Norma Española

UNE-ISO 31000

Marzo 2018

Gestión del riesgo

Directrices

Esta norma ha sido elaborada por el comité técnico CTN 307 *Gestión de riesgos*, cuya secretaría desempeña UNE.

Asociación Española
de Normalización
Génova, 6 - 28004 Madrid
915 294 900
info@une.org
www.une.org

UNE-ISO 31000

Gestión del riesgo
Directrices

Risk management. Guidelines.

Management du risque. Lignes directrices.

Esta norma es idéntica a la Norma Internacional ISO 31000:2018.

Esta norma anula y sustituye a la Norma UNE-ISO 31000:2010.

Las observaciones a este documento han de dirigirse a:

Asociación Española de Normalización
Génova, 6
28004 MADRID-España
Tel.: 915 294 900
info@une.org
www.une.org
Depósito legal: M 10593:2018

Índice

Prólogo **4**

Prólogo de la versión en español **5**

0 Introducción **6**

1 Objeto y campo de aplicación **7**

2 Normas para consulta **7**

3 Términos y definiciones **7**

4 Principios **8**

5 Marco de referencia **10**
5.1 Generalidades **10**
5.2 Liderazgo y compromiso **11**
5.3 Integración **12**
5.4 Diseño **13**
5.4.1 Comprensión de la organización y de su contexto **13**
5.4.2 Articulación del compromiso con la gestión del riesgo **13**
5.4.3 Asignación de roles, autoridades, responsabilidades y obligación de rendir cuentas en la organización **14**
5.4.4 Asignación de recursos **14**
5.4.5 Establecimiento de la comunicación y la consulta **15**
5.5 Implementación **15**
5.6 Valoración **15**
5.7 Mejora **15**
5.7.1 Adaptación **15**
5.7.2 Mejora continua **16**

6 Proceso **16**
6.1 Generalidades **16**
6.2 Comunicación y consulta **17**
6.3 Alcance, contexto y criterios **17**
6.3.1 Generalidades **17**
6.3.2 Definición del alcance **17**
6.3.3 Contextos externo e interno **18**
6.3.4 Definición de los criterios del riesgo **18**
6.4 Evaluación del riesgo **19**
6.4.1 Generalidades **19**
6.4.2 Identificación del riesgo **19**
6.4.3 Análisis del riesgo **20**
6.4.4 Valoración del riesgo **21**
6.5 Tratamiento del riesgo **21**
6.5.1 Generalidades **21**
6.5.2 Selección de las opciones para el tratamiento del riesgo **21**
6.5.3 Preparación e implementación de los planes de tratamiento del riesgo **22**
6.6 Seguimiento y revisión **23**
6.7 Registro e informe **23**

Bibliografía **25**

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 esta norma y para su mantenimiento posterior. En particular debería tomarse nota de los diferentes criterios de aprobación necesarios para los distintos tipos de documentos ISO. Esta norma 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 esta norma 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 esta norma 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 esta norma 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.

0 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.

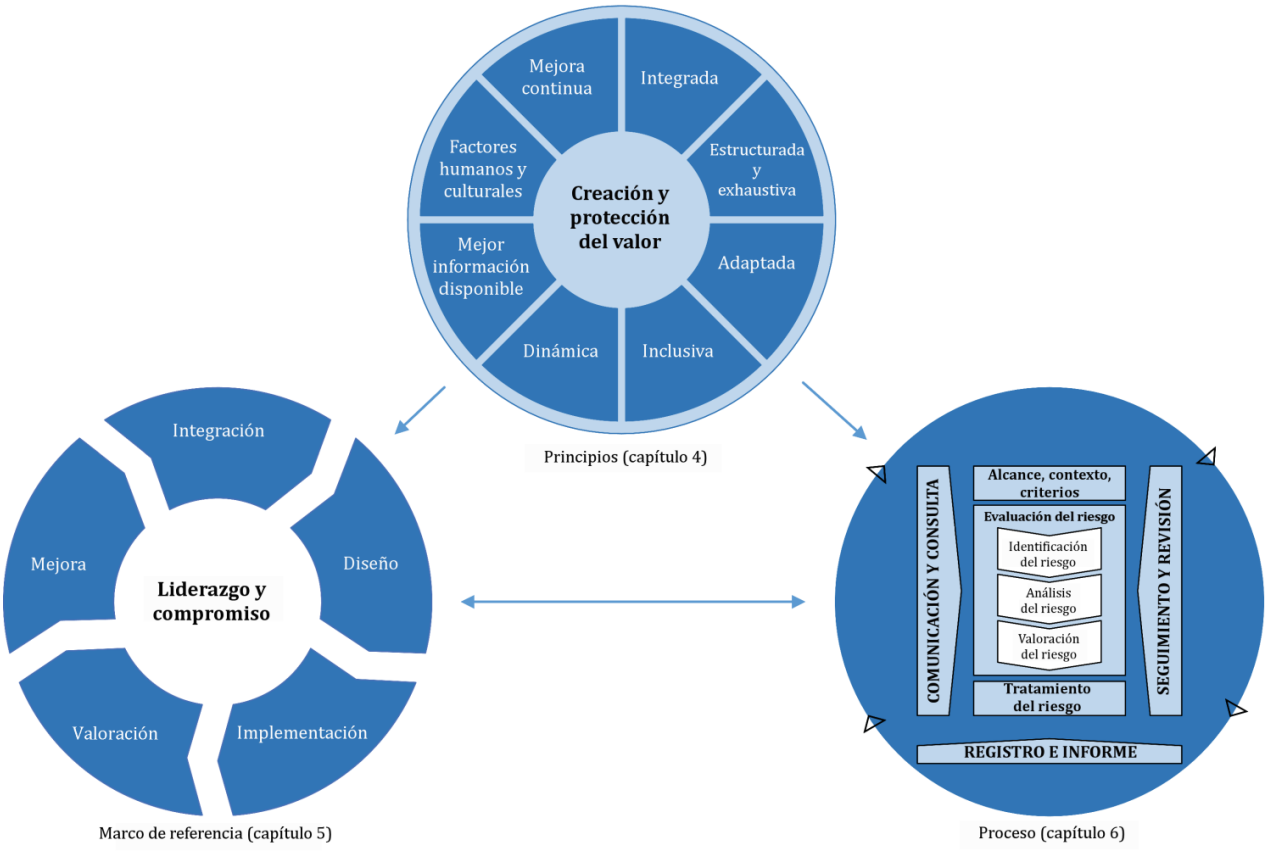

Figura 1 – Principios, marco de referencia y proceso

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 Normas para consulta

El presente documento no contiene normas para consulta.

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.

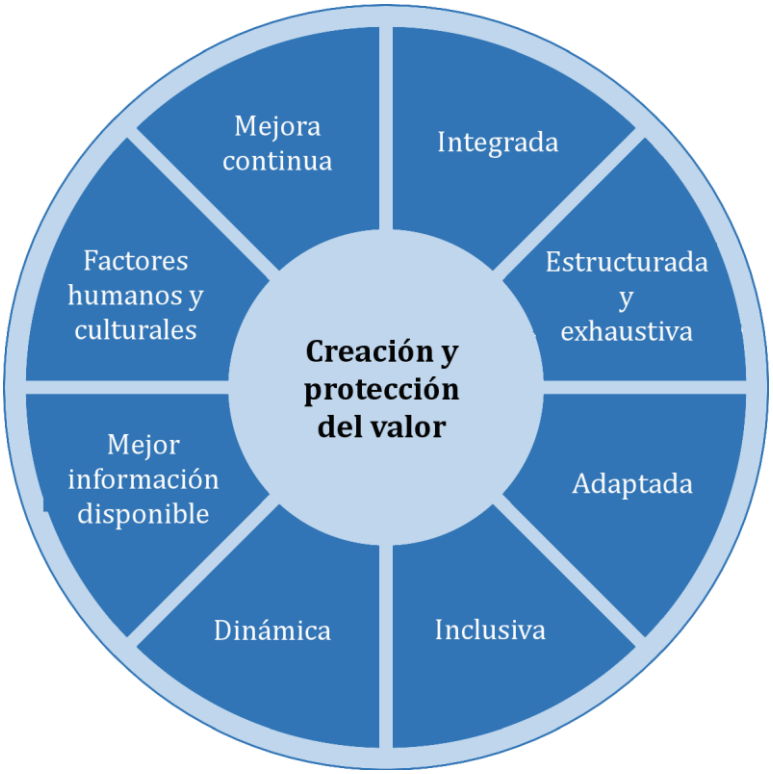

Figura 2 – Principios

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;
- establecer la magnitud y el tipo de riesgo que puede o no ser tomado para guiar el desarrollo de los criterios del riesgo, asegurando que se comunican a la organización y a sus partes interesadas.
- comunicar el valor de la gestión del riesgo a la organización y sus partes interesadas;
- promover el seguimiento sistemático de los riesgos;
- asegurarse de que el marco de referencia de la gestión del riesgo permanezca apropiado al contexto de la organización.

La alta dirección rinde cuentas por gestionar el riesgo mientras que los órganos de supervisión rinden cuentas por la supervisión de la gestión del riesgo. Frecuentemente se espera o se requiere que los órganos de supervisión:

- se aseguren de que los riesgos se consideran apropiadamente cuando se establezcan los objetivos de la organización;
- comprendan los riesgos a los que hace frente la organización en la búsqueda de sus objetivos;
- se aseguren de que los sistemas para gestionar estos riesgos se implementen y operen eficazmente;
- se aseguren de que estos riesgos sean apropiados en el contexto de los objetivos de la organización;
- se aseguren de que la información sobre estos riesgos y su gestión se comunique de la manera apropiada.

5.3 Integración

La integración de la gestión del riesgo depende de la comprensión de las estructuras y el contexto de la organización. Las estructuras difieren dependiendo del propósito, las metas y la complejidad de la organización. El riesgo se gestiona en cada parte de la estructura de la organización. Todos los miembros de una organización tienen la responsabilidad de gestionar el riesgo.

La gobernanza guía el curso de la organización, sus relaciones externas e internas y las reglas, los procesos y las prácticas necesarios para alcanzar su propósito. Las estructuras de gestión convierten la orientación de la gobernanza en la estrategia y los objetivos asociados requeridos para lograr los niveles deseados de desempeño sostenible y de viabilidad en el largo plazo. La determinación de los roles para la rendición de cuentas y la supervisión de la gestión del riesgo dentro de la organización son partes integrales de la gobernanza de la organización.

La integración de la gestión del riesgo en la organización es un proceso dinámico e iterativo, y se debería adaptar a las necesidades y a la cultura de la organización. La gestión del riesgo debería ser una parte de, y no estar separada del propósito, la gobernanza, el liderazgo y compromiso, la estrategia, los objetivos y las operaciones de la organización.

5.4 Diseño

5.4.1 Comprensión de la organización y de su contexto

La organización debería analizar y comprender sus contextos externo e interno cuando diseñe el marco de referencia para gestionar el riesgo.

El análisis del contexto externo de la organización puede incluir, pero no limitarse a:

- los factores sociales, culturales, políticos, legales, reglamentarios, financieros, tecnológicos, económicos y ambientales ya sea a nivel internacional, nacional, regional o local;
- los impulsores clave y las tendencias que afectan a los objetivos de la organización;
- las relaciones, percepciones, valores, necesidades y expectativas de las partes interesadas externas;
- las relaciones contractuales y los compromisos;
- la complejidad de las redes y dependencias.

El análisis del contexto interno de la organización puede incluir, pero no limitarse a:

- la visión, la misión y los valores;
- la gobernanza, la estructura de la organización, los roles y la rendición de cuentas;
- la estrategia, los objetivos y las políticas;
- la cultura de la organización;
- las normas, las directrices y los modelos adoptados por la organización;
- las capacidades, entendidas en términos de recursos y conocimiento (por ejemplo, capital, tiempo, personas, propiedad intelectual, procesos, sistemas y tecnologías);
- los datos, los sistemas de información y los flujos de información;
- las relaciones con partes interesadas internas, teniendo en cuenta sus percepciones y valores;
- las relaciones contractuales y los compromisos;
- las interdependencias e interconexiones.

5.4.2 Articulación del compromiso con la gestión del riesgo

La alta dirección y los organismos de supervisión, cuando sea aplicable, deberían articular y demostrar su compromiso continuo con la gestión del riesgo mediante una política, una declaración u otras formas que expresen claramente los objetivos y el compromiso de la organización con la gestión del riesgo. El compromiso debería incluir, pero no limitarse a:

- el propósito de la organización para gestionar el riesgo y los vínculos con sus objetivos y otras políticas;
- el refuerzo de la necesidad de integrar la gestión del riesgo en toda la cultura de la organización;
- el liderazgo en la integración de la gestión del riesgo en las actividades principales del negocio y la toma de decisiones;
- las autoridades, las responsabilidades y la obligación de rendir cuentas;
- la disponibilidad de los recursos necesarios;
- la manera de manejar los objetivos en conflicto;
- la medición e informe como parte de los indicadores de desempeño de la organización;
- la revisión y la mejora.

El compromiso con la gestión del riesgo se debería comunicar dentro de la organización y a las partes interesadas, de manera apropiada.

5.4.3 Asignación de roles, autoridades, responsabilidades y obligación de rendir cuentas en la organización

La alta dirección y los órganos de supervisión, cuando sea aplicable, deberían asegurarse de que las autoridades, las responsabilidades y la obligación de rendir cuentas de los roles relevantes con respecto a la gestión del riesgo se asignen y comuniquen a todos los niveles de la organización y deberían:

- enfatizar que la gestión del riesgo es una responsabilidad principal;
- identificar a las personas que tienen asignada la obligación de rendir cuentas y la autoridad para gestionar el riesgo (dueños del riesgo).

5.4.4 Asignación de recursos

La alta dirección y los órganos de supervisión, cuando sea aplicable, deberían asegurar la asignación de los recursos apropiados para la gestión del riesgo, que puede incluir, pero no limitarse a:

- las personas, las habilidades, la experiencia y las competencias;
- los procesos, los métodos y las herramientas de la organización a utilizar para gestionar el riesgo;
- los procesos y procedimientos documentados;
- los sistemas de gestión de la información y del conocimiento;
- el desarrollo profesional y las necesidades de formación.

La organización debería considerar las competencias y limitaciones de los recursos existentes.

5.4.5 Establecimiento de la comunicación y la consulta

La organización debería establecer un enfoque aprobado con relación a la comunicación y la consulta, para apoyar el marco de referencia y facilitar la aplicación eficaz de la gestión del riesgo. La comunicación implica compartir información con el público objetivo. La consulta además implica que los participantes proporcionen retroalimentación con la expectativa de que ésta contribuya y de forma a las decisiones u otras actividades. Los métodos y el contenido de la comunicación y la consulta deberían reflejar las expectativas de las partes interesadas, cuando sea pertinente.

La comunicación y la consulta deberían ser oportunas y asegurar que se recopile, consolide, sintetice y comparta la información pertinente, cuando sea apropiado, y que se proporcione retroalimentación y se lleven a cabo mejoras.

5.5 Implementación

La organización debería implementar el marco de referencia de la gestión del riesgo mediante:

- el desarrollo de un plan apropiado incluyendo plazos y recursos;
- la identificación de dónde, cuándo, cómo y quién toma diferentes tipos de decisiones en toda la organización;
- la modificación de los procesos aplicables para la toma de decisiones, cuando sea necesario;
- el aseguramiento de que las disposiciones de la organización para gestionar el riesgo son claramente comprendidas y puestas en práctica.

La implementación con éxito del marco de referencia requiere el compromiso y la toma de conciencia de las partes interesadas. Esto permite a las organizaciones abordar explícitamente la incertidumbre en la toma de decisiones, al tiempo que asegura que cualquier incertidumbre nueva o subsiguiente se pueda tener en cuenta cuando surja.

Si se diseña e implementa correctamente, el marco de referencia de la gestión del riesgo asegurará que el proceso de la gestión del riesgo sea parte de todas actividades en toda la organización, incluyendo la toma de decisiones, y que los cambios en los contextos externo e interno se captarán de manera adecuada.

5.6 Valoración

Para valorar la eficacia del marco de referencia de la gestión del riesgo, la organización debería:

- medir periódicamente el desempeño del marco de referencia de la gestión del riesgo con relación a su propósito, sus planes para la implementación, sus indicadores y el comportamiento esperado;
- determinar si permanece idóneo para apoyar el logro de los objetivos de la organización.

5.7 Mejora

5.7.1 Adaptación

La organización debería realizar el seguimiento continuo y adaptar el marco de referencia de la gestión del riesgo en función de los cambios externos e internos. Al hacer esto, la organización puede mejorar su valor.

5.7.2 Mejora continua

La organización debería mejorar continuamente la idoneidad, adecuación y eficacia del marco de referencia de la gestión del riesgo y la manera en la que se integra el proceso de la gestión del riesgo.

Cuando se identifiquen brechas u oportunidades de mejora pertinentes, la organización debería desarrollar planes y tareas y asignarlas a quienes tuviesen que rendir cuentas de su implementación. Una vez implementadas, estas mejoras deberían contribuir al fortalecimiento de la gestión del riesgo.

6 Proceso

6.1 Generalidades

El proceso de la gestión del riesgo implica la aplicación sistemática de políticas, procedimientos y prácticas a las actividades de comunicación y consulta, establecimiento del contexto y evaluación, tratamiento, seguimiento, revisión, registro e informe del riesgo. Este proceso se ilustra en la figura 4.

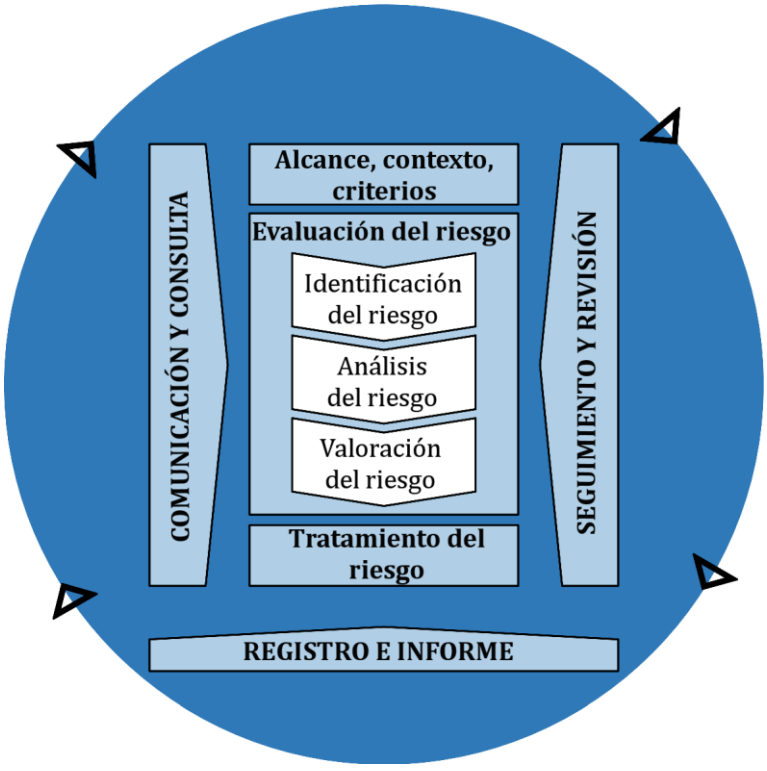

Figura 4 – Proceso

El proceso de la gestión del riesgo debería ser una parte integral de la gestión y de la toma de decisiones y se debería integrar en la estructura, las operaciones y los procesos de la organización. Puede aplicarse a nivel estratégico, operacional, de programa o de proyecto.

Puede haber muchas aplicaciones del proceso de la gestión del riesgo dentro de la organización, adaptadas para lograr objetivos, y apropiadas a los contextos externo e interno en los cuales se aplican.

A lo largo del proceso de la gestión del riesgo se debería considerar la naturaleza dinámica y variable del comportamiento humano y de la cultura.

Aunque el proceso de la gestión del riesgo se presenta frecuentemente como secuencial, en la práctica es iterativo.

6.2 Comunicación y consulta

El propósito de la comunicación y consulta es asistir a las partes interesadas pertinentes a comprender el riesgo, las bases con las que se toman decisiones y las razones por las que son necesarias acciones específicas. La comunicación busca promover la toma de conciencia y la comprensión del riesgo, mientras que la consulta implica obtener retroalimentación e información para apoyar la toma de decisiones. Una coordinación cercana entre ambas debería facilitar un intercambio de información basado en hechos, oportuno, pertinente, exacto y comprensible, teniendo en cuenta la confidencialidad e integridad de la información, así como el derecho a la privacidad de las personas.

La comunicación y consulta con las partes interesadas apropiadas, externas e internas, se debería realizar en todas y cada una de las etapas del proceso de la gestión del riesgo.

La comunicación y consulta pretende:

- reunir diferentes áreas de experiencia para cada etapa del proceso de la gestión del riesgo;
- asegurar que se consideren de manera apropiada los diferentes puntos de vista cuando se definen los criterios del riesgo y cuando se valoran los riesgos;
- proporcionar suficiente información para facilitar la supervisión del riesgo y la toma de decisiones;
- construir un sentido de inclusión y propiedad entre las personas afectadas por el riesgo.

6.3 Alcance, contexto y criterios

6.3.1 Generalidades

El propósito del establecimiento del alcance, contexto y criterios es adaptar el proceso de la gestión del riesgo, para permitir una evaluación del riesgo eficaz y un tratamiento apropiado del riesgo. El alcance, el contexto y los criterios implican definir el alcance del proceso, y comprender los contextos externo e interno.

6.3.2 Definición del alcance

La organización debería definir el alcance de sus actividades de gestión del riesgo.

Como el proceso de la gestión del riesgo puede aplicarse a niveles distintos (por ejemplo: estratégico, operacional, de programa, de proyecto u otras actividades), es importante tener claro el alcance considerado, los objetivos pertinentes a considerar y su alineamiento con los objetivos de la organización.

En la planificación del enfoque se incluyen las siguientes consideraciones:

- los objetivos y las decisiones que se necesitan tomar;
- los resultados esperados de las etapas a ejecutar en el proceso;
- el tiempo, la ubicación, las inclusiones y las exclusiones especificas;
- las herramientas y las técnicas apropiadas de evaluación del riesgo;
- los recursos requeridos, responsabilidades y registros a conservar;
- las relaciones con otros proyectos, procesos y actividades.

6.3.3 Contextos externo e interno

Los contextos externo e interno son el entorno en el cual la organización busca definir y lograr sus objetivos.

El contexto del proceso de la gestión del riesgo se debería establecer a partir de la comprensión de los entornos externo e interno en los cuales opera la organización y debería reflejar el entorno específico de la actividad en la cual se va a aplicar el proceso de la gestión del riesgo.

La comprensión del contexto es importante porque:

- la gestión del riesgo tiene lugar en el contexto de los objetivos y las actividades de la organización;
- los factores organizacionales pueden ser una fuente de riesgo;
- el propósito y alcance del proceso de la gestión del riesgo puede estar interrelacionado con los objetivos de la organización como un todo;

La organización debería establecer los contextos externo e interno del proceso de la gestión del riesgo considerando los factores mencionados en 5.4.1.

6.3.4 Definición de los criterios del riesgo

La organización debería precisar la cantidad y el tipo de riesgo que puede o no puede tomar, con relación a los objetivos. También debería definir los criterios para valorar la importancia del riesgo y para apoyar los procesos de toma de decisiones. Los criterios del riesgo se deberían alinear con el marco de referencia de la gestión del riesgo y adaptar al propósito y al alcance específicos de la actividad considerada. Los criterios del riesgo deberían reflejar los valores, objetivos y recursos de la organización y ser coherentes con las políticas y declaraciones acerca de la gestión del riesgo. Los criterios se deberían definir teniendo en consideración las obligaciones de la organización y los puntos de vista de sus partes interesadas.

Aunque los criterios del riesgo se deberían establecer al principio del proceso de la evaluación del riesgo, éstos son dinámicos, y deberían revisarse continuamente y si fuese necesario, modificarse.

Para establecer los criterios del riesgo, se debería considerar lo siguiente:

- la naturaleza y los tipos de las incertidumbres que pueden afectar a los resultados y objetivos (tanto tangibles como intangibles);
- cómo se van a definir y medir las consecuencias (tanto positivas como negativas) y la probabilidad;
- los factores relacionados con el tiempo;
- la coherencia en el uso de las mediciones;
- cómo se va a determinar el nivel de riesgo;
- cómo se tendrán en cuenta las combinaciones y las secuencias de múltiples riesgos;
- la capacidad de la organización.

6.4 Evaluación del riesgo

6.4.1 Generalidades

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

La evaluación del riesgo se debería llevar a cabo de manera sistemática, iterativa y colaborativa, basándose en el conocimiento y los puntos de vista de las partes interesadas. Se debería utilizar la mejor información disponible, complementada por investigación adicional, si fuese necesario.

6.4.2 Identificación del riesgo

El propósito de la identificación del riesgo es encontrar, reconocer y describir los riesgos que pueden ayudar o impedir a una organización lograr sus objetivos. Para la identificación de los riesgos es importante contar con información pertinente, apropiada y actualizada.

La organización puede utilizar un rango de técnicas para identificar incertidumbres que pueden afectar a uno o varios objetivos. Se deberían considerar los factores siguientes y la relación entre estos factores:

- las fuentes de riesgo tangibles e intangibles;
- las causas y los eventos;
- las amenazas y las oportunidades;
- las vulnerabilidades y las capacidades;
- los cambios en los contextos externo e interno;
- los indicadores de riesgos emergentes;
- la naturaleza y el valor de los activos y los recursos;

– las consecuencias y sus impactos en los objetivos;

– las limitaciones de conocimiento y la confiabilidad de la información;

– los factores relacionados con el tiempo;

– los sesgos, los supuestos y las creencias de las personas involucradas.

La organización debería identificar los riesgos, tanto si sus fuentes están o no bajo su control. Se debería considerar que puede haber más de un tipo de resultado, que puede dar lugar a una variedad de consecuencias tangibles o intangibles.

6.4.3 Análisis del riesgo

El propósito del análisis del riesgo es comprender la naturaleza del riesgo y sus características incluyendo, cuando sea apropiado, el nivel del riesgo. El análisis del riesgo implica una consideración detallada de incertidumbres, fuentes de riesgo, consecuencias, probabilidades, eventos, escenarios, controles y su eficacia. Un evento puede tener múltiples causas y consecuencias y puede afectar a múltiples objetivos.

El análisis del riesgo se puede realizar con diferentes grados de detalle y complejidad, dependiendo del propósito del análisis, la disponibilidad y la confiabilidad de la información y los recursos disponibles. Las técnicas de análisis pueden ser cualitativas, cuantitativas o una combinación de éstas, dependiendo de las circunstancias y del uso previsto.

El análisis del riesgo debería considerar factores tales como:

– la probabilidad de los eventos y de las consecuencias;

– la naturaleza y la magnitud de las consecuencias;

– la complejidad y la interconexión;

– los factores relacionados con el tiempo y la volatilidad;

– la eficacia de los controles existentes;

– los niveles de sensibilidad y de confianza.

El análisis del riesgo puede estar influenciado por cualquier divergencia de opiniones, sesgos, percepciones del riesgo y juicios. Las influencias adicionales son la calidad de la información utilizada, los supuestos y las exclusiones establecidos, cualquier limitación de las técnicas y cómo se ejecutan éstas. Estas influencias se deberían considerar, documentar y comunicar a las personas que toman decisiones.

Los eventos de alta incertidumbre pueden ser difíciles de cuantificar. Esto puede ser una cuestión importante cuando se analizan eventos con consecuencias severas. En tales casos, el uso de una combinación de técnicas generalmente proporciona una visión más amplia.

El análisis del riesgo proporciona una entrada para la valoración del riesgo, para las decisiones sobre la manera de tratar los riesgos y si es necesario hacerlo y sobre la estrategia y los métodos más apropiados de tratamiento del riesgo. Los resultados proporcionan un entendimiento profundo para tomar decisiones, cuando se está eligiendo entre distintas alternativas, y las opciones implican diferentes tipos y niveles de riesgo.

6.4.4 Valoración del riesgo

El propósito de la valoración del riesgo es apoyar a la toma de decisiones. La valoración del riesgo implica comparar los resultados del análisis del riesgo con los criterios del riesgo establecidos para determinar cuándo se requiere una acción adicional. Esto puede conducir a una decisión de:

- no hacer nada más;
- considerar opciones para el tratamiento del riesgo;
- realizar un análisis adicional para comprender mejor el riesgo;
- mantener los controles existentes;
- reconsiderar los objetivos.

Las decisiones deberían tener en cuenta un contexto más amplio y las consecuencias reales y percibidas por las partes interesadas externas e internas.

Los resultados de la valoración del riesgo se deberían registrar, comunicar y luego validar a los niveles apropiados de la organización.

6.5 Tratamiento del riesgo

6.5.1 Generalidades

El propósito del tratamiento del riesgo es seleccionar e implementar opciones para abordar el riesgo. El tratamiento del riesgo implica un proceso iterativo de:

- formular y seleccionar opciones para el tratamiento del riesgo;
- planificar e implementar el tratamiento del riesgo;
- evaluar la eficacia de ese tratamiento;
- decidir si el riesgo residual es aceptable;
- si no es aceptable, efectuar tratamiento adicional.

6.5.2 Selección de las opciones para el tratamiento del riesgo

La selección de las opciones más apropiadas para el tratamiento del riesgo implica hacer un balance entre los beneficios potenciales, derivados del logro de los objetivos contra costos, esfuerzo o desventajas de la implementación.

Las opciones de tratamiento del riesgo no necesariamente son mutuamente excluyentes o apropiadas en todas las circunstancias. Las opciones para tratar el riesgo pueden implicar una o más de las siguientes:

- evitar el riesgo decidiendo no iniciar o continuar con la actividad que genera el riesgo;
- aceptar o aumentar el riesgo en busca de una oportunidad;
- eliminar la fuente de riesgo;
- modificar la probabilidad;
- modificar las consecuencias;
- compartir el riesgo (por ejemplo: a través de contratos, compra de seguros);
- retener el riesgo con base en una decisión informada.

La justificación para el tratamiento del riesgo es más amplia que las simples consideraciones económicas y debería tener en cuenta todas las obligaciones de la organización, los compromisos voluntarios y los puntos de vista de las partes interesadas. La selección de las opciones para el tratamiento del riesgo debería realizarse de acuerdo con los objetivos de la organización, los criterios del riesgo y los recursos disponibles.

Al seleccionar opciones para el tratamiento del riesgo, la organización debería considerar los valores, las percepciones, el involucrar potencialmente a las partes interesadas y los medios más apropiados para comunicarse con ellas y consultarlas. A igual eficacia, algunas partes interesadas pueden aceptar mejor que otras los diferentes tratamientos del riesgo.

Los tratamientos del riesgo, a pesar de un cuidadoso diseño e implementación, pueden no producir los resultados esperados y puede producir consecuencias no previstas. El seguimiento y la revisión necesitan ser parte integral de la implementación del tratamiento del riesgo para asegurar que las distintas maneras del tratamiento sean y permanezcan eficaces.

El tratamiento del riesgo a su vez puede introducir nuevos riesgos que necesiten gestionarse.

Si no hay opciones disponibles para el tratamiento o si las opciones para el tratamiento no modifican suficientemente el riesgo, éste se debería registrar y mantener en continua revisión.

Las personas que toman decisiones y otras partes interesadas deberían ser conscientes de la naturaleza y el nivel del riesgo residual después del tratamiento del riesgo. El riesgo residual se debería documentar y ser objeto de seguimiento, revisión y, cuando sea apropiado, de tratamiento adicional.

6.5.3 Preparación e implementación de los planes de tratamiento del riesgo

El propósito de los planes de tratamiento del riesgo es especificar la manera en la que se implementarán las opciones elegidas para el tratamiento, de manera tal que los involucrados comprendan las disposiciones, y que pueda realizarse el seguimiento del avance respecto de lo planificado. El plan de tratamiento debería identificar claramente el orden en el cual el tratamiento del riesgo se debería implementar.

Los planes de tratamiento deberían integrarse en los planes y procesos de la gestión de la organización, en consulta con las partes interesadas apropiadas.

La información proporcionada en el plan del tratamiento debería incluir:

- el fundamento de la selección de las opciones para el tratamiento, incluyendo los beneficios esperados;
- las personas que rinden cuentas y aquellas responsables de la aprobación e implementación del plan;
- las acciones propuestas;
- los recursos necesarios, incluyendo las contingencias;
- las medidas del desempeño;
- las restricciones;
- los informes y seguimiento requeridos;
- los plazos previstos para la realización y la finalización de las acciones.

6.6 Seguimiento y revisión

El propósito del seguimiento y la revisión es asegurar y mejorar la calidad y la eficacia del diseño, la implementación y los resultados del proceso. El seguimiento continuo y la revisión periódica del proceso de la gestión del riesgo y sus resultados debería ser una parte planificada del proceso de la gestión del riesgo, con responsabilidades claramente definidas.

El seguimiento y la revisión deberían tener lugar en todas etapas del proceso. El seguimiento y la revisión incluyen planificar, recopilar y analizar información, registrar resultados y proporcionar retroalimentación.

Los resultados del seguimiento y la revisión deberían incorporarse a todas las actividades de la gestión del desempeño, de medición y de informe de la organización.

6.7 Registro e informe

El proceso de la gestión del riesgo y sus resultados se deberían documentar e informar a través de los mecanismos apropiados. El registro e informe pretenden:

- comunicar las actividades de la gestión del riesgo y sus resultados a lo largo de la organización;
- proporcionar información para la toma de decisiones;
- mejorar las actividades de la gestión del riesgo;
- asistir la interacción con las partes interesadas, incluyendo a las personas que tienen la responsabilidad y la obligación de rendir cuentas de las actividades de la gestión del riesgo.

Las decisiones con respecto a la creación, conservación y tratamiento de la información documentada deberían tener en cuenta, pero no limitarse a su uso, la sensibilidad de la información y los contextos externo e interno.

El informe es una parte integral de la gobernanza de la organización y debería mejorar la calidad del diálogo con las partes interesadas, y apoyar a la alta dirección y a los órganos de supervisión a cumplir sus responsabilidades. Los factores a considerar en el informe incluyen, pero no se limitan a:

- las diferentes partes interesadas, sus necesidades y requisitos específicos de información;
- el costo, la frecuencia y los tiempos del informe;
- el método del informe;
- la pertinencia de la información con respecto a los objetivos de la organización y la toma de decisiones.

Bibliografía

[1] IEC 31010, *Risk management. Risk assessment techniques.*

Para información relacionada con el desarrollo de las normas contacte con:

Asociación Española de Normalización
Génova, 6
28004 MADRID-España
Tel.: 915 294 900
info@une.org
www.une.org

Para información relacionada con la venta y distribución de las normas contacte con:

AENOR INTERNACIONAL S.A.U.
Tel.: 914 326 000
normas@aenor.com
www.aenor.com

UNE NormalizaciónEspañola organismo de normalización español en: