norma española

UNE-ISO 31000

Julio 2010

TÍTULO

Gestión del riesgo

Principios y directrices

Risk management. Principles and guidelines.

Management du risque. Principes et lignes directrices.

CORRESPONDENCIA

Esta norma es idéntica a la Norma Internacional ISO 31000:2009.

OBSERVACIONES

ANTECEDENTES

Esta norma ha sido elaborada por el Grupo Específico de Carácter Temporal AEN/GET13 *Gestión de riesgos* cuya Secretaría desempeña AENOR.

Editada e impresa por AENOR
Depósito legal: M 34496:2010

© AENOR 2010
Reproducción prohibida

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

30 Páginas

Grupo 19

Este documento forma parte de la biblioteca de UNIVERSIDAD POLITECNICA VALENCIA-HEMEROTECA

Este documento forma parte de la biblioteca de UNIVERSIDAD POLITECNICA VALENCIA-HEMEROTECA

ÍNDICE

Página

PRÓLOGO **4**

INTRODUCCIÓN **5**

1 OBJETO Y CAMPO DE APLICACIÓN **8**

2 TÉRMINOS Y DEFINICIONES **8**

3 PRINCIPIOS **13**

4 MARCO DE TRABAJO **15**
4.1 Generalidades **15**
4.2 Mandato y compromiso **16**
4.3 Diseño del marco de trabajo de la gestión del riesgo **16**
4.3.1 Comprensión de la organización y de su contexto **16**
4.3.2 Establecimiento de la política de gestión del riesgo **17**
4.3.3 Obligación de rendir cuentas **17**
4.3.4 Integración en los procesos de la organización **17**
4.3.5 Recursos **18**
4.3.6 Establecimiento de los mecanismos internos de comunicación y de información **18**
4.3.7 Establecimiento de los mecanismos externos de comunicación y de información **18**
4.4 Implementación de la gestión del riesgo **19**
4.4.1 Implementación del marco de trabajo de la gestión del riesgo **19**
4.4.2 Implementación del proceso de gestión del riesgo **19**
4.5 Seguimiento y revisión del marco de trabajo **19**
4.6 Mejora continua del marco de trabajo **19**

5 PROCESO **20**
5.1 Generalidades **20**
5.2 Comunicación y consulta **20**
5.3 Establecimiento del contexto **21**
5.3.1 Generalidades **21**
5.3.2 Establecimiento del contexto externo **21**
5.3.3 Establecimiento del contexto interno **22**
5.3.4 Establecimiento del contexto del proceso de gestión del riesgo **22**
5.3.5 Definición de los criterios de riesgo **23**
5.4 Apreciación del riesgo **23**
5.4.1 Generalidades **23**
5.4.2 Identificación del riesgo **23**
5.4.3 Análisis del riesgo **24**
5.4.4 Evaluación del riesgo **24**
5.5 Tratamiento del riesgo **25**
5.5.1 Generalidades **25**
5.5.2 Selección de opciones de tratamiento del riesgo **25**
5.5.3 Preparación e implementación de los planes de tratamiento del riesgo **26**
5.6 Seguimiento y revisión **26**
5.7 Registro del proceso de gestión del riesgo **27**

ANEXO A (Informativo) ATRIBUTOS DE UNA GESTIÓN DEL RIESGO OPTIMIZADA **28**

BIBLIOGRAFÍA **30**

Este documento forma parte de la biblioteca de UNIVERSIDAD POLITECNICA VALENCIA-HEMEROTECA

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.

Las normas internacionales se redactan de acuerdo con las reglas establecidas en la Parte 2 de las Directivas ISO/IEC.

La tarea principal de los comités técnicos es preparar normas internacionales. Los proyectos de normas internacionales adoptados por los comités técnicos se envían a los organismos miembros para votación. La publicación como norma internacional requiere la aprobación por al menos el 75% de los organismos miembros que emiten voto.

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.

La Norma ISO 31000 fue preparada por el grupo de trabajo del Consejo de Gestión Técnica de ISO (ISO/TMB) sobre gestión del riesgo.

Este documento forma parte de la biblioteca de UNIVERSIDAD POLITECNICA VALENCIA-HEMEROTECA

INTRODUCCIÓN

Organizaciones de todos los tipos y tamaños se enfrentan a factores e influencias internas y externas que hacen incierto saber si y cuando conseguirán sus objetivos. La incidencia que esta incertidumbre tiene sobre la consecución de los objetivos de una organización constituye el "riesgo".

Todas las actividades de una organización implican riesgos. Las organizaciones gestionan el riesgo identificándolo, analizándolo y evaluando después si el riesgo se debería modificar mediante un tratamiento que satisfaga sus criterios de riesgo. A lo largo de todo este proceso, las organizaciones comunican y consultan a las partes interesadas y realizan seguimiento y revisan el riesgo y los controles que lo modifican para asegurar que no es necesario un tratamiento adicional del riesgo.

Mientras todas las organizaciones gestionan el riesgo a diferentes niveles, esta norma internacional establece una serie de principios que se deben satisfacer para que la gestión del riesgo sea eficaz. Esta norma internacional recomienda que las organizaciones desarrollen, implementen y mejoren de manera continuada un marco de trabajo cuyo objetivo sea integrar el proceso de gestión del riesgo en los procesos de gobierno, de estrategia y de planificación, de gestión, y de elaboración de informes, así como en las políticas, los valores y en la cultura de toda la organización.

La gestión del riesgo se puede aplicar a la totalidad de una organización, a todas sus áreas y niveles principales, en todo momento, así como a las funciones, los proyectos y las actividades específicas.

Aunque la práctica de la gestión del riesgo se ha desarrollado a lo largo del tiempo y en numerosos sectores con objeto de satisfacer diversas necesidades, la adopción de procesos coherentes dentro de un marco de trabajo exhaustivo puede contribuir a asegurar que el riesgo se gestiona de una manera eficaz, eficiente y coherente en el seno de la organización. El enfoque genérico que se describe en esta norma internacional proporciona los principios y las directrices para gestionar cualquier forma de riesgo de una manera sistemática, transparente y fiable, dentro de cualquier alcance y de cualquier contexto.

Cada sector o aplicación específicos de gestión del riesgo implica necesidades, audiencias, percepciones y criterios individuales. Por ello, uno de los puntos clave de esta norma internacional consiste en la inclusión del "establecimiento del contexto" como una actividad al comienzo de este proceso de gestión del riesgo genérico. El establecimiento del contexto permitirá captar los objetivos de la organización, el entorno en el que se persiguen estos objetivos, las partes interesadas y la diversidad de los criterios de riesgo. Todos estos elementos contribuirán a revelar y evaluar la naturaleza y complejidad de sus riesgos.

La figura 1 muestra las relaciones entre los principios para gestionar el riesgo, el marco de trabajo en el que se produce y el proceso de gestión del riesgo que se describe en esta norma internacional.

La gestión del riesgo, cuando se implanta y mantiene de acuerdo con esta norma internacional, permite a una organización, por ejemplo:

- aumentar la probabilidad de alcanzar los objetivos;
- estimular una gestión proactiva;
- ser consciente de la necesidad de identificar y tratar el riesgo en toda la organización;
- mejorar la identificación de oportunidades y de amenazas;
- cumplir los requisitos legales y reglamentarios pertinentes y las normas internacionales;
- mejorar la redacción de informes obligatorios y voluntarios;
- mejorar el gobierno;
- mejorar la seguridad y la confianza de las partes interesadas;

Este documento forma parte de la biblioteca de UNIVERSIDAD POLITECNICA VALENCIA-HEMEROTECA

- establecer una base fiable para la toma de decisiones y la planificación;
- mejorar los controles;
- asignar y utilizar de manera eficaz los recursos para el tratamiento del riesgo;
- mejorar la eficacia y la eficiencia operacional;
- aumentar las prestaciones en materia de salud y seguridad, así como la protección ambiental;
- mejorar la prevención de pérdidas y la gestión de incidentes;
- minimizar las pérdidas;
- mejorar el aprendizaje de la organización; y
- mejorar la resiliencia de la organización.

Esta norma internacional está prevista para satisfacer las necesidades de una gran diversidad de partes interesadas incluyendo:

a) las personas responsables de desarrollar la política de gestión del riesgo dentro de su organización;

b) las personas encargadas de asegurar que el riesgo se gestiona de manera eficaz dentro de la organización, considerada en su totalidad o en un área, un proyecto o una actividad específicos;

c) las personas que necesitan evaluar la eficacia de una organización en materia de gestión del riesgo; y

d) las personas que desarrollan normas, guías, procedimientos y códigos de buenas prácticas que, en su totalidad o en parte, establecen cómo se debe tratar el riesgo dentro del contexto específico de estos documentos.

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

En esta norma internacional, se utilizan las dos expresiones "gestión del riesgo" y "gestionar el riesgo". En términos generales, "gestión del riesgo" se refiere a la arquitectura (principios, marco de trabajo y proceso) para gestionar los riesgos de manera eficaz, mientras que "gestionar el riesgo" se refiere a la aplicación de esta arquitectura a los riesgos particulares.

Este documento forma parte de la biblioteca de UNIVERSIDAD POLITECNICA VALENCIA-HEMEROTECA

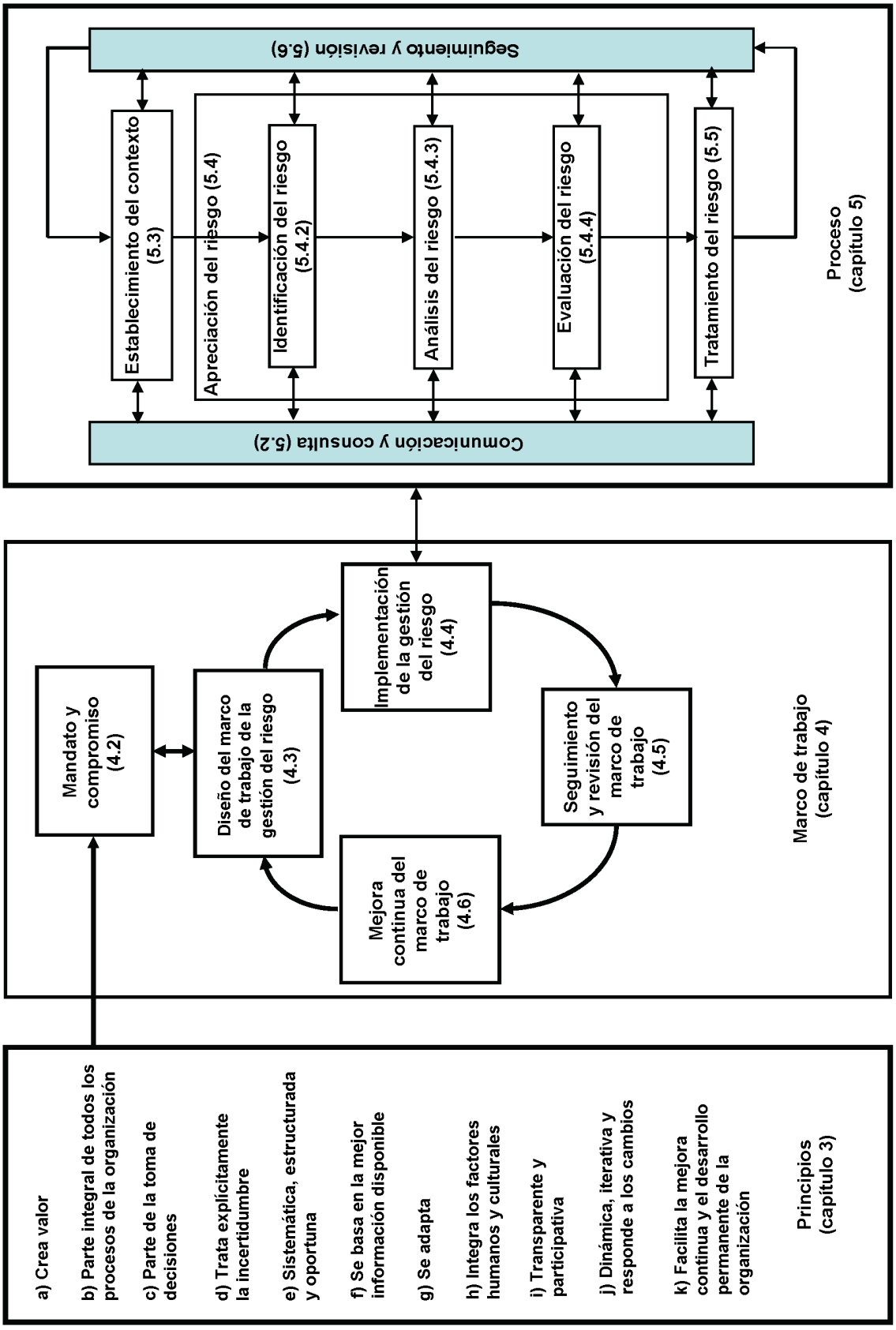

Figura 1 – Relaciones entre los principios, el marco de trabajo y el proceso de gestión del riesgo

Este documento forma parte de la biblioteca de UNIVERSIDAD POLITECNICA VALENCIA-HEMEROTECA

1 OBJETO Y CAMPO DE APLICACIÓN

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

Esta norma internacional puede utilizarse por cualquier empresa pública, privada o social, asociación, grupo o individuo. Por tanto, esta norma internacional no es específica de una industria o sector concreto.

NOTA Por comodidad, todos los diferentes usuarios de esta norma internacional se citan con el término general de "organización".

Esta norma internacional se puede aplicar a lo largo de toda la vida de una organización, y a una amplia gama de actividades, incluyendo estrategias y decisiones, operaciones, procesos, funciones, proyectos, productos, servicios y activos.

Esta norma internacional se puede aplicar a cualquier tipo de riesgo, cualquiera que sea su naturaleza, y tanto si sus consecuencias son positivas o negativas.

Aunque esta norma internacional proporciona directrices genéricas, no tiene como objetivo promover la uniformidad en la gestión del riesgo en el seno de las organizaciones. El diseño y la implementación de planes y marcos de trabajo de gestión del riesgo necesitarán tener en cuenta las diversas necesidades de una organización específica, sus objetivos particulares, su contexto, su estructura, sus operaciones, sus procesos, sus funciones, sus proyectos, sus productos, sus servicios, o sus activos y prácticas específicas utilizadas.

Se pretende que esta norma internacional se utilice para armonizar los procesos de gestión del riesgo establecidos en las normas existentes o futuras. Proporciona un enfoque común en el apoyo de las normas que tratan riesgos y/o sectores específicos, y no sustituye a dichas normas.

Esta norma internacional no está prevista para fines de certificación.

2 TÉRMINOS Y DEFINICIONES

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

2.1 riesgo:

Efecto de la incertidumbre sobre la consecución de los objetivos.

NOTA 1 Un efecto es una desviación, positiva y/o negativa, respecto a lo previsto.

NOTA 2 Los objetivos pueden tener diferentes aspectos (tales como financieros, de salud y seguridad, o ambientales) y se pueden aplicar a diferentes niveles (tales como, nivel estratégico, nivel de un proyecto, de un producto, de un proceso o de una organización completa).

NOTA 3 Con frecuencia, el riesgo se caracteriza por referencia a **sucesos** potenciales (2.17) y a sus **consecuencias** (2.18), o a una combinación de ambos.

NOTA 4 Con frecuencia, el riesgo se expresa en términos de combinación de las consecuencias de un suceso (incluyendo los cambios en las circunstancias) y de su **probabilidad** (2.19).

NOTA 5 La incertidumbre es el estado, incluso parcial, de deficiencia en la información relativa a la comprensión o al conocimiento de un suceso, de sus consecuencias o de su probabilidad.

[ISO Guía 73:2009, definición 1.1]

2.2 gestión del riesgo:

Actividades coordinadas para dirigir y controlar una organización en lo relativo al **riesgo** (2.1).

[ISO Guía 73:2009, definición 2.1]

Este documento forma parte de la biblioteca de UNIVERSIDAD POLITECNICA VALENCIA-HEMEROTECA

2.3 marco de trabajo de la gestión del riesgo:
Conjunto de elementos que proporcionan los fundamentos y las disposiciones de la organización para el diseño, la implantación, el **seguimiento** (2.28), la revisión y la mejora continua de la **gestión del riesgo** (2.2) en toda la organización.

NOTA 1 Los fundamentos incluyen la política, los objetivos, el mandato y el compromiso para gestionar el **riesgo** (2.1).

NOTA 2 Las disposiciones de la organización incluyen los planes, las relaciones, la obligación de rendir cuentas, los recursos, los procesos y las actividades.

NOTA 3 El marco de trabajo de la gestión del riesgo es parte integrante de las políticas y prácticas estratégicas y operacionales generales de la organización.

[ISO Guía 73:2009, definición 2.1.1]

2.4 política de gestión del riesgo:
Declaración de las intenciones y orientaciones generales de una organización en relación con la **gestión del riesgo** (2.2).

[ISO Guía 73:2009, definición 2.1.2]

2.5 actitud ante el riesgo:
Enfoque de la organización para apreciar un **riesgo** (2.1) y eventualmente buscarlo, retenerlo, tomarlo o rechazarlo.

[ISO Guía 73:2009, definición 3.7.1.1]

2.6 plan de gestión del riesgo:
Esquema incluido en el marco de trabajo de **la gestión del riesgo** (2.3) que especifica el enfoque, los componentes de gestión y los recursos a aplicar para la gestión del **riesgo** (2.1).

NOTA 1 Por lo general, los componentes de gestión incluyen los procedimientos, las prácticas, la asignación de responsabilidades, la secuencia y la cronología de las actividades.

NOTA 2 El plan de gestión del riesgo se puede aplicar a un producto, un proceso o un proyecto particular, y a una parte o a la totalidad de la organización.

[ISO Guía 73:2009, definición 2.1.3]

2.7 dueño del riesgo:
Persona o entidad que tiene la responsabilidad y autoridad para gestionar un **riesgo** (2.1).

[ISO Guía 73:2009, definición 3.5.1.5]

2.8 proceso de gestión del riesgo:
Aplicación sistemática de políticas, procedimientos y prácticas de gestión a las actividades de comunicación, consulta, establecimiento del contexto, e identificación, análisis, evaluación, tratamiento, **seguimiento** (2.28) y revisión del **riesgo** (2.1).

[ISO Guía 73:2009, definición 3.1]

2.9 establecimiento del contexto:
Definición de los parámetros externos e internos a tener en cuenta cuando se gestiona el riesgo, y se establecen el alcance y los **criterios de riesgo** (2.22) para la **política de gestión del riesgo** (2.4).

[ISO Guía 73:2009, definición 3.3.1]

2.10 contexto externo:
Entorno externo en el que la organización busca alcanzar sus objetivos.

Este documento forma parte de la biblioteca de UNIVERSIDAD POLITECNICA VALENCIA-HEMEROTECA

NOTA El entorno externo puede incluir:

- el entorno cultural, social, político, legal, reglamentario, financiero, tecnológico, económico, natural y competitivo, a nivel internacional, nacional, regional o local;
- los factores y las tendencias que tengan impacto sobre los objetivos de la organización; y
- las relaciones con las **partes interesadas externas** (2.13), sus percepciones y sus valores.

[ISO Guía 73:2009, definición 3.3.1.1]

2.11 contexto interno:
Entorno interno en el que la organización busca alcanzar sus objetivos.

NOTA El contexto interno puede incluir:

- el gobierno, la estructura de la organización, las funciones y la obligación de rendir cuentas;
- las políticas, los objetivos y las estrategias que se establecen para conseguirlo;
- las capacidades, entendidas en términos de recursos y conocimientos (por ejemplo, capital, tiempo, personas, procesos, sistemas y tecnologías);
- los sistemas de información, los flujos de información y los procesos de toma de decisiones (tanto formales como informales);
- las relaciones con, y las percepciones y los valores de las partes interesadas internas;
- la cultura de la organización;
- las normas, las directrices y los modelos adoptados por la organización; y
- la forma y amplitud de las relaciones contractuales.

[ISO Guía 73:2009, definición 3.3.1.2]

2.12 comunicación y consulta:
Procesos iterativos y continuos que realiza una organización para proporcionar, compartir u obtener información y para establecer el diálogo con las **partes interesadas** (2.13), en relación con la gestión del **riesgo** (2.1).

NOTA 1 La información puede corresponder a la existencia, la naturaleza, la forma, la **probabilidad** (2.19) la importancia, la evaluación, la aceptabilidad y el tratamiento de la gestión del riesgo.

NOTA 2 La consulta constituye un proceso de comunicación informada de doble sentido entre una organización y sus partes interesadas, sobre una cuestión antes de tomar una decisión o determinar una orientación sobre dicha cuestión. La consulta es:

- un proceso que impacta sobre una decisión a través de la influencia más que por la autoridad; y
- una contribución para una toma de decisión, y no una toma de decisión conjunta.

[ISO Guía 73:2009, definición 3.2.1]

2.13 parte interesada:
Persona u organización que puede afectar, ser afectada, o percibir que está afectada por una decisión o actividad.

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

[ISO Guía 73:2009, definición 3.2.1.1]

2.14 apreciación del riesgo:
Proceso global que comprende la **identificación del riesgo** (2.15), el **análisis del riesgo** (2.21) y la **evaluación del riesgo** (2.24).

[ISO Guía 73:2009, definición 3.4.1]

Este documento forma parte de la biblioteca de UNIVERSIDAD POLITECNICA VALENCIA-HEMEROTECA

2.15 identificación del riesgo:
Proceso que comprende la búsqueda, el reconocimiento y la descripción de los **riesgos** (2.1).

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

NOTA 2 La identificación del riesgo puede implicar datos históricos, análisis teóricos, opiniones informadas y de expertos, así como necesidades de las **partes interesadas** (2.13).

[ISO Guía 73:2009, definición 3.5.1]

2.16 fuente de riesgo:
Elemento que, por sí solo o en combinación con otros, presenta el potencial intrínseco de engendrar un **riesgo** (2.1).

NOTA Una fuente de riesgo puede ser tangible o intangible.

[ISO Guía 73:2009, definición 3.5.1.2]

2.17 suceso:
Ocurrencia o cambio de un conjunto particular de circunstancias.

NOTA 1 Un suceso puede ser único o repetirse, y se puede deber a varias causas.

NOTA 2 Un suceso puede consistir en algo que no se llega a producir.

NOTA 3 Algunas veces, un suceso se puede calificar como un "incidente" o un "accidente".

NOTA 4 Un suceso sin **consecuencias** (2.18) también se puede citar como "cuasi accidente" o "incidente".

[ISO Guía 73:2009, definición 3.5.1.3]

2.18 consecuencia:
Resultado de un **suceso** (2.17) que afecta a los objetivos.

NOTA 1 Un suceso puede conducir a una serie de consecuencias.

NOTA 2 Una consecuencia puede ser cierta o incierta y puede tener efectos positivos o negativos sobre la consecución de los objetivos.

NOTA 3 Las consecuencias se pueden expresar de forma cualitativa o cuantitativa.

NOTA 4 Las consecuencias iniciales pueden convertirse en reacciones en cadena.

[ISO Guía 73:2009, definición 3.6.1.3]

2.19 probabilidad *(likehood)*:
Posibilidad de que algún hecho se produzca.

NOTA 1 En la terminología de la gestión del riesgo, la palabra "probabilidad" se utiliza para indicar la posibilidad de que algún hecho se produzca, que esta posibilidad está definida, medida o determinada objetiva o subjetivamente, cualitativa o cuantitativamente, y descrita utilizando términos generales o de forma matemática (tales como una probabilidad o una frecuencia sobre un periodo de tiempo dado).

NOTA 2 La palabra inglesa "likelihood" no tiene una equivalencia directa en algunos idiomas; en su lugar se utiliza con frecuencia la palabra "probability" (probabilidad). Sin embargo, en inglés la palabra "probability" se interpreta frecuentemente de forma más limitada como un término matemático. Por ello, en la terminología de la gestión del riesgo la palabra "likelihood" se utiliza con la misma interpretación amplia que tiene la palabra "probability" (probabilidad) en otros idiomas distintos del inglés.

[ISO Guía 73:2009, definición 3.6.1.1]

Este documento forma parte de la biblioteca de UNIVERSIDAD POLITECNICA VALENCIA-HEMEROTECA

2.20 perfil del riesgo:
Descripción de cualquier conjunto de **riesgos** (2.1).

NOTA El conjunto de riesgos puede incluir los riesgos relativos a toda la organización, a parte de la organización, o definirse de otra manera.

[ISO Guía 73:2009, definición 3.8.2.5]

2.21 análisis del riesgo:
Proceso que permite comprender la naturaleza del **riesgo** (2.1) y determinar el **nivel de riesgo** (2.23).

NOTA 1 El análisis del riesgo proporciona las bases para la **evaluación del riesgo** (2.24) y para tomar las decisiones relativas al **tratamiento del riesgo** (2.25).

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

[ISO Guía 73:2009, definición 3.6.1]

2.22 criterios de riesgo:
Términos de referencia respecto a los que se evalúa la importancia de un **riesgo** (2.1).

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

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

[ISO Guía 73:2009, definición 3.3.1.3]

2.23 nivel de riesgo:
Magnitud de un **riesgo** (2.1) o combinación de riesgos, expresados en términos de la combinación de las **consecuencias** (2.18) y de su **probabilidad** (2.19).

[ISO Guía 73:2009, definición 3.6.1.8]

2.24 evaluación del riesgo:
Proceso de comparación de los resultados del **análisis del riesgo** (2.21) con los **criterios de riesgo** (2.22) para determinar si el **riesgo** (2.1) y/o su magnitud son aceptables o tolerables.

NOTA La evaluación del riesgo ayuda a la toma de decisiones sobre el **tratamiento del riesgo** (2.25).

[ISO Guía 73:2009, definición 3.7.1]

2.25 tratamiento del riesgo:
Proceso destinado a modificar el **riesgo** (2.1).

NOTA 1 El tratamiento del riesgo puede implicar:

- evitar el riesgo, decidiendo no iniciar o continuar con la actividad que motiva el riesgo;
- aceptar o aumentar el riesgo con objeto de buscar una oportunidad;
- eliminar **la fuente de riesgo** (2.16);
- cambiar la **probabilidad** (2.19);
- cambiar las **consecuencias** (2.18);
- compartir el riesgo con otra u otras partes (incluyendo los contratos y la financiación del riesgo); y
- mantener el riesgo en base a una decisión informada.

Este documento forma parte de la biblioteca de UNIVERSIDAD POLITECNICA VALENCIA-HEMEROTECA

NOTA 2 Los tratamientos del riesgo que conducen a consecuencias negativas, en ocasiones se citan como "mitigación del riesgo", "eliminación del riesgo", "prevención del riesgo" y "reducción del riesgo".

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

[ISO Guía 73:2009, definición 3.8.1]

2.26 control:
Medida que modifica un **riesgo** (2.1).

NOTA 1 Los controles incluyen cualquier proceso, política, dispositivo, práctica, u otras acciones que modifiquen un riesgo.

NOTA 2 Los controles no siempre pueden proporcionar el efecto de modificación previsto o asumido.

[ISO Guía 73:2009, definición 3.8.1.1]

2.27 riesgo residual:
Riesgo (2.1) remanente después del **tratamiento del riesgo** (2.25).

NOTA 1 El riesgo residual puede contener riesgos no identificados.

NOTA 2 El riesgo residual también se puede conocer como "riesgo retenido".

[ISO Guía 73:2009, definición 3.8.1.6]

2.28 seguimiento:
Verificación, supervisión, observación crítica o determinación del estado con objeto de identificar de una manera continua los cambios que se puedan producir en el nivel de desempeño requerido o previsto.

NOTA El seguimiento se puede aplicar a un marco de trabajo de **la gestión del riesgo** (2.3), a un **proceso de gestión del riesgo** (2.8), a un **riesgo** (2.1) o al **control** (2.26).

[ISO Guía 73:2009, definición 3.8.2.1]

2.29 revisión:
Actividad que se realiza para determinar la idoneidad, la adecuación y la eficacia del tema estudiado para conseguir los objetivos establecidos.

NOTA La revisión se puede aplicar a un marco de trabajo de **la gestión del riesgo** (2.3), a un **proceso de gestión del riesgo** (2.8), a un **riesgo** (2.1) o al **control** (2.26).

[ISO Guía 73:2009, definición 3.8.2.2]

3 PRINCIPIOS

Para que la gestión del riesgo sea eficaz, las organizaciones deberían cumplir en todos sus niveles los principios siguientes.

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.

Este documento forma parte de la biblioteca de UNIVERSIDAD POLITECNICA VALENCIA-HEMEROTECA

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.

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.

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

La gestión del riesgo tiene en cuenta explícitamente la incertidumbre, la naturaleza de esa incertidumbre, y la manera en que se puede tratar.

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.

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 expertos. No obstante, las personas que toman decisiones deberían informarse y tener en cuenta todas las limitaciones de los datos o modelos utilizados, así como las posibles divergencias entre expertos.

g) **La gestión del riesgo se adapta**

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

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.

i) **La gestión del riesgo es transparente y participativa**

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.

j) **La gestión del riesgo es dinámica, iterativa, y responde a los cambios**

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.

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.

El anexo A proporciona información adicional para las organizaciones que deseen gestionar el riesgo de manera más eficaz.

Este documento forma parte de la biblioteca de UNIVERSIDAD POLITECNICA VALENCIA-HEMEROTECA

4 MARCO DE TRABAJO

4.1 Generalidades

El éxito de la gestión del riesgo dependerá de la eficacia del marco de trabajo de gestión que proporcione las bases y las disposiciones que permitirán su integración a todos los niveles de la organización. El marco de trabajo facilita una gestión eficaz del riesgo mediante la aplicación del proceso de gestión del riesgo (véase el capítulo 5) a diferentes niveles y dentro de contextos específicos de la organización. El marco de trabajo garantiza que la información sobre el riesgo obtenida de este proceso de gestión del riesgo se comunica y utiliza adecuadamente como una base para la toma de decisiones y la obligación de rendir cuentas en todos los niveles pertinentes de la organización.

Este capítulo describe los componentes necesarios del marco de trabajo para la gestión del riesgo y la forma en que estos componentes se interrelacionan de una manera iterativa, como muestra la figura 2.

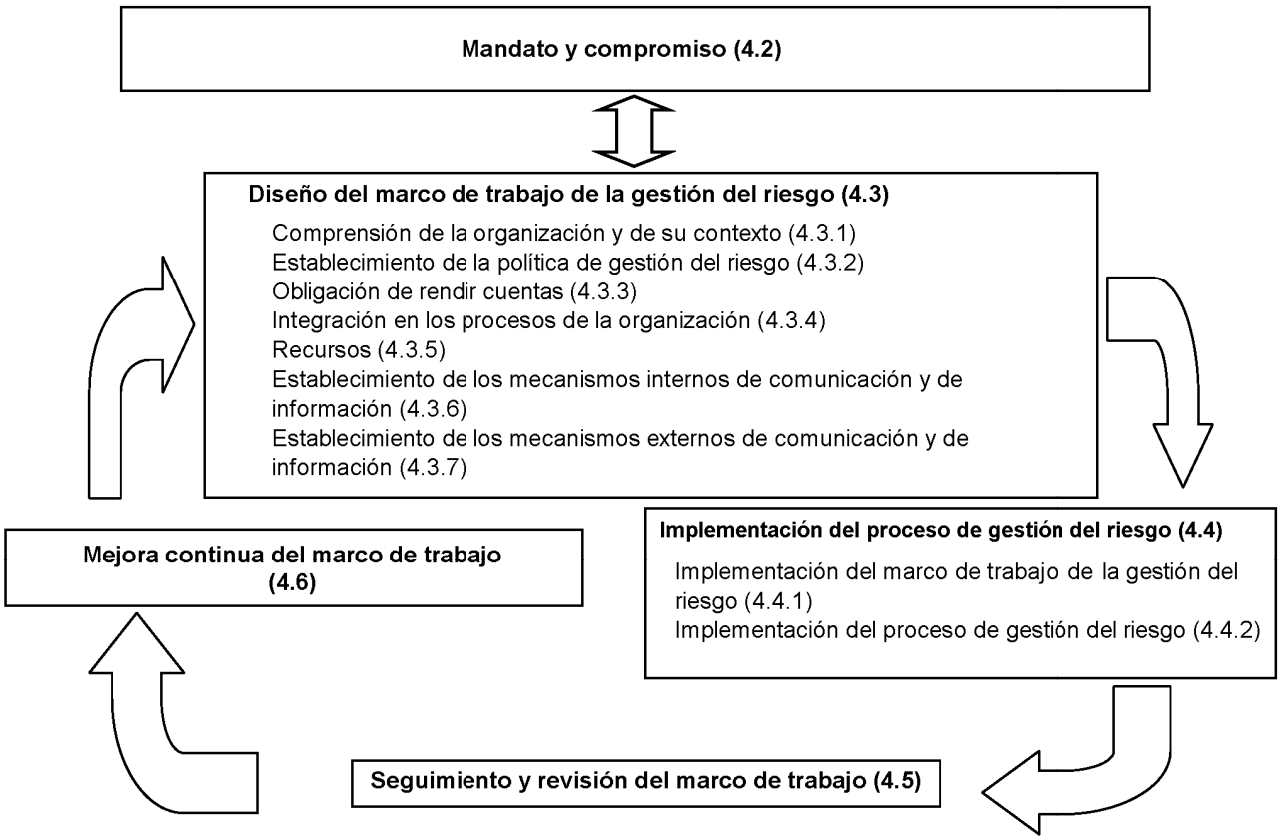

Figura 2 – Relaciones entre los componentes del marco de trabajo de la gestión del riesgo

Este marco de trabajo no está destinado para prescribir un sistema de gestión, sino más bien para ayudar a la organización a integrar la gestión del riesgo en su sistema de gestión global. Por ello, las organizaciones deberían adaptar los componentes del marco de trabajo a sus necesidades específicas.

Si las prácticas y procesos de gestión existentes en una organización incluyen componentes de gestión del riesgo, o si la organización ya ha adoptado un proceso formalizado de gestión del riesgo para tipos particulares de riesgo o de situaciones de riesgo, entonces estos tipos se deberían revisar y evaluar de forma crítica de acuerdo con esta norma internacional, incluyendo los atributos contenidos en el anexo A, a fin de determinar si han sido adecuados, así como su eficacia.

Este documento forma parte de la biblioteca de UNIVERSIDAD POLITECNICA VALENCIA-HEMEROTECA

4.2 Mandato y compromiso

La introducción de la gestión del riesgo y el aseguramiento de su eficacia continua requieren un compromiso fuerte y sostenido de la dirección de la organización, así como el establecimiento de una planificación estratégica y rigurosa para conseguir el compromiso a todos los niveles. La gestión debería:

- definir y aprobar la política de gestión del riesgo;
- asegurar que la cultura de la organización y la política de gestión del riesgo estén alineadas;
- determinar los indicadores de desempeño de la gestión del riesgo que son coherentes con los indicadores de desempeño de la organización;
- alinear los objetivos de la gestión del riesgo con los objetivos y estrategias de la organización;
- asegurar el cumplimiento legal y reglamentario;
- asignar la obligación de rendir cuentas y las responsabilidades que corresponden a los diferentes niveles de la organización;
- asegurar que la gestión del riesgo tiene asignados los recursos necesarios;
- comunicar los beneficios de la gestión del riesgo a todas las partes interesadas; y
- asegurar que el marco de trabajo para gestionar el riesgo continúa siendo adecuado.

4.3 Diseño del marco de trabajo de la gestión del riesgo

4.3.1 Comprensión de la organización y de su contexto

Antes de iniciar el diseño y la implementación del marco de trabajo de la gestión del riesgo, es importante evaluar y entender el contexto externo y el contexto interno de la organización, dado que ambos pueden influir significativamente en el diseño del marco de trabajo.

La evaluación del contexto externo de la organización puede incluir, aunque sin limitarse a ello:

a) el entorno social y cultural, político, legal, reglamentario, financiero, tecnológico, económico, natural y competitivo, a nivel internacional, nacional, regional o local;

b) los factores y las tendencias que tienen impacto sobre los objetivos de la organización; y

c) las relaciones con las partes interesadas, sus percepciones y sus valores.

La evaluación del contexto interno de la organización puede incluir, aunque sin limitarse a ello:

- el gobierno, la estructura de la organización, las funciones y la obligación de rendir cuentas;
- las políticas, los objetivos y las estrategias que se establecen para conseguirlo;
- las aptitudes, entendidas en términos de recursos y conocimientos (por ejemplo, capital, tiempo, personas, procesos, sistemas y tecnologías);
- los sistemas de información, los flujos de información y los procesos de toma de decisiones (tanto formales como informales);
- las relaciones con las partes interesadas, sus percepciones y sus valores;

Este documento forma parte de la biblioteca de UNIVERSIDAD POLITECNICA VALENCIA-HEMEROTECA

- la cultura de la organización;
- las normas, las directrices y los modelos adoptados por la organización; y
- la forma y profundidad de las relaciones contractuales.

4.3.2 Establecimiento de la política de gestión del riesgo

La política de gestión del riesgo debería indicar claramente los objetivos y el compromiso de la organización en materia de la gestión del riesgo, y abordar normalmente lo siguiente:

- las razones de la organización en materia de gestión del riesgo;
- las relaciones entre los objetivos y las políticas de la organización y la política de gestión del riesgo;
- la obligación de rendir cuentas y las responsabilidades en materia de gestión del riesgo;
- la manera en la que se tratan los intereses que entran en conflicto;
- el compromiso para tener disponibles los recursos necesarios para facilitar la obligación de rendir cuentas y las responsabilidades para gestionar el riesgo;
- la manera en la que se mide e informa sobre el desempeño de la gestión del riesgo, y
- el compromiso para revisar y mejorar la política de gestión del riesgo y el marco de trabajo, periódicamente y como respuesta a un suceso o a un cambio de las circunstancias.

La política de gestión del riesgo se debería comunicar de manera apropiada.

4.3.3 Obligación de rendir cuentas

La organización debería asegurarse de que están establecidas la obligación de rendir cuentas, la autoridad y las competencias apropiadas para gestionar el riesgo, incluyendo la implementación y el mantenimiento del proceso de gestión del riesgo y asegurar la idoneidad, la eficacia y la eficiencia de todos los controles. Esto se puede facilitar mediante:

- la identificación de los dueños del riesgo que tienen la responsabilidad y autoridad para gestionar los riesgos;
- la identificación de quiénes tienen obligación de rendir cuentas del desempeño, la implementación, y el mantenimiento del marco de trabajo para la gestión del riesgo;
- la identificación de otras responsabilidades de las personas, a todos los niveles en la organización, para el proceso de gestión del riesgo;
- el establecimiento de los procesos de medición del desempeño y de información externa y/o interna, así como los procesos de transmisión a un nivel superior; y
- el establecimiento de niveles de reconocimiento adecuados.

4.3.4 Integración en los procesos de la organización

La gestión del riesgo debería estar integrada en todas las prácticas y procesos de la organización, de una manera que sea relevante, eficaz y eficiente. El proceso de gestión del riesgo debería formar parte de los procesos de la organización, y no ser independiente de ellos. En particular, la gestión del riesgo debería estar integrada en el desarrollo de la política, en la planificación y revisión de la actividad y la estrategia, y en los procesos de gestión de cambios.

Este documento forma parte de la biblioteca de UNIVERSIDAD POLITECNICA VALENCIA-HEMEROTECA

Debería existir un plan de gestión del riesgo que abarque a toda la organización, para garantizar que se implementa la política de gestión del riesgo y que se integra en todas las prácticas y procesos de la organización. El plan de gestión del riesgo se puede integrar en otros planes de la organización, como un plan estratégico.

4.3.5 Recursos

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

Se debería tener en consideración lo siguiente:

- las personas, las habilidades, la experiencia y las competencias;
- los recursos necesarios para cada etapa del proceso de gestión del riesgo;
- los procesos de la organización, los métodos y las herramientas a utilizar para gestionar el riesgo;
- los procesos y procedimientos documentados;
- los sistemas de gestión de la información y del conocimiento; y
- los programas de formación.

4.3.6 Establecimiento de los mecanismos internos de comunicación y de información

La organización debería establecer mecanismos internos de comunicación y de información con objeto de apoyar y fomentar la obligación de rendir cuentas y la propiedad del riesgo. Estos mecanismos deberían garantizar:

- la comunicación adecuada de los componentes clave del marco de trabajo de la gestión del riesgo, así como de todas las modificaciones posteriores;
- la existencia de informes internos adecuados sobre el marco de trabajo, su eficacia y sus resultados;
- la disponibilidad de información apropiada obtenida de la aplicación de la gestión del riesgo en los niveles y tiempos apropiados; y
- la existencia de procesos para realizar consultas con las partes interesadas.

Cuando corresponda, estos mecanismos deberían incluir procesos para consolidar la información relativa al riesgo procedente de fuentes diferentes, y puede ser necesario considerar la sensibilidad de la información.

4.3.7 Establecimiento de los mecanismos externos de comunicación y de información

La organización debería desarrollar e implementar un plan para comunicarse con las partes interesadas externas. Este plan debería implicar:

- la participación de las partes interesadas externas apropiadas, asegurándose un intercambio eficaz de información;
- el establecimiento de informes externos conformes con los requisitos legales, reglamentarios y de gobierno de la organización;
- la disponibilidad de retroalimentación y de informes sobre comunicación y consulta;
- la utilización de comunicaciones para generar confianza en la organización; y
- la comunicación con las partes interesadas en caso de crisis o contingencias,

Este documento forma parte de la biblioteca de UNIVERSIDAD POLITECNICA VALENCIA-HEMEROTECA

Cuando corresponda, estos mecanismos deberían incluir procesos para consolidar la información relativa al riesgo procedente de fuentes diferentes, y puede ser necesario considerar la sensibilidad de la información.

4.4 Implementación de la gestión del riesgo

4.4.1 Implementación del marco de trabajo de la gestión del riesgo

Para la implementación del marco de trabajo de la gestión del riesgo, la organización debería:

- definir el calendario y la estrategia apropiados para la implementación del marco de trabajo;
- aplicar la política y el proceso de gestión del riesgo a los procesos de la organización;
- cumplir los requisitos legales y reglamentarios;
- garantizar que la toma de decisiones, incluyendo el desarrollo y el establecimiento de los objetivos, se alinean con los resultados de los procesos de gestión del riesgo;
- organizar sesiones de información y de formación; y
- comunicar y consultar a las partes interesadas para garantizar que su marco de trabajo de la gestión del riesgo continua siendo apropiado.

4.4.2 Implementación del proceso de gestión del riesgo

La gestión del riesgo se debería implementar de manera que se asegure que el proceso de gestión del riesgo, descrito en el capítulo 5 se aplica mediante un plan de gestión del riesgo en todos los niveles y funciones pertinentes de la organización, como parte de sus prácticas y procesos.

4.5 Seguimiento y revisión del marco de trabajo

Con objeto de asegurar que la gestión del riesgo es eficaz y contribuye a ayudar al desempeño de la organización, ésta debería:

- medir el desempeño de la gestión del riesgo respecto a los indicadores, que se revisan periódicamente en cuanto a su idoneidad;
- medir periódicamente el progreso y las desviaciones respecto al plan de gestión del riesgo;
- revisar periódicamente si el marco de trabajo, la política y el plan de gestión del riesgo siguen siendo apropiados, a la vista del contexto interno y externo de la organización;
- establecer informes sobre los riesgos, sobre el progreso del plan de gestión del riesgo y sobre la forma en que se está siguiendo la política de gestión del riesgo; y
- revisar la eficacia del marco de trabajo de la gestión del riesgo.

4.6 Mejora continua del marco de trabajo

En base a los resultados obtenidos del seguimiento y de las revisiones, se deberían tomar decisiones sobre cómo mejorar el marco de trabajo, la política y el plan de gestión del riesgo. Estas decisiones deberían conducir a mejoras en la gestión del riesgo por parte de la organización, así como a mejoras de su cultura de gestión del riesgo.

Este documento forma parte de la biblioteca de UNIVERSIDAD POLITECNICA VALENCIA-HEMEROTECA

5 PROCESO

5.1 Generalidades

El proceso de gestión del riesgo debería:

- ser una parte integrante de la gestión;
- integrarse en la cultura y en las prácticas; y
- adaptarse a los procesos de negocio de la organización.

El proceso de gestión del riesgo comprende las actividades descritas en los apartados 5.2 al 5.6. La figura 3 muestra el proceso de gestión del riesgo.

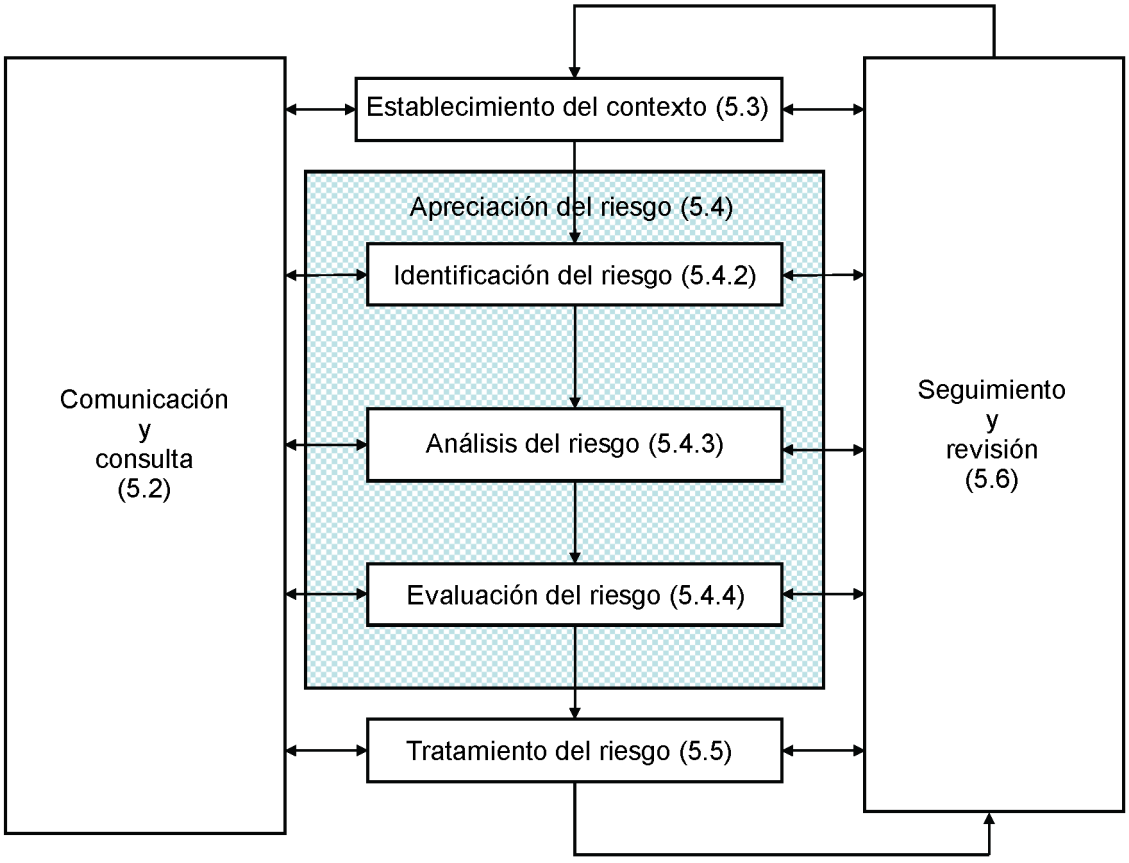

Figura 3 – Proceso de gestión del riesgo

5.2 Comunicación y consulta

Las comunicaciones y las consultas con las partes interesadas externas e internas se deberían realizar en todas las etapas del proceso de gestión del riesgo.

Por ello, en una de las primeras etapas se deberían desarrollar los planes de comunicación y consulta. Estos planes deberían tratar temas relativos al riesgo en sí mismo, a sus causas, a sus consecuencias (si se conocen), y a las medidas a tomar para tratarlo. Se deberían realizar comunicaciones y consultas externas e internas eficaces para asegurarse de que las personas responsables de la implementación del proceso de gestión del riesgo y las partes interesadas comprenden las bases que han servido para tomar decisiones y las razones por las que son necesarias determinadas acciones.

Este documento forma parte de la biblioteca de UNIVERSIDAD POLITECNICA VALENCIA-HEMEROTECA

Un enfoque consultivo en equipo puede:

- ayudar a establecer adecuadamente el contexto;
- asegurar que los intereses de las partes interesadas se comprenden y se tienen en consideración;
- ayudar a asegurar que los riesgos se identifican adecuadamente;
- reunir diferentes áreas de experiencia para analizar los riesgos;
- asegurar que las diferentes opiniones se tienen en cuenta de forma adecuada, al definir los criterios de riesgo y en la evaluación de los riesgos;
- conseguir la aprobación y el apoyo para un plan de tratamiento;
- favorecer una gestión de cambio adecuada durante el proceso de gestión del riesgo; y
- desarrollar un plan adecuado de comunicación y consultas externas e internas.

Las comunicaciones y consultas con las partes interesadas son importantes ya que éstas pueden emitir juicios sobre el riego basados en sus percepciones de riesgo. Estas percepciones pueden variar debido a diferencias en los valores, las necesidades, las hipótesis, los conceptos y las inquietudes de las partes interesadas. Como sus opiniones pueden tener un impacto importante en las decisiones tomadas, las percepciones de las partes interesadas se deberían identificar, registrar y tomar en consideración en el proceso de toma de decisiones.

Las comunicaciones y consultas deberían facilitar intercambios de información que sean veraces, pertinentes, exactos y entendibles, teniendo en cuenta los aspectos confidenciales y de integridad personal.

5.3 Establecimiento del contexto

5.3.1 Generalidades

Mediante el establecimiento del contexto, la organización articula sus objetivos, define los parámetros externos e internos a tener en cuenta en la gestión del riesgo, y establece el alcance y los criterios de riesgo para el proceso restante. Aunque muchos de estos parámetros son similares a los considerados en el diseño del marco de trabajo de la gestión del riesgo (véase 4.3.1), cuando se establece el contexto para el proceso de gestión del riesgo tales parámetros se deben considerar en mayor detalle, y en particular cómo están relacionados con el alcance del proceso particular de gestión del riesgo.

5.3.2 Establecimiento del contexto externo

El contexto externo es el entorno externo en que la organización busca conseguir sus objetivos.

La comprensión del contexto externo es importante para asegurarse de que los objetivos e inquietudes de las partes interesadas externas se tienen en cuenta cuando se desarrollan los criterios de riesgo. El contexto externo se basa en el contexto a escala de la organización, pero con detalles específicos de requisitos legales y reglamentarios, con las percepciones de las partes interesadas y con otros aspectos de riesgos específicos del alcance del proceso de gestión del riesgo.

El contexto externo puede incluir, pero no se limita a:

- el entorno social y cultural, político, legal, reglamentario, financiero, tecnológico, económico, natural y competitivo, a nivel internacional, nacional, regional o local;
- los factores y las tendencias clave que tengan impacto en los objetivos de la organización; y
- las relaciones con las partes interesadas externas, sus percepciones y sus valores.

Este documento forma parte de la biblioteca de UNIVERSIDAD POLITECNICA VALENCIA-HEMEROTECA

5.3.3 Establecimiento del contexto interno

El contexto interno es el entorno interno en que la organización busca conseguir sus objetivos.

El proceso de gestión del riesgo debería alinearse con la cultura, los procesos, la estructura y la estrategia de la organización. El contexto interno lo constituye todo aquello que en el seno de la organización puede influir en la manera en la que una organización gestionará el riesgo. Este contexto se debería establecer, ya que:

a) la gestión del riesgo se realiza en el contexto de los objetivos de la organización;

b) los objetivos y los criterios de un proyecto, de un proceso o de una actividad específicos se deberían considerar a la vista de los objetivos de la organización en su conjunto; y

c) algunas organizaciones no reconocen todas las oportunidades que les permiten conseguir sus objetivos en materia de estrategia, de proyecto o de negocio, y esto afecta a la continuidad del compromiso, la credibilidad, la confianza y los valores de la organización.

Es necesario comprender el contexto interno. Puede incluir, pero no se limita a:

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

5.3.4 Establecimiento del contexto del proceso de gestión del riesgo

Se deberían establecer los objetivos, las estrategias, el alcance y los parámetros de las actividades de la organización, o de aquellas partes de la organización donde se aplica el proceso de gestión del riesgo. La gestión del riesgo se debería emprender teniendo en cuenta todo lo necesario para justificar los recursos que se han de utilizar para llevarla a cabo. También se deberían especificar los recursos requeridos, las responsabilidades y autoridades, y los registros que se deben conservar.

El contexto del proceso de la gestión del riesgo variará de acuerdo con las necesidades de la organización. Puede implicar, pero no se limita a:

- la definición de las metas y objetivos de las actividades de gestión del riesgo;
- la definición de las responsabilidades relativas al proceso de gestión del riesgo;
- la definición del alcance, así como el grado y la amplitud de las actividades de gestión del riesgo a realizar, incluyendo las inclusiones y exclusiones específicas;
- la definición de la actividad, del proceso, de la función, del proyecto, del producto, del servicio o del activo, en términos de tiempo y de ubicación;

Este documento forma parte de la biblioteca de UNIVERSIDAD POLITECNICA VALENCIA-HEMEROTECA

- la definición de las relaciones entre un proyecto, un proceso o una actividad particulares y otros proyectos, procesos o actividades de la organización;
- la definición de las metodologías de apreciación del riesgo;
- la definición del método para evaluar el desempeño y la eficacia en la gestión del riesgo;
- la identificación y la especificación de las decisiones a tomar; y
- la identificación, el alcance o el marco de los estudios requeridos, su amplitud y sus objetivos, así como los recursos necesarios para tales estudios.

Se deberían tener en cuenta estos y otros factores pertinentes para asegurar que el enfoque adoptado de la gestión del riesgo es apropiado a las circunstancias, a la organización y a los riesgos que afectan al logro de sus objetivos.

5.3.5 Definición de los criterios de riesgo

La organización debería definir los criterios que se aplican para evaluar la importancia del riesgo. Los criterios deberían reflejar los valores, los objetivos y los recursos de la organización. Algunos criterios pueden estar impuestos o derivarse de requisitos legales o reglamentarios, o de otros requisitos suscritos por la organización. Los criterios de riesgo deberían ser coherentes con la política de gestión del riesgo de la organización (véase 4.3.2), definirse al comienzo de cualquier proceso de gestión del riesgo, y revisarse continuamente.

Al definir los criterios de riesgo, se deberían considerar una serie de factores entre los cuales se incluyen los siguientes:

- la naturaleza y los tipos de las causas y de las consecuencias que se pueden producir, y cómo se deben medir;
- el método de definición de la probabilidad;
- los plazos de la probabilidad y/o de las consecuencias;
- el método para determinar el nivel de riesgo;
- las opiniones de las partes interesadas;
- el nivel al que el riesgo comienza a ser aceptable o tolerable; y
- si se deberían tener en cuenta combinaciones de riesgos múltiples y, en caso afirmativo, cómo y qué combinaciones se deberían considerar.

5.4 Apreciación del riesgo

5.4.1 Generalidades

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

NOTA La Norma ISO/IEC 31010 proporciona directrices sobre las técnicas de apreciación del riesgo.

5.4.2 Identificación del riesgo

La organización debería identificar los orígenes de riesgo, las áreas de impactos, los sucesos (incluyendo los cambios de circunstancias), así como sus causas y sus consecuencias potenciales. El objetivo de esta etapa consiste en generar una lista de riesgos exhaustiva basada en aquellos sucesos que podrían crear, mejorar, prevenir, degradar, acelerar o retrasar el logro de los objetivos. Es importante identificar los riesgos asociados al hecho de no buscar una oportunidad. Es esencial realizar una identificación exhaustiva, ya que un riesgo que no se identifica en esta etapa no se incluirá en análisis posteriores.

Este documento forma parte de la biblioteca de UNIVERSIDAD POLITECNICA VALENCIA-HEMEROTECA

La identificación debería incluir los riesgos, tanto si su origen está o no bajo el control de la organización, incluso aunque el origen o la causa del riesgo no pueda ser evidente. La identificación del riesgo debería incluir el examen de los efectos en cadena de consecuencias particulares, incluyendo los efectos en cascada o acumulativos. También debería considerar un amplio rango de consecuencias, incluso aunque el origen o la causa del riesgo no puedan ser evidentes. Además de identificar lo que podría ocurrir, es necesario considerar las posibles causas y escenarios que muestran las consecuencias que se pueden producir. Todas las causas y consecuencias significativas se deberían tener en consideración.

La organización debería aplicar herramientas y técnicas de identificación del riesgo que se adapten a sus objetivos y aptitudes, así como a los riesgos a los que está expuesta. Para la identificación de los riesgos es esencial disponer de información pertinente y actualizada. Siempre que sea posible, esta información debería ir acompañada de antecedentes apropiados. En la identificación de los riesgos deberían intervenir personas con conocimientos apropiados.

5.4.3 Análisis del riesgo

El análisis del riesgo implica desarrollar una comprensión del riesgo. El análisis del riesgo proporciona elementos de entrada para la evaluación del riesgo y para tomar decisiones acerca de si es necesario tratar los riesgos, así como sobre las estrategias y los métodos de tratamiento del riesgo más apropiados. El análisis del riesgo también puede proporcionar elementos de entrada para tomar decisiones cuando se deben hacer elecciones, y las opciones implican diferentes tipos de niveles de riesgo.

El análisis del riesgo implica la consideración de las causas y las fuentes del riesgo, sus consecuencias positivas y negativas, y la probabilidad de que estas consecuencias puedan ocurrir. Se deberían identificar los factores que afectan a las consecuencias y a la probabilidad. El riesgo se analiza determinando las consecuencias y su probabilidad, así como otros atributos del riesgo. Un suceso puede tener múltiples consecuencias y puede afectar a múltiples objetivos. También se deberían tener en cuenta los controles existentes, así como su eficacia y su eficiencia.

La forma de expresar las consecuencias y la probabilidad, así como la manera en que éstas se combinan para determinar un nivel de riesgo, debería corresponder al tipo de riesgo, a la información disponible y al objetivo para el que se utiliza el resultado de la apreciación del riesgo. Todos estos datos deberían ser coherentes con los criterios de riesgo. También es importante considerar la interdependencia de los diferentes riesgos y de sus fuentes.

La confianza en la determinación del nivel de riesgo y su sensibilidad a las condiciones previas y a las hipótesis se debería considerar en el análisis y comunicar de manera eficaz a las personas que han de tomar decisiones y, cuando corresponda, a otras partes interesadas. Factores tales como las diferencias de opinión entre expertos, la incertidumbre, la disponibilidad, la calidad, la cantidad y la validez de la pertinencia de la información, o las limitaciones respecto a modelos establecidos se deberían indicar y pueden resaltarse.

El análisis del riesgo se puede realizar con diferentes grados de detalle, dependiendo del riesgo, de la finalidad del análisis y de la información, así como de los datos y los recursos disponibles. El análisis puede ser cualitativo, semi-cuantitativo o cuantitativo, o una combinación de los tres casos, dependiendo de las circunstancias.

Las consecuencias y su probabilidad se pueden determinar realizando el modelo de los resultados de un suceso o conjunto de sucesos, o por extrapolación de estudios experimentales o de datos disponibles. Las consecuencias se pueden expresar en términos de impactos tangibles o intangibles. En algunos casos, se requiere más de un valor numérico o descriptor para especificar las consecuencias y su probabilidad para diferentes momentos, lugares, grupos o situaciones.

5.4.4 Evaluación del riesgo

En base a los resultados del análisis del riesgo la finalidad de la evaluación del riesgo es ayudar a la toma de decisiones, determinando los riesgos a tratar y la prioridad para implementar el tratamiento.

La evaluación del riesgo implica comparar el nivel de riesgo encontrado durante el proceso de análisis con los criterios de riesgo establecidos cuando se consideró el contexto. En base a esta comparación, se puede considerar la necesidad del tratamiento.

Este documento forma parte de la biblioteca de UNIVERSIDAD POLITECNICA VALENCIA-HEMEROTECA

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

En algunas circunstancias, la evaluación del riesgo puede llevar a la decisión de realizar un análisis en mayor profundidad. La evaluación del riesgo también puede llevar a la decisión de no tratar el riesgo de ninguna otra manera que manteniendo los controles existentes. Esta decisión estará influenciada por la actitud ante el riesgo por parte de la organización y por los criterios de riesgo que se hayan establecido.

5.5 Tratamiento del riesgo

5.5.1 Generalidades

El tratamiento del riesgo implica la selección y la implementación de una o varias opciones para modificar los riesgos. Una vez realizada la implementación, los tratamientos proporcionan o modifican los controles.

El tratamiento del riesgo supone un proceso cíclico de:

- evaluar un tratamiento del riesgo;
- decidir si los niveles de riesgo residual son tolerables;
- si no son tolerables, generar un nuevo tratamiento del riesgo; y
- evaluar la eficacia de este tratamiento.

Las opciones de tratamiento del riesgo no se excluyen necesariamente unas a otras, ni son apropiadas en todas las circunstancias. Las opciones pueden incluir lo siguiente:

a) evitar el riesgo decidiendo no iniciar o continuar con la actividad que causa el riesgo;

b) aceptar o aumentar el riesgo a fin de perseguir una oportunidad;

c) eliminar la fuente del riesgo;

d) modificar la probabilidad;

e) modificar las consecuencias;

f) compartir el riesgo con otras partes (incluyendo los contratos y la financiación del riesgo); y

g) retener el riesgo en base a una decisión informada.

5.5.2 Selección de opciones de tratamiento del riesgo

La selección de la opción más apropiada de tratamiento del riesgo implica obtener una compensación de los costes y los esfuerzos de implementación en función de las ventajas que se obtengan, teniendo en cuenta los requisitos legales, reglamentarios y de otro tipo, tales como la responsabilidad social y la protección del entorno natural. Las decisiones también se deberían tomar teniendo en cuenta los riesgos cuyo tratamiento no es justificable en el plano económico, por ejemplo, riesgos severos (consecuencias altamente negativas) pero raros (baja probabilidad).

Un determinado número de opciones de tratamiento se puede considerar y aplicar bien individualmente o bien en combinación. Normalmente, la organización puede beneficiarse de la adopción de una combinación de opciones de tratamiento.

Este documento forma parte de la biblioteca de UNIVERSIDAD POLITECNICA VALENCIA-HEMEROTECA

Al seleccionar opciones de tratamiento del riesgo, la organización debería tener en consideración los valores y las percepciones de las partes interesadas y los medios más apropiados para comunicarse con ellas. Cuando las opciones de tratamiento del riesgo puedan impactar sobre el riesgo en cualquier otra parte de la organización o en las partes interesadas, éstas se deberían involucrar en la decisión. A igual eficacia, algunos tratamientos del riesgo pueden ser más aceptables que otros para algunas partes interesadas.

El plan de tratamiento debería identificar con claridad el orden de prioridad en que se deberían implementar los tratamientos de riesgo individuales.

El tratamiento del riesgo a su vez puede introducir nuevos riesgos. El fallo o la ineficacia de las medidas de tratamiento del riesgo pueden constituir un riesgo importante. Para tener la seguridad de que las medidas son eficaces, es necesario que el seguimiento sea una parte integrante del plan de tratamiento del riesgo.

El tratamiento del riesgo también puede introducir riesgos secundarios que necesitan que se aprecien, se traten, se realice seguimiento y se revisen. Estos riesgos secundarios se deberían incorporar en el mismo plan de tratamiento que el riesgo original, y no tratarse como riesgos nuevos. La relación entre los dos riesgos debería identificarse y mantenerse.

5.5.3 Preparación e implementación de los planes de tratamiento del riesgo

La finalidad de los planes de tratamiento del riesgo consiste en documentar la manera en que se implantarán las opciones de tratamiento elegidas. La información proporcionada en los planes de tratamiento debería incluir lo siguiente:

- las razones que justifican la selección de las opciones de tratamiento, incluyendo los beneficios previstos;
- las personas responsables de la aprobación del plan y las personas responsables de la implementación del plan;
- las acciones propuestas;
- las necesidades de recursos, incluyendo las contingencias;
- las medidas del desempeño y las restricciones;
- los requisitos en materia de información y de seguimiento; y
- el calendario y la programación.

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

Las personas que toman decisiones y las otras partes interesadas deberían estar enteradas de la naturaleza y amplitud del riesgo residual después del tratamiento del riesgo. El riesgo residual se debería documentar y someter a seguimiento, revisión y, cuando sea apropiado, a tratamiento adicional.

5.6 Seguimiento y revisión

El seguimiento y la revisión deberían planificarse en el proceso de tratamiento del riesgo y someterse a una verificación o una vigilancia regular. Esta verificación o vigilancia puede ser periódica o eventual.

Las responsabilidades del seguimiento y de la revisión deberían estar claramente definidas.

Los procesos de seguimiento y de revisión de la organización deberían abarcar todos los aspectos del proceso de gestión del riesgo, con la finalidad de:

- asegurar que los controles son eficaces y eficientes tanto en su diseño como en su utilización;
- obtener la información adicional para mejorar la apreciación del riesgo;

Este documento forma parte de la biblioteca de UNIVERSIDAD POLITECNICA VALENCIA-HEMEROTECA

- analizar y sacar conclusiones de los sucesos (incluyendo los cuasi-accidentes), cambios, tendencias, éxitos y fallos;
- detectar los cambios en el contexto interno y externo, incluidos los cambios en los criterios de riesgo y en el propio riesgo, que puedan requerir la revisión de los tratamientos de riesgo y de las prioridades; e
- identificar los riesgos emergentes.

El avance en la implantación de los planes de tratamiento del riesgo proporciona una medida del funcionamiento. Los resultados se pueden incorporar en la gestión del funcionamiento global de la organización, en su medición y en las actividades externas e internas.

Los resultados del seguimiento y de la revisión se deberían registrar e incluir en informes internos y externos, según sea apropiado, y también se deberían utilizar como elementos de entrada para la revisión del marco de trabajo de la gestión del riesgo (véase 4.5).

5.7 Registro del proceso de gestión del riesgo

Las actividades de gestión del riesgo deberían ser trazables. En el proceso de gestión del riesgo los registros proporcionan la base para la mejora de los métodos y de las herramientas, así como del proceso en su conjunto.

Las decisiones relativas a la creación de registros deberían tener en cuenta:

- las necesidades de la organización en materia de aprendizaje continuo;
- los beneficios de reutilizar la información para fines de gestión;
- los costes y los esfuerzos que suponen la creación y el mantenimiento de los registros;
- las necesidades legales, reglamentarias y operacionales para efectuar los registros;
- el método de acceso, la facilidad de recuperación y los medios de almacenaje;
- el periodo de conservación; y
- el carácter sensible de la información.

Este documento forma parte de la biblioteca de UNIVERSIDAD POLITECNICA VALENCIA-HEMEROTECA

ANEXO A (Informativo)

ATRIBUTOS DE UNA GESTIÓN DEL RIESGO OPTIMIZADA

A.1 Generalidades

Todas las organizaciones deberían tener como objetivo disponer de un nivel apropiado de desempeño de su marco de trabajo de la gestión del riesgo, en línea con el grado de criticidad de las decisiones a tomar. La lista de atributos que figura a continuación representa un nivel elevado de desempeño de la gestión del riesgo. Para ayudar a las organizaciones a medir su propio desempeño con respecto a estos criterios, se proporcionan algunos indicadores tangibles para cada atributo.

A.2 Puntos clave

A.2.1 La organización tiene una comprensión exhaustiva, correcta y actualizada de sus riesgos.

A.2.2 Los riesgos de la organización están en los límites de sus criterios de riesgo.

A.3 Atributos

A.3.1 Mejora continua

Se pone énfasis en la mejora continua de la gestión del riesgo mediante el establecimiento de metas de desempeño organizacional, medición, revisión y la modificación posterior de los procesos, los sistemas, los recursos, la capacidad y las habilidades.

Los indicadores tangibles son, por ejemplo, la existencia de objetivos de desempeño explícitos que permitan medir el desempeño individual de los responsables y el de la propia organización. El desempeño de la organización se puede publicar y comunicar. Normalmente, habrá al menos una revisión anual del desempeño y después una revisión de los procesos y del establecimiento de los objetivos de desempeño revisados para el periodo siguiente.

Esta evaluación del desempeño de la gestión del riesgo es una parte integral de la evaluación del desempeño global de la organización y del sistema de medición del desempeño de los departamentos y de las personas.

A.3.2 Responsabilidad completa de los riesgos

La gestión del riesgo optimizada incluye una responsabilidad exhaustiva totalmente definida y aceptada de los riesgos, los controles y las tareas de tratamiento del riesgo. Las personas designadas deben aceptar la responsabilidad completa, tener las habilidades necesarias, disponer de los recursos adecuados para verificar los controles, realizar el seguimiento de los riesgos, mejorar los controles, y comunicar eficazmente a las partes interesadas externas e internas todo lo referente a los riesgos y a su gestión.

Los indicadores tangibles son, por ejemplo, el hecho de que todos los miembros de una organización hayan tomado conciencia plenamente de los riesgos, de los controles, y de las tareas de las que son responsables. Normalmente, esto estará registrado en las descripciones del puesto de trabajo/ocupación, y en las bases de datos o en los sistemas de información. La definición de las funciones, la obligación de rendir cuentas y las responsabilidades en materia de gestión del riesgo deberían formar parte de todos los programas de acogida para las incorporaciones nuevas a un puesto o una función.

La organización debe asegurase de que todas las personas responsables disponen de todo lo necesario para cumplir su función, proporcionándoles la autoridad, el tiempo, la formación, los recursos y las habilidades necesarias para asumir sus responsabilidades.

Este documento forma parte de la biblioteca de UNIVERSIDAD POLITECNICA VALENCIA-HEMEROTECA

A.3.3 Aplicación de la gestión del riesgo en todas las tomas de decisiones

Todas las tomas de decisiones dentro de la organización, cualquiera que sea el nivel de importancia y de relevancia, implican la consideración explícita de los riesgos y la aplicación de la gestión del riesgo hasta el grado apropiado.

Los indicadores tangibles son, por ejemplo, la existencia de registros de las reuniones y de las decisiones, donde se muestre la realización de las discusiones explícitas sobre los riesgos. Además, debería ser posible comprobar que todos los componentes de la gestión del riesgo están representados en los procesos clave de toma de decisiones en la organización, por ejemplo, en las decisiones sobre la asignación del capital, sobre proyectos importantes, y sobre reestructuración o cambios de la organización. Por estas razones, en el seno de una organización se considera que una gestión del riesgo que esté bien consolidada proporciona las bases para un gobierno eficaz.

A.3.4 Comunicación continua

Una gestión del riesgo optimizada incluye comunicaciones continuas con las partes interesadas externas e internas en la empresa, incluyendo informes exhaustivos y frecuentes sobre el desempeño de la gestión del riesgo, como parte de un buen gobierno.

La comunicación con las partes interesadas como un componente integral y esencial de la gestión del riesgo es un ejemplo de indicador tangible. La comunicación se contempla como un proceso de doble sentido, de manera que se puedan tomar decisiones informadas correctamente sobre el nivel de riesgo y la necesidad de un tratamiento del riesgo, en función de criterios de riesgo exhaustivos y adecuadamente establecidos.

Los informes externos e internos exhaustivos y frecuentes, tanto sobre los riesgos significativos como sobre el desempeño de la gestión del riesgo, contribuyen sustancialmente a un gobierno eficaz dentro de una organización.

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

La gestión del riesgo se considera central en los procesos de gestión de la organización, de manera que los riesgos se consideran en términos del efecto de la incertidumbre sobre los objetivos. La estructura y el proceso de gobierno se basan en la gestión del riesgo. Una gestión del riesgo eficaz se considera esencial por la dirección para la consecución de los objetivos de la organización.

Los indicadores tangibles son, por ejemplo, el lenguaje de la dirección, así como los materiales escritos de la organización importantes que utilizan el término "incertidumbre" en relación con los riesgos. Este atributo también se refleja normalmente en las declaraciones de la política de la organización, en particular las relativas a la gestión del riesgo. Normalmente, este atributo se podría verificar a través de las entrevistas con la dirección y a través de la evidencia de sus acciones y declaraciones.

Este documento forma parte de la biblioteca de UNIVERSIDAD POLITECNICA VALENCIA-HEMEROTECA

BIBLIOGRAFÍA

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

[2] ISO/IEC 31010, *Risk management. Risk assessment techniques.*

Este documento forma parte de la biblioteca de UNIVERSIDAD POLITECNICA VALENCIA-HEMEROTECA

Este documento forma parte de la biblioteca de UNIVERSIDAD POLITECNICA VALENCIA-HEMEROTECA

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

Este documento forma parte de la biblioteca de UNIVERSIDAD POLITECNICA VALENCIA-HEMEROTECA