informe UNE

UNE-ISO/TR 31004 IN

Octubre 2015

TÍTULO

Gestión del riesgo

Orientación para la implementación de la Norma ISO 31000

Risk management. Guidance for the implementation of ISO 31000.

Management du risque. Lignes directrices pour l'implementation de l´ISO 31000.

CORRESPONDENCIA

Este informe es equivalente al Informe Técnico ISO/TR 31004:2013.

OBSERVACIONES

ANTECEDENTES

Este informe ha sido elaborado por el comité técnico AEN/CTN 307 *Gestión de riesgos* cuya Secretaría desempeña AENOR.

Editada e impresa por AENOR
Depósito legal: M 33484:2015

LAS OBSERVACIONES A ESTE DOCUMENTO HAN DE DIRIGIRSE A:

AENOR Asociación Española de Normalización y Certificación

Génova, 6
28004 MADRID-España

info@aenor.es
www.aenor.es

Tel.: 902 102 201
Fax: 913 104 032

43 Páginas

Índice

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 Directiva 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 a la atención de los usuarios y no constituyen una recomendación.

Para una explicación del significado de los términos específicos de ISO y de las expresiones relativas a la evaluación de la conformidad, así como para la información sobre la adhesión de ISO a los principios de la organización mundial del comercio (WTO) en el Technical Barriers to Trade (TBT) véase la siguiente URL: Foreword – Supplementary information.

El comité responsable de esta norma es el ISO/TC 262, *Gestión de riesgos*.

0 Introducción

0.1 Generalidades

Las organizaciones usan diferentes métodos para gestionar el efecto de la incertidumbre sobre sus objetivos, es decir, para gestionar el riesgo mediante la detección y comprensión del riesgo, y su modificación, cuando sea necesario.

Este informe técnico está previsto para ayudar a las organizaciones a mejorar la eficacia de sus esfuerzos en gestión del riesgo mediante la alineación de estos con la Norma ISO 31000:2009, la cual presenta un enfoque genérico de gestión del riesgo que pueden aplicar todas las organizaciones para lograr sus objetivos.

Este informe técnico está previsto para ser empleado dentro de las organizaciones por parte de quienes toman las decisiones que tienen impacto en sus objetivos, incluidos los responsables del gobierno y quienes brindan a las organizaciones servicios de asesoría y soporte en gestión del riesgo. Este informe técnico también está previsto para ser empleado por cualquier persona interesada en el riesgo y su gestión, incluidos profesores, estudiantes, legisladores y organismos de reglamentación.

Está prevista su lectura conjunta con la Norma ISO 31000 y es aplicable a cualquier tipo y tamaño de organización. En el anexo A se presentan los conceptos y definiciones esenciales para comprender la Norma ISO 31000.

El capítulo 3 presenta una metodología genérica para ayudar a las organizaciones a adoptar la política de gestión del riesgo existente para alinearse con la Norma ISO 31000 de una manera planificada y según un marco de referencia. También prevé el ajuste dinámico a medida que ocurren cambios en el entorno interno y externo de la organización.

El resto de anexos ofrecen consejos, ejemplos y explicaciones concernientes a la implementación de aspectos seleccionados de la Norma ISO 31000, con el fin de ayudar a los lectores, de acuerdo con su experiencia y necesidades individuales.

Los ejemplos que se ofrecen en este informe técnico se pueden aplicar o no directamente a situaciones u organizaciones particulares, y su propósito es únicamente ilustrativo.

0.2 Conceptos y principios fundamentales

Algunas palabras y conceptos son fundamentales para comprender tanto la Norma ISO 31000 como el presente informe técnico, y se explican en la Norma ISO 31000:2009, capítulo 2, y en el anexo A.

La Norma ISO 31000 enumera once principios para una gestión eficaz del riesgo. El objetivo de estos principios es informar y orientar todos los aspectos del enfoque de la organización a la gestión del riesgo. Los principios describen las características de una gestión eficaz del riesgo. En vez de solo implementar los principios, es importante que la organización los refleje en todos los aspectos de la gestión. Estos funcionan como indicadores del desempeño de la gestión del riesgo, y refuerzan el valor que tiene para la organización gestionar el riesgo de una manera eficaz. También influyen en todos los elementos del proceso de transición descritos en este informe técnico, y los aspectos técnicos que son tratados en los anexos. En el anexo B se presenta asesoría adicional.

En este informe técnico se usan las expresiones “alta dirección” y “órgano de supervisión”: “alta dirección” hace referencia a la persona o grupo de personas que dirige y controla la organización al nivel más alto, mientras que el “órgano de supervisión” hace referencia a la persona o grupo de personas que gobierna una organización, establece mandato y asume la responsabilidad.

NOTA En muchas organizaciones, el órgano de supervisión se podría denominar comité de dirección, consejo de administración, consejo de supervisión, etc.

1 Objeto y campo de aplicación

Este informe técnico proporciona orientación a las organizaciones con relación a la gestión eficaz del riesgo mediante la implementación de la Norma ISO 31000:2009. Proporciona:

– un marco de trabajo para que las organizaciones hagan la transición en sus disposiciones de gestión del riesgo para lograr coherencia con la Norma ISO 31000 de una manera adaptada a las características de la organización;

– una explicación de los conceptos fundamentales de la Norma ISO 31000;

– orientación sobre aspectos de los principios y marco de trabajo de gestión del riesgo que se describen en la Norma ISO 31000.

Cualquier individuo, empresa, asociación o grupo público o privado puede usar este informe técnico.

NOTA Por conveniencia, se hace referencia a todos los diferentes usuarios del presente informe técnico con el término general de "organización".

Este informe técnico no es específico para alguna industria o sector, o para algún tipo de riesgo particular, y se puede aplicar a todas las actividades y partes de las organizaciones.

2 Normas para consulta

Los documentos indicados a continuación, en su totalidad o en parte, son normas para consulta indispensables para la aplicación de este documento. Para las referencias con fecha, sólo se aplica la edición citada. Para las referencias sin fecha se aplica la última edición (incluyendo cualquier modificación de ésta).

ISO 31000:2009, *Gestión del riesgo. Principios y directrices.*

3 Implementación de la Norma ISO 31000

3.1 Generalidades

Este capítulo proporciona orientación a las organizaciones que buscan alinear su enfoque y prácticas de gestión del riesgo con la Norma ISO 31000, y mantener estas prácticas alineadas de manera continua.

Presenta una metodología general que es adecuada para la aplicación de una forma planificada, por cualquier organización, independientemente de la naturaleza de sus disposiciones de gestión del riesgo vigentes. Esta metodología incluye lo siguiente:

– comparación de las prácticas actuales con las descritas en la Norma ISO 31000;

– identificación de lo que es necesario cambiar, y preparar e implementar un plan para hacerlo;

– mantenimiento del seguimiento y revisión continuos para asegurar la mejora continua y la vigencia.

Esto permitirá que la organización tenga una comprensión actual y amplia con relación a sus riesgos, y asegurará que estos riesgos son coherentes con su actitud y criterios de riesgo.

Independientemente de la razón para implementar la Norma ISO 31000, se espera que el hacerlo posibilite que una organización gestione mejor sus riesgos, como apoyo a sus objetivos. En alguna medida, todas las organizaciones hacen gestión del riesgo. La estrategia para implementar la Norma ISO 31000 debería reconocer cómo una organización ya está haciendo gestión del riesgo. El proceso de implementación, como se describe en 3.2, evaluará las disposiciones existentes, y si es necesario, las adaptará y modificará para alinearlas con la Norma ISO 31000.

La Norma ISO 31000 identifica diferentes elementos de un marco de trabajo de gestión del riesgo. Existen varias ventajas que pueden surgir cuando los elementos de ese marco de trabajo están integrados en el gobierno, funciones y procesos de una organización. Estas se relacionan con la eficacia de la organización, la toma de decisiones correctas, y la eficacia.

a) El marco de trabajo para la gestión del riesgo se debería elaborar integrando sus componentes en el sistema global de gestión y de toma de decisiones de la organización, independientemente de si el sistema es formal o informal; los procesos de gestión existentes se pueden mejorar mediante referencia a la Norma ISO 31000.

b) La comprensión y la gestión de la incertidumbre se convierten en componentes integrales en los sistemas de gestión, al establecer un enfoque común para la organización.

c) La implementación del proceso de gestión del riesgo se puede adaptar proporcionalmente al tamaño y a los requisitos de la organización.

d) El gobierno (es decir, dirección y supervisión) de la política de gestión del riesgo, el marco de trabajo y los procesos se pueden integrar en las disposiciones de gobierno existentes de la organización.

e) El informe de gestión del riesgo se integra con otros informes de gestión.

f) El desempeño de la gestión del riesgo se convierte en parte integral del enfoque global de desempeño.

g) La interacción y la conexión entre campos de gestión del riesgo de una organización que están separados con frecuencia (por ejemplo, gestión del riesgo de la empresa, gestión del riesgo financiero, gestión del riesgo de proyectos, gestión de la protección y la seguridad, gestión de la continuidad de negocio, gestión de seguros) se pueden asegurar o mejorar, ya que la atención estará ahora enfocada principalmente en establecer y lograr los objetivos de la organización, teniendo en cuenta el riesgo.

h) Se mejora la comunicación entre equipos y niveles de gestión, acerca de la incertidumbre y el riesgo.

i) Las áreas de gestión del riesgo tienen enfoques comunes para la consecución de los objetivos de la organización. Como consecuencia de ello, puede haber beneficios sociales indirectos, ya que las partes interesadas externas de la organización pueden motivarse a mejorar su actividad de gestión del riesgo respectiva.

j) El tratamiento y los controles del riesgo pueden llegar a ser parte integral de las operaciones diarias.

3.2 Cómo implementar la Norma ISO 31000

Aunque la Norma ISO 31000 explica cómo gestionar el riesgo de forma eficaz, no explica cómo integrar la gestión del riesgo en los procesos de gestión de las organizaciones. Aunque las organizaciones sean diferentes y sus puntos de partida puedan ser diferentes, en todos los casos es aplicable un enfoque de implementación genérico y sistemático.

La organización debería determinar si son necesarios cambios en su marco de trabajo existente para la gestión del riesgo, antes de planificarlos e implementarlos, y luego supervisar la eficacia regular del marco de trabajo corregido. Esto permitirá a la organización:

– alinear sus actividades de gestión del riesgo con los principios para una gestión eficaz del riesgo, descritos en la Norma ISO 31000:2009, capítulo 3;

– aplicar el proceso de gestión del riesgo descrito en la Norma ISO 31000:2009, capítulo 5;

– satisfacer los atributos de la gestión del riesgo mejorada en la Norma ISO 31000:2009, capítulo A.3;

– de este modo, lograr los resultados clave de la Norma ISO 31000:2009, capítulo A.2.

Este enfoque también es aplicable a las organizaciones que ya son coherentes con la Norma ISO 31000, pero que desean mejorar continuamente su marco de trabajo y el proceso de gestión del riesgo recomendado en la Norma ISO 31000:2009, apartados 4.6 y 5.6.

Todos los aspectos de la transición se pueden apoyar en la experiencia de otras organizaciones que gestionan tipos de riesgos similares o que han pasado por procesos similares.

3.3 Integración de la Norma ISO 31000 a los procesos de gestión de la organización

3.3.1 Generalidades

La Norma ISO 31000 presenta un marco de trabajo y un proceso genérico para gestionar los riesgos de cualquier tipo de organización, en su totalidad o en parte. Este apartado presenta orientación para la integración de elementos de la Norma ISO 31000 en el enfoque de gestión de una organización, incluidas sus actividades, procesos y funciones. Las organizaciones pueden integrar los conceptos de la Norma ISO 31000 a sus procesos ya existentes, o pueden diseñar o establecer un nuevo enfoque basado en la Norma ISO 31000. Este apartado describe los elementos esenciales del marco de trabajo y del proceso, y las acciones necesarias para la integración exitosa de estos elementos para cumplir los objetivos de la organización. Hay muchas formas de integrar la Norma ISO 31000 a una organización. La selección y el orden de los elementos se deberían adaptar a las necesidades de la organización y de sus partes involucradas. Es necesario prestar atención cuando se aplica este informe técnico, para asegurar que la integración brinde soporte a la estrategia global de negocio de la organización. De esta manera se conducen los esfuerzos de la organización para el logro de los objetivos de la organización relacionados con protección y creación de valor. El enfoque también necesita considerar la cultura de la organización, al igual que las metodologías de gestión de proyectos y de cambios.

Este apartado describe los elementos esenciales del marco de trabajo y del proceso, y las acciones necesarias para la integración exitosa de estos elementos para el logro de los objetivos de la organización.

La implementación de la Norma ISO 31000 es un proceso regular dinámico y reiterativo. Además, la implementación del marco de trabajo está interconectada con el proceso de gestión del riesgo descrito en la Norma ISO 31000:2009, capítulo 5. El éxito se mide tanto en términos de la integración del marco de trabajo, y en términos de la mejora continua de la gestión del riesgo en toda la organización.

La integración ocurre dentro de un contexto dinámico. La organización debería supervisar ambos cambios provocados por el proceso de implementación, y por los cambios en el contexto interno y externo. Pueden incluir la necesidad de cambio en sus criterios de riesgo.

3.3.2 Mandato y compromiso

Cualquier actividad de gestión de negocio comienza con un análisis del fundamento y de las etapas de los procesos, y con un análisis coste-beneficio. A continuación, la alta dirección y el órgano de supervisión toman la decisión de implementar y aportar el compromiso y los recursos necesarios.

Habitualmente, el proceso de implementación incluye lo siguiente:

a) obtener el mandato y el compromiso, si se requieren;

b) un análisis de brecha;

c) adaptar y ajustar en base a las necesidades de la organización, la cultura, y la creación y la protección del valor;

d) evaluar los riesgos asociados a la transición;

e) desarrollar un plan de negocio:

   – establecer objetivos, prioridades y métricas,

- establecer el caso de negocio, incluida la alineación con los objetivos de la organización,
- determinar el alcance, rendición de cuentas, tiempos y recursos,

f) identificar el contexto de la implementación, incluida la comunicación con las partes involucradas.

3.3.3 Diseño del marco de trabajo

3.3.3.1 Se deberían evaluar los enfoques existentes para gestión del riesgo en la organización, incluidos el contexto y la cultura.

a) Es importante considerar cualquier obligación legal, de reglamentación o del cliente, y los requisitos de certificación que surjan de cualquier sistema y norma de gestión que la organización decida adoptar. El propósito de esta etapa es permitir la adaptación cuidadosa del diseño del marco de trabajo de gestión del riesgo y la implementación del propio plan, y permitir la alineación con el marco de trabajo, cultura y sistema general de gestión de la organización.

b) Es importante considerar el proceso para gestionar los riesgos, y los aspectos del marco de trabajo existente que posibiliten que se aplique este proceso.

c) Se deberían establecer criterios de riesgo apropiados. Es necesario que los criterios de riesgo sean coherentes con los objetivos de la organización y que estén alineados con su actitud hacia el riesgo. Si los objetivos cambian, es necesario ajustar consecuentemente los criterios de riesgo. Para la gestión efectiva del riesgo es importante desarrollar criterios de riesgo que reflejen la actitud hacia el riesgo y los objetivos de la organización.

Para diseñar el nuevo marco de trabajo, se debería evaluar específicamente lo siguiente:

- principios y atributos, como se describen en la Norma ISO 31000;
- el marco de trabajo anterior, cuya evaluación debería comparar, en particular, las prácticas actuales, con los requisitos de los siguientes apartados de la Norma ISO 31000:2009:
  - 4.3.2 (política de gestión del riesgo),
  - 4.3.3 (obligación de rendir cuentas),
  - 4.3.4 (integración en los procesos de la organización),
  - 4.3.5 (recursos),
  - 4.3.6 y 4.3.7 (mecanismos internos y externos de comunicación e información),
- el proceso, cuya evaluación debería comparar los elementos de los procesos existentes contra los de la Norma ISO 31000:2009, capítulo 5, al igual que los principios fundamentales que promueven y brindan la razón de ser para los procesos con los principios establecidos en la Norma ISO 31000:2009, capítulo 3 (por ejemplo, si este proceso se aplicó realmente a la toma de decisiones a todos los niveles):
  - evaluar si el proceso actual suministra a quienes toman las decisiones, la información sobre riesgo que necesitan para tomar decisiones acertadas y cumplir o superar los objetivos,
  - evaluar si los enfoques existentes para la gestión del riesgo tienen en cuenta lo suficiente los riesgos interrelacionados y los riesgos que ocurren en múltiples lugares.

3.3.3.2 Se deberían identificar los requisitos de diseño del marco de trabajo.

En base a las evaluaciones descritas en 3.3.3.1, la organización debería decidir qué aspectos del enfoque actual de gestión del riesgo:

a) se pueden continuar usando en el futuro (posiblemente ampliados a otros tipos de toma de decisiones);

b) necesitan correcciones o mejoras;

c) ya no agregan valor, y se deberían eliminar.

La organización debería desarrollar, documentar y comunicar cómo se gestionará el riesgo. El alcance y contenido de las normas, directrices y modelos internos de la organización relacionados con la gestión del riesgo deberían reflejar la cultura y el contexto organizacional.

Los documentos pueden especificar que:

– los riesgos se gestionan en toda la organización usando enfoques consistentes;

– existen diferentes niveles de rendición de cuentas para gestionar el riesgo;

– las competencias y deberes de todas las personas que rinden cuentas sobre la gestión del riesgo están claramente definidos;

– las partes interesadas internas y externas están involucradas, según sea apropiado, por medio de comunicación y consulta amplias;

– la información acerca de los riesgos y de la salida de todas las aplicaciones del proceso de gestión del riesgo se registran de manera consistente y segura, con el acceso apropiado.

También se debería prever la revisión periódica de los requisitos de la organización, las herramientas, formación y recursos para la gestión del riesgo, si hay cambios posteriores en la organización y su contexto, o si mediante el seguimiento y revisión regulares se identifican debilidades o ineficiencias.

3.3.3.3 Se deberían definir el alcance, los objetivos, las metas, los recursos, las medidas para el éxito y el seguimiento y los criterios de revisión para la fase de implementación.

3.3.3.4 Se deberían establecer mecanismos de comunicación y reporte internos y externos.

3.3.4 Implementación de la gestión del riesgo

Es necesario un plan de implementación detallado para asegurar que los cambios necesarios ocurran en un orden coherente y que se puedan suministrar y aplicar los recursos necesarios. El plan debería estar apoyado en los recursos requeridos para su implementación, lo cual puede requerir asignaciones específicas en el presupuesto, cuyo desarrollo debería ser parte del proceso de planificación.

El propio plan debería ser objeto de apreciación del riesgo de acuerdo con la Norma ISO 31000:2009, 5.4, y a cualquier acción necesaria implementada para el tratamiento del riesgo.

El plan debería exigir y permitir el seguimiento del progreso y su informe a la alta dirección y al órgano de supervisión, y se deberían prever las revisiones periódicas del plan.

Por tanto, el plan debería:

– presentar en detalle las acciones específicas por tomar, su secuencia, quién las realiza, y el plazo de tiempo para su realización: incluir la corrección de las normas y directrices internas, explicaciones y formación sobre construcción de capacidad, y ajustes en la rendición de cuentas;

– identificar cualquier acción que se implemente como parte de algunas acciones más amplias asociadas al desarrollo organizacional, o que esté vinculada de otra manera (por ejemplo, el desarrollo de material de formación y contratación de formadores);

– definir responsabilidades para la implementación;

– incorporar un mecanismo para reportar la finalización, el progreso y los problemas;

– identificar y registrar cualquier criterio que provocará una revisión del plan.

Llevar a cabo la totalidad de la implementación puede tomar algún tiempo, y se puede llevar a cabo por etapas. Se debería adoptar la práctica usual de dar prioridad, siempre que sea posible, a los cambios que tengan el mayor impacto en el logro del propósito final. Esta implementación puede ocurrir en diferentes etapas de madurez y estructura de la organización. También puede ser más eficaz integrar la implementación con otros programas de cambio.

3.3.5 Seguimiento y revisión

Se debería hacer seguimiento, analizar e informar de forma oportuna (mensual, trimestral, etc.) a la alta dirección del progreso en relación con el plan.

Los informes de progreso en relación con el plan, y el desempeño en base a las medidas, se deberían validar periódicamente en un proceso de revisión objetivo y sin sesgo. Las revisiones deberían incluir el examen del marco de trabajo, los procesos, los propios riesgos y los cambios en el ambiente.

Se debería llevar a cabo una revisión periódica de la estrategia para la implementación y de la medición del progreso, la consistencia con el plan de gestión del riesgo, y la desviación con relación a éste. También pueden ocurrir revisiones si hay factores que desencadenan los criterios de revisión establecidos en el plan.

Se debería evaluar el desempeño con relación a la eficacia del cambio y de la gestión del riesgo, al igual que identificar las lecciones aprendidas y las oportunidades de mejora.

Se debería informar a los responsables de los aspectos significativos del seguimiento.

Los resultados de este paso se retroalimentarán en el contexto y en otras funciones, de manera que se puedan identificar los nuevos riesgos, se puedan descubrir los riesgos existentes, y se pueda registrar el estado de ejecución del marco de trabajo, para mejora (véase la Norma ISO 31000:2009, 4.6 y 5.7).

3.4 Mejora continua

Tanto el marco de trabajo de gestión del riesgo como el proceso de gestión del riesgo se deberían revisar para evaluar si su diseño es apropiado y si la implementación añade valor a la organización, como se tiene previsto. Si los resultados del seguimiento y la revisión muestran que se pueden hacer mejoras, éstas se deberían implementar a la mayor brevedad posible.

Para organizaciones que han hecho la transición a la Norma ISO 31000, debería haber toma de conciencia y asimilación de la oportunidad de mejora. Las mismas etapas usadas en el proceso de transición también son útiles para hacer verificaciones periódicas de si ha habido desviación del proceso.

Existen varios factores desencadenantes de la mejora continua, que incluyen los siguientes:

– el seguimiento y revisión periódica del marco de trabajo de gestión del riesgo y del proceso de gestión del riesgo, que identifican oportunidades de mejora;

– nuevo conocimiento disponible;

– un cambio sustancial en el contexto interno y externo de la organización.

Anexo A (Informativo)

Conceptos y principios fundamentales

A.1 Generalidades

En este anexo se explican algunos términos y conceptos (por ejemplo, "riesgo") que son de uso diario y pueden tener varios significados, pero que tienen un significado particular en la Norma ISO 31000 y en el presente informe técnico.

La Norma ISO 31000 define riesgo como el "efecto de la incertidumbre sobre la consecución de los objetivos".

NOTA Es recomendable que los lectores se familiaricen con los términos y definiciones de este anexo.

A.2 Riesgo y objetivos

Las organizaciones de todo tipo enfrentan factores e influencias internas y externas que hacen que sea incierto si lograrán o excederán sus objetivos, cuándo y en qué medida. El efecto que esta incertidumbre tiene sobre los objetivos de la organización es el riesgo.

Los objetivos a los que se hace referencia en la Norma ISO 31000 y en este informe técnico son los resultados que la organización busca. Habitualmente, estos son la mayor expresión de intención y propósito, y reflejan sus metas explícitas e implícitas, valores e imperativos, incluida la consideración de las obligaciones sociales y de los requisitos legales y de reglamentación. En general, la gestión del riesgo se facilita si los objetivos están expresados en términos mensurables. Sin embargo, con frecuencia hay múltiples objetivos, y la inconsistencia entre ellos puede ser fuente de riesgo.

La posibilidad no es solamente aquella de que ocurra un suceso, sino también la posibilidad general de experimentar las consecuencias que surgen del suceso, y la magnitud de la consecuencia, ya sea en términos positivos o negativos. Habitualmente, puede haber una variedad de posibles consecuencias que se pueden derivar de un suceso, y cada uno tendrá su propia posibilidad. El nivel de riesgo se puede expresar como la posibilidad de que se experimenten consecuencias particulares (incluida la magnitud). Las consecuencias se relacionan directamente con los objetivos, y surgen cuando algo ocurre o deja de ocurrir.

Riesgo es el efecto de la incertidumbre sobre los objetivos, independientemente del ámbito o circunstancias, por tanto un suceso o un peligro (o cualquier otra fuente de riesgo) no se debería describir como riesgo. El riesgo se debería describir como la combinación de la posibilidad de un suceso (o peligro o fuente de riesgo) y su consecuencia.

Un concepto central y vital que tiene que comprender la alta dirección es que el riesgo puede tener consecuencias positivas o negativas. El riesgo puede exponer la organización a una oportunidad, a una amenaza o a ambas.

Un riesgo se crea o se altera cuando se toman decisiones. Debido a que casi siempre hay alguna incertidumbre asociada con la toma de decisiones, casi siempre existe riesgo. Los responsables del logro de los objetivos necesitan apreciar que el riesgo es una parte inevitable de las actividades de la organización, que habitualmente se crea o altera cuando se toman decisiones. Los riesgos asociados con una decisión se deberían comprender en el momento en que se toma la decisión, y por tanto, el riesgo se asume en forma intencional. El uso del proceso de gestión del riesgo descrito en la Norma ISO 31000 hace posible esto.

A.3 Incertidumbre

La incertidumbre que, junto con los objetivos, da lugar al riesgo, se origina en el ambiente interno y externo en el que opera la organización. Esta puede ser incertidumbre que:

– es una consecuencia de factores sociológicos, psicológicos y culturales asociados con el comportamiento humano;

– se produce por procesos naturales caracterizados por variabilidad inherente, por ejemplo, en el clima, la variación entre observaciones en una población;

– surge de información incompleta o inexacta, por ejemplo, debido a datos que hacen falta, están interpretados de forma equivocada, no son confiables, son contradictorios internamente, o son inaccesibles;

– cambia en el tiempo, por ejemplo, debido a la competencia, tendencias, nueva información, cambios en los factores subyacentes;

– se produce por la percepción de incertidumbre que puede variar entre partes de la organización y sus partes involucradas.

A.4 Tratamiento y control de riesgos

Los controles son medidas implementadas por las organizaciones para modificar los riesgos que posibilitan el logro de los objetivos. Los controles pueden modificar el riesgo mediante el cambio de cualquier fuente de incertidumbre (por ejemplo, haciendo más o menos posible que algo ocurra) o cambiando el rango de consecuencias posibles y en donde pueden ocurrir.

El tratamiento del riesgo, como se define en la Norma ISO 31000, es el proceso previsto para cambiar o crear controles, e incluye la retención del riesgo.

A.5 Marco de trabajo de gestión del riesgo

El marco de trabajo de gestión del riesgo hace referencia a las disposiciones (incluidas las prácticas, procesos, sistemas, recursos y cultura) dentro del sistema de gestión de la organización, que permiten gestionar el riesgo. Las características de un marco de trabajo, y la medida en la que está integrado en el sistema de gestión de la organización, a la larga determinará la eficacia para gestionar el riesgo.

El marco de trabajo incluye declaraciones claras de la alta dirección sobre la intención de la organización con respecto a la gestión del riesgo (descritas en la Norma ISO 31000 como mandato y compromiso) y la capacidad necesaria (recursos y capacidad) para cumplir con esta intención.

Dicha capacidad no existe como un único sistema o entidad. Esta capacidad comprende numerosos elementos integrados en los procesos globales de gestión de la organización. Pueden ser exclusivos para la tarea de gestionar el riesgo (por ejemplo, un sistema de información especializado), o pueden ser aspectos del sistema de la organización para la gestión (por ejemplo, sus prácticas de recursos humanos).

A.6 Criterios del riesgo

Los criterios del riesgo son los parámetros definidos por la organización que le permiten describir los riesgos y tomar decisiones acerca de la importancia del riesgo, reflejan la actitud de la organización frente al riesgo. Estas decisiones posibilitan evaluar el riesgo y seleccionar el tratamiento.

A.7 Gestión, gestión del riesgo y gestionar el riesgo

La gestión involucra actividades coordinadas que dirigen y controlan una organización en la búsqueda del logro de sus objetivos.

La gestión del riesgo es un componente integral de la gestión, ya que involucra actividades coordinadas relacionadas con el efecto de la incertidumbre sobre estos objetivos. Esta es la razón por la cual, para ser eficaz, es importante que la gestión del riesgo esté integrada completamente en el sistema y los procesos de gestión de la organización.

En este informe técnico, al igual que en la Norma ISO 31000, la expresión “gestión del riesgo” se refiere generalmente a la arquitectura que usan las organizaciones (principios, marco de trabajo y proceso) para gestionar el riesgo eficazmente, y "gestionar el riesgo" hace referencia a aplicar esa arquitectura a decisiones, actividades y riesgos particulares.

Anexo B (Informativo)

Aplicación de los principios de la Norma ISO 31000

B.1 Generalidades

Aunque todas las organizaciones gestionan el riesgo en algún grado, la Norma ISO 31000 establece once principios que necesita satisfacer para que la gestión del riesgo sea eficaz. Los principios proporcionan orientación sobre:

a) la justificación para gestionar eficazmente el riesgo (por ejemplo, crea y protege el valor de la gestión del riesgo);

b) las características para una gestión eficaz de los riesgos, por ejemplo, principio b) el cual especifica que la gestión del riesgo es una parte integral en todos los procesos de la organización).

En la Norma ISO 31000, se recoge un resumen de cada principio y esta guía nos aporta la explicación y los detalles.

Al diseñar los objetivos de la gestión del riesgo de la organización, deberían considerarse los once principios, aunque cada uno de ellos puede variar según el marco de trabajo considerado en la organización y su aplicación en la misma.

La implementación eficaz de estos principios determinará tanto la eficacia como la eficiencia de la gestión del riesgo en la organización. Los once principios deberían tenerse en cuenta todo el tiempo, a pesar de que la importancia de los principios individuales pueden variar de acuerdo al marco de trabajo considerado.

Aunque los principios se expresan en forma resumida, era necesario comprender a fondo las implicaciones de cada uno, con el fin de hacerlos aplicables en forma continua.

Posteriormente, los resultados de este tipo de análisis deberían reflejarse en el diseño o la mejora del marco de trabajo (por ejemplo, en la asignación de responsabilidades, formación, comunicación con las partes interesadas y el diseño del seguimiento y revisión de los resultados de la gestión de riesgo).

Este anexo proporciona una orientación sobre cómo aplicar cada principio, y además para algunos principios, hay también ayudas prácticas en cajas.

B.2 Los principios

B.2.1 La gestión del riesgo crea y protege el valor

B.2.1.1 Principio

a) La gestión del riesgo crea y protege el valor

La gestión del riesgo contribuye de manera tangible al logro de los objetivos y a la mejora del desempeño, por ejemplo, en lo referente a la salud y seguridad de las personas, a la conformidad con los requisitos legales y reglamentos, a la aceptación por el público, a la protección ambiental, a la calidad del producto, a la gestión del proyecto, a la eficacia en las operaciones, y a su gobierno y reputación.

B.2.1.2 Cómo aplicar el principio

El principio explica que el propósito de la gestión del riesgo es crear y proteger el valor ayudando a la organización a lograr sus objetivos. Esto se logra ayudando a la organización a identificar y abordar los factores, tanto internos como externos, que dan lugar a la incertidumbre asociada con sus objetivos. El vínculo entre la eficacia de la gestión del riesgo y cómo contribuye al éxito de la misma debería claramente demostrarse y comunicarse. El principio aclara que el riesgo no debería ser gestionado para su propio bien, sino para lograr los objetivos y la mejora del desempeño.

Algunos atributos y valores son fácilmente medibles (por ejemplo en términos de dinero), pero también contribuyen considerablemente al desempeño, reputación y cumplimiento legal. Los valores humanos, sociales y ecológicos son particularmente importantes para gestionar los riesgos relacionados con la seguridad, la protección y el cumplimiento, así como los asociados con los activos intangibles, por lo tanto la creación de valor puede necesitar expresarse usando medidas cualitativas más que cuantitativas.

B.2.2 La gestión del riesgo es una parte integral de todos los procesos de la organización

B.2.2.1 Principio

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

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

B.2.2.2 Cómo aplicar el principio

Las actividades de una organización, incluida la toma de decisiones, dan lugar a riesgos. Los cambios en el contexto externo van más allá de la influencia y el control de la organización, lo que dan lugar a nuevos riesgos. Todas las actividades y procesos de la organización se llevan a cabo en un ambiente interno y externo en el cual existe incertidumbre. Por consiguiente:

a) el marco de trabajo para la gestión del riesgo debería realizarse integrando sus componentes al sistema global de gestión y a la toma de decisiones de la organización, independientemente de si el sistema es formal o informal, ya que los procesos de gestión existentes se pueden mejorar mediante referencias a la Norma ISO 31000;

b) el proceso para gestionar el riesgo debería ser parte integral de las actividades que generan riesgo; de lo contrario, la organización descubrirá que necesita modificar decisiones cuando se hayan comprendido posteriormente los riesgos asociados;

c) si no existe un sistema de gestión formal, el marco de trabajo de gestión del riesgo puede servir para este propósito.

Si la gestión del riesgo no está integrada a otras actividades y procesos de gestión, se puede percibir como una tarea administrativa adicional, o considerar como un área administrativa que no crea ni protege el valor.

Los dos métodos principales de aplicación de este principio son los siguientes:

– en el desarrollo del marco de trabajo de la gestión del riesgo (incluyendo mantenimiento y mejora);

– en la aplicación del proceso de gestión del riesgo para la toma de decisiones y actividades relacionadas.

El método seguido por la organización para el establecimiento (es decir obligación y compromiso) de la gestión del riesgo debería ser similar a la forma en que se establecen sus otras políticas (véase el anexo C). Siempre que sea posible, se deberían incluir los componentes del marco de trabajo de gestión del riesgo en los componentes de sistemas de gestión ya existentes en la organización (consejos adicionales se proporcionan en el anexo E y en la Norma ISO 31000).

Los auditores, pueden desempeñar un papel importante al cuestionar cómo la dirección ha llegado a una decisión, y comprobar si esto influye en una aplicación adecuada de los procesos de gestión de riesgo.

B.2.3 La gestión del riesgo es parte de la toma de decisiones

B.2.3.1 Principio

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

La gestión del riesgo ayuda a las personas que toman decisiones a realizar elecciones informadas, a definir las prioridades de las acciones y a distinguir entre planes de acción diferentes.

B.2.3.2 Cómo aplicar el principio

Este principio establece que la gestión del riesgo proporciona la base para la toma de decisiones. La gestión del riesgo debería integrarse en las actividades para la consecución de los objetivos y el proceso de toma de decisiones. El proceso de toma de decisiones debería evaluarse constantemente y, en caso necesario, proceder al tratamiento del riesgo. La toma o no de decisiones implica riesgos y es importante comprender los riesgos asociados en ambas situaciones.

La gestión del riesgo se debería aplicar de forma proactiva como parte de la toma de decisiones y nunca después de que la decisión se haya tomado (forma reactiva), por ejemplo:

– la toma de decisiones sobre objetivos estratégicos debería tener en cuenta los riesgos ambientales, al igual que los cambios en los recursos de la organización;

– el proceso de innovación debería tener en cuenta no solo la incertidumbre que determina el éxito de la innovación, sino también los riesgos humanos, sociales, de seguridad y ambientales, y tratados de acuerdo con las normas legales (por ejemplo, seguridad del producto);

– los planes de inversión (I+D) deberían especificar las pautas de la toma de decisiones para la evaluación cuantitativa del riesgo.

La política de la organización sobre la gestión del riesgo y la forma en que se comunica debería reflejar este principio.

Las otras partes del marco de trabajo deberían tener en cuenta la forma en la que se toman las decisiones, de manera que el proceso sea eficaz y consistente en toda la toma de decisiones, por ejemplo, gestión de proyectos, valoraciones de inversiones, adquisiciones.

Los responsables de la toma de decisiones en toda la organización deberían comprender la política de gestión del riesgo de la organización, y deberían tener competencias para aplicar el proceso de gestión del riesgo para la toma de decisiones. Esto requerirá la asignación de responsabilidades, apoyada en la formación de habilidades y en la revisión del desempeño.

Ejemplos prácticos

Con el fin de aplicar el principio, se presentan unas preguntas que deberían realizarse desde el principio del proceso:

- ¿Cómo puede ayudar a crear y proteger el valor? [Principio a)]
- ¿Cómo y dónde se toman las decisiones en la organización?
- ¿Quién está involucrado en la toma de decisiones?
- ¿Qué conocimiento y habilidades son necesarios para que quienes toman las decisiones?
- ¿Cómo adquieren los conocimientos y habilidades necesarios quienes toman las decisiones?
- ¿Qué indicación y apoyo es necesaria para el personal de la organización?
- ¿En el futuro, de qué manera se introducirá al personal a este método de toma de decisiones?
- ¿Cómo se verán afectadas las partes involucradas externas?
- ¿Qué decisiones se tendrían que cambiar dentro del proceso en la organización?
- ¿Cómo se establece el control del proceso al aplicar este principio?

B.2.4 La gestión del riesgo trata explícitamente la incertidumbre

B.2.4.1 Principio

d) La gestión del riesgo trata explícitamente la incertidumbre

La gestión del riesgo tiene en cuenta explícitamente la incertidumbre, su naturaleza y la forma de tratarla.

B.2.4.2 Cómo aplicar el principio

Lo que hace a la gestión del riesgo única entre otros tipos de gestión es que aborda específicamente el efecto de la incertidumbre sobre los objetivos. El riesgo solo se puede evaluar o tratar satisfactoriamente si se conoce la naturaleza y el origen de esa incertidumbre.

La incertidumbre de todos los tipos requiere consideración, y es necesario no sobreestimarla ni subestimarla.

El enfoque en la incertidumbre también es importante cuando se seleccionan tratamientos para el riesgo, y se consideran el efecto y la fiabilidad de los controles. Asimismo, habrá incertidumbre asociada con las medidas de apoyo del proceso de la gestión del riesgo, por ejemplo, si la información ha sido satisfactoriamente transmitida cuando hay comunicación y consultas con las partes involucradas, o si los intervalos seleccionados por los procesos de seguimiento son suficientes para detectar cambio.

Quienes están involucrados en la gestión del riesgo deberían tener una comprensión adecuada de la incertidumbre, y de los tipos y fuentes de incertidumbre. El número y tipos de métodos de evaluación del riesgo usados para abordar la incertidumbre deberían ser apropiados y pertinentes a la importancia de la decisión: se pueden justificar múltiples métodos.

Indique las hipótesis cuando se registra el proceso de gestión del riesgo (ISO 31000:2009, 5.7). Las hipótesis reflejan generalmente alguna forma de incertidumbre, al igual que cualquier incertidumbre explícita que se haya considerado en los diversos pasos del proceso.

Cuando se evalúa el riesgo, es importante considerar la incertidumbre asociada con la estimación de las calificaciones de probabilidad y consecuencia.

Cuando se analiza el riesgo y se proponen tratamientos, se deberían usar análisis de sensibilidad para entender la influencia real de estas incertidumbres.

Ejemplos prácticos

- Quienes toman las decisiones deberían adoptar la práctica preguntando siempre: "¿Cuáles son las hipótesis? y "¿Cuáles son las incertidumbres asociadas con estas hipótesis?" No es necesario limitar esta práctica a evaluaciones formales del riesgo, por ejemplo, puede aplicarse a todas las previsiones.
- Cuando se considera el ambiente interno y externo como parte del establecimiento del contexto, se debería tomar nota de cualquier característica que tenga probabilidad de estar asociada con una alta volatilidad. Esta es una fuente de incertidumbre, y también informa la manera en la que el contexto es supervisado y revisa en forma continuada.
- Si la incertidumbre significa que se sabe que un valor particular existe solo en un rango determinado, ese rango se debería comunicar.

B.2.5 La gestión del riesgo es sistemática, estructurada y oportuna

B.2.5.1 Principio

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

Un enfoque sistemático, oportuno y estructurado de la gestión del riesgo contribuye a la eficacia y a resultados coherentes, comparables y fiables.

B.2.5.2 Cómo aplicar el principio

Un enfoque consistente para gestionar el riesgo en el momento en que se toman decisiones creará eficiencia en una organización, y puede proporcionar resultados que construyan confianza y éxito. Para esto se requieren prácticas organizacionales que consideren los riesgos asociados con todas las decisiones, y el uso de criterios de riesgo consistentes que se relacionen con los objetivos de las organizaciones y el alcance de sus actividades.

Un enfoque puntual significa que el proceso de gestión del riesgo se aplica en el punto óptimo del proceso de toma de decisiones. En parte, esto depende del diseño del marco de trabajo al que se aplica también este principio. Si se realizan las consideraciones de riesgo demasiado pronto o demasiado tarde, se pueden perder oportunidades o los costes de revisar la decisión pueden ser sustanciales. Las dependencias de tiempo deberían ser evaluadas y entendidas para determinar el enfoque más eficaz de gestión del riesgo.

Un enfoque estructurado significa la aplicación del proceso de gestión del riesgo de la forma descrita en la Norma ISO 31000:2009, capítulo 5, incluso haciendo los preparativos apropiados para estas actividades. Dependiendo de las necesidades, el método debería ser coherente con un enfoque ascendente o descendente, con el fin de abordar el nivel apropiado de gestión.

B.2.6 La gestión del riesgo se basa en la mejor información disponible

B.2.6.1 Principio

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

Los elementos de entrada del proceso de gestión del riesgo se basan en fuentes de información tales como datos históricos, experiencia, retroalimentación de las partes interesadas, observación, previsiones y juicios de los expertos. No obstante, las personas que toman decisiones deberían informarse y tener en cuenta todas las limitaciones los datos o modelos utilizados, así como las posibles divergencias entre los expertos.

B.2.6.2 Cómo aplicar el principio

Sólo se puede comprender correctamente un riesgo si está basado en la mejor información disponible. En consecuencia, las decisiones de la gestión del riesgo deberían incluir métodos (por ejemplo, investigación) para recoger o generar información. Sin embargo, a pesar de los mejores esfuerzos, la información disponible algunas veces puede estar limitada, por ejemplo, prever lo que ocurrirá en el futuro puede estar limitado al uso de proyecciones estadísticas.

Se debería entender la sensibilidad de las decisiones de cualquier incertidumbre en la información. La fiabilidad de la evaluación del riesgo dependerá, en parte, de la claridad y precisión de los criterios de riesgo. La recopilación de datos relacionados con el riesgo (por ejemplo, la ocurrencia de eventos y otra información basada en la experiencia) puede ayudar a los análisis estadísticos.

Aunque el objetivo final es la toma de decisiones basada en evidencias, esto no siempre es posible con el tiempo o con los recursos disponibles. En estos casos, se debería usar el juicio de expertos, en combinación con la información que está disponible. Sin embargo, es necesario evitar sesgo en el grupo cuando se aplica este juicio. Además, la evidencia del pasado no puede predecir exactamente el futuro. En situaciones con eventos con impactos muy altos, la falta de información puede provocar acciones si hay evidencia de daño potencial, en lugar de una prueba definitiva de daños.

Este principio también es aplicable al diseño (o mejora) del marco de trabajo de gestión del riesgo debido a que habrá aspectos del marco (por ejemplo, aquellos que proporcionan capacidad de investigación o que recopilan, analizan, actualizan y ponen a disposición información para apoyar la aplicación del proceso) que determinarán cómo se aplica este principio.

La fiabilidad y exactitud de la información deberían evaluarse regularmente por relevancia, puntualidad y fiabilidad, mediante hipótesis documentadas. El marco de trabajo debería prever la revisión periódica y la emisión de actualizaciones o correcciones.

Ejemplos prácticos

- Cuando se diseña la forma en que se deberían reportar los incidentes, primero que todo se debería considerar cuidadosamente a qué decisiones ayudaría esa información, es decir, ¿quiénes son los usuarios finales presentes y futuros?, ¿cómo puede ser necesario clasificar la información?, ¿cómo se puede mejorar la integridad?, y ¿cómo se puede acceder a esta información?. Una vez que se ha hecho esto, se puede diseñar el cuestionario de presentación de informes, teniendo en cuenta que la calidad suministrada puede estar influenciada por el tiempo necesario para alimentarla.
- La descripción del contexto (junto con su fecha de preparación) siempre se debería incluir como parte de las descripciones detalladas y documentadas de los riesgos clave enfrentados (por ejemplo, inscripción del riesgo). Esto permite a los usuarios tener en cuenta cualquier cambio en el contexto que pueda haber ocurrido posteriormente, con los cambios resultantes en el riesgo.
- Cuando en una evaluación se han hecho hipótesis, se debería registrar y comprender claramente la justificación de dichas hipótesis, incluida cualquier limitación.
- Cuando se diseñan tratamientos del riesgo, se debería considerar cómo se hará el seguimiento del desempeño de los controles resultantes, y cómo se pondrán a disposición de las personas que tomarán las decisiones en el futuro, quienes serán responsables de estos controles.

B.2.7 La gestión del riesgo está adaptada

B.2.7.1 Principio

g) La gestión del riesgo está adaptada

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

B.2.7.2 Cómo aplicar el principio

La Norma ISO 31000 proporciona un enfoque genérico para la gestión del riesgo, que es aplicable a todo tipo de organizaciones y a todo tipo de riesgo. Todas las organizaciones tienen su propia cultura y características, criterios de riesgo y contextos de la operación. La gestión del riesgo se debería adaptar para satisfacer las necesidades de cada organización.

No hay una forma única y correcta de diseñar e implementar el marco de trabajo y los procesos de gestión del riesgo, ya que requieren flexibilidad y adaptación en cada organización. El diseño se puede determinar por muchos aspectos, incluyendo estilo, tamaño, cultura, sector, configuración y gestión organizacional.

Diferentes áreas de riesgo pueden requerir procesos diferentes dentro de la misma organización. Aunque todos los procesos deberían ser consistentes con la Norma ISO 31000, habrá diferencias en los sistemas, modelos y nivel de juicio involucrado, por ejemplo, entre los involucrados en la evaluación de riesgos relacionados con la tecnología de la información, riesgos de tesorería y de inversiones, o riesgos de la competencia. Cada proceso se debería adaptar a su propósito específico.

Puesto que el propósito del marco de trabajo es asegurar que el proceso de gestión del riesgo se aplique a la toma de decisiones en una manera que sea eficaz y que refleje la política, el diseño del marco de trabajo debería reflejar cómo y en dónde se tomaron las decisiones, y debería tener en cuenta cualquier obligación legal u otras con la que esté comprometida la organización.

Es importante tener presente que la adaptación no implica que los elementos del marco de trabajo (como se describen en la Norma ISO 31000:2009, capítulo 4) o los pasos del proceso (véase la Norma ISO 31000:2009, capítulo 5) deberían variar. Todos son esenciales para una gestión eficaz del riesgo.

Este principio es importante durante el diseño y mejora del marco de trabajo de gestión del riesgo, pero también será relevante en la forma en que los aspectos del proceso estén estructurados.

Este principio también puede significar que la organización necesite considerar cuestiones internas, por ejemplo, rotación de personal (que si es muy alto puede requerir mejoras en la formación con el fin de asegurar que los empleados nuevos sean capaces de cumplir lo que se les requiere en relación a la gestión del riesgo).

Es necesaria la adaptación del marco de trabajo, para lograr la integración con los procesos de la toma de decisiones de la organización. También es posible que esos procesos de toma de decisiones necesiten modificarse o regularse para ajustarse a un marco de trabajo de gestión del riesgo estructurado.

Ejemplos prácticos

– El diseño del marco de trabajo de gestión del riesgo debería incluir los puntos de vista de quienes están involucrados en su implementación.

– Construir una comprensión más profunda de los conceptos fundamentales de la Norma ISO 31000 ayudará a asegurar que la adaptación tanto del marco de trabajo como del proceso alcanzarán los atributos de una gestión eficaz del riesgo, como se trata en la Norma ISO 31000:2009, anexo A. Por el contrario, esto no se logrará simplemente llevando a cabo los procesos de rutina.

B.2.8 La gestión del riesgo integra los factores humanos y culturales

B.2.8.1 Principio

h) La gestión del riesgo integra los factores humanos y culturales

La gestión del riesgo permite identificar las aptitudes, las percepciones y las intenciones de las personas externas e internas que pueden facilitar u obstruir el logro de los objetivos de la organización.

B.2.8.2 Cómo aplicar el principio

Este principio consiste en obtener las opiniones de las partes interesadas, así como entender que esas opiniones pueden estar influenciadas por las características humanas y culturales. Los factores a considerar incluyen conceptos sociales, políticos y culturales, al igual que los conceptos de tiempo. Los tipos de error más comunes son los siguientes:

a) falta de detección y respuesta a las alertas;

b) indiferencia a los puntos de vista de otros, o falta de conocimiento de las mismas;

c) sesgo debido a estrategias de procesamiento de información simplificadas para abordar temas complejos;

d) Incapacidad para reconocer la complejidad.

Cuando se diseña el marco de trabajo y cuando se aplican todos los aspectos del proceso de gestión del riesgo, son necesarias acciones específicas con el fin de comprender y aplicar dichos factores humanos y culturales.

El diseño del marco de referencia y la comunicación acerca del riesgo debería tener en cuenta las características culturales y los niveles de conocimiento de los receptores.

Ejemplos prácticos

- Los directores deberían actuar de manera que demuestren que promueven y apoyan el respeto y la comprensión de las diferencias individuales.
- Las personas aprecian que se les pregunte su punto de vista.
- Por regla general, las organizaciones recompensan lo que valoran. Si la selección, promoción y remuneración de los empleados no está vinculada abiertamente con el desempeño real de la gestión del riesgo, es improbable que este desempeño cumpla con los estándares esperados. Se deberían reconocer adecuadamente los esfuerzos individuales.
- Por regla general, no es prudente que el control dependa de una sola persona, para hacer una modificación considerable al riesgo.
- Las organizaciones transnacionales actuarán en forma sensata si reconocen la importancia de la cultura para determinar el comportamiento de las personas.

Ejemplos prácticos

Algunos ejemplos de preguntas útiles acerca de factores humanos y organizacionales incluyen las siguientes:

- ¿Es la estructura de la organización adecuada para las necesidades de la organización?
- ¿Se han identificado claramente los individuos que deben rendir cuentas de manera formal?
- ¿Todas las descripciones de los cargos contienen especificaciones claras acerca de las autoridades y responsabilidades de los individuos?
- ¿Todos los canales de comunicación son claros y eficaces?
- ¿Ocasionalmente se verifica que las comunicaciones se entienden e interpretan correctamente a todos los niveles en la organización?
- ¿En la organización se monitorea el nivel de motivación?
- ¿Se revisan todas las interfaces entre los equipos?
- ¿Existen mecanismos para reconocer y responder a rumores dentro de la organización, antes de que causen un impacto negativo?
- ¿Existen políticas claras para contratación, remuneración y promoción?
- Si las políticas son dudosas, ¿existe un proceso para revisarlas?
- ¿Se observan políticas y procedimientos? Si no se observan, ¿se lleva a cabo una investigación? ¿Se hacen cumplir?
- ¿Los auditores internos y externos buscan en la organización comportamientos no seguros o no éticos?

B.2.9 La gestión del riesgo es transparente e inclusiva

B.2.9.1 Principio

i) La gestión del riesgo es transparente e inclusiva

La implicación apropiada y oportuna de las partes interesadas y, en particular, de las personas que toman decisiones a todos los niveles de la organización, asegura que la gestión del riesgo se mantenga pertinente y actualizada. La implicación también permite a las partes interesadas estar correctamente representadas y que sus opiniones se tengan en cuenta en la determinación de los criterios de riesgo.

B.2.9.2 Cómo aplicar el principio

Este principio se puede aplicar a múltiples niveles. Se puede reflejar en la política de gestión del riesgo de la organización (por ejemplo "Informar y consultar a las partes involucradas siempre que sea posible, con el fin de que comprendan nuestros objetivos y puedan contribuir con su conocimiento y puntos de vista a la toma de decisiones").

La consulta con las partes involucradas, como parte de la aplicación del proceso de gestión del riesgo, necesita una planificación cuidadosa. Es aquí en donde se puede construir o destruir confianza. Para ser eficiente y fortalecer la confianza en los resultados, las partes involucradas pertinentes deberían participar en todos los aspectos del proceso de gestión del riesgo, incluido el diseño del proceso de comunicación y consulta.

La implementación de este principio debería considerar aspectos de confidencialidad, seguridad y privacidad, por ejemplo, puede requerir la limitación de accesos a alguna información en las inscripciones sobre los riesgos.

Ejemplos prácticos

- Se debería incluir el juego de roles en relación con la comunicación y la consulta en la formación en gestión del riesgo.
- Se debería llevar a cabo una evaluación acerca de cómo se percibe la información recibida.
- Se debería suministrar retroalimentación periódica para demostrar cómo se llevó a cabo en la práctica el desempeño prometido o proyectado.
- Los puntos de vista no solicitados se deberían estimular, reconocer y apreciar, y siempre que sea posible, se debería suministrar retroalimentación acerca de ellos.

B.2.10 La gestión del riesgo es dinámica, reiterativa y receptiva al cambio

B.2.10.1 Principio

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

La gestión del riesgo es sensible de manera continuada a los cambios y responde a ellos. Como se producen sucesos externos e internos, el contexto y los conocimientos cambian, se realiza el seguimiento y la revisión de riesgos, surgen nuevos riesgos, algunos cambian y otros desaparecen.

B.2.10.2 Cómo aplicar el principio

Cualquier cambio en los objetivos de la organización o cualquier aspecto de las circunstancias internas o externas, inevitablemente cambiará el riesgo (por ejemplo, una reestructuración interna, un importante proveedor nuevo o un cambio en la normativa legal). Asimismo, los cambios en el contexto organizacional (por ejemplo, la adquisición de otra compañía o conseguir un nuevo contrato importante) pueden requerir cambios en el marco de trabajo (por ejemplo, en formación, en especialistas de riesgos). Los procesos de gestión del riesgo deberían diseñarse para reflejar la dinámica de la organización (por ejemplo, rapidez del cambio).

La Norma ISO 31000 contiene dos regímenes de seguimiento y revisión (para el marco de trabajo y para el proceso). Cada uno es específico para su propósito, y requiere reflexión e implementación.

El marco de trabajo se debería supervisar y revisar para asegurar que puede continuar aplicándose a estos principios de gestión eficaz del riesgo, a la política de gestión del riesgo de la organización, y a apoyar la aplicación del proceso de toma de decisiones en toda la organización.

La supervisión y la revisión se deberían incorporar a cada uno de los pasos fundamentales en el proceso de gestión del riesgo.

Los controles también se deberían revisar para asegurar su eficacia en la respuesta con respecto al cambio. Por ejemplo, los controles manuales no serían tan eficaces si hay cambios en el personal de la organización.

La supervisión y la revisión se deberían adaptar cuidadosamente, de manera que sean sensibles a los factores de cambio que pueden tener los mayores efectos. La supervisión y la revisión deberían evaluar la importancia continua de los indicadores supervisados, y si es necesario, los indicadores se adaptarán a los cambios o a las nuevas circunstancias.

La supervisión y la revisión son actividades distintas, como se explica en la Norma ISO 31000:2009, 4.5 y 5.6. La supervisión está relacionada con la observación continua de los parámetros clave para determinar si se siguen en la forma prevista o supuesta. La revisión ocurre de vez en cuando, se estructura en cuanto a su propósito, y generalmente está prevista para determinar si las hipótesis en base a las cuales se tomaron las decisiones (por ejemplo, el diseño del marco de referencia) permanecen vigentes, y por tanto, si es necesario revisar las decisiones resultantes. La revisión también debería tener en cuenta los nuevos conocimientos y tecnologías.

Ejemplos prácticos

- Cuando se aplica el proceso de gestión del riesgo y se desarrolla la declaración del contexto, se deberían identificar los componentes (por ejemplo, las características del entorno externo) que tienen más posibilidad de cambiar, y se deberían supervisar de cerca para determinar los cambios. Cualquier cambio podría requerir la reevaluación de todos o de algunos riesgos documentados.
- Se debería motivar a las personas para que informen de sus inquietudes acerca del estado de la situación actual (incluidas las reclamaciones internas).
- Incluso las organizaciones pequeñas deberían tener en mente cambios globales, por ejemplo, la crisis financiera de 2008 tuvo impactos profundos en los pequeños proveedores cuyos clientes principales eran organizaciones afectadas directa o indirectamente por quiebras de los bancos. Estos eventos externos o circunstancias emergentes pueden requerir cambios proactivos al marco de trabajo de gestión del riesgo.

B.2.11 La gestión del riesgo facilita la mejora continua de la organización

B.2.11.1 Principio

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

Las organizaciones deberían desarrollar e implementar estrategias para mejorar su madurez en la gestión del riesgo en todos los demás aspectos de la organización.

B.2.11.2 Cómo aplicar el principio

La mejora continua del desempeño organizacional está interrelacionada con la mejora continua del desempeño de la gestión del riesgo. La mejora de la gestión del riesgo, fundamentada en la toma de decisiones basadas en el riesgo, puede reducir la incertidumbre en el logro de los objetivos, minimizar la volatilidad e incrementar la agilidad. Sin embargo, se debería no manipular excesivamente la gestión del riesgo, hasta el punto de reprimir la búsqueda de oportunidades y la flexibilidad de la respuesta.

En cambio, la importancia de este principio radica en que las organizaciones permanezcan alerta a nuevas oportunidades de mejora. Estas oportunidades pueden surgir internamente (por ejemplo, del aprendizaje de incidentes reportados) o externamente (por ejemplo, por la disponibilidad de nuevas herramientas y conocimientos que pueden mejorar la gestión del riesgo).

Este principio también es relevante para buscar continuamente mejoras en la eficiencia de la gestión del riesgo, por ejemplo, implementación de nuevas tecnologías que conectan mejor la información a quienes toman las decisiones.

El objetivo de la mejora continua debería estar clara en la política de gestión del riesgo de la organización y se debería comunicar continuamente de manera formal e informal. La mejora continua puede incluir lo siguiente:

- mejorar el grado de integración de la actividad de gestión del riesgo a la actividad general;
- mejorar la calidad de las evaluaciones del riesgo;
- mejorar el marco de referencia, por ejemplo, la calidad y el acceso a la información;
- mejorar la rapidez en la toma de decisiones.

La mejora continua se basa en indicadores cualitativos y cuantitativos del progreso. Las organizaciones que usan modelos de madurez y enfoques por fases deberían diseñar estos como impulsores de la mejora continua en base a los recursos y cultura de la organización. Deberían reconocer que en muchas tareas humanas el éxito alimenta el éxito. El propósito de la gestión eficaz del riesgo se encuentra únicamente en incrementar la probabilidad de que una organización alcance sus objetivos en su totalidad. Cuanto más rápidamente una organización pueda llevar a cabo una gestión eficaz del riesgo, más eficientes serán sus objetivos.

En términos prácticos, algunas mejoras pueden tomar tiempo para lograr, por ejemplo, la asignación de un presupuesto o una planificación y el lanzamiento al mercado. Los planes de mejora deberían considerar las prioridades y beneficios relativos, y deberían permitir el seguimiento del progreso.

Ejemplos prácticos

- Usando los elementos de supervisión y de revisión del marco de referencia, se debería llevar a cabo una revisión anual del desempeño en base a estas mejoras del diseño y principios de gestión del riesgo.
- La adecuación, idoneidad y eficiencia del marco de trabajo de gestión del riesgo se deberían evaluar y revisar.
- El sistema de información de incidencias se debería usar para llevar a cabo el análisis de causa raíz, considerando no solamente las causas probables del incidente, sino también las características del marco de trabajo de gestión del riesgo que hicieron posible que el incidente ocurriera.
- El éxito (por ejemplo, un proyecto a tiempo/dentro del presupuesto) se debería supervisar para comprender qué características del marco de trabajo de gestión del riesgo facilitaron principalmente el éxito, y esto se debería comunicar para reforzar el valor.

Anexo C (Informativo)

Cómo expresar mandato y compromiso

C.1 Generalidades

Este anexo proporciona orientación y estrategias acerca de cómo una organización puede expresar y comunicar el mandato y el compromiso.

Para que el mandato y el compromiso sean eficaces, la alta dirección y el órgano de supervisión de la organización deberían expresar de forma clara a las partes involucradas el enfoque para gestionar el riesgo, y documentar y comunicar esto, según sea apropiado. El mandato para la gestión del riesgo involucra generalmente cambios en el comportamiento, cultura, política, procesos y desempeño esperado en la gestión del riesgo, que se verán reflejados en el marco de trabajo de gestión del riesgo. El mandato y el compromiso podrían ser una breve declaración de la política, que se comunique ampliamente.

El desarrollo del mandato implica decidir sobre cómo llevar a cabo la acción requerida, al igual que la autorización para que ocurra. Invariablemente, en las organizaciones existentes, esto necesariamente implicará la autoridad necesaria para provocar los cambios. No tendría mucho sentido identificar una acción a tomar a menos que, al mismo tiempo, haya un compromiso para llevarla a cabo.

El mandato y el compromiso son una parte fundamental del marco de trabajo de gestión del riesgo. Deberían ser parte de los marcos de referencia de gestión y de gobierno de la organización, y deberían influir en el diseño de ambos.

El mandato y el compromiso deberían reflejar los once principios establecidos en la Norma ISO 31000:2009, capítulo 3.

En la práctica, el mandato de la organización y su compromiso con ella, se expresa y percibe de manera explícita e implícita. Las expresiones implícitas (por ejemplo, las acciones cotidianas de la alta dirección y del órgano de supervisión dentro de la cultura reinante en la organización) habitualmente brindan un estímulo más poderoso que las expresiones explícitas (por ejemplo, una política de gestión del riesgo escrita).

C.2 Métodos para expresar mandato y compromiso

C.2.1 Aspectos clave

La expresión del mandato y el compromiso debería cumplir los criterios siguientes:

a) debería ser compatible con el plan estratégico de la organización, sus objetivos, políticas, estilos de comunicación y sistema de gestión;

b) debería ser compatible con los criterios de riesgo determinados por el órgano de supervisión;

c) debería cumplir los principios de la Norma ISO 31000, para lograr la gestión eficaz del riesgo, como se presenta en la Norma ISO 31000:2009, anexo A;

d) debería ser fácil de comunicar, y probarse para determinar su comprensión dentro y fuera de la organización;

e) debería tener expectativas razonables de implementación exitosa;

f) debería abordar las responsabilidades de los dueños de los riesgos.

Si el mandato existente de gestión del riesgo y el compromiso de la organización con la gestión del riesgo no cumplen actualmente estos requisitos, será necesario cambiar ambos aspectos, el explícito y el implícito.

EJEMPLO Si el órgano de supervisión o la alta dirección han tomado decisiones que no se han sometido a una profunda evaluación del riesgo, esta es una clara indicación de que la organización no está comprometida con la comprensión de los riesgos.

Una parte esencial de adoptar un mandato actualizado es el desarrollo de un plan para cambiar la comprensión de lo que se requiere. El objetivo de este plan es asegurar que tanto el mandato como sus beneficios se comprendan y se crea en ellos ampliamente, que se vean como algo no negociable, y que la organización está comprometida en forma consistente con el mandato y actúe en consecuencia. El mayor efecto sobre la aceptación o no del mandato por las diferentes partes involucradas lo tendrá el comportamiento de la organización, y la forma en que éste se compara con las declaraciones explícitas acerca del mandato.

C.2.2 Establecimiento, comunicación y compromiso de la política de gestión del riesgo

Una forma de expresar y comunicar el mandato de una manera explícita es por medio del establecimiento de la política y su posterior comunicación. La Norma ISO 31000:2009, 4.3.2, especifica que la organización debería no solamente hacer que su política acerca de la gestión del riesgo sea clara, sino también comunicarla interna y externamente. La Norma ISO 31000:2009, 4.3.2, identifica también aspectos específicos que habitualmente se deberían reflejar en la política.

Teniendo en mente el principio g) (es decir, la gestión del riesgo está adaptada), la expresión de la política debería ser apropiada y coherente con la forma general en la que opera la organización. De lo contrario, puede no considerarse como pertinente y como parte del sistema general mediante el que opera la organización.

Para grandes organizaciones, el establecimiento de una política normalmente implica el desarrollo de una declaración formal acerca del mandato para la gestión del riesgo que formará parte de su conjunto general de políticas. En consecuencia, irá firmada por el órgano de supervisión, y luego se comunicará y reforzará por medio del sistema de gestión.

Ayuda práctica

La participación y el compromiso de la alta dirección y el órgano de supervisión son clave para el éxito de cualquier programa de gestión del riesgo. La organización debería considerar las siguientes preguntas cuando establezca su mandato y compromiso con la gestión del riesgo:

- ¿Cuáles son los objetivos estratégicos de la organización? ¿Son claros? ¿Qué es implícito y qué es explícito en estos objetivos?
- ¿La alta dirección tiene conocimiento claro sobre la naturaleza y alcance de los riesgos significativos que desea asumir, y de las oportunidades que desea aprovechar con el logro de sus objetivos estratégicos?
- ¿La alta dirección necesita establecer un gobierno más claro con relación a la actitud ante el riesgo de la organización?
- ¿Qué pasos ha tomado la alta dirección para asegurar la supervisión de la gestión de los riesgos?
- ¿Los directores que toman decisiones comprenden el grado en el cual están autorizados (individualmente) para exponer la organización a las consecuencias de un suceso o situación? Cualquier actitud hacia el riesgo necesita ser práctica, para orientar a los directores a tomar decisiones en base al riesgo.
- ¿Los ejecutivos comprenden su nivel de riesgo agregado e interrelacionado, de manera que puedan determinar si es aceptable o no?
- ¿La alta dirección y los altos directivos comprenden el nivel de riesgo agregado e interrelacionado para la organización, como un todo?
- ¿Tanto los gerentes como los ejecutivos tienen claridad acerca de que la actitud frente al riesgo no es constante? Puede cambiar a medida que cambian las condiciones del ambiente y del negocio. Cualquier cosa aprobada por la alta dirección necesita tener alguna flexibilidad implícita.
- ¿Las decisiones de riesgo se toman considerando completamente las consecuencias? El marco de trabajo de actitud hacia el riesgo ayuda a los directores y ejecutivos a asumir un nivel apropiado de riesgo para el negocio, teniendo en cuenta el potencial de retribución.
- ¿Cuáles son los riesgos significativos que la alta dirección está dispuesta a asumir, y las oportunidades que desea aprovechar? ¿Cuáles son los riesgos significativos que la alta dirección no desea asumir? Cualquiera que sea el modelo de política acerca de la gestión del riesgo, debería estar al lado de otras políticas que dirigen la forma en la que opera la organización.

La política debería estar sustentada tanto de manera explícita como implícita y reflejarlo como corresponde, y debería cumplir los seis criterios de C.2.1.

C.2.3 Refuerzo

La alta dirección y el órgano de supervisión deberían demostrar y reforzar el compromiso de la organización con el mandato por medio de una mezcla de acciones explícitas e implícitas que incluyan:

– aclarar que los objetivos de gestión del riesgo están vinculados a otros objetivos de gestión, y no separados de ellos;

– aclarar que la gestión del riesgo trata del cumplimiento eficaz de los objetivos de la organización;

– asegurar que el tipo de actividades de gestión del riesgo exigidas por el mandato están integradas a los procesos de gobierno y gestión existentes, y a los procesos estratégicos, operacionales y de proyectos;

– exigir el seguimiento regular del marco de trabajo de gestión del riesgo de la organización y reportar acerca de él, para asegurar que el proceso sigue siendo apropiado y eficaz;

– supervisar que la organización tenga una comprensión actualizada y amplia acerca de sus riesgos y de aquellos riesgos que están dentro de los criterios de riesgo determinados, y emprender acciones correctivas en donde estos criterios no se cumplan;

– orientar con el ejemplo, con relación a sus propias actividades;

– renovar el compromiso con el mandato, a medida que cambia el tiempo, los sucesos y la alta dirección.

La implementación de la Norma ISO 31000 puede llevarse a cabo en toda la organización, o parte por parte, por ejemplo, dentro de negocios subsidiarios.

C.3 Orientación sobre el desarrollo del mandato y del compromiso

Para establecer el mandato para la gestión del riesgo se requiere una reflexión cuidadosa, una perspectiva estratégica y consulta entre el órgano de supervisión y la alta dirección. Esto ayudará a asegurar que una vez que se adopte el mandato, la organización lo cumplirá.

La expresión del mandato y del compromiso se debería considerar a niveles tácticos y estratégicos. La organización debería definir y evaluar las competencias para cumplir sus objetivos, y cultivar las habilidades y experiencia necesarias para alcanzarlas.

Las implicaciones de los cambios exigidos por un mandato necesitarán considerarse cuidadosamente. Esto incluye quién lideraría el cambio y quién necesitaría orientación o soporte. Algunas veces el alcance de los cambios puede ser bastante radical (por ejemplo, los cambios en las especificaciones de los cargos, los procesos de seguimiento y gestión) y de esta manera absorberán parte de la capacidad de la organización para el cambio. Será necesario tener esto en cuenta en el contexto de otros cambios que estén en progreso, y si puede haber integración.

Se debería consultar a las personas que estarán afectadas significativamente por los cambios, especialmente los dueños de riesgos de nichos específicos dentro de la organización (como por ejemplo seguridad e higiene o gestión de la seguridad física) de tal forma que las implicaciones de los cambios puedan ser entendidos.

Ayuda práctica

Algunas de las formas en las que se puede lograr esto incluyen las siguientes:

– considerar cómo se explicará el mandato a la organización, y cómo estas explicaciones se reforzarán mediante acciones regulares;

– considerar el período de tiempo para hacer aplicable el mandato (esto se debería respetar e integrar en los otros imperativos de la organización, aunque sus beneficios plenos no se lograrán, o la gestión del riesgo no será tan eficaz como pudiera ser, sino hasta que el marco de trabajo esté completo);

– identificar los roles clave para producir los cambios necesarios en el enfoque a la gestión del riesgo y para dirigir y liderar las actividades de gestión del riesgo;

– especificar qué aspectos del marco de trabajo y de las actividades de gestión del riesgo serán monitoreados a los niveles de la alta dirección, dirección y comités, y cómo se recopilará y presentará esta información;

– incluir el desempeño de la gestión del riesgo como un punto habitual en la agenda de todas las reuniones clave de supervisión y de la alta dirección;

– desarrollar métodos eficaces para comunicar acerca del desempeño de la gestión del riesgo (por ejemplo, la publicación de un boletín para el personal, en el estilo de un informe de gestión del riesgo);

– considerar cuáles deberían ser los factores desencadenantes de la revisión del mandato.

Anexo D (Informativo)

Seguimiento y revisión

D.1 Antecedentes

D.1.1 Generalidades

En este anexo se presentan pautas para el seguimiento y la revisión del marco de trabajo y de los procesos de gestión del riesgo de acuerdo con la Norma ISO 31000:2009, 4.5, 4.6 y 5.6.

El seguimiento y la revisión son dos actividades diferenciadas previstas para determinar si las hipótesis y decisiones siguen siendo válidas. Las técnicas se usan tanto en el mantenimiento de un marco de trabajo eficaz de gestión del riesgo como en cada uno de los pasos del proceso de gestión del riesgo.

– El seguimiento considera la vigilancia rutinaria del desempeño real y su comparación con el desempeño requerido o esperado. Involucra la comprobación o investigación, la supervisión, la observación crítica o la determinación continua del estado, con el fin de identificar los cambios en el nivel de desempeño requerido o esperado, al igual que los cambios en el contexto.

– La revisión involucra la comprobación periódica o de improviso, para detectar cambios en el ambiente, en las prácticas de la industria o en las prácticas de la organización. Esta actividad se lleva a cabo para determinar la idoneidad, adecuación y eficacia del marco de trabajo y el proceso para lograr los objetivos establecidos. Las revisiones deberían considerar las salidas de las actividades de seguimiento.

– Una auditoría es un proceso de revisión sistemática basada en evidencias, contra criterios predeterminados. Aunque cada auditoría es una revisión, no toda revisión es una auditoría.

En conjunto, el seguimiento y la revisión brindan seguridad de que el desempeño de la gestión del riesgo es el esperado, si se puede mejorar, y si han ocurrido cambios que requieren ajuste o actualización del marco de trabajo o de algún aspecto del proceso.

El seguimiento y la revisión están dirigidos a aportar seguridad razonable de que los riesgos se gestionan adecuadamente, a identificar deficiencias en la gestión del riesgo, y a identificar oportunidades de mejora de la gestión de los riesgos. Ambos son necesarios para asegurar que la organización mantiene una compresión actualizada de sus riesgos en relación con sus criterios de riesgo, en coherencia con su actitud de riesgo. Ambos requieren un enfoque sistemático integral a los sistemas de gestión generales de la organización.

Las actividades de seguimiento y revisión y las acciones tomadas en respuesta a los hallazgos se caracterizan con frecuencia como un sistema de aseguramiento, ya que tienen el potencial para detectar y corregir las debilidades antes de que ocurran efectos adversos, o para aportar confianza en que los riesgos continúan dentro de los criterios de la organización. Estas actividades también se pueden usar para aportar a las partes internas y externas seguridad razonable de que el riesgo se está gestionando de forma eficaz.

A medida que cambian los factores en el contexto interno y externo, también cambiará el riesgo. De forma similar, el seguimiento del contexto externo puede alertar a la organización con relación a cambios que pueden presentar una oportunidad para mejorar el desempeño o para una nueva actividad. Al permanecer alerta a estos cambios, al desempeño, a las no conformidades y a los cuasi-accidentes, la organización estará capacitada para identificar oportunidades de mejora del marco de trabajo de la gestión del riesgo, y del desempeño total de la organización.

Debería haber un programa amplio para supervisar y registrar los indicadores de desempeño del riesgo que se alineen con los indicadores de desempeño de la organización.

El programa debería advertir sobre las tendencias adversas que pueden requerir acciones preventivas e intervención.

Una actividad individual de seguimiento o revisión se puede dirigir a un riesgo individual o a varios riesgos relacionados. Se puede enfocar en los riesgos o en los controles que los abordan.

D.1.2 Rendición de cuentas de seguimiento y revisión

La responsabilidad general de las actividades de seguimiento y revisión reside en el órgano de supervisión y en la alta dirección, no en los proveedores de aseguramiento, por ejemplo, la auditoría interna. Las funciones de aseguramiento de la calidad, las funciones de revisión independientes y el seguimiento reglamentario son ayudas útiles en el proceso de información jerárquica de gestión, debido a que estas actividades ofrecen un punto de vista alternativo.

Las actividades de seguimiento y revisión se pueden considerar como actividades al más alto nivel: Si está diseñada apropiadamente, proporciona el nivel de aseguramiento más poderoso. Sin embargo, un programa de seguimiento y revisión debería incluir los tres elementos.

El programa de seguimiento y revisión debería verificar que la política de gestión del riesgo esté implementada y sea eficaz. La forma en que la alta dirección reacciona a los resultados del programa de seguimiento puede afectar el comportamiento de los empleados, y es importante que la alta dirección actúe dando ejemplo como modelo a seguir.

D.1.3 Revisiones independientes

Aunque la revisión la lleven a cabo fuentes internas o externas, la independencia es necesaria en la revisión entre el revisor/auditor y la parte contratante.

La independencia es la base de la imparcialidad de la revisión y de la objetividad de las conclusiones de ésta. Siempre que sea factible, los revisores y auditores deberían tener independencia de la actividad que se revisa/audita, y en todos los casos deberían actuar libres de sesgo y conflicto de intereses.

Para las auditorías internas, los auditores deberían tener independencia de los gerentes operativos de la función que se audita. Los revisores y auditores deberían mantener la objetividad durante todo el proceso de auditoría de revisión, para asegurar que los hallazgos y conclusiones se basen solamente en evidencias.

En las organizaciones pequeñas, es posible que los revisores y auditores no sean completamente independientes de la actividad revisada o auditada, pero es conveniente hacer todos los esfuerzos posibles por eliminar el sesgo y estimular la objetividad.

La independencia de revisores y auditores ayuda a que las revisiones y auditorías sean una herramienta eficaz y confiable como soporte de las políticas y controles de gestión del riesgo, mediante el suministro de información que la organización puede usar para mejorar su desempeño.

Estas revisiones se pueden enfocar en el cumplimiento de normas (internas o externas), procedimientos o requisitos legislativos. Con frecuencia también consideran la idoneidad, la eficacia y la eficiencia de los controles, por ejemplo, pueden considerar si las actividades de gestión del riesgo suministran los valores expresados en los principios de la Norma ISO 31000.

Muchas organizaciones tienen funciones de asesoría y revisión por la dirección (tales como asesores de gestión del riesgo, funcionarios responsables del cumplimiento, y directores de aseguramiento de la calidad) que llevan a cabo revisiones de rutina; la auditoría interna habitualmente informa al órgano de supervisión y a la alta dirección. El objetivo de estas revisiones es aportar seguridad al órgano de supervisión y a la alta dirección de la organización de que:

– sus criterios de riesgo son coherentes con sus objetivos y con el contexto en el que opera;

– se ha usado un proceso sistemático y apropiado para identificar, evaluar y tratar los riesgos, y hay confianza en que este proceso continuará operando;

– los riesgos inaceptables se abordan mediante un tratamiento de riesgo apropiado;

– los controles que se cree que modifican riesgos, que de otra forma serían inaceptables, son idóneos y eficaces;

– se logra el proceso apropiado mediante planes de tratamiento de riesgos.

Las actividades de un proceso de revisión independiente no eximen a la estructura jerárquica de sus responsabilidades de seguimiento y revisión.

D.1.4 Obtención de información adecuada

Al igual que en otros aspectos de gestión del riesgo, el seguimiento y la revisión requieren el uso de la mejor información disponible [véase el Principio f)]. Para que sea idónea para el propósito, es necesario que la información sea pertinente para los usuarios y representar fielmente lo que busca representar. La utilidad de la información se incrementa si es comparable, verificable, oportuna y comprensible. La información se puede obtener de dos tipos de fuentes:

a) fuentes directas: observaciones y mediciones de las operaciones reales de los procesos, o de sus resultados;

b) fuentes indirectas: medidas que se obtienen de los procesos o resultados que se consideran.

Las combinaciones de mediciones de diferentes fuentes se escogen por necesidad (dependiendo de la disponibilidad) o por conveniencia (oportunidad, coste, etc.).

D.1.5 Informar del proceso de revisión

El informe debería aportar información al órgano de supervisión, a la alta dirección y a las partes involucradas de la organización acerca de si los riesgos de la organización están dentro de sus criterios de riesgo, o si cuenta con planes creíbles de tratamiento de riesgos que finalmente conducirán a este resultado. Adicionalmente, puede aportar información adicional acerca de riesgos nuevos y emergentes.

Cualquier conjunto de información de riesgos (por ejemplo, en un registro de riesgos) se debería actualizar periódicamente. El tipo y la frecuencia de informe dependerán de la naturaleza, del tamaño y del alcance de la evaluación del riesgo.

La salida de una revisión o de una auditoría será un informe que resuma los hallazgos y brinde conclusiones de la evaluación, en base a criterios predeterminados. El informe puede aportar recomendaciones para mejoras del sistema en base a lo que los revisores han observado. Ocasionalmente, el revisor puede hacer sugerencias más amplias con relación a los propios criterios. La respuesta a cualquier revisión se debería enfocar en la mejora del sistema y en abordar las causas raíz de los problemas.

D.1.6 Acciones correctivas y mejora continua

Se deberían establecer procesos para asegurar que las recomendaciones sean consideradas activamente por la dirección de la organización, y las respuestas acordadas se ejecuten. Las acciones en respuesta a las revisiones se deberían informar al órgano de supervisión y supervisar rutinariamente hasta su implementación.

D.2 Seguimiento y revisión del marco de trabajo

D.2.1 Generalidades

El propósito del seguimiento y de la revisión es mantener actualizado el marco de trabajo de gestión del riesgo, y compatible con las intenciones de gestión del riesgo de la organización. El marco de trabajo hace referencia a los componentes y procesos dentro del sistema de gestión de la organización, que permite gestionar el riesgo.

La Norma ISO 31000:2009, capítulo 4, contiene orientación sobre los componentes necesarios de un marco de trabajo y hace la observación de que deberían estar relacionados con el contexto interno y externo de la organización.

A medida que ocurren cambios en el contexto interno y externo de la organización, puede ser necesario ajustar el marco de trabajo para asegurar que sigue siendo eficaz.

Aun cuando no haya cambios internos o externos que requieran cambios en el diseño, sigue siendo necesario asegurar que el marco de trabajo está funcionando en la forma diseñada, en cualquier momento. Para las organizaciones que están en transición para alinearse con la Norma ISO 31000, esto puede involucrar la comprobación de los componentes del marco de trabajo del plan de implementación, para asegurarse de que se han implementado correctamente. Para organizaciones que ya tienen implementada la Norma ISO 31000, supondrá asegurar que los componentes del marco de trabajo continúan existiendo y funcionando de la manera planificada.

D.2.2 Rendición de cuentas

La dirección es responsable de asegurar que el marco de trabajo se actualice periódicamente y se controle en base a los indicadores de desempeño. Como parte de la asignación de responsabilidades de gestión del riesgo, una persona (por ejemplo, un director), o una función organizacional (por ejemplo, la función de soporte corporativa de gestión del riesgo) se debería asignar como el administrador del marco de trabajo, y una de las responsabilidades clave debería ser asegurar que el marco de trabajo sigue siendo eficaz.

D.2.3 Establecimiento de una línea base

Se debería establecer una línea base para la gestión del riesgo en la organización. La línea base se puede describir de diferentes maneras, pero debería incluir:

a) los componentes del marco de trabajo (como se describe en la Norma ISO 31000:2009, 4.3) que suministran la capacidad para posibilitar que se cumpla esta intención;

b) el alcance del soporte suministrado por el órgano de supervisión y la alta dirección en el mandato y compromiso para la gestión del riesgo (a menudo se expresa en forma de una política de gestión del riesgo).

La forma y arquitectura previstas del marco de trabajo generalmente se podrían haber registrado cuando ésta se diseñó, y la información como la que se ilustra en la tabla D.1 estará disponible. Esto forma una línea base o punto de referencia para comparaciones durante el seguimiento y la revisión.

Tabla D.1 – Ejemplo de tabla que presenta los componentes del marco de referencia

Componente	En dónde se despliega	Objetivo	Acciones clave	Responsabilidad y programación	Medidas del desempeño	Estado de la implementación
Rendición de cuentas	Nivel de la organización	Mantener actualizada la política de gestión del riesgo de la organización	– Determinar los criterios – Documentar los informes – Delegar autoridad	– Publicar la política – Formalizar el programa de delegaciones – Próxima revisión: xx/xx/xx	...	...
...						
Recursos: Formación	Nivel de división	Suministrar los componentes de gestión del riesgo para estimular toda la formación Poner a disposición actualizaciones de la formación	– Obtener asesoría – Diseñar la formación – Formar a los formadores	– Diseño: Gestión del riesgo corporativa – Lanzamiento: Gestión de divisiones – Próxima revisión: xx/xx/xx	– Realizado: Informes mensuales – Calidad: Parte de formación	...

La organización también debería establecer los indicadores de desempeño que están vinculados a los objetivos de la organización, para dar una indicación de la eficacia del marco de referencia total para gestionar el riesgo. Los indicadores de desempeño, que algunas veces se denominan colectivamente como indicadores retrospectivos, incluyen lo siguiente:

– incidentes, accidentes y cuasi-accidentes;

– pérdidas reales;

– faltas de alineación;

– quejas de los clientes;

– deudas pendientes;

– tiempo productivo del sistema;

– el grado en el cual se cumplen los objetivos de la organización;

– el grado en el cual se cumplen los objetivos de gestión del riesgo de la organización.

D.2.4 Evaluar si las características y el contexto de la información han cambiado

Determinar si el contexto interno o externo de la organización ha experimentado cambios significativos desde que se desarrolló o modificó el marco de trabajo de gestión del riesgo.

Ayuda práctica

Las características que podrían haber cambiado incluyen:

– estructura;

– prácticas y requisitos de gobierno;

– políticas, normas internas y modelos;

– requisitos contractuales;

– sistemas estratégicos y operacionales afectados por factores internos o externos (por ejemplo, cambios en la reglamentación legal);

– capacidad y recursos (por ejemplo, capital financiero y buena reputación, tiempo, personas, procesos, sistemas y tecnologías);

– conocimiento, habilidades y propiedad intelectual;

– sistemas y flujos de información;

– comportamiento social, ambiental y cultural;

– otras prioridades e imperativos organizacionales que es posible percibir que compiten con las intenciones de la organización en cuanto a gestionar el riesgo.

Los indicadores anticipados, que podrían reflejar cambios en el contexto externo, se encuentran con frecuencia externamente en informes y encuestas, los cuales reflejan los cambios y tendencias en la industria en la que opera la organización. Algunos ejemplos son:

– precio de las ‘mercancías’, tasas de interés bancario, rendimientos de bonos, tasas de cambio, índices del mercado de acciones, índice de precios al consumidor (tendencia);

– índice (tendencia);

– nivel de incidentes o fraude en organizaciones similares;

– cifras de tamaño y crecimiento del mercado, y cambios repentinos en el volumen de órdenes;

– estabilidad política y social, malestar social y activismo.

Si el contexto organizacional ha cambiado desde que se desarrolló el marco de trabajo de gestión del riesgo, este marco de trabajo se debería reevaluar y alinearlo para explicar estos cambios. El propósito de esta actividad es confirmar que el marco de trabajo y los procesos son adecuados para su propósito y son coherentes con los objetivos y prioridades de la organización.

Como consecuencia de esta revisión, la organización puede necesitar cambiar su línea base.

EJEMPLO 1 Un cambio en la estructura de una organización podría requerir alguna actualización de la política de gestión del riesgo y una reasignación de responsabilidades y recursos para permitir que el riesgo continúe gestionándose en forma eficaz. Si la organización ha crecido, por ejemplo, debido a una fusión o adquisición, será necesario considerar la adecuación regular de los recursos de gestión del riesgo, al igual que un análisis cuidadoso de la diferencia entre las organizaciones en su enfoque a la gestión del riesgo. Podría ser necesario desarrollar un plan de transición para implementar cualquier cambio que surja del análisis.

EJEMPLO 2 Si se han promulgado nuevos requisitos legislativos, podría ser necesario corregir o ampliar aspectos del marco de trabajo que conciernen a las responsabilidades, formación y captura o informe de información.

D.2.5 Revisión del marco de trabajo

Una vez que se ha realizado la evaluación completa de las características y del contexto externo, se debería llevar a cabo una revisión amplia del marco de trabajo para determinar si:

a) el plan de gestión del riesgo se está llevando a cabo en la forma planificada;

b) el marco de trabajo y los procesos adoptados están operando en la forma planificada;

c) el nivel de riesgo está dentro de los criterios;

d) los objetivos esenciales de la organización están influenciados positivamente por la gestión del riesgo;

e) se está informando lo suficiente a las partes involucradas relevantes, para permitirles ‘descargar’ sus roles y responsabilidades en la estructura de gobierno;

f) las personas en la organización cuentan con suficientes habilidades, conocimiento y competencia en gestión del riesgo para llevar a cabo sus responsabilidades identificadas;

g) los recursos de la gestión del riesgo son adecuados;

h) se han aprendido lecciones de los resultados reales, incluidas las pérdidas, cuasi-accidentes y oportunidades que se presentan;

i) los objetivos establecidos para gestión del riesgo se están cumpliendo.

Debería haber un programa acordado para la revisión regular, con la capacidad para llevar a cabo revisiones para un propósito específico si las circunstancias cambian, por ejemplo, cuando las consecuencias de los riesgos son repentinas o severas.

Los entregables de esta revisión deberían incluir:

– un informe general sobre el desempeño del marco de trabajo de gestión del riesgo;

– un informe sobre el progreso de la implementación del plan de gestión del riesgo (incluido el análisis de cualquier retraso en la implementación);

– un informe que indique la posición de madurez de la organización con respecto a las mejores prácticas;

– recomendaciones de cambios que son necesarios para mejorar la gestión del riesgo y su eficacia en la organización;

– actualizar la política, objetivos y plan de gestión del riesgo en la medida en que sea necesario;

– actualizar la descripción del contexto en el que opera la organización, según el caso;

– un informe sobre tendencias en los indicadores clave de riesgo;

– un plan de acción para abordar los cambios requeridos para cumplir los objetivos de gestión del riesgo.

D.3 Seguimiento y revisión del proceso

D.3.1 Generalidades

El propósito del seguimiento y de la revisión del proceso de gestión del riesgo es asegurar que:

– son adecuados para la actividad del negocio;

– funcionan según lo planificado.

Los riesgos, sus controles y tratamientos subyacentes se pueden modificar con el tiempo, y los responsables de la gestión del riesgo necesitan ser conscientes de las implicaciones de estos cambios. Las fallas en los tratamientos pueden conducir a que el riesgo sea inaceptable. Además, los controles cuyo propósito es modificar los riesgos, pueden cambiar en términos de idoneidad y eficacia, de manera que, a menos que se controlen y revisen los riesgos, es posible que estos no permanezcan dentro de los criterios de riesgo aceptables de la organización, y es posible que ésta no tenga una comprensión actualizada de sus riesgos.

Los resultados del seguimiento y la revisión se retroalimentarán al establecimiento de la fase de contexto, brindando la base para una evaluación del riesgo renovada, cumpliendo con la naturaleza reiterativa y dinámica del proceso de gestión del riesgo y del diseño del marco de trabajo de la gestión del riesgo.

D.3.2 Rendición de cuentas

El seguimiento debería ser parte integral de la gestión. Los riesgos y controles se deberían asignar a sus dueños, quienes son responsables de su seguimiento. Esta responsabilidad se debería registrar en las descripciones de puesto o de cargo.

Las organizaciones deberían considerar la incorporación de indicadores de desempeño de gestión del riesgo, las cuales reflejan el rango de ‘motivadores’ organizacionales clave, en las revisiones formales de los empleados, por ejemplo, de manera que se consideren los objetivos financieros, de las partes involucradas, de eficiencia interna, de aprendizaje y de crecimiento. El desempeño contra el mismo grupo de indicadores se puede medir a todos los niveles de la organización y luego informar según sea apropiado.

Los planes de tratamiento de riesgos también se deberían supervisar para asegurarse del progreso logrado, y de que las actividades se finalicen a tiempo.

D.3.3 Aprendizaje de la experiencia

La organización debería aprender de los resultados reales. Estos deberían incluir las pérdidas, cuasi-accidentes, no conformidades y oportunidades que se identificaron previamente, que ocurrieron y aún no se ha actuado sobre ellas. Los puntos que se pueden considerar en una revisión incluyen:

– lo que ocurrió;

– cómo y por qué se produjo ese resultado;

– si es necesario revisar alguna de las hipótesis como resultado de esta consecuencia;

– qué acción se ha tomado (si la hay) en respuesta;

– la posibilidad de que este resultado ocurra nuevamente;

– cualquier respuesta adicional o pasos por seguir;

– los puntos de aprendizaje claves y a quién es necesario comunicarlos.

D.3.4 Seguimiento

D.3.4.1 Los enfoques típicos para el seguimiento incluyen los siguientes:

a) Los dueños del riesgo pueden analizar el ambiente para supervisar los cambios de contexto. La frecuencia de esta revisión dependerá del nivel de riesgo y de la dinámica de los cambios en el contexto. En algunos casos, puede ser suficiente el informe de indicadores que excedan lo ordinario. El dueño del riesgo compara los factores internos o externos pertinentes contra la declaración del contexto para determinar si ha ocurrido un cambio importante. Esto puede involucrar la comunicación y consulta periódica con las partes involucradas para determinar si sus puntos de vista u objetivos han cambiado.

b) Los dueños del riesgo también deberían supervisar los planes de tratamiento de riesgos para determinar las acciones oportunas y responder a cambios en el ambiente.

c) Los dueños de los controles son responsables del seguimiento de los controles asignados a ellos, que pueden involucrar la comprobación periódica o el seguimiento continuo. Debido a que la gestión del riesgo es más eficaz cuando está integrada completamente a la toma de decisiones normal, y al sistema de gestión de la organización, la gestión del desempeño de la organización se debería usar para el seguimiento de los riesgos y la eficacia del proceso de gestión del riesgo. Los indicadores de desempeño deberían reflejar el rango de objetivos organizacionales clave definidos cuando se estableció el contexto al inicio del proceso. También se pueden desarrollar los que se relacionan con riesgos y controles específicos y la aplicación del proceso de gestión del riesgo.

NOTA Al igual que sucede con los riesgos, es recomendable que los dueños de los controles sean los responsables de su operación. El dueño u operador del control normalmente sería la persona que ejecuta el control diariamente y puede ser alguien diferente del dueño del riesgo. Esto no afecta a la responsabilidad global del dueño del riesgo en cuanto a la modificación apropiada de ese riesgo, y para el diseño, implementación, aplicación, seguimiento y evaluación de los controles correspondientes.

D.3.4.2 Los indicadores de desempeño pueden medir resultados (por ejemplo, pérdidas o ganancias) o procesos (por ejemplo, tiempo de finalización de los planes de tratamiento de riesgos). Normalmente se puede usar una mezcla de indicadores, pero los indicadores de desempeño de resultados usualmente retrasan en forma significativa los cambios que dan lugar a ellos. Como resultado, en un ambiente en continuo cambio, es probable que sean más útiles los indicadores de proceso (indicadores de tendencia).

Al escoger indicadores de desempeño, es importante comprobar que:

– sean medibles;

– su uso sea eficiente en términos de demanda de tiempo, esfuerzo y recursos;

– el proceso de medición o de vigilancia estimule o facilite un comportamiento deseable, y no motive uno indeseable (por ejemplo, creación de datos);

– los involucrados comprenden el proceso y los beneficios esperados y tienen la oportunidad de aportar al establecimiento de indicadores;

– los resultados se recopilan y el desempeño se analiza y se informa en un formato que facilite el aprendizaje y la mejora en toda la organización.

D.3.4.3 Al aplicar la gestión del desempeño al proceso de gestión del riesgo, se debería tener en cuenta que:

– la medición eficaz del desempeño requiere recursos que se deberían identificar y asignar como parte del desarrollo de los indicadores de desempeño;

– algunas actividades de gestión del riesgo pueden ser difíciles de medir, lo que no las hace menos importantes, pero puede ser necesario usar indicadores sustitutivos, por ejemplo, los recursos dedicados a las actividades de gestión del riesgo pueden ser una medida sustitutiva del compromiso para una gestión eficaz del riesgo;

– cualquier variación entre los datos de medición de indicadores de desempeño y lo que nos dice el instinto es importante y se debería investigar, por ejemplo, si la gerencia continúa preocupada porque los riesgos no se están gestionando apropiadamente, a pesar de que numerosas evaluaciones del riesgo indican bajos niveles de riesgo, estas inquietudes se deberían investigar y no se deberían desestimar;

– mientras que el deterioro repentino en los indicadores usualmente atraerá la atención, el deterioro progresivo puede ser igualmente problemático, y se debería hacer seguimiento y analizar las tendencias en los indicadores de desempeño.

D.3.5 Revisión

La dirección debería llevar a cabo periódicamente la revisión de procesos, sistemas y actividades para asegurar que:

a) no hayan surgido nuevos riesgos;

b) los controles y tratamiento de riesgos continúen siendo idóneos y eficaces.

Estas revisiones se deberían programar (véase el programa y el enfoque de auditoría basada en el riesgo, y cómo seleccionar a los revisores, como se establece en la Norma ISO 19011).

Para estas revisiones se pueden usar las mismas técnicas que para el seguimiento regular, pero si las realiza alguien que no está involucrado directamente en la operación de los procesos, pueden proporcionar un análisis más objetivo. La frecuencia de la revisión se puede ver influenciada por el nivel de riesgo, el ciclo de planificación del negocio, la dinámica en el ambiente/contexto o por el acuerdo con el organismo de gobierno que es responsable de supervisar los riesgos y la gestión de éstos.

Si se encuentran problemas, la organización debería considerar cómo sucedieron y por qué no se detectaron antes.

Los controles se deberían asegurar por medio de las acciones de los gerentes responsables (dueños del riesgo) como parte de sus trabajos y roles normales. La asignación de controles específicos a los dueños de los controles facilita la implementación de estos, pero para que sean eficaces, estos dueños necesitarán formación en los procesos de aseguramiento de los controles.

Cuando se planifican cambios organizacionales o se detectan cambios externos, puede haber cambios en:

– el ambiente externo o interno, o las partes involucradas y sus puntos de vista;

– el contexto de gestión del riesgo, los objetivos de la organización y sus criterios de riesgo;

– los riesgos y sus diferentes niveles;

– la necesidad de tratamientos para los riesgos;

– el efecto y la eficacia de los controles.

Por esta razón, es esencial que las organizaciones revisen sus riesgos, sus tratamientos y controles para los riesgos, cuando desarrollan o actualizan planes de negocio o planes estratégicos. Además, debido a que los planes de negocio y los planes estratégicos pueden crear o actualizar los objetivos de una organización, es de gran valor usar el proceso de evaluación del riesgo para enfatizar en llevar a cabo pruebas a los borradores de los planes, con el fin de asegurar que los objetivos propuestos se pueden lograr, y también para definir la medida de tratamiento de riesgos requerida para asegurar resultados satisfactorios. Quienes llevan a cabo procesos de gestión del riesgo también deberían revisar regularmente sus experiencias y resultados para identificar oportunidades de mejora.

Anexo E (Informativo)

Integración de la gestión del riesgo a un sistema de gestión

E.1 Generalidades

La gestión del riesgo es una parte integral de un sistema de gestión del riesgo de la organización. La Norma ISO 31000 asesora a las organizaciones para que desarrollen, implementen y mejoren continuamente un marco de referencia cuyo propósito sea integrar la gestión del riesgo al sistema de gestión de la organización (incluidos el gobierno y la estrategia). Específicamente, la integración debería asegurar que la información acerca del riesgo se use como base para la toma de decisiones a todos los niveles de la organización. Las personas y las organizaciones gestionan los riesgos cada día como parte de la forma en que toman decisiones. La gestión del riesgo ya está integrada naturalmente en todo lo que hacemos antes de decidir acerca de algo. Algunos son mejores que otros en esto, pero todos pueden mejorar la calidad de la gestión del riesgo y la toma de decisiones, lo que da como resultado la mejora en el logro de los objetivos, y una mayor confianza. Si el propósito de integrar la gestión del riesgo es añadir valor, lógicamente implica la adopción de formas para influenciar lo que ya existe, incrementarlo y mejorarlo, en vez de reemplazarlo por algo diferente. No puede implicar adicionar o forzar algo diferente en lo que ya ocurre, como una función natural de la toma de decisiones.

La integración no solamente involucra introducir herramientas y procesos de gestión del riesgo establecidos y normalizados a un sistema o a varios sistemas de gestión existentes; se requiere la adaptación y alteración de dichas herramientas y procesos para ajustarse a las necesidades de quienes toman las decisiones y a los procesos existentes para la toma de decisiones.

Este anexo presenta algunos ejemplos prácticos de cómo se puede integrar la gestión del riesgo al sistema o sistemas de gestión existentes.

E.2 ¿Qué es un sistema de gestión?

Todas las organizaciones usan algún tipo de sistema de gestión. En años recientes se han creado sistemas de gestión formalizados compuestos de una variedad de requisitos que proporcionan un marco de referencia en el que la organización puede establecer prácticas y procedimientos de gestión para dirigir y controlar sus actividades. Muchas normas internacionales tratan sobre sistemas de gestión en general, o con relación a contenidos específicos.

Un sistema de gestión es un conjunto de elementos de una organización interrelacionados o que interactúan para establecer políticas y objetivos, y procesos para lograr estos objetivos. Desde una perspectiva de gestión del negocio, se logra eficiencia al contar con un sistema de gestión integrado.

Por ejemplo, la gestión de la calidad como se aborda en la Norma ISO 9001 tiene un amplio enfoque dirigido a la satisfacción del cliente, mientras que la gestión del riesgo trata los efectos de la incertidumbre sobre objetivos que no solo pueden ser pertinentes para los clientes, sino para una variedad de otras partes involucradas. Muchas organizaciones han implementado un sistema de gestión de la calidad basado en los requisitos de la Norma ISO 9001, y la gestión del riesgo se puede integrar en estos sistemas de gestión, creando sinergias y evitando la duplicación.

E.3 Sistema de gestión integrado y gestión del riesgo

Al igual que es necesario integrar la gestión del riesgo a los procesos esenciales del negocio, también lo es crear interacción entre todos los enfoques de sistemas de gestión, por ejemplo, la gestión de la calidad, la gestión ambiental, la gestión de la seguridad, la gestión de la protección, la gestión del cumplimiento, financiera y de información, e incluso con la gestión de seguros que trata sobre sucesos que se pueden transferir financieramente a otras organizaciones.

Estos sistemas de gestión individuales deberían formar un sistema de gestión integrado basado en la política y la estrategia de cualquier organización. Aun cuando una organización tenga sistemas de gestión individuales para gestionar riesgos particulares, el marco de referencia de gestión del riesgo se debería extender e incorporar a estos sistemas.

Este enfoque de gestión del riesgo transversal a la organización puede:

a) incrementar el enfoque de la alta dirección sobre los objetivos estratégicos de la organización;

b) posibilitar que todos los riesgos en el sistema de gestión integrado se manejen de acuerdo con los principios y directrices de la Norma ISO 31000.

Este enfoque puede involucrar lo siguiente:

– la aplicación al sistema de gestión de la calidad de técnicas de gestión del riesgo que conciernen principalmente a la gestión del riesgo de productos y de proyectos;

– el tratamiento de las incertidumbres en la gestión ambiental, por ejemplo, incidentes y accidentes potenciales en lugares peligrosos, la disposición de materiales y sustancias peligrosas;

– la gestión de riesgos combinado con operaciones tales como seguridad en el trabajo;

– la gestión de riesgos de seguridad, por ejemplo, actos de violencia contra la organización o sus empleados o clientes;

– la gestión de riesgos de seguridad de tecnología de la información (TI), por ejemplo, colapso en las operaciones de TI, pérdida de datos, violación de la confidencialidad y aseguramiento de la continuidad del negocio;

– la gestión de riesgos de continuidad del negocio que aseguran la preparación y pronta respuesta ante incidentes perturbadores;

– el establecimiento de controles para proteger los activos de la organización, asegurar la información correcta, asegurar el cumplimiento de los requisitos legales o gestionar riesgos asegurables de una manera que se minimicen las primas.

E.4 Implementación de la gestión del riesgo en un marco de referencia del sistema de gestión de la calidad

E.4.1 Generalidades

El proceso de gestión del riesgo se debería integrar en los procesos de toma de decisiones de una organización, independientemente del nivel y función en los que se toman decisiones.

E.4.2 Identificación y toma de conciencia de la toma de decisiones

Los siguientes métodos ayudan a reconocer cuándo y dónde se toman las decisiones, en línea con el ciclo Planificar-Hacer-Verificar-Actuar

a) Identifique todas las formas de prácticas formalizadas de toma de decisiones que ya existen dentro de la organización. En las organizaciones grandes, existen numerosos procedimientos que requieren aprobaciones formales para una amplia gama de decisiones, por ejemplo, la aprobación del plan estratégico anual, los desembolsos de capital, la contratación de nuevo personal, la modificación de controles de procesos, los viajes del personal.

b) Use un diagrama de flujo o cualquier otra técnica para representar las principales prácticas y secuencias de toma de decisiones que son aplicables a proyectos específicos y a todos los aspectos del negocio. Esto se puede considerar en base a una división o una función, y se debería extender al gobierno, al igual que a la toma de decisiones de la dirección. Si hay actividades que se están gestionando mediante la aplicación de un sistema de gestión formalizado (por ejemplo, gestión de la calidad por medio de la aplicación de la Norma ISO 9001), los puntos de decisión en estos sistemas deberían formar parte de este análisis. En forma similar, si la organización tiene alguna forma de autoridad delegada para la toma de decisiones, estas delegaciones se deberían incluir en el análisis. El resultado final debería ser una imagen coherente y documentada de dónde se toman las decisiones, quién las toma, y los procesos existentes aplicables a estas decisiones.

Una combinación de las técnicas anteriores debería crear un alto grado de toma de conciencia tanto organizacional como personal para la toma de decisiones.

E.4.3 Evaluación de riesgos

En algunos tipos de decisiones (por ejemplo, el desarrollo y realización de un nuevo producto, o la planificación e implementación de un proyecto importante), será apropiado incluir la evaluación formal del riesgo en las diferentes etapas del proyecto. Por ejemplo, la mayoría de proyectos tienen múltiples puntos de decisión, es decir, viabilidad, caso de negocio, presupuesto y planificación detallados, implementación y entrega. En cada uno de estos puntos es apropiada una evaluación formal del riesgo, para decidir entre opciones. Esto incrementa la posibilidad de éxito del proyecto y también mejora la eficiencia.

Para la evaluación del riesgo de las decisiones operacionales se pueden desarrollar formas normalizadas simples del proceso de gestión del riesgo, para uso por el personal involucrado. Estos métodos son adecuados especialmente en situaciones en las que las personas trabajan sin supervisión directa. Un componente clave de estos métodos es la creación de toma de conciencia de las hipótesis como entradas para las decisiones. Por definición, las hipótesis son una fuente de incertidumbre.

Estos procesos normalizados pueden ser específicos del tipo de toma de decisiones involucrada, del grupo particular de personas que ejecutan una tarea particular, y del contexto típico en el que ocurren. Los sistemas simples se pueden codificar en una tarjeta de instrucciones de tamaño bolsillo, que contiene una lista de chequeo, y que portan todos los involucrados en este tipo de trabajo.

E.4.4 Implicaciones para el marco de referencia de gestión del riesgo

La implementación de las técnicas descritas en este apartado requerirá el suministro o ajuste apropiado del marco de referencia de gestión del riesgo, por ejemplo:

– corrección de la política de gestión del riesgo de la organización;

– disposiciones para llevar a cabo la investigación inicial y la representación de la práctica de toma de decisiones;

– correcciones a los manuales de procedimientos;

– formación de directores y personal;

– formación específica de aquellos cuyo trabajo se lleva a cabo de acuerdo con un sistema de gestión específico (por ejemplo, los involucrados con la gestión de tipos de riesgo particulares);

– los ajustes al sistema de aseguramiento de la organización y a la capacidad de información de gestión del riesgo;

– comunicación interna efectiva y consulta.

Bibliografía

[1] ISO 9000, *Quality management systems. Fundamentals and vocabulary.*

[2] ISO 9001, *Quality management systems. Requirements.*

[3] ISO 19011, *Guidelines for auditing management systems.*

[4] ISO Guide 73:2009, *Risk management. Vocabulary.*

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

AENOR Asociación Española de Normalización y Certificación

Génova, 6
28004 MADRID-España

info@aenor.es
www.aenor.es

Tel.: 902 102 201
Fax: 913 104 032