NORMA INTERNACIONAL

ISO 31000

Traducción oficial
Official translation
Traduction officielle

Segunda edición
2018-02

Gestión del riesgo — Directrices

Risk management — Guidelines

Management du risque — Lignes directrices

Publicado por la Secretaría Central de ISO en Ginebra, Suiza, como traducción oficial en español avalada por el *Translation Management Group*, que ha certificado la conformidad en relación con las versiones inglesa y francesa.

Número de referencia
ISO 31000:2018
(traducción oficial)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Ginebra, Suiza
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Versión española publicada en 2018

Índice

Página

Prólogo ..... **iv**

Prólogo de la versión en español ..... **v**

Introducción ..... **vi**

1 Objeto y campo de aplicación **1**

2 Referencias normativas **1**

3 Términos y definiciones **1**

4 Principios **3**

5 Marco de referencia **4**

5.1 Generalidades 4
5.2 Liderazgo y compromiso 5
5.3 Integración 6
5.4 Diseño 6
5.4.1 Comprensión de la organización y de su contexto 6
5.4.2 Articulación del compromiso con la gestión del riesgo 7
5.4.3 Asignación de roles, autoridades, responsabilidades y obligación de rendir cuentas en la organización 8
5.4.4 Asignación de recursos 8
5.4.5 Establecimiento de la comunicación y la consulta 8
5.5 Implementación 9
5.6 Valoración 9
5.7 Mejora 9
5.7.1 Adaptación 9
5.7.2 Mejora continua 9

6 Proceso **10**

6.1 Generalidades 10
6.2 Comunicación y consulta 11
6.3 Alcance, contexto y criterios 11
6.3.1 Generalidades 11
6.3.2 Definición del alcance 11
6.3.3 Contextos externo e interno 12
6.3.4 Definición de los criterios del riesgo 12
6.4 Evaluación del riesgo 13
6.4.1 Generalidades 13
6.4.2 Identificación del riesgo 13
6.4.3 Análisis del riesgo 13
6.4.4 Valoración del riesgo 14
6.5 Tratamiento del riesgo 15
6.5.1 Generalidades 15
6.5.2 Selección de las opciones para el tratamiento del riesgo 15
6.5.3 Preparación e implementación de los planes de tratamiento del riesgo 16
6.6 Seguimiento y revisión 16
6.7 Registro e informe 17

Bibliografía **18**

Prólogo

ISO (Organización Internacional de Normalización) es una federación mundial de organismos nacionales de normalización (organismos miembros de ISO). El trabajo de preparación de las Normas Internacionales normalmente se realiza a través de los comités técnicos de ISO. Cada organismo miembro interesado en una materia para la cual se haya establecido un comité técnico, tiene el derecho de estar representado en dicho comité. Las organizaciones internacionales, públicas y privadas, en coordinación con ISO, también participan en el trabajo. ISO colabora estrechamente con la Comisión Electrotécnica Internacional (IEC) en todas las materias de normalización electrotécnica.

En la Parte 1 de las Directivas ISO/IEC se describen los procedimientos utilizados para desarrollar este documento y para su mantenimiento posterior. En particular debería tomarse nota de los diferentes criterios de aprobación necesarios para los distintos tipos de documentos ISO. Este documento se redactó de acuerdo a las reglas editoriales de la Parte 2 de las Directivas ISO/IEC. www.iso.org/directives.

Se llama la atención sobre la posibilidad de que algunos de los elementos de este documento puedan estar sujetos a derechos de patente. ISO no asume la responsabilidad por la identificación de cualquiera o todos los derechos de patente. Los detalles sobre cualquier derecho de patente identificado durante el desarrollo de este documento se indican en la introducción y/o en la lista ISO de declaraciones de patente recibidas. www.iso.org/patents.

Cualquier nombre comercial utilizado en este documento es información que se proporciona para comodidad del usuario y no constituye una recomendación.

Para obtener una explicación sobre el significado de los términos específicos de ISO y expresiones relacionadas con la evaluación de la conformidad, así como información de la adhesión de ISO a los principios de la Organización Mundial del Comercio (OMC) respecto a los Obstáculos Técnicos al Comercio (OTC), véase la siguiente dirección: www.iso.org/iso/foreword.html.

El comité responsable de este documento es el ISO/TC 262, *Gestión del riesgo.*

Esta segunda edición anula y sustituye a la primera edición (ISO 31000:2009) que ha sido revisada técnicamente.

Los principales cambios en comparación con la edición anterior son los siguientes:

— se revisan los principios de la gestión del riesgo, que son los criterios clave para su éxito;

— se destaca el liderazgo de la alta dirección y la integración de la gestión del riesgo, comenzando con la gobernanza de la organización;

— se pone mayor énfasis en la naturaleza iterativa de la gestión del riesgo, señalando que las nuevas experiencias, el conocimiento y el análisis pueden llevar a una revisión de los elementos del proceso, las acciones y los controles en cada etapa del proceso;

— se simplifica el contenido con un mayor enfoque en mantener un modelo de sistemas abiertos para adaptarse a múltiples necesidades y contextos.

Prólogo de la versión en español

Este documento ha sido traducido por el Grupo de Trabajo *Spanish Translation Task Force* (STTF) del Comité Técnico ISO/TC 262, *Gestión del riesgo*, en el que participan representantes de los organismos nacionales de normalización y representantes del sector empresarial de los siguientes países:

Argentina, Chile, Colombia, Costa Rica, Ecuador, El Salvador, España, México, Panamá, Perú, y Uruguay.

Igualmente, en el citado Grupo de Trabajo participan representantes de COPANT (Comisión Panamericana de Normas Técnicas) e INLAC (Instituto Latinoamericano de la Calidad).

Esta traducción es parte del resultado del trabajo que el Grupo ISO/TC 262/STTF viene desarrollando desde su creación en el año 2017 para lograr la unificación de la terminología en lengua española en el ámbito de la gestión del riesgo.

Introducción

Este documento está dirigido a las personas que crean y protegen el valor en las organizaciones gestionando riesgos, tomando decisiones, estableciendo y logrando objetivos y mejorando el desempeño.

Las organizaciones de todos los tipos y tamaños se enfrentan a factores e influencias externas e internas que hacen incierto si lograrán sus objetivos.

La gestión del riesgo es iterativa y asiste a las organizaciones a establecer su estrategia, lograr sus objetivos y tomar decisiones informadas.

La gestión del riesgo es parte de la gobernanza y el liderazgo y es fundamental en la manera en que se gestiona la organización en todos sus niveles. Esto contribuye a la mejora de los sistemas de gestión.

La gestión del riesgo es parte de todas las actividades asociadas con la organización e incluye la interacción con las partes interesadas.

La gestión del riesgo considera los contextos externo e interno de la organización, incluido el comportamiento humano y los factores culturales.

La gestión del riesgo está basada en los principios, el marco de referencia y el proceso descritos en este documento, conforme se ilustra en la Figura 1. Estos componentes podrían existir previamente en toda o parte de la organización, sin embargo, podría ser necesario adaptarlos o mejorarlos para que la gestión del riesgo sea eficiente, eficaz y coherente.

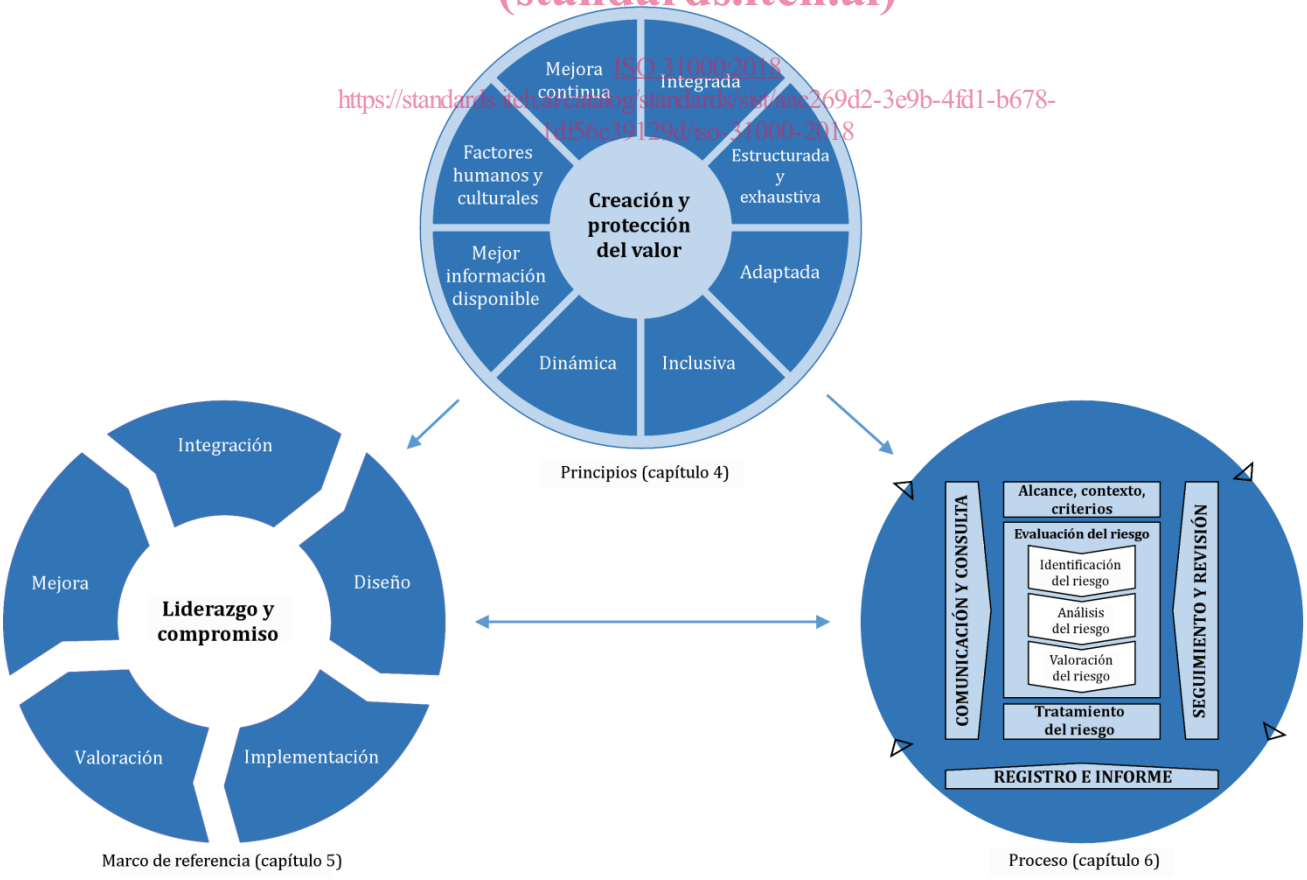

Figura 1 — Principios, marco de referencia y proceso

Gestión del riesgo — Directrices

1 Objeto y campo de aplicación

Este documento proporciona directrices para gestionar el riesgo al que se enfrentan las organizaciones. La aplicación de estas directrices puede adaptarse a cualquier organización y a su contexto.

Este documento proporciona un enfoque común para gestionar cualquier tipo de riesgo y no es específico de una industria o un sector.

Este documento puede utilizarse a lo largo de la vida de la organización y puede aplicarse a cualquier actividad, incluyendo la toma de decisiones a todos los niveles.

2 Referencias normativas

El presente documento no contiene referencias normativas.

3 Términos y definiciones

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

ISO e IEC mantienen bases de datos terminológicas para su utilización en normalización en las siguientes direcciones:

— Plataforma de búsqueda en línea de ISO: disponible en http://www.iso.org/obp

— Electropedia de IEC: disponible en http://www.electropedia.org

3.1
riesgo
efecto de la incertidumbre sobre los objetivos

Nota 1 a la entrada: Un efecto es una desviación respecto a lo previsto. Puede ser positivo, negativo o ambos, y puede abordar, crear o resultar en oportunidades y amenazas.

Nota 2 a la entrada: Los objetivos pueden tener diferentes aspectos y categorías, y se pueden aplicar a diferentes niveles.

Nota 3 a la entrada: Con frecuencia, el riesgo se expresa en términos de *fuentes de riesgo* (3.4), *eventos* (3.5) potenciales, sus *consecuencias* (3.6) y sus *probabilidades* (3.7).

3.2
gestión del riesgo
actividades coordinadas para dirigir y controlar la organización con relación al *riesgo* (3.1)

3.3
parte interesada
persona u organización que puede afectar, verse afectada, o percibirse como afectada por una decisión o actividad

Nota 1 a la versión en español: Los términos en inglés "interested party" y "stakeholder" tienen una traducción única al español como "parte interesada".

3.4
fuente de riesgo
elemento que, por sí solo o en combinación con otros, tiene el potencial de generar *riesgo* (3.1)

3.5
evento
ocurrencia o cambio de un conjunto particular de circunstancias

Nota 1 a la entrada: Un evento puede tener una o más ocurrencias y puede tener varias causas y varias *consecuencias* (3.6).

Nota 2 a la entrada: Un evento también puede ser algo previsto que no llega a ocurrir, o algo no previsto que ocurre.

Nota 3 a la entrada: Un evento puede ser una fuente de riesgo.

3.6
consecuencia
resultado de un *evento* (3.5) que afecta a los objetivos

Nota 1 a la entrada: Una consecuencia puede ser cierta o incierta y puede tener efectos positivos o negativos, directos o indirectos sobre los objetivos.

Nota 2 a la entrada: Las consecuencias se pueden expresar de manera cualitativa o cuantitativa.

Nota 3 a la entrada: Cualquier consecuencia puede incrementarse por efectos en cascada y efectos acumulativos.

3.7
probabilidad (*likelihood*)
posibilidad de que algo suceda

Nota 1 a la entrada: En la terminología de *gestión del riesgo* (3.2), la palabra "probabilidad" se utiliza para indicar la posibilidad de que algo suceda, esté definida, medida o determinada objetiva o subjetivamente, cualitativa o cuantitativamente, y descrita utilizando términos generales o matemáticos (como una probabilidad matemática o una frecuencia en un periodo de tiempo determinado).

Nota 2 a la entrada: El término inglés "likelihood" (probabilidad) no tiene un equivalente directo en algunos idiomas; en su lugar se utiliza con frecuencia el término probabilidad. Sin embargo, en inglés la palabra "probability" (probabilidad matemática) se interpreta frecuentemente de manera más limitada como un término matemático. Por ello, en la terminología de gestión del riesgo, "likelihood" se utiliza con la misma interpretación amplia que tiene la palabra probabilidad en otros idiomas distintos del inglés.

3.8
control
medida que mantiene y/o modifica un *riesgo* (3.1)

Nota 1 a la entrada: Los controles incluyen, pero no se limitan a cualquier proceso, política, dispositivo, práctica u otras condiciones y/o acciones que mantengan y/o modifiquen un riesgo.

Nota 2 a la entrada: Los controles no siempre pueden producir el efecto de modificación previsto o asumido.

4 Principios

El propósito de la gestión del riesgo es la creación y la protección del valor. Mejora el desempeño, fomenta la innovación y contribuye al logro de objetivos.

Los principios descritos en la Figura 2 proporcionan orientación sobre las características de una gestión del riesgo eficaz y eficiente, comunicando su valor y explicando su intención y propósito. Los principios son el fundamento de la gestión del riesgo y se deberían considerar cuando se establece el marco de referencia y los procesos de la gestión del riesgo de la organización. Estos principios deberían habilitar a la organización para gestionar los efectos de la incertidumbre sobre sus objetivos.

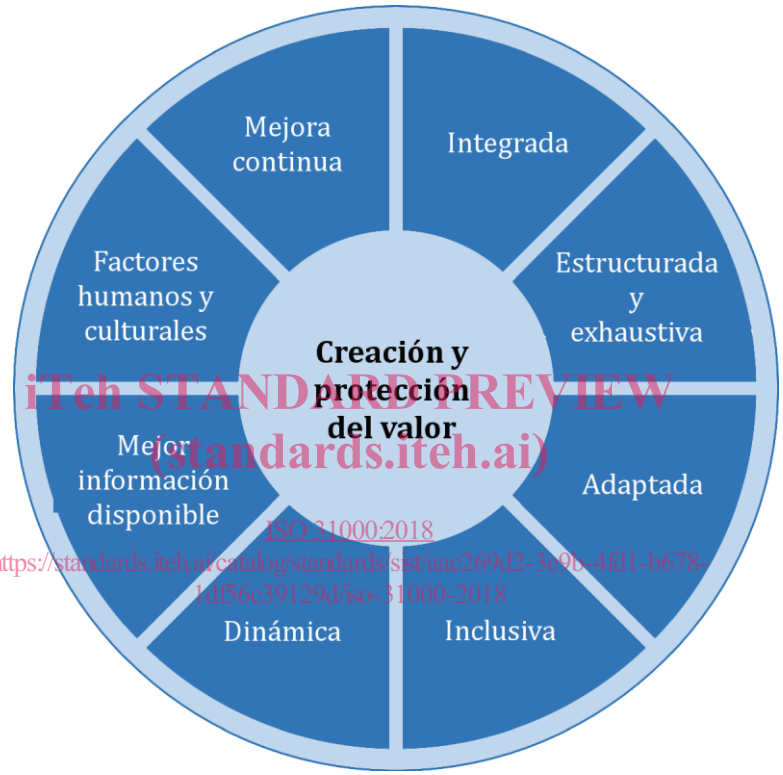

Figura 2 — Principios

La gestión del riesgo eficaz requiere los elementos de la Figura 2 y puede explicarse como sigue.

a) Integrada

La gestión del riesgo es parte integral de todas las actividades de la organización.

b) Estructurada y exhaustiva

Un enfoque estructurado y exhaustivo hacia la gestión del riesgo contribuye a resultados coherentes y comparables.

c) Adaptada

El marco de referencia y el proceso de la gestión del riesgo se adaptan y son proporcionales a los contextos externo e interno de la organización relacionados con sus objetivos.

d) Inclusiva

La participación apropiada y oportuna de las partes interesadas permite que se consideren su conocimiento, puntos de vista y percepciones. Esto resulta en una mayor toma de conciencia y una gestión del riesgo informada.

e) Dinámica

Los riesgos pueden aparecer, cambiar o desaparecer con los cambios de los contextos externo e interno de la organización. La gestión del riesgo anticipa, detecta, reconoce y responde a esos cambios y eventos de una manera apropiada y oportuna.

f) Mejor información disponible

Las entradas a la gestión del riesgo se basan en información histórica y actualizada, así como en expectativas futuras. La gestión del riesgo tiene en cuenta explícitamente cualquier limitación e incertidumbre asociada con tal información y expectativas. La información debería ser oportuna, clara y disponible para las partes interesadas pertinentes.

g) Factores humanos y culturales

El comportamiento humano y la cultura influyen considerablemente en todos los aspectos de la gestión del riesgo en todos los niveles y etapas.

h) Mejora continua

La gestión del riesgo mejora continuamente mediante aprendizaje y experiencia.

5 Marco de referencia

5.1 Generalidades

El propósito del marco de referencia de la gestión del riesgo es asistir a la organización en integrar la gestión del riesgo en todas sus actividades y funciones significativas. La eficacia de la gestión del riesgo dependerá de su integración en la gobernanza de la organización, incluyendo la toma de decisiones. Esto requiere el apoyo de las partes interesadas, particularmente de la alta dirección.

El desarrollo del marco de referencia implica integrar, diseñar, implementar, valorar y mejorar la gestión del riesgo a lo largo de toda la organización. La Figura 3 ilustra los componentes del marco de referencia.

Figura 3 — Marco de referencia

La organización debería valorar sus prácticas y procesos existentes de la gestión del riesgo, valorar cualquier brecha y abordar estas brechas en el marco de referencia.

Los componentes del marco de referencia y la manera en la que trabajan juntos, deberían adaptarse a las necesidades de la organización.

5.2 Liderazgo y compromiso

La alta dirección y los órganos de supervisión, cuando sea aplicable, deberían asegurar que la gestión del riesgo esté integrada en todas las actividades de la organización y deberían demostrar el liderazgo y compromiso:

— adaptando e implementando todos los componentes del marco de referencia;

— publicando una declaración o una política que establezca un enfoque, un plan o una línea de acción para la gestión del riesgo;

— asegurando que los recursos necesarios se asignan para gestionar los riesgos;

— asignando autoridad, responsabilidad y obligación de rendir cuentas en los niveles apropiados dentro de la organización;

Esto ayudará a la organización a:

— alinear la gestión del riesgo con sus objetivos, estrategia y cultura;

— reconocer y abordar todas las obligaciones, así como sus compromisos voluntarios;