NORMA INTERNACIONAL

ISO 31000

Segunda edición
2018-02

Administración/Gestión de riesgos — Lineamientos guía

Número de referencia
ISO 31000:2018

Índice

Página

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 debiera 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, *Administración/Gestión de riesgos.*

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 administración/gestión de riesgos, que son los criterios clave para su éxito;

— se destaca el liderazgo de la alta dirección y la integración de la administración/gestión de riesgos, comenzando con la gobernanza de la organización;

— se pone mayor énfasis en la naturaleza iterativa de la administración/gestión de riesgos, 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.

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 tipos y tamaños se enfrentan a factores e influencias internas y externas que hacen incierto si lograrán sus objetivos.

La administración/gestión de riesgos es iterativa y apoya a las organizaciones a establecer su estrategia, lograr sus objetivos y tomar decisiones informadas.

La administración/gestión de riesgos 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 administración/gestión.

La administración/gestión de riesgos es parte de todas las actividades asociadas con la organización e incluye la interacción con las partes interesadas.

La administración/gestión de riesgos considera los contextos interno y externo de la organización, incluyendo el comportamiento humano y los factores culturales.

La administración/gestión de riesgos 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 administración/gestión de riesgos sea eficiente, efectiva y coherente.

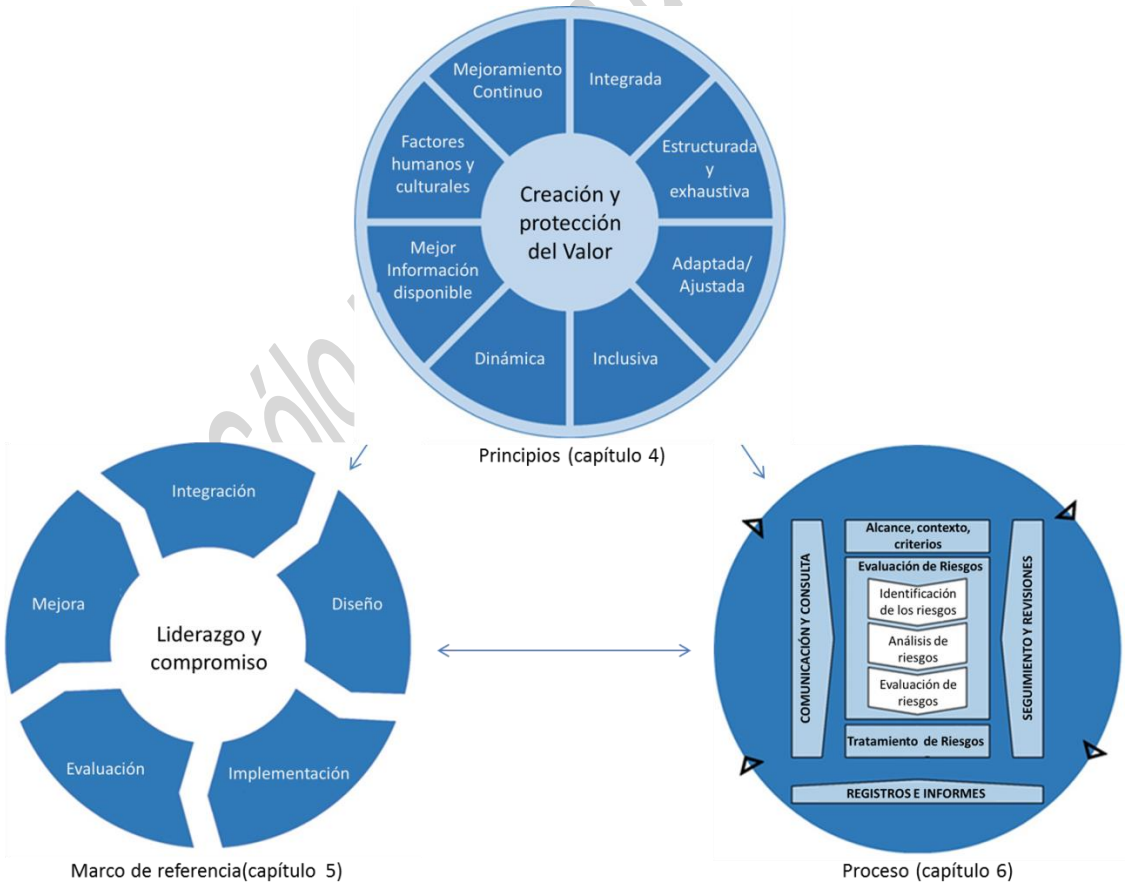

Figura 1 — Principios, marco de referencia y proceso

Administración/Gestión de riesgos — Lineamientos guía

1 Alcance

Este documento ofrece lineamientos guía para administrar/gestionar los riesgos a los que las organizaciones se enfrentan. La aplicación de estos lineamientos puede adaptarse a cualquier organización y a su contexto.

Este documento proporciona un enfoque común para administrar/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 incertidumbre sobre los objetivos

Nota 1 de 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 de entrada: Los objetivos pueden tener diferentes aspectos y categorías, y se pueden aplicar a diferentes niveles.

Nota 3 de 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
administración/gestión de riesgos
actividades coordinadas para dirigir y controlar la organización con relación a los *riesgos* (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 de 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 riesgos
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 de entrada: Un evento puede tener una o más ocurrencias y puede tener varias causas y varias *consecuencias* (3.6).

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

Nota 3 de 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 de entrada: Una consecuencia puede ser cierta o incierta y puede tener efectos positivos o negativos, directos o indirectos sobre los objetivos.

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

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

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

Nota 1 de entrada: En la terminología de *administración/gestión de riesgos* (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 de 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 administración/gestión de riesgos, "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 de 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 de entrada: Los controles no siempre pueden producir el efecto de modificación previsto o asumido.

4 Principios

El propósito de la administración/gestión de riesgos 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 administración/gestión de riesgos efectiva y eficiente, comunicando su valor y explicando su intención y propósito. Los principios son el fundamento de la administración/gestión de riesgos y se debieran considerar cuando se establece el marco de referencia y los procesos de la administración/gestión de riesgos de la organización. Estos principios debieran habilitar a la organización para administrar/gestionar los efectos de incertidumbres sobre sus objetivos.

Figura 2 — Principios

La administración/gestión de riesgos efectiva requiere los elementos de la Figura 2 y pueden explicarse como sigue.

a) Integrada

La administración/gestión de riesgos es parte integral de todas las actividades de la organización.

b) Estructurada y exhaustiva

Un enfoque estructurado y exhaustivo hacia la administración/gestión de riesgos contribuye a resultados coherentes y comparables.

c) Adaptada/Ajustada

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

d) Inclusiva

La participación apropiada y oportuna de las partes interesadas permite que se consideren sus conocimientos, puntos de vista y percepciones. Esto resulta en una mayor toma de concientización y una administración/gestión de riesgos informada.

e) Dinámica

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

f) Mejor información disponible

Las entradas a la administración/gestión de riesgos se basan en información histórica y actualizada, así como en expectativas futuras. La administración/gestión de riesgos tiene en cuenta explícitamente cualquier limitación e incertidumbre asociada con tal información y expectativas. La información debiera 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 administración/gestión de riesgos en todos los niveles y etapas.

h) Mejora continua

La administración/gestión de riesgos mejora continuamente mediante aprendizaje y experiencia.

5 Marco de referencia

5.1 Generalidades

El propósito del marco de referencia de la administración/gestión de riesgos es apoyar a las organizaciones en integrar la administración/gestión de riesgos en todas sus actividades y funciones significativas. La efectividad de la administración/gestión de riesgos dependerá de su integración en la gobernanza de las organizaciones, 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, evaluar y mejorar la administración/gestión de riesgos a lo largo de toda la organización. La Figura 3 ilustra los componentes del marco de referencia.

Figura 3 — Marco de referencia

Las organizaciones debieran evaluar sus prácticas y procesos existentes de la administración/gestión de riesgos, evaluar 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, debieran adaptarse a las necesidades de las organizaciones.

5.2 Liderazgo y compromiso

La alta dirección y los órganos de supervisión, cuando sea aplicable, debieran asegurar que la administración/gestión de riesgos esté integrada en todas las actividades de la organización y debieran 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 administración/gestión de riesgos;

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

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

Esto ayudará a las organizaciones a:

— alinear la administración/gestión de riesgos con sus objetivos, estrategias y cultura;

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

— establecer la magnitud y el tipo de riesgos que puede o no ser tomados para guiar el desarrollo de los criterios de los riesgos mismos, asegurando que se comunican a la organización y a sus partes interesadas.

— comunicar el valor de la administración/gestión de riesgos a las organizaciones y sus partes interesadas;

— promover el seguimiento sistemático de los riesgos;

— asegurarse de que el marco de referencia de la administración/gestión de riesgos permanezca apropiado al contexto de la organización.

La alta dirección rinde cuentas por administrar/gestionar los riesgos mientras que los órganos de supervisión rinden cuentas por la supervisión de la administración/gestión de riesgos. 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 administrar/gestionar estos riesgos se implementen y operen efectivamente;

— 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 administración/gestión se comunique de la manera apropiada.

5.3 Integración

La integración de la administración/gestión de riesgos depende de la comprensión de las estructuras y el contexto de las organizaciones. Las estructuras difieren dependiendo del propósito, las metas y la complejidad de las organizaciones. Los riesgos se gestionan en cada parte de la estructura de la organización. Todos los miembros de una organización tienen la responsabilidad de administrar/gestionar los riesgos.

La gobernanza guía el curso de las organizaciones, sus relaciones internas y externas y las reglas, los procesos y las prácticas necesarios para alcanzar sus propósitos. Las estructuras de administración/gestión convierten la orientación de la gobernanza en las estrategias y objetivos asociados requeridos para lograr los niveles deseados del desempeño sostenible y de viabilidad en el largo plazo. La determinación de los roles para la rendición de cuentas y la supervisión de la administración/gestión de riesgos dentro de las organizaciones son partes integrales de la gobernanza de la organizaciones mismas.

La integración de la administración/gestión de riesgos en las organizaciones es un proceso dinámico e iterativo, y se debiera adaptar a las necesidades y a la cultura de las organizaciones mismas. La administración/gestión de riesgos debiera ser una parte de, y no estar separada del propósito, la gobernanza, el liderazgo y compromiso, las estrategias, los objetivos y las operaciones de las organizaciones.

5.4 Diseño

5.4.1 Comprensión de las organizaciones y su contexto

Las organizaciones debiera analizar y comprender sus contextos interno y externo cuando diseñe el marco de referencia para administrar/gestionar sus riesgos.

El análisis del contexto externo de las organizaciones 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 las organizaciones puede incluir, pero no limitarse a:

— la visión, la misión y los valores;

— la gobernanza, la estructura de las organizaciones, los roles y la rendición de cuentas;

— las estrategias, los objetivos y las políticas;

— la cultura de las organizaciones;

— las normas, las directrices y los modelos adoptados por las organizaciones;

— las capacidades, entendidas en términos de recursos y conocimientos (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 administración/gestión de riesgos

La alta dirección y los organismos de supervisión, cuando sea aplicable, debieran articular y demostrar su compromiso continuo con la administración/gestión de riesgos mediante una política, una declaración u otras formas que expresen claramente los objetivos y el compromiso de las organizaciones con la administración/gestión de riesgos. El compromiso debiera incluir, pero no limitarse a:

— el propósito de las organizaciones para administrar/gestionar el riesgo y los vínculos con sus objetivos y otras políticas;

— el refuerzo de la necesidad de integrar la administración/gestión de riesgos en toda la cultura de las organizaciones mismas;

— el liderazgo en la integración de la administración/gestión de riesgos 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 y reporte como parte de los indicadores de desempeño de las organizaciones;

— la revisión y la mejora.

El compromiso con la administración/gestión de riesgos se debiera 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, debieran asegurarse de que las autoridades, las responsabilidades y la obligación de rendir cuentas de los roles relevantes con respecto a la administración/gestión de riesgos se asignen y comuniquen a todos los niveles de la organización y debieran:

— enfatizar que la administración/gestión de riesgos es una responsabilidad principal;

— identificar a las personas que tienen asignada la obligación de rendir cuentas y la autoridad para administrar/gestionar los riesgos (dueños de los riesgos).

5.4.4 Asignación de recursos

La alta dirección y los órganos de supervisión, cuando sea aplicable, debieran asegurar la asignación de los recursos apropiados para la administración/gestión de riesgos, 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 administrar/gestionar los riesgos;

— los procesos y procedimientos documentados;

— los sistemas de administración/gestión de la información y del conocimiento;

— el desarrollo profesional y las necesidades de formación.

Las organizaciones debieran considerar las competencias y limitaciones de sus recursos existentes.

5.4.5 Establecimiento de la comunicación y la consulta

Las organizaciones debiera establecer un enfoque aprobado con relación a la comunicación y la consulta, para apoyar el marco de referencia y facilitar la aplicación efectiva de la administración/gestión de riesgos. 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 debieran reflejar las expectativas de las partes interesadas, cuando sea pertinente.

La comunicación y la consulta debieran 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

Las organizaciones debieran implementar el marco de referencia para la administración/gestión de riesgos 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 las organizaciones para administrar/gestionar el riesgo sean claramente comprendidas y puestas en práctica.

La implementación con éxito del marco de referencia requiere del compromiso y la concientización 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 administración/gestión de riesgos asegurará que el proceso de la administración/gestión de riesgos sea parte de todas actividades en toda la organización, incluyendo la toma de decisiones, y que los cambios en los contextos interno y externo se captarán de manera adecuada.

5.6 Evaluación

Para evaluar la efectividad del marco de referencia de la administración/gestión de riesgos, las organizaciones debiera:

— medir periódicamente el desempeño del marco de referencia de la administración/gestión de riesgos 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 las organizaciones mismas.

5.7 Mejora

5.7.1 Adaptación

Las organizaciones debieran realizar el seguimiento continuo y adaptar el marco de referencia de la administración/gestión de riesgos en función de los cambios internos y externos. Al hacer esto, las organizaciones puede mejorar su valor.

5.7.2 Mejora continua

Las organizaciones debieran mejorar continuamente la idoneidad, adecuación y efectividad del marco de referencia de la administración/gestión de riesgos y la manera en la que se integra el proceso de la administración/gestión de riesgos.

Cuando se identifiquen brechas u oportunidades de mejora pertinentes, las organizaciones debieran desarrollar planes y tareas y asignarlas a quienes tuviesen que rendir cuentas de su implementación. Una vez implementadas, estas mejoras debieran contribuir al fortalecimiento de la administración/gestión de riesgos.

6 Proceso

6.1 Generalidades

El proceso de administración/gestión de riesgos implica la aplicación sistemática de políticas, procedimientos y prácticas a las actividades de comunicación y consulta, establecimiento del contexto y evaluación, tratamiento, seguimiento, revisión, registros y reportes de los riesgos. Este proceso se ilustra en la Figura 4.

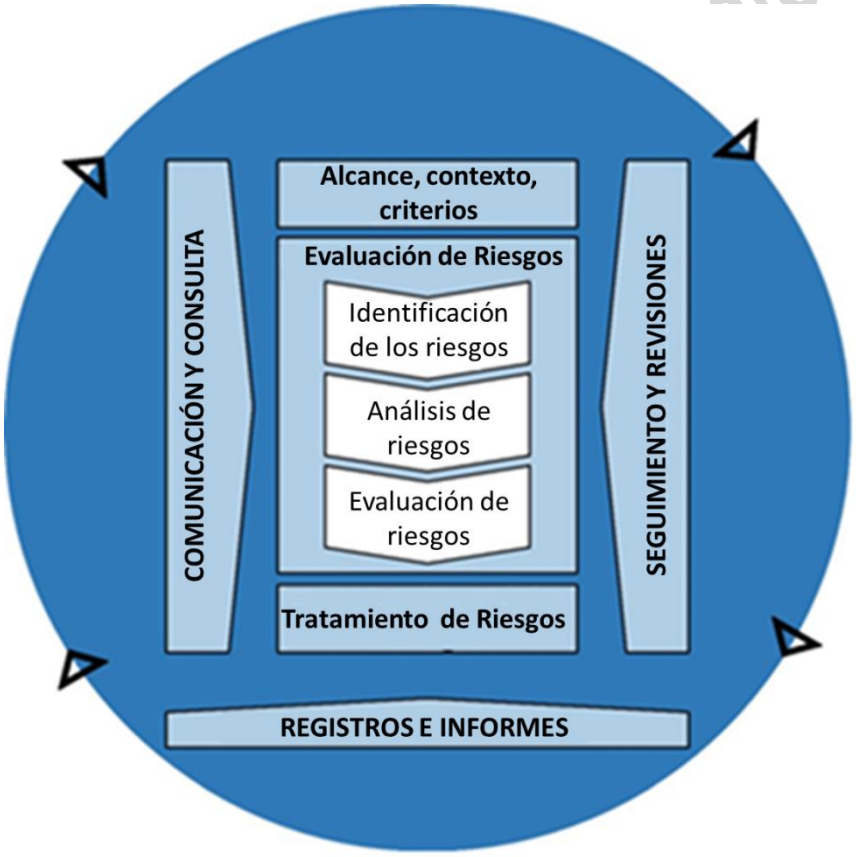

Figura 4 — Proceso

El proceso de la administración/gestión de riesgos debiera ser una parte integral de la administración/gestión y de la toma de decisiones y se debiera integrar en la estructura, las operaciones y los procesos de la organización. Puede aplicarse a nivel estratégico, operacional, de programas o de proyectos.

Puede haber muchas aplicaciones del proceso de la administración/gestión de riesgos dentro de las organizaciones, adaptadas para lograr objetivos, y apropiadas a los contextos interno y externo en los cuales se aplican.

A lo largo del proceso de la administración/gestión de riesgos se debiera considerar la naturaleza dinámica y variable del comportamiento humano y la cultura.

Aunque el proceso de administración/gestión de riesgos se presenta frecuentemente como secuencial, en la práctica es iterativo.

6.2 Comunicación y consulta

El propósito de la comunicación y consulta es apoyar a las partes interesadas pertinentes a comprender los riesgos, las bases con las que se toman decisiones y las razones por las que son necesarias acciones específicas. La comunicación busca promover la concientización y la comprensión de los riesgos, mientras que la consulta implica obtener retroalimentación e información para apoyar la toma de decisiones. Una coordinación cercana entre ambas debiera 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, internas y externas, se debieran realizar en todas y cada una de las etapas del proceso de la administración/gestión de riesgos.

La comunicación y consulta pretende:

— reunir diferentes áreas de experiencia para cada etapa del proceso de la administración/gestión de riesgos;

— asegurar que se consideren de manera apropiada los diferentes puntos de vista cuando se definen los criterios de riesgos y cuando se valoran los riesgos mismos;

— proporcionar suficiente información para facilitar la supervisión de los riesgos y la toma de decisiones;

— construir un sentido de inclusión y propiedad entre las personas afectadas por los riesgos.

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 administración/gestión de riesgos, para permitir una evaluación de riesgos efectiva y un tratamiento apropiado de los riesgos mismos. El alcance, contexto y criterios implican definir el alcance del proceso, y comprender los contextos interno y externo.

6.3.2 Definición del alcance

Las organizaciones debiera definir el alcance de sus actividades de administración/gestión de riesgos.

Como el proceso de la administración/gestión de riesgos puede aplicarse a niveles distintos (por ejemplo: estratégico, operacional, de programas, de proyectos 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 planeación 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 de riesgos;

— los recursos requeridos, responsabilidades y registros a conservar;

— las relaciones con otros proyectos, procesos y actividades.

6.3.3 Contextos interno y externo

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

El contexto del proceso de la administración/gestión de riesgos se debiera establecer a partir de la comprensión de los entornos interno y externo en los cuales opera las organizaciones y debiera reflejar el entorno específico de la actividad en la cual se va a aplicar el proceso de la administración/gestión de riesgos.

La comprensión del contexto es importante porque:

— la administración/gestión de riesgos tiene lugar en el contexto de los objetivos y las actividades de las organizaciones;

— los factores organizacionales pueden ser una fuente de riesgos;

— el propósito y alcance del proceso de la administración/gestión de riesgos puede estar interrelacionado con los objetivos de la organización como un todo;

Las organizaciones debieran establecer los contextos interno y externo del proceso de la administración/gestión de riesgos considerando los factores mencionados en 5.4.1.

6.3.4 Definición de los criterios para riesgos

Las organizaciones debieran precisar la cantidad y el tipo de riesgos que pueden o no tomar, con relación a los objetivos. También debieran definir los criterios para evaluar la importancia de los riesgos y apoyar los procesos de toma de decisiones. Los criterios para riesgos se debieran alinear con el marco de referencia de la administración/gestión de riesgos y adaptar al propósito y al alcance específicos de la actividad considerada. Los criterios para riesgos debieran reflejar los valores, objetivos y recursos de la organización y ser coherentes con las políticas y declaraciones acerca de la administración/gestión de riesgos. Los criterios se debieran definir teniendo en consideración las obligaciones de las organizaciones y los puntos de vista de sus partes interesadas.

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

Para establecer los criterios para riesgos, se debiera considerar lo siguiente:

— la naturaleza y los tipos de 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 riesgos;

— cómo se tendrán en cuenta las combinaciones y las secuencias de múltiples riesgos;

— la capacidad de las organizaciones mismas.

6.4 Evaluación de riesgos

6.4.1 Generalidades

La evaluación de riesgos es el proceso global de identificación, análisis y evaluación de los riesgos mismos.

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

6.4.2 Identificación de riesgos

El propósito de la identificación de riesgos 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.

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

— las fuentes de riesgos tangibles e intangibles;

— las causas y los eventos,

— las amenazas y las oportunidades;

— las vulnerabilidades y las capacidades;

— los cambios en los contextos interno y externo;

— 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.

Las organizaciones debieran identificar los riesgos, tanto si sus fuentes están o no bajo su control. Se debiera 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 de riesgos

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

El análisis de riesgos 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 de riesgos debiera 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 efectividad de los controles existentes;

— los niveles de sensibilidad y de confianza.

El análisis de riesgos puede estar influenciado por cualquier divergencia de opiniones, sesgos, percepciones de los riesgo mismos 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 debieran 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 de riesgos proporciona una entrada para la evaluación de los riesgos, para las decisiones sobre la manera de tratar los riesgos y si es necesario hacerlo y sobre las estrategias y métodos más apropiados de tratamiento para riesgos. 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 Evaluación de riesgos

El propósito de la evaluación de los riesgos es apoyar a la toma de decisiones. La evaluación de los riesgos implica comparar los resultados del análisis del riesgo con los criterios para riesgos 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 para riesgos;

— realizar un análisis adicional para comprender mejor el riesgo;

— mantener los controles existentes;

— reconsiderar los objetivos.

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

Los resultados de evaluaciones de los riesgos se debieran registrar, comunicar y luego validar a los niveles apropiados de la organización.

6.5 Tratamiento de los riesgos

6.5.1 Generalidades

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

— formular y seleccionar opciones para el tratamiento de los riesgos;

— planear e implementar el tratamiento de los riesgos;

— evaluar la efectividad de dicho tratamiento;

— decidir si los riesgos residuales son aceptables;

— si no son aceptables, efectuar algún tratamiento adicional.

6.5.2 Selección de las opciones para el tratamiento de riesgos

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

— evitar el riesgo decidiendo no iniciar o continuar con la actividad que genera el riesgo mismo;

— 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 de riesgos es más amplia que las simples consideraciones económicas y debiera 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 de riesgos debiera realizarse de acuerdo con los objetivos de la organización, los criterios para riesgos y los recursos disponibles.

Al seleccionar opciones para el tratamiento de riesgos, las organizaciones debieran 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 efectividad, algunas partes interesadas pueden aceptar mejor que otras los diferentes tratamientos de los riesgos.

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

El tratamiento de los riesgos a su vez puede introducir nuevos riesgos que necesiten administrarse/gestionarse.

Si no hay opciones disponibles para un tratamiento o si las opciones para un tratamiento no modifican suficientemente los riesgos, esto se debiera registrar y mantener en continua revisión.

Las personas que toman decisiones y otras partes interesadas debieran ser conscientes de la naturaleza y el nivel de los riesgos residuales después del tratamiento de un riesgo. Los riesgos residuales se debieran documentar y ser objeto de seguimiento, revisión y, cuando sea apropiado, de tratamiento adicional.

6.5.3 Preparación e implementación de los planes para el tratamiento de riesgos

El propósito de los planes para el tratamiento de los riesgos 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 planeado. El plan de tratamiento debiera identificar claramente el orden en el cual el tratamiento del riesgo se debiera implementar.

Los planes de tratamientos debieran integrarse en los planes y procesos de la administración/gestión de las organizaciones, en consulta con las partes interesadas apropiadas.

La información proporcionada en los planes de tratamiento debiera 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 de desempeño;

— las restricciones;

— los reportes y seguimientos requeridos;

— los plazos previstos para la realización y la finalización de las acciones.

6.6 Seguimiento y revisiones

El propósito del seguimiento y las revisiones es asegurar y mejorar la calidad y efectividad del diseño, la implementación y los resultados del proceso. El seguimiento continuo y la revisión periódica del proceso de la administración/gestión de riesgos y sus resultados debiera ser una parte planeada del proceso de la administración/gestión de riesgos, con responsabilidades claramente definidas.

El seguimiento y las revisiones debieran tener lugar en todas etapas del proceso. El seguimiento y las revisiones incluyen planear, recopilar y analizar información, registrar resultados y proporcionar retroalimentación.

Los resultados del seguimiento y las revisiones debieran incorporarse a todas las actividades de la administración/gestión del desempeño, de medición y de reportes de la organización misma.

6.7 Registros e informes

El proceso de la administración/gestión de riesgos y sus resultados se debieran documentar e informar a través de los mecanismos apropiados. Los registros y reportes pretenden:

— comunicar las actividades de la administración/gestión de riesgos y sus resultados a lo largo de la organización;

— ofrecer información para la toma de decisiones;

— mejorar las actividades de la administración/gestión de riesgos;

— apoyar en 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 administración/gestión de riesgos.

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

El reporte es una parte integral de la gobernanza de la organización y debiera 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 reporte incluyen, pero no se limitan a:

— las diferentes partes interesadas, sus necesidades y requisitos específicos de información;

— el costo, la frecuencia y los tiempos de los reportes;

— el método de los reportes;

— la pertinencia de la información con respecto a los objetivos de la organización y la toma de decisiones.

Bibliografía

[1] IEC 31010, *Administración/Gestión de riesgos — Técnicas de evaluación de riesgos*

ICS 03.100.01
Precio basado en 16 páginas