideren la sensibilidad de la información.

### **4.4 IMPLEMENTAR LA GESTIÓN DEL RIESGO**

#### **4.4.1 Implementar el marco de referencia para gestionar el riesgo**

Al implementar el marco de referencia de la organización para la gestión del riesgo, la organización debería:

- definir el tiempo y la estrategia adecuados para la implementación del marco de referencia;
- aplicar el proceso y la política para la gestión del riesgo a los procesos de la organización;
- cumplir con los requisitos legales y reglamentarios;
- garantizar que la toma de decisiones, incluyendo el desarrollo y establecimiento de objetivos, está en línea con los resultados de los procesos para la gestión del riesgo;
- llevar a cabo sesiones de información y entrenamiento; y
- comunicarse y consultar a las partes involucradas para garantizar que el marco para la gestión del riesgo sigue siendo adecuado.

#### **4.4.2 Implementar el proceso para la gestión del riesgo**

La gestión del riesgo se debería implementar garantizando que el proceso para la gestión del riesgo que se describe en el numeral 5 se aplica a través de un plan para la gestión del riesgo en todos los niveles y las funciones pertinentes de la organización como parte de sus prácticas y procesos.

### **4.5 MONITOREAR Y REVISAR EL MARCO DE REFERENCIA**

Con el fin de garantizar que la gestión del riesgo es eficaz y continúa sustentando el desempeño de la organización, la organización debería:

---

## NORMA TÉCNICA COLOMBIANA NTC-ISO 31000

---

- medir el desempeño de la gestión del riesgo frente a los indicadores, los cuales se revisan periódicamente para determinar su idoneidad;
- medir periódicamente el progreso frente al plan para la gestión del riesgo y las desviaciones con respecto a éste;
- revisar periódicamente si el marco de referencia, la política y el plan para la gestión del riesgo siguen siendo adecuados, según el contexto externo e interno de la organización;
- presentar informes sobre el riesgo, el progreso con el plan para la gestión del riesgo y sobre que tanto se cumple la política para la gestión del riesgo; y
- revisar la eficacia del marco de referencia para la gestión del riesgo.

### 4.6 MEJORA CONTINUA DEL MARCO DE REFERENCIA

Con base en los resultados del monitoreo y las revisiones, se deberían tomar decisiones sobre la forma en que se podrían mejorar el marco de referencia, la política y el plan para la gestión del riesgo. Estas decisiones deberían originar mejoras en la gestión del riesgo de la organización y en su cultura de la gestión del riesgo.

## 5. PROCESO

### 5.1 GENERALIDADES

El proceso para la gestión del riesgo debería:

- ser parte integral de la gestión,
- estar incluido en la cultura y las prácticas, y
- estar adaptado a los procesos de negocio de la organización.

El proceso comprende las actividades que se describen en los numerales 5.2 al 5.6. El proceso para la gestión del riesgo se ilustra en la Figura 3.

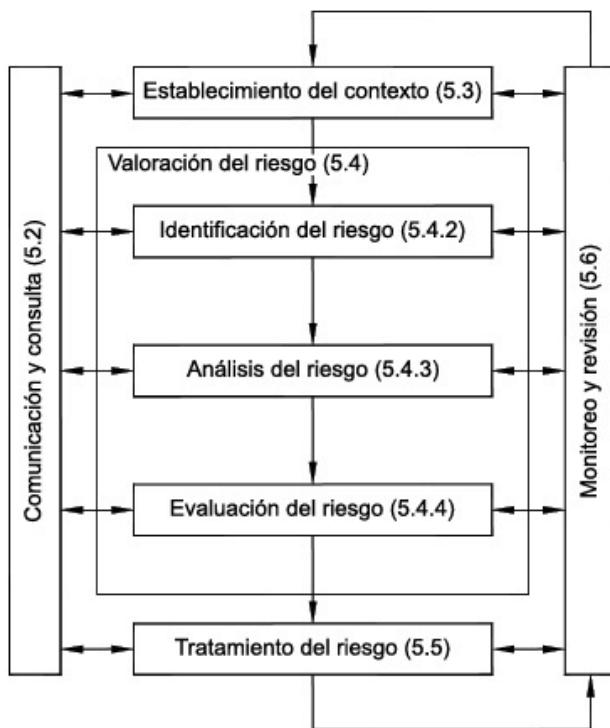
### 5.2 COMUNICACIÓN Y CONSULTA

La comunicación y la consulta con las partes involucradas externas e internas deberían tener lugar durante todas las etapas del proceso para la gestión del riesgo.

Por lo tanto, se deberían desarrollar tempranamente los planes para la comunicación y la consulta. Éstos deberían abordar aspectos relacionados con el propio riesgo, sus causas, sus consecuencias (si se conocen), y las medidas que se toman para tratarlo. Es conveniente

---

## 32 GESTIÓN DEL RIESGO



**Figura 3. Proceso para la gestión del riesgo**

que tengan lugar la comunicación y las consultas externas e internas eficaces para garantizar que aquellos responsables de la implementación del proceso para la gestión del riesgo y las partes involucradas entiendan las bases sobre las cuales se toman las decisiones, y las razones por las cuales se requieren acciones particulares.

Un enfoque de equipo consultor puede:

- ayudar a establecer correctamente el contexto;
  - garantizar que se entienden y se toman en consideración los intereses de las partes involucradas;
  - ayudar a garantizar que los riesgos estén correctamente identificados;
  - reunir diferentes áreas de experticia para analizar los riesgos,
  - garantizar que los diversos puntos de vista se toman en consideración adecuadamente al definir los criterios del riesgo y al evaluar los riesgos;

---

## NORMA TÉCNICA COLOMBIANA NTC-ISO 31000

---

- asegurar la aprobación y el soporte para el plan de tratamiento;
- fomentar la gestión adecuada del cambio durante el proceso para la gestión del riesgo; y
- desarrollar un plan adecuado de comunicación y consulta externo e interno.

La comunicación y la consulta con las partes involucradas son importantes dado que ellas dan sus opiniones acerca del riesgo con base en sus percepciones de éste. Estas percepciones pueden variar debido a las diferencias en los valores, las necesidades, las asunciones, los conceptos y los intereses de las partes involucradas. Dado que sus puntos de vista pueden tener un impacto significativo en las decisiones que se toman, las percepciones de las partes involucradas se deberían identificar, registrar y tomar en consideración en el proceso de toma de decisiones.

La comunicación y la consulta deberían facilitar los intercambios de información veraz, pertinente, precisa y fácil de entender, teniendo en cuenta los aspectos de la integridad personal y confidencial.

### 5.3 ESTABLECIMIENTO DEL CONTEXTO

#### 5.3.1 Generalidades

Al establecer el contexto, la organización articula sus objetivos, define los parámetros externos e internos que se van a considerar al gestionar el riesgo y establece el alcance y los criterios del riesgo para el resto del proceso. Aunque muchos de estos parámetros son similares a aquellos que se consideran en el diseño del marco de referencia para la gestión del riesgo (véase el numeral 4.3.1), al establecer el contexto del proceso para la gestión del riesgo, es necesario que estos parámetros se consideren en mayor detalle y, en particular, la manera como se relacionan con el alcance del proceso para la gestión del riesgo particular.

#### 5.3.2 Establecer el contexto externo

El contexto externo es el ambiente externo en el cual la organización busca alcanzar sus objetivos.

Entender el contexto externo es importante con el fin de garantizar que los objetivos y las preocupaciones de las partes involucradas externas se toman en consideración al desarrollar los criterios del riesgo. Esto se basa en el contexto a todo lo ancho de la organización, pero con detalles específicos de los requisitos legales y reglamentarios, las percepciones de las partes involucradas y otros aspectos de los riesgos específicos para el alcance del proceso para gestionar el riesgo.

El contexto externo puede incluir, entre otros:

- el ambiente social y cultural, político, legal, reglamentario, financiero, tecnológico, económico, natural y competitivo, bien sea internacional, nacional, regional o local;

---

## 34 GESTIÓN DEL RIESGO

## NORMA TÉCNICA COLOMBIANA NTC-ISO 31000

- los impulsores clave y las tendencias que tienen impacto en los objetivos de la organización; y
- las relaciones con las partes involucradas externas y sus percepciones y valores.

### 5.3.3 Establecer el contexto interno

El contexto interno es el ambiente interno en el cual la organización busca alcanzar sus objetivos.

El proceso para la gestión del riesgo debería estar alineado con la cultura, los procesos, la estructura y la estrategia de la organización. El contexto interno es todo aquello dentro de la organización que pueda tener influencia en la forma en que la organización gestionará el riesgo. Este contexto se debe establecer porque:

- a) la gestión del riesgo tiene lugar en el contexto de los objetivos de la organización;
- b) los objetivos y los criterios de un proyecto, proceso o actividad en particular se deberían considerar a la luz de los objetivos de la organización como un todo; y
- c) algunas organizaciones fracasan en reconocer las oportunidades para alcanzar sus objetivos estratégicos, del proyecto o el negocio, y esto afecta la continuidad del compromiso, la credibilidad, la confianza y el valor de la organización.

Es necesario entender el contexto interno. Éste puede incluir, entre otros:

- gobierno, estructura de la organización, funciones y responsabilidades;
- políticas, objetivos y las estrategias implementadas para lograrlos;
- capacidades, entendidas en términos de recursos y conocimientos (por ejemplo capital, tiempo, personas, procesos, sistemas y tecnologías);
- las relaciones con las partes involucradas internas y sus percepciones y valores;
- la cultura de la organización;
- sistemas de información, flujos de información y procesos de toma de decisiones (tanto formales como informales);
- normas, directrices y modelos adoptados por la organización; y
- forma y extensión de las relaciones contractuales.

### 5.3.4 Establecer el contexto del proceso para la gestión del riesgo

Se recomienda establecer los objetivos, las estrategias, el alcance y los parámetros de las actividades de la organización, o de aquellas partes de la organización en donde se aplica

---

## NORMA TÉCNICA COLOMBIANA NTC-ISO 31000

---

el proceso para la gestión del riesgo. La gestión del riesgo se debería emprender con total consideración de la necesidad de justificar los recursos utilizados para llevar a cabo dicha gestión. También se deberían especificar los recursos necesarios, las responsabilidades y autoridades, y los registros que se deben conservar.

El contexto del proceso para la gestión del riesgo variará de acuerdo con las necesidades de la organización. Este contexto puede involucrar, entre otros:

- definición de las metas y los objetivos de las actividades de gestión del riesgo;
- definición de las responsabilidades del proceso para la gestión del riesgo y dentro de este;
- definición del alcance, así como de la profundidad y extensión de las actividades de gestión del riesgo que se van a llevar a cabo, incluyendo las exclusiones e inclusiones específicas;
- definir actividad, proceso, función, proyecto, producto, servicio o activo en términos de tiempo y ubicación;
- definición de las relaciones entre el proyecto, el proceso o la actividad particulares y otros proyectos, procesos o actividades de la organización;
- definición de las metodologías para la valoración del riesgo;
- definición de la forma de evaluar el desempeño y la eficacia en la gestión del riesgo;
- identificación y especificación de las decisiones que se deben tomar; y
- identificación, establecimiento del alcance o el marco de los estudios necesarios, su extensión y objetivos, y los recursos necesarios para tales estudios.

La atención a estos y otros factores importantes debería ayudar a garantizar que el enfoque para la gestión del riesgo que se ha adoptado es el adecuado para las circunstancias, la organización y los riesgos que afectan el logro de sus objetivos.

### 5.3.5 Definir los criterios del riesgo

La organización debería definir los criterios que se van a utilizar para evaluar la importancia del riesgo. Los criterios deberían reflejar los valores, objetivos y recursos de la organización. Algunos criterios pueden estar impuestos por los requisitos legales y reglamentarios o derivarse de ellos y de otros requisitos a los cuales la organización se suscribe. Los criterios del riesgo deberían ser consistentes con la política para la gestión del riesgo de la organización (véase el numeral 4.3.2), estar definidos al comienzo de todo proceso para la gestión del riesgo y ser revisados continuamente.

Al definir los criterios del riesgo, los factores que se van a considerar deberían incluir los siguientes:

---

## 36 GESTIÓN DEL RIESGO

---

## NORMA TÉCNICA COLOMBIANA NTC-ISO 31000

- la naturaleza y los tipos de causas y consecuencias que se pueden presentar y la forma en que se van a medir;
- cómo se va a definir la probabilidad;
- los marcos temporales de la probabilidad, las consecuencias, o ambas;
- cómo se va a determinar el nivel de riesgo;
- los puntos de vista de las partes involucradas;
- el nivel en el cual el riesgo se torna aceptable o tolerable; y
- si se debería o no tener en cuenta combinaciones de riesgos múltiples y, si es así, cómo y cuáles combinaciones se deberían considerar.

### 5.4 VALORACIÓN DEL RIESGO

#### 5.4.1 Generalidades

La valoración del riesgo es el proceso total de identificación del riesgo, análisis del riesgo y evaluación del riesgo.

NOTA ISO/IEC 31010 brinda directrices sobre las técnicas de valoración del riesgo.

#### 5.4.2 Identificación del riesgo

La organización debería identificar las fuentes de riesgo, las áreas de impacto, los eventos (incluyendo los cambios en las circunstancias) y sus causas y consecuencias potenciales. El objeto de esta fase es generar una lista exhaustiva de riesgos con base en aquellos eventos que podrían crear, aumentar, prevenir, degradar, acelerar o retrasar el logro de los objetivos. Es importante identificar los riesgos asociados a la no búsqueda de una oportunidad. La identificación exhaustiva es crítica porque un riesgo que no se identifique en esta fase no será incluido en el análisis posterior.

La identificación debería incluir los riesgos independientemente de si su origen está o no bajo control de la organización, aún cuando el origen del riesgo o su causa pueden no ser evidentes. La identificación del riesgo debería incluir el examen de los efectos colaterales de las consecuencias particulares, incluyendo los efectos en cascada y acumulativos. También se debería considerar un rango amplio de consecuencias incluso si el origen del riesgo o su causa pueden no ser evidentes. Al igual que la identificación de lo que podría suceder, es necesario considerar las causas y los escenarios posibles que muestran que las consecuencias se podrían presentar. Se recomienda considerar todas las causas y consecuencias significativas.

La organización debería aplicar herramientas y técnicas para la identificación del riesgo que sean adecuadas a sus objetivos y capacidades, y a los riesgos que se enfrentan. La información pertinente y actualizada es importante para identificar los riesgos. Esta información

debería incluir, siempre que sea posible, la información básica. En la identificación del riesgo se deberían involucrar las personas con el conocimiento apropiado.

#### **5.4.3 Análisis del riesgo**

El análisis del riesgo implica el desarrollo y la comprensión del riesgo. Este análisis brinda una entrada para la evaluación del riesgo y para las decisiones sobre si es necesario o no tratar los riesgos y sobre las estrategias y métodos más adecuados para su tratamiento. El análisis del riesgo también brinda una entrada para la toma de decisiones, en la cual se deben hacer elecciones y las opciones implican diversos tipos y niveles de riesgo.

El análisis del riesgo involucra la consideración de las causas y las fuentes de riesgo, sus consecuencias positivas y negativas, y la probabilidad de que tales consecuencias puedan ocurrir. Se deberían identificar los factores que afectan a las consecuencias y a la probabilidad. El riesgo es analizado determinando las consecuencias y su probabilidad, y otros atributos del riesgo. Un evento puede tener consecuencias múltiples y puede afectar a objetivos múltiples. También se deberían considerar los controles existentes y su eficacia y eficiencia.

La forma en la cual las consecuencias y la probabilidad se expresan y la forma en la cual ellas se combinan para determinar un nivel de riesgo debería reflejar el tipo de riesgo, la información disponible y el propósito para el cual se va a usar la salida de la valoración del riesgo. Todo esto debería ser consistente con los criterios del riesgo. También es importante considerar la interdependencia de los diferentes riesgos y sus orígenes.

La confianza en la determinación del nivel de riesgo y su sensibilidad a las precondiciones y asunciones se debería considerar en el análisis y comunicar eficazmente a quienes toman las decisiones y, según corresponda, a otras partes involucradas. Factores tales como la divergencia de opinión entre los expertos, la incertidumbre, la disponibilidad, la calidad, la cantidad y la pertinencia continua de la información, o los limitantes en el modelado se deberían establecer y se pueden enfatizar.

El análisis del riesgo se puede realizar con diversos grados de detalle, dependiendo del riesgo, el propósito del análisis y la información, datos y recursos disponibles. El análisis puede ser cualitativo, semicuantitativo o cuantitativo, o una combinación de ellos, dependiendo de las circunstancias.

Las consecuencias y su probabilidad se pueden determinar modelando los resultados de un evento o grupo de eventos, o mediante extrapolación a partir de estudios experimentales o de los datos disponibles. Las consecuencias se pueden expresar en términos de impactos tangibles e intangibles. En algunos casos, se requiere más de un valor numérico o descriptor para especificar las consecuencias y su probabilidad en diferentes momentos, lugares, grupos o situaciones.

#### **5.4.4 Evaluación del riesgo**

El propósito de la evaluación del riesgo es facilitar la toma de decisiones, basada en los resultados de dicho análisis, a acerca de cuáles riesgos necesitan tratamiento y la prioridad para la implementación del tratamiento.

## **NORMA TÉCNICA COLOMBIANA NTC-ISO 31000**

La evaluación del riesgo implica la comparación del nivel de riesgo observado durante el proceso de análisis y de los criterios del riesgo establecidos al considerar el contexto. Con base en esta comparación, se puede considerar la necesidad de tratamiento.

En las decisiones se debería tener en cuenta el contexto más amplio del riesgo e incluir consideración de la tolerancia de los riesgos que acarrean otras partes diferentes de la organización que se benefician de los riesgos. Las decisiones se deberían tomar de acuerdo con los requisitos legales, reglamentarios y otros.

En algunas circunstancias, la evaluación del riesgo puede llevar a la decisión de emprender un análisis adicional. La evaluación del riesgo también puede tener como resultado la decisión de no tratar el riesgo de ninguna manera diferente del mantenimiento de los controles existentes. Esta decisión estará influida por la actitud de la organización hacia el riesgo y por los criterios del riesgo que se han establecido.

### **5.5 TRATAMIENTO DEL RIESGO**

#### **5.5.1 Generalidades**

El tratamiento del riesgo involucra la selección de una o más opciones para modificar los riesgos y la implementación de tales opciones. Una vez implementado, el tratamiento suministra controles o los modifica.

El tratamiento del riesgo implica un proceso cíclico de:

- valoración del tratamiento del riesgo;
- decisión sobre si los niveles de riesgo residual son tolerables;
- si no son tolerables, generación de un nuevo tratamiento para el riesgo; y
- valoración de la eficacia de dicho tratamiento.

Las opciones para el tratamiento del riesgo no necesariamente son mutuamente excluyentes ni adecuadas en todas las circunstancias. Las opciones pueden incluir las siguientes:

- a) evitar el riesgo al decidir no iniciar o continuar la actividad que lo originó;
- b) tomar o incrementar el riesgo para perseguir una oportunidad;
- c) retirar la fuente de riesgo;
- d) cambiar la probabilidad;
- e) cambiar las consecuencias;
- f) compartir el riesgo con una o varias de las partes, (incluyendo los contratos y la financiación del riesgo); y

- g) retener el riesgo mediante una decisión informada.

#### **5.5.2 Selección de las opciones para el tratamiento del riesgo**

La selección de las opciones más adecuadas para el tratamiento del riesgo implica equilibrar los costos y los esfuerzos de la implementación frente a los beneficios derivados con respecto a los requisitos legales, reglamentarios y otros, como por ejemplo la responsabilidad social y la protección del ambiente natural. En las decisiones también se deberían considerar los riesgos que pueden ameritar el tratamiento que no es justificable en términos económicos, por ejemplo los riesgos graves (consecuencia negativa alta) pero raros (baja probabilidad).

Se puede considerar y aplicar una cantidad de opciones para el tratamiento ya sea individualmente o en combinación. Normalmente, la organización se puede beneficiar de la adopción de una combinación de opciones de tratamiento.

Al seleccionar las opciones para tratar el riesgo, la organización debería considerar los valores y las percepciones de las partes involucradas, y las vías más adecuadas para comunicarse con ellos. Cuando las opciones para tratar el riesgo pueden tener impacto en el riesgo en otras partes de la organización o para otras partes involucradas, estas opciones se deberían incluir en la decisión. Aunque tienen igual eficacia, algunos tratamientos para el riesgo pueden ser más aceptables para algunas partes involucradas que para otras.

El plan de tratamiento debería identificar claramente el orden de prioridad en el cual se deberían implementar los tratamientos individuales para el riesgo.

El tratamiento en sí mismo puede introducir riesgos. Un riesgo significativo puede ser la falla o la ineficacia de las medidas del tratamiento. Es necesario que el monitoreo sea parte integral del plan de tratamiento del riesgo para garantizar que las medidas sigan siendo eficaces.

El tratamiento también puede introducir riesgos secundarios que es necesario valorar, tratar, monitorear y revisar. Estos riesgos secundarios se deberían incorporar en el mismo plan de tratamiento definido para el riesgo original y no se deberían tratar como riesgos nuevos. Es recomendable identificar y mantener el vínculo entre los dos riesgos.

#### **5.5.3 Preparación e implementación de los planes para el tratamiento del riesgo**

El propósito de los planes para el tratamiento del riesgo es documentar la forma en que se van a implementar las opciones de tratamiento seleccionadas. La información suministrada en los planes de tratamiento debería incluir:

- las razones para la selección de las opciones de tratamiento, que incluyan los beneficios que se espera obtener;
- aquellos que son responsables de aprobar el plan y los responsables de implementarlo;
- acciones propuestas;

## NORMA TÉCNICA COLOMBIANA NTC-ISO 31000

- requisitos de recursos, incluyendo las contingencias;
- medidas y restricciones de desempeño;
- requisitos de monitoreo y reporte; y
- tiempo y cronograma.

Los planes de tratamiento se deberían integrar con los procesos de gestión de la organización y se deberían discutir con las partes involucradas pertinentes.

Los encargados de tomar las decisiones y otras partes involucradas deberían conocer la naturaleza y la extensión del riesgo residual después del tratamiento del riesgo. El riesgo residual se debería documentar y someter a monitoreo, revisión y, cuando así corresponda, a tratamiento adicional.

### 5.6 MONITOREO Y REVISIÓN

Tanto el monitoreo como la reedición debería ser una parte planificada del proceso para la gestión del riesgo e incluir verificación o vigilancia regulares. Pueden ser periódicos o según convenga.

Las responsabilidades del monitoreo y la revisión deberían estar claramente definidas.

Los procesos de monitoreo y revisión de la organización deberían comprender todos los aspectos del proceso para la gestión del riesgo con el fin de:

- garantizar que los controles son eficaces y eficientes tanto en el diseño como en la operación;
- obtener información adicional para mejorar la valoración del riesgo;
- analizar y aprender lecciones a partir de los eventos (incluyendo los cuasi accidentes), los cambios, las tendencias, los éxitos y los fracasos;
- detectar cambios en el contexto externo e interno, incluyendo los cambios en los criterios del riesgo y en el riesgo mismo que puedan exigir revisión de los tratamientos del riesgo y las prioridades; y
- identificar los riesgos emergentes.

El avance en la implementación de los planes para tratamiento del riesgo suministra una medida de desempeño. Los resultados se pueden incorporar en las actividades globales de gestión del desempeño, medición y reporte externo e interno de la organización.

Los resultados del monitoreo y la revisión se deberían registrar y reportar interna y externamente según corresponda, y se deberían utilizar como una entrada para la revisión del marco de referencia para la gestión del riesgo (véase el numeral 4.5).

### 5.7 REGISTRO DEL PROCESO PARA LA GESTIÓN DEL RIESGO

Las actividades para la gestión del riesgo deberían tener trazabilidad. En el proceso para la gestión del riesgo, los registros brindan la base para la mejora de los métodos y las herramientas, así como del proceso global.

En las decisiones con respecto a la creación de registros se debería tener en cuenta:

- las necesidades de la organización con respecto al aprendizaje continuo;
- los beneficios de reutilizar la información con propósitos de gestión;
- los costos y esfuerzos involucrados en la creación y el mantenimiento de los registros;
- las necesidades legales, reglamentarias y operativas para los registros;
- los métodos de acceso, la facilidad de recuperación y los medios de almacenamiento;
- el periodo de retención; y
- la sensibilidad de la información.

**ANEXO A**  
(Informativo)

**ATRIBUTOS DE LA GESTIÓN MEJORADA DEL RIESGO**

**A.1 GENERALIDADES**

Todas las organizaciones deberían tener como meta el nivel adecuado de desempeño de su marco de referencia para la gestión del riesgo en concordancia con la importancia crítica de las decisiones que se deben tomar. La lista de atributos que se indica a continuación representa un nivel alto de desempeño en la gestión del riesgo. Para ayudar a las organizaciones a medir su propio desempeño en comparación con estos criterios, se brindan algunos indicadores tangibles para cada atributo.

**A.2 RESULTADOS IMPORTANTES**

- A.2.1** La organización tiene una comprensión actual, correcta y exhaustiva de sus riesgos.
- A.2.2** Los riesgos de la organización se encuentran dentro de sus criterios del riesgo.

**A.3 ATRIBUTOS**

**A.3.1 Mejora continua**

Se hace énfasis en la mejora continua de la gestión del riesgo a través del establecimiento de las metas de desempeño de la organización, la medición, revisión y modificación posterior de procesos, sistemas, recursos, capacidad y habilidades.

El indicador podría ser la existencia de metas explícitas de desempeño en comparación con las cuales se mide el desempeño de la organización y del director individual. El desempeño de la organización se puede publicar y comunicar. Normalmente, habrá por lo menos una revisión anual del desempeño, después una revisión de los procesos, y luego el establecimiento de objetivos revisados de desempeño para el período siguiente.

La valoración del desempeño de la gestión del riesgo es una parte integral de la valoración global del desempeño de la organización y del sistema de medición para los departamentos y los individuos.

**A.3.2 Rendición total de cuentas con respecto a los riesgos**

La gestión mejorada del riesgo incluye la rendición de cuentas exhaustiva, totalmente definida y aceptada de los riesgos, los controles y las tareas para el tratamiento del riesgo. Los individuos asignados aceptan totalmente la responsabilidad, tienen las habilidades adecuadas y los recursos pertinentes para verificar los controles, monitorear los riesgos, mejorar

los controles y comunicarse eficazmente acerca de los riesgos y su gestión con las partes involucradas externas e internas.

El indicador podría estar constituido por todos los miembros de una organización que conocen totalmente los riesgos, los controles y las labores de las cuales son responsables. Normalmente, la responsabilidad estará registrada en las descripciones del trabajo o el cargo, en las bases de datos o los sistemas de información. La definición de las funciones, obligaciones y responsabilidades en la gestión del riesgo debería ser parte de los programas de inducción de la organización

La organización garantiza que los responsables están equipados para cumplir esa función brindándoles la autoridad, el tiempo, el entrenamiento, los recursos y las habilidades suficientes para asumir sus obligaciones.

#### **A.3.3 Aplicación de la gestión del riesgo en la toma de decisiones**

La toma de decisiones en la organización, independientemente del nivel de importancia y significado, involucra la consideración explícita de los riesgos y la aplicación, en algún grado, de la gestión de riesgos.

El indicador podría consistir en registros de las reuniones y las decisiones que muestren que tuvieron lugar las discusiones explícitas sobre los riesgos. Además, debería ser posible ver que todos los componentes de la gestión del riesgo están representados en los procesos clave para la toma de decisiones en la organización, por ejemplo para las decisiones sobre asignación de capital o proyectos principales y sobre los cambios de estructurales y organizacionales. Por estas razones, una base sólida para la gestión del riesgo se considera en la organización aquella que brinda las bases para el gobierno eficaz.

#### **A.3.4 Comunicaciones continuas**

La gestión mejorada del riesgo incluye las comunicaciones continuas con las partes involucradas externas e internas, que incluyan el reporte exhaustivo y frecuente del desempeño de la gestión del riesgo como parte del buen gobierno.

El indicador podría ser la comunicación con las partes involucradas como componente integral y esencial de la gestión del riesgo. La comunicación puede bien considerarse un proceso de doble vía, de modo que se pueden tomar decisiones correctamente informadas acerca del nivel del riesgo y la necesidad de tratamiento frente a criterios del riesgo adecuadamente establecidos y exhaustivos.

El reporte exhaustivo y frecuente, externo e interno, tanto sobre los riesgos significativos como sobre el desempeño de la gestión del riesgo contribuye significativamente al gobierno eficaz dentro de la organización.

#### **A.3.5 Integración completa en la estructura de gobierno de la organización**

La gestión del riesgo se considera parte central de los procesos de gestión de la organización, de modo que los riesgos están considerados en términos del efecto de la incertidumbre en

## NORMA TÉCNICA COLOMBIANA NTC-ISO 31000

los objetivos. La estructura y los procesos de gobierno se basan en la gestión del riesgo. La gestión eficaz del riesgo es considerada por los directores un factor esencial para el logro de los objetivos de la organización.

El indicador podría ser el lenguaje de los directores y el material escrito importante en la organización que utiliza el término "incertidumbre" en conexión con los riesgos. Este atributo también está reflejado normalmente en las declaraciones de la política de la organización, en particular las que se relacionan con la gestión del riesgo. Normalmente, este atributo se verificaría a través de entrevistas con los directores y a través de la evidencia de sus actos y declaraciones.

### BIBLIOGRAFÍA

- [1] ISO Guide 73:2009, *Risk Management. Vocabulary.*
- [2] ISO/IEC 31010, *Risk Management. Risk Assessment Techniques.*

---

**NORMA TÉCNICA COLOMBIANA NTC-ISO 31000**

---

**DOCUMENTO DE REFERENCIA**

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. *Risk Management. Principles and Guidelines*. Geneva: ISO, 2009, 24p (ISO /IEC 31000:2009 (E)).

---

GESTIÓN DEL RIESGO **47**