Guía para la aplicación de UNE-ISO 31000:2018

Ángel Escorial Bonet
Jorge Escalera Alcázar
Sergio Simón Quintana
Julián Cid Méndez

AENOR | ediciones

Guía para la aplicación de UNE-ISO 31000:2018

Guía para la aplicación de UNE-ISO 31000:2018

Ángel Escorial Bonet
Jorge Escalera Alcázar
Sergio Simón Quintana
Julián Cid Méndez

AENOR | ediciones

Título: *Guía para la aplicación de UNE-ISO 31000:2018*
Autores: Ángel Escorial Bonet, Jorge Escalera Alcázar, Sergio Simón Quintana y Julián Cid Méndez

ISBN: 978-84-8143-970-0
Depósito Legal: M-23468-2019
Impreso en España – *Printed in Spain*

Edita: AENOR Internacional, S.A.U.
Maqueta y diseño de cubierta: AENOR Internacional, S.A.U.
Imprime: StockCERO

Nota: AENOR Internacional, S.A.U. no se hace responsable de las opiniones expresadas por los autores en esta obra.

AENOR

Génova, 6. 28004 Madrid
Tel.: 914 326 036 • normas@aenor.com • www.aenor.com

Índice

Presentación

Sobre la norma ISO 31000 y sus antecedentes

La gestión del riesgo es una actividad crítica para que las organizaciones puedan alcanzar sus objetivos y viene efectuándose desde hace varias décadas desde distintas áreas (seguridad e higiene, medio ambiente, auditoría interna, tecnologías de la información, seguros…).

Diversos modelos de gestión del riesgo sectoriales, como Solvencia en las compañías de seguros, Basilea para la banca o COSO en el campo empresarial, han tenido sucesivas versiones desde la segunda mitad del siglo XX. Pero la normalización internacional de esta área de la gestión no ha iniciado su desarrollo hasta el siglo XXI.

El primer paso dado en este sentido por la Organización Internacional de Normalización (ISO, International Organization for Standardization) en colaboración con la Comisión Electrotécnica Internacional (IEC, International Electrotechnical Commission), fue consensuar entre todos los expertos una terminología común para la buena comprensión de los conceptos relacionados con el riesgo. Para ello, ISO publicó una guía terminológica (ISO Guía 73:2002).

Asimismo, la publicación de la norma australiano-neozelandesa AZ-NZS 4360:2004 fue un aliciente para que ISO crease un comité técnico en cuyo seno se consensuó la primera norma internacional de gestión del riesgo aplicable a cualquier tipo de organización (pública o privada) y de cualquier tamaño: la Norma ISO 31000:2009. A esto se sumó la publicación de una nueva versión de la ISO Guía 73 con una terminología mucho más amplia que la anterior, y de la norma ISO/IEC 31010:2009 *Gestión del riesgo. Técnicas de apreciación del riesgo*.

Posteriormente, el comité técnico de ISO siguió trabajando en la normalización del riesgo al desarrollar una guía de implementación de la Norma ISO 31000, que dio lugar a la Norma ISO 31004.

Todas estas normas han sido adoptadas y publicadas por la Asociación Española de Normalización, UNE, desde donde los expertos nacionales del comité técnico CTN 307 *Gestión de riesgos* han participado activamente en los trabajos del comité internacional de ISO.

Tras la publicación en 2012 del Anexo SL del suplemento de ISO consolidado de las Directivas ISO/IEC, Parte 1, donde se desarrolló la Estructura de Alto Nivel o HLS (siglas en inglés de *High Level Structure*), y en el cual se establece como obligatorio para la elaboración de normas que se definan requisitos de sistemas de gestión independientemente de su ámbito de aplicación, la Norma ISO 31000 cobra una especial relevancia, ya que todas las normas ISO que definan sistemas de gestión tienen que incluir la consideración del riesgo.

Finalmente, en 2014 ISO decidió revisar la Norma ISO 31000, tarea que culminó con su publicación en 2018, consensuada por expertos de más de 70 países, en el seno del comité técnico internacional de normalización ISO/TC 262 *Risk Management*. Actualmente esta norma es la referencia mundial sobre gestión del riesgo, con amplia aplicación para todas las partes interesadas, ya que sirve de base para la consideración del riesgo en más de 60 normas ISO de sistemas de gestión. Esta norma no supone un sistema de gestión: es una guía de directrices; no obstante, da soporte al tratamiento de la incertidumbre en los sistemas de gestión de la organización.

Su traducción al español, consensuada por representantes de los países de habla hispana, fue realizada en el seno del Comité Técnico ISO/TC 262 por el grupo de trabajo *Spanish Translations Task Force* (STTF), cuya secretaría técnica fue desempeñada por España a través de UNE y cuya presidencia fue desempeñada por México.

Las ventajas de contar con una traducción unificada al español de la versión de 2018 son innegables después de haber contado con distintas traducciones de la versión anterior en muchos de los países hispanohablantes.

La adopción a nivel nacional de la norma se ha realizado en UNE a través del comité técnico nacional CTN 307 *Gestión del riesgo*, dando lugar a la Norma UNE-ISO 31000:2018.

Los principales cambios en esta versión de la norma, aparte del cambio de su título son:

- Revisión de los principios de la gestión del riesgo, que son los criterios clave para su éxito.
- Se destaca el liderazgo de la alta dirección y la integración de la gestión del riesgo, comenzando con la gobernanza de la organización.
- Mayor énfasis en la naturaleza iterativa de la gestión del riesgo, señalando que las nuevas experiencias, el conocimiento y el análisis pueden llevar a una

revisión de los elementos del proceso, las acciones y los controles en cada etapa del proceso.

- Simplificación del contenido, centrándose en mantener un modelo de sistemas abiertos para adaptarse a múltiples necesidades y contextos.

Sobre este libro

Esta guía pretende facilitar la comprensión y aplicación de la norma, cuyo contenido se reproduce, a través de explicaciones y ejemplos, ya que al ser una guía de directrices aplicable a cualquier tipo de organización y de cualquier tamaño, puede ser en ocasiones demasiado genérica. Es por ello que nuestro principal objetivo ha sido aclarar al lector las definiciones, los principios, el marco de referencia y el proceso de gestión del riesgo tratados en ella.

Este libro no sustituye ni interpreta lo redactado en la norma, simplemente pretende servir de ayuda a quienes quieran abordar la gestión de riesgos. Por tanto, ante cualquier duda o discrepancia, debe prevalecer siempre lo establecido en la norma.

Esperamos que todo ello sea de utilidad al lector. Con ese fin la hemos redactado.

Introducción

0 Introducción

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

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

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

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

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

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

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

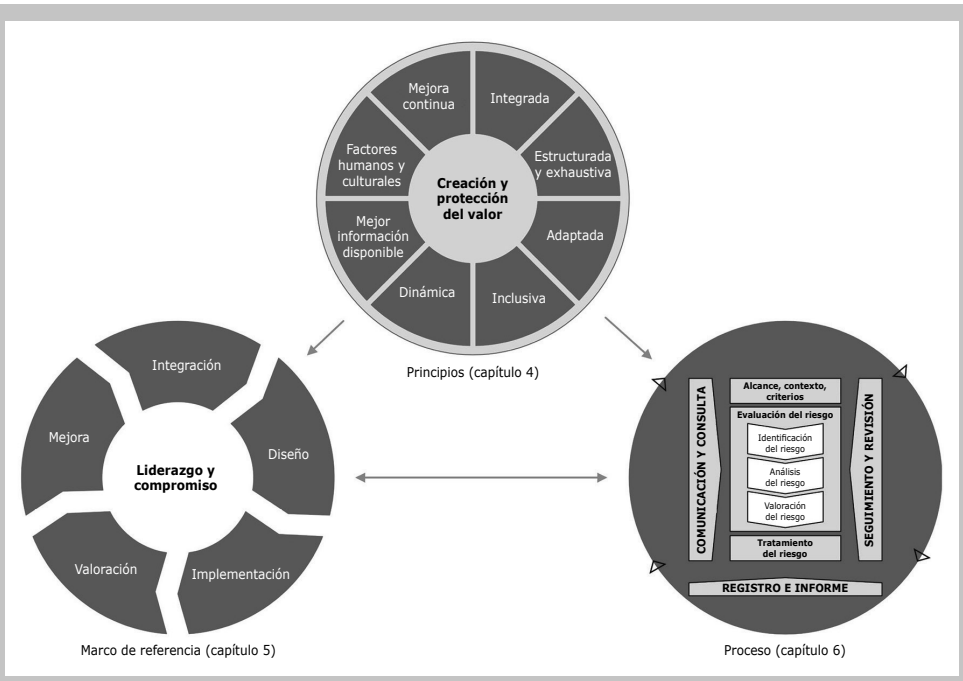

Figura 1 – Principios, marco de referencia y proceso

En este apartado se presenta la norma, poniendo en antecedentes al usuario del documento sobre las motivaciones que han llevado a revisarla, el objeto que persigue la gestión del riesgo y los factores que se consideran necesarios para alcanzar el éxito con su implantación en las organizaciones.

Se inicia este apartado con una novedad fundamental respecto de la versión de 2010, al dirigirla a las personas que crean y protegen el valor en las organizaciones. Esta modificación es fundamental, ya que el primer principio de la versión de 2010 se transforma en el propósito del estándar revisado en 2018: el propósito de la gestión del riesgo es la creación y protección del valor en la organización.

Por tanto, en 2018 se cambia una orientación a los procesos de la versión de 2010 a otra dirigida a las personas que crean y protegen el valor en las organizaciones.

La norma enumera las características de quienes crean y protegen el valor:

- Gestionando riesgos.
- Tomando decisiones.
- Estableciendo y logrando objetivos.
- Mejorando el desempeño.

El riesgo como efecto de la incertidumbre en los objetivos precisa de una adecuada gestión que permita el establecimiento y logro de esos objetivos gracias al apoyo en la toma de decisiones informadas y a la mejora del desempeño organizacional.

En la figura 0.1 se muestran estos conceptos (riesgo, incertidumbre, objetivos, toma de decisiones y desempeño) y uno adicional (asignación óptima de recursos), ya que la gestión del riesgo sirve para optimizar los recursos gracias a su aproximación iterativa. Esta filosofía de ISO 31000 permite a distintos públicos y usuarios abordar el riesgo y su gestión desde distintas perspectivas y con distintos alcances, como auditoría, seguros, cumplimiento, seguridad, etc.

Figura 0.1. **Filosofía de la gestión del riesgo**

A continuación, la norma repite un concepto ya existente en la versión de 2010 al indicar que las organizaciones de todos los tipos y tamaños se enfrentan a factores e influencias externos e internos que hacen incierto el logro de sus objetivos. Es decir, se mantiene el alcance de la norma para todo tipo y tamaño de organizaciones, y se introducen los contextos externo e interno, cuyos factores e influencias pueden provocar incertidumbre en el logro de los objetivos de la organización.

Otro concepto que se realza en esta nueva versión es el carácter iterativo de la gestión del riesgo y su idoneidad para asistir a las organizaciones a:

- Establecer su estrategia.
- Lograr sus objetivos.
- Tomar decisiones informadas.

Este carácter iterativo será visible en el desarrollo de esta norma a través de los antiguos tres pilares de la versión original (principios, marco de referencia y proceso), que en esta revisión se convierten en círculos (véase la figura 1 de la norma) que giran a modo de engranajes, activándose y retroalimentándose unos a otros gracias a ese carácter iterativo de la gestión del riesgo. El círculo de los principios gira alrededor del propósito de la gestión del riesgo: la creación y protección del valor. Este engranaje mueve los otros dos mediante las flechas que parten del mismo. El marco de referencia, que ya estaba representado en un ciclo de mejora continua de Deming, cambia "mandato y compromiso" por un nuevo eje (liderazgo y compromiso), alineándose así con las nuevas normas que dan lugar a sistemas de gestión. El marco de referencia, movido por los principios, alimenta y se retroalimenta del tercer engranaje, el proceso. En esta nueva visión circular, el presunto carácter lineal del proceso de gestión del riesgo visualiza mejor el carácter iterativo con su seguimiento y revisión aplicados a todas las etapas del proceso mediante unas flechas horarias en el exterior del círculo. Igualmente, este engranaje del proceso alimentado por los principios, se alimenta y retroalimenta el engranaje del marco de referencia mediante una flecha de doble sentido.

La gestión del riesgo es parte de la gobernanza y el liderazgo de las organizaciones (véase la figura 0.2). El cumplimiento legal y regulatorio marca un mínimo que las organizaciones tienen que acatar aunque, en ocasiones, si las sanciones no son lo suficientemente severas, hay organizaciones que pueden decidir no respetar ni tan siquiera ese mínimo de cumplimiento legal. La gestión del riesgo amplía la actitud reactiva del simple cumplimiento a la adopción de buenas prácticas no obligatorias para las organizaciones que les van a permitir manejar la incertidumbre en los objetivos; es decir, el riesgo. Pero la gobernanza en las organizaciones más proactivas va más allá de la propia organización, incluyendo en su día a día elementos como la responsabilidad social, la sostenibilidad y el liderazgo.

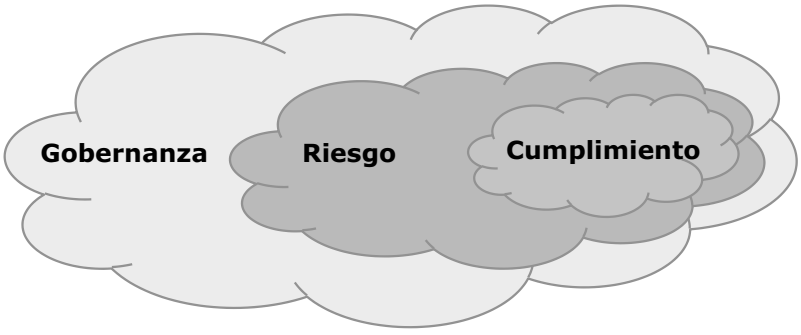

Figura 0.2. **Relación entre gobernanza, riesgo y cumplimiento**

La gestión del riesgo es fundamental en la forma de gestionar la organización en todos sus niveles y contribuye a la mejora de los sistemas de gestión. La estructura

de alto nivel ha establecido el pensamiento basado en el riesgo en los sistemas de gestión incluso en los sistemas integrados, y el pensamiento basado en el riesgo es esa base para todos los sistemas y los objetivos de la organización (véase la figura 0.3).

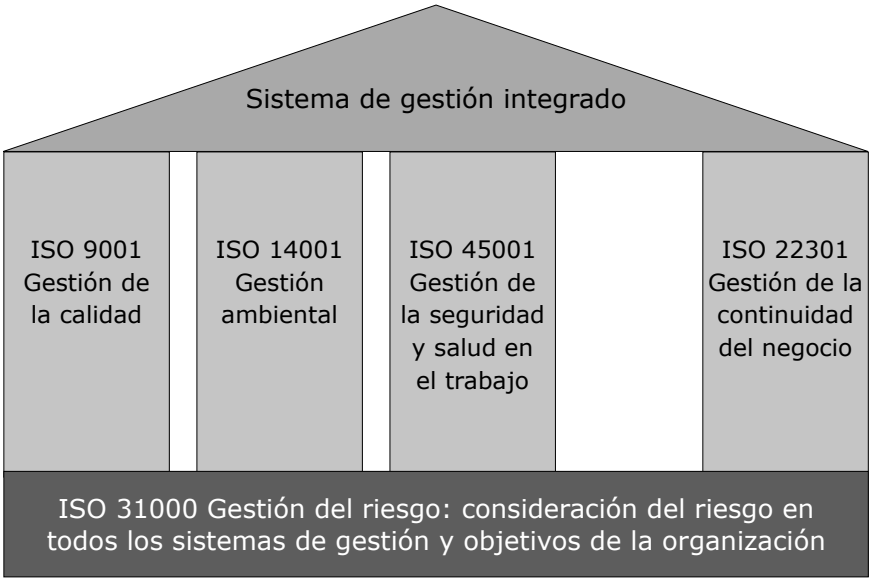

Figura 0.3. **Consideración del riesgo en los sistemas de gestión**

Para que la gestión del riesgo sea efectiva debe estar integrada en todas las actividades y ser parte de las mismas. Este puede parecer un objetivo utópico, pero es necesario que cualquier toma de decisiones que pueda afectar a los objetivos tenga integrada la gestión del riesgo en el ADN de la organización. La consideración de las partes interesadas es vital en la gestión del riesgo y el proceso de comunicación y consulta con las mismas es parte de esa integración.

Igualmente, la consideración de los contextos externo e interno es otra de las partes fundamentales de la gestión del riesgo a la hora de lograr esa perseguida integración completa del pensamiento basado en el riesgo en todas las facetas significativas de la organización. Dentro de estos contextos, el comportamiento humano y los factores culturales son elementos diferenciales que hacen a cada organización única en su gestión del riesgo, la cual debe adaptarse especialmente a estos elementos.

Finalmente, la revisión de la norma indica que, aun en el caso de que los tres componentes que venimos tratando (principios, marco de referencia y proceso) existan previamente en la organización, puede resultar necesaria su adaptación o mejora con el fin de lograr los objetivos de eficiencia, eficacia y coherencia en la gestión del riesgo.

Sobre los autores

Ángel Escorial Bonet es Licenciado en Ciencias Físicas por la Universidad Nacional de Educación a Distancia, máster en Ingeniería de Caminos por la Universidad Politécnica de Madrid, y postgraduado en Comercio Exterior por CEPADE-UPM y en Management & International Marketing por la St. Louis University.

Desde hace más de 30 años dirige proyectos de gestión del riesgo y continuidad del negocio para todo tipo de organizaciones en España y Latinoamérica. Actualmente es director general de Riskia, S.A. Además, entre otras actividades, es vocal del comité técnico nacional CTN 307 *Gestión de riesgos*, ha sido delegado español en el comité técnico ISO/TC 262 *Risk management* responsable de la elaboración de la Norma ISO 31000 y miembro del grupo de trabajo *Spanish Translation Task Force* (STTF) del comité técnico ISO/TC 262 *Gestión del riesgo*, responsable de la traducción de la norma al español. Es presidente de la Asociación de Profesionales de Lengua Española para la Gestión del Riesgo y la Incertidumbre (APEGRI) y vicepresidente del The Global Institute for Risk Management Standards (G31000).

Jorge Escalera Alcázar es Ingeniero Químico Administrador del Tecnológico de Monterrey, MBA por la EGADE Business School y Master Business Continuity Professional (MBCP) por DRI International.

Desde hace más de 24 años es consultor en gestión de resiliencia, gestión integral de riesgos y continuidad del negocio. Actualmente es director de Risk México. Además, entre otras actividades, es presidente del comité técnico mexicano CMISO/TC 262 *Gestión de riesgos*, y ha sido presidente del *Spanish Translation Task Force* (STTF) del comité técnico ISO/TC 262 *Gestión del riesgo*, responsable de la traducción de la norma ISO 31000 al español.

Sergio Simón Quintana es Licenciado en Ciencias Biológicas por la Universidad de Barcelona, postgraduado en Estadística Aplicada por la Universidad Politécnica de Catalunya y actualmente cursa el grado de Economía en la Universitat Oberta de Catalunya.

Consultor desde hace más 20 años en riesgos financieros de componente ambiental. Actualmente desarrolla su labor profesional en el campo de la didáctica del riesgo, la formación y la consultoría especializada en proyectos de cuantificación y monetización del impacto económico derivado del cambio climático.

Julián Cid Méndez es Licenciado en Ciencias de la Información, sección Periodismo por la Universidad San Pablo CEU y la Universidad Complutense de Madrid, máster en Dirección de empresas y recursos humanos por el Instituto de Empresa, y Certificado de Aptitud Pedagógica (CAP) por el Instituto de las Ciencias de la Educación de la Universidad Complutense de Madrid.

Ha desarrollado su carrera profesional en las áreas de comunicación (externa, interna y crisis), responsabilidad social corporativa, reputación corporativa y recursos humanos en empresas nacionales e internacionales, ocupando distintos cargos directivos. Actualmente, entre otras actividades, es mediador en Mapfre, colaborador en las consultoras JRH, y Riskia, en las revistas *Riesgo y empresa* y *Actualidad aseguradora* de la editorial Inese, y en Executive Interim Management.

La Norma UNE-ISO 31000:2018 proporciona directrices para gestionar el riesgo al que se enfrentan las organizaciones, y está dirigida a las personas que crean y protegen el valor en las mismas gestionando riesgos, tomando decisiones, estableciendo y logrando objetivos y mejorando el desempeño.

Esta guía pretende facilitar la comprensión y aplicación de la norma, cuyo contenido se reproduce, a través de explicaciones y ejemplos. Su principal objetivo es aclarar al lector las definiciones, los principios, el marco de referencia y el proceso de gestión del riesgo tratados en ella.

Sobre los autores

Ángel Escorial Bonet dirige proyectos de gestión del riesgo y continuidad del negocio desde hace más de 30 años. Además, ha sido delegado español en el comité técnico de ISO responsable de la elaboración de la Norma ISO 31000. Es presidente de APEGRI y vicepresidente de G31000.

Jorge Escalera Alcázar es, desde hace más de 24 años, consultor en gestión de resiliencia, gestión integral de riesgos y continuidad del negocio. Entre otras actividades ha desempeñado la presidencia del grupo de trabajo responsable de la traducción de la norma ISO 31000 al español.

Sergio Simón Quintana es consultor en riesgos financieros de componente ambiental, y actualmente desarrolla su labor profesional en el campo de la didáctica del riesgo, la formación y la consultoría.

Julián Cid Méndez ha desarrollado su carrera profesional en las áreas de comunicación, responsabilidad social corporativa, reputación corporativa y recursos humanos. En la actualidad es mediador y colaborador en consultoras y revistas.

GUÍA

ISBN: 978-84-8143-970-0

AENOR

www.aenor.com