CUADERNOS DE LA CÁTEDRA

Guía para implantar la gestión del riesgo en la empresa paso a paso

Introducción a la gestión del riesgo

Ángel Santiago Fernández Castro (coord.)
Rubén Lado Sestayo
Fernando de Llano Paz

FUNDACIÓN INADE
UDC
CÁTEDRA
LA GESTIÓN DEL RIESGO Y EL SEGURO

EFI
EDITORIAL FUNDACIÓN INADE

A nuestras familias, por su apoyo.
Especialmente a María, Rubén, Valeria y Alicia,
por ayudarnos a imaginar el futuro.

Colección CUADERNOS DE LA CÁTEDRA
Título n.º 5: Guía para implantar la gestión del riesgo en la empresa paso a paso: introducción a la gestión del riesgo

1.ª edición: Santiago de Compostela, 2021

Calle de la Paz, 2, bajo
36202 Vigo (Pontevedra)
http://fundacioninade.org/ · fundacion@fundacioninade.org

Maestranza, 9
15001 A Coruña (A Coruña)
www.udc.gal

Diseño e impresión: Tórculo Comunicación Gráfica, S. A.
Impreso en España · *Printed in Spain*

Depósito legal: VG 12-2021
ISBN: 978-84-09-26841-2

ÍNDICE

Presentación 11

Prólogo 13

Preámbulo 15

Introducción 17

I Definiciones y principios 21

1 Presentación 23

2 Definiciones 23

3 Principios 26

II Marco de referencia 31

1 Presentación 33

2 Liderazgo y compromiso 34

3 Integración 34

4 Diseño 35

4.1 Comprender la organización y el contexto 35

4.2 Articular el compromiso con la gestión del riesgo 40

4.3 Asignar roles, autoridades, responsabilidades y obligación de rendir cuentas en la organización 41

4.4 Asignar recursos 44

4.5 Establecer la comunicación y la consulta 44

5 Implementación 45

6 Valoración 45

7 Mejora 46

8 Modelos y plantillas 46

III Proceso 49

1 Presentación 51

2 Comunicación y consulta 52

3 Alcance, contexto y criterios 53

3.1 Alcance 53

3.2 Contexto 58

3.3 Criterios 59

IV Evaluación 61

1 Presentación 63

2 Técnicas y Metodologías 63

3 El mapa de riesgos 74

4 Tratamiento 76

4.1 Presentación 76

4.2 Plan de tratamiento de riesgos 78

5 Seguimiento y revisión 80

6 Registro e informe 82

7 Modelos y plantillas 88

Bibliografía 91

PRESENTACIÓN

En una cátedra institucional que se designa a sí misma como cátedra sobre «la gestión del riesgo y el seguro», resultaba un poco extraño que todavía no hubiésemos publicado un libro específicamente sobre gestión de riesgos. Desde luego, después de cuatro «cuadernos de la cátedra» acerca de diversos temas de Derecho de los seguros y de la responsabilidad civil, creo que ya iba siendo hora de incorporar a nuestro catálogo un libro como el que tienen entre manos.

Por lo tanto, no fue nada difícil la decisión acerca del tema de este quinto libro de nuestra pequeña colección de obras (los referidos «cuadernos de la cátedra»)[1]. Después de cinco años de eventos, cursos y actividades destinados a divulgar y fomentar la cultura de la gerencia de los riesgos en las empresas gallegas, publicar un pequeño manual destinado a explicar, con sencillez pero con seriedad, cómo se lleva a cabo esa faceta de la administración empresarial que llamamos gestión de riesgos parecía una idea estupenda.

El siguiente problema era a quién convenía encargarle la labor de diseño y redacción del manual. Sin embargo, tampoco esta tarea de búsqueda de los autores nos resultó complicada. Fue una feliz coincidencia que, justo cuando tuvimos la idea de publicar el libro, se incorporó a la Comisión de Seguimiento de la Cátedra INADE-UDC el Prof. Ángel Fernández Castro, del departamento de Economía Financiera y Contabilidad de la Universidade da Coruña. Dado que una de las líneas de investigación de su grupo de colaboradores es, precisamente, la gestión del riesgo, lo cierto es que no tuve más que proponerle el trabajo para que, amablemente, accediese a dirigir y coordinar el libro que estoy presentando. Desde aquí quiero agradecer especialmente al Profesor Fernández Castro y a los Profesores Fernando de Llano y Rubén Lado por haberse prestado a llevar a cabo el proyecto.

---

[1] Todos los Cuadernos de la Cátedra están gratuitamente a disposición de cualquier interesado en formato digital en nuestra página web (www.catedrafundacioninade.org), junto con muchos otros materiales sobre gestión de riesgos y seguros.

La finalidad fundamental de nuestra «Guía para implantar la gestión del riesgo en la empresa paso a paso» era la de proporcionar un pequeño marco de referencia a todas aquellas personas que participan en las actividades de la cátedra o de la Fundación, y que están oyendo hablar constantemente de la importancia de gestionar bien los riesgos. ¿Qué significa, desde el punto de vista del empresario, gestionar bien el riesgo? La respuesta ahora resulta más fácil: consiste en concretar dentro de una organización empresarial cualquiera el proceso que, en abstracto, describe el libro. Nuestra guía pretende ser, por lo tanto, una explicación sintética —paso a paso como indica el título—, de ese aspecto de la gestión interna de la empresa que se denomina gestión del riesgo. A partir de las ideas y principios de la guía podría construirse un sistema de gestión del riesgo en cualquier empresa.

Alguien estará pensando, con razón, que concretar las ideas y principios del libro adaptándolas a la idiosincrasia de una empresa no es fácil. Las diferencias de tamaño, fines, medios y posición en el mercado que existen entre las empresas son tremendas. Obviamente, una guía de apenas cien páginas es imposible que de cuenta de semejante variabilidad. Tampoco era ese el objetivo. Creo poder hablar también por los autores si digo que nos sentiremos más que satisfechos si el libro es capaz de despertar el interés o la reflexión de algunos de nuestros lectores empresarios, y hacerles ver que introducir aspectos de la gestión del riesgo en su empresa podría ser un buen proyecto de futuro. Ojalá que así sea.

No quiero terminar este prólogo sin agradecer, una vez más, a la Fundación INADE su constante aliento, así como todo el trabajo que las personas que la forman han dedicado siempre a este proyecto. Sobre todo, después de un año tan complicado como el que llevamos a nuestras espaldas. También quiero darle las gracias, de nuevo, al IGAPE y a la Consellería de Economía, Emprego e Industrial de la Xunta de Galicia por volver a colaborar en la publicación de este tomo, el quinto ya, de nuestros cuadernos.

A Coruña, 7 de diciembre de 2020

Fernando PEÑA LÓPEZ

Director de la Cátedra Fundación Inade - UDC

PRÓLOGO

En el momento actual, tanto en el entorno académico como en el ámbito de cualquier gran organización empresarial, afirmar que es importante que las empresas tengan una política interna de gestión de riesgos resulta superfluo. La gestión del riesgo, hoy en día, forma parte de los programas de formación en administración de empresas. Así mismo, no hay ninguna entidad empresarial de un cierto tamaño o relevancia que no tenga un departamento o un grupo de personas dedicadas a esta tarea.

La configuración de nuestro tejido productivo –con una presencia destacada de pequeñas y medianas empresas– hace necesario reforzar las políticas de apoyo a la gestión del riesgo, y muy especialmente ante el contexto actual marcado por una elevada incertidumbre ante los efectos de la pandemia sanitaria. Por ello, la Xunta de Galicia tiene el firme compromiso de seguir ofreciendo su cooperación al sector empresarial gallego para que aspire a ganar posiciones en este ámbito. Para ello, una de las condiciones que debe cumplir es hacer de la gestión de riesgos uno de los aspectos básicos de la gerencia empresarial.

La apuesta decidida por la divulgación de la idea de la gestión de riesgos y su trascendencia, así como por la formación de personas capaces de ayudar a nuestras empresas a dar el salto cualitativo que necesitan, es lo que terminará por conducirnos en la dirección que deseamos.

Este libro es una buena oportunidad para emprender este camino. Con esta obra se trata de ofrecer a todos los empresarios, de forma didáctica, una formación inicial en materia de gerencia de riesgos. Su pretensión es la de despertar el interés del emprendedor en el mundo de la identificación, evaluación y administración de los riesgos que afectan a las organizaciones.

La experiencia demuestra que, a veces, basta con un pequeño impulso inicial, como el que puede proporcionar un pequeño manual como este, para que se produzca un cambio sustancial en la empresa. Desde aquí, me gustaría animar a todos los empresarios a introducir la gestión de riesgos en su día a día. Cada uno encontrará un camino distinto, tan diverso como diferentes son unas empresas de otras.

No quiero terminar este prólogo sin referirme brevemente a la actividad de la entidad que está detrás de la Cátedra institucional que patrocina el libro. La Fundación INADE ha dedicado una gran parte de su actividad en los últimos años al fomento de la cultura de la gestión del riesgo en el tejido productivo gallego.

Desde el año 2016, la bandera de la gestión del riesgo se convirtió en el santo y seña de la Fundación, que está desarrollando una labor constante de concienciación de las empresas, de las administraciones públicas y del propio sector asegurador gallego acerca de la necesidad de que Galicia cuente con entidades empresariales que gestionen bien sus riesgos. Una tarea en la que, además, siempre ha sabido acompañarse de los principales focos de creación de conocimiento de nuestra comunidad autónoma: las universidades públicas del Sistema Universitario de Galicia (SUG). La aparición de este nuevo producto del trabajo de la fundación en cooperación con la Universidade da Coruña es la mejor prueba de que su proyecto está vivo y en marcha. Creo que es una buena noticia para Galicia.

Francisco CONDE LÓPEZ
Vicepresidente segundo y conselleiro de
Economía, Empresa e Innovación de la Xunta de Galicia

PREÁMBULO

La Real Academia Española de la Lengua, asigna los siguientes significados al término «riesgo»:

> *Del ant. riesco 'risco', por el peligro que suponen.*
> 1. m. Contingencia o proximidad de un daño.
> 2. m. Cada una de las contingencias que pueden ser objeto de un contrato de seguro.

La primera acepción de «riesgo» nos invita a reflexionar acerca de la importancia y proximidad del daño. A este respecto, resulta particularmente ilustrativo un reciente estudio sobre la mortalidad empresarial en Galicia entre 1972 y 2008, financiado por la Fundación INADE,[2] que concluye que el aseguramiento insuficiente afectó en ese período a una de cada ocho de las empresas analizadas. Si esto representa ya una cifra importante de por sí, cobra mayor relevancia aun cuando se complementa con el hallazgo de que estas empresas representaban más del 25% del empleo total perdido. Por sí solo, este dato justificaría la necesidad de poner el foco sobre la importancia de la gestión del riesgo en nuestro entorno.

Además, en el año 2020 es inevitable al hablar del riesgo (en realidad, al hablar de casi cualquier asunto), hacer referencia a la actual pandemia del COVID-19. Con motivo de ésta, «el consumidor adopta una posición de miedo, está tomando una mayor conciencia del riesgo, buscando las personas protección con el seguro».[3] Esta conexión entre el problema (el riesgo) y la posible respuesta (el seguro) es tan poderosa que incluso en la segunda acepción del

---

[2] MORTALIDAD EMPRESARIAL EN GALICIA 1972-2008. FACTORES DE IMPACTO Y GESTIÓN DEL RIESGO. 1.ª edición: Santiago de Compostela, 2020. Editorial Fundación INADE. Xoán Carmona Badía y Adrián Dios Vicente.

[3] Community of Insurance. (2020). INFORME Covid-19: Impacto y perspectivas para la industria aseguradora. Recuperado de: https://communityofinsurance.es/2020/04/19/covid-19-impacto-y-perspectivas-para-el-seguro/

término riego del diccionario de la RAE se identifica como tal aquella contingencia que puede ser objeto de aseguramiento.

Aunque la etimología de la palabra riesgo, la referencia a los riscos, resulte llamativa, tanto por lo específico del tipo de peligro concernido como por su potencial evocador (dejaremos a los especialistas la evaluación del atractivo comercial de la imagen del despeñamiento), es evidente que el término riesgo hace referencia a un conjunto de situaciones muy amplio y en constante evolución. Así, el Consejo General de Colegios de Mediadores de Seguros de España incluye entre las líneas de mayor crecimiento esperado en la era post-COVID algunas tan poco tradicionales como los ciberseguros o los seguros de altos cargos, así como otras, tales como los seguros de viajes o de cancelación de eventos, que venían teniendo una importancia marginal.

Conectando la cuestión de la deficiente gestión del riesgo en nuestro entorno empresarial con la del aseguramiento, cabe mencionar que a lo largo del período que cubre el citado estudio del fracaso empresarial se produjo la convergencia de la penetración del seguro (de no vida) en España con otros países de su entorno, ya que en 2008 se situaba en cifras cercanas a la media de la Europa-15 (en torno al 3% del PIB), cuando tres décadas antes este grupo de países doblaba la ratio española. No obstante, dando por supuesta la importancia nuclear del aseguramiento dentro de los tratamientos del riesgo, lo que la presente guía pretende enfatizar es que la gestión de riesgos es un complejo proceso que trasciende la mera contratación de seguros. La gestión de riesgos se presenta como un proceso iterativo y dinámico, integrado en las actividades y operaciones del negocio, y, por ende, condicionado por los factores humanos y culturales de la empresa. Este dinamismo cobra una importancia crucial en un momento en que la pandemia ha acelerado el ritmo de implantación de muchas tendencias sociales (teletrabajo, reuniones virtuales, compras en línea) que se habían iniciado previamente.

En el contexto actual, todas las iniciativas que contribuyan a la mejora de la gestión de riesgos resultan particularmente oportunas. Los autores de la guía han realizado un encomiable esfuerzo para intentar compaginar el rigor académico que los caracteriza con la claridad y brevedad que, confiamos, harán de ella un instrumento útil para el empresariado gallego.

Ángel S. FERNÁNDEZ CASTRO
Coordinador de la Guía

INTRODUCCIÓN

Un reciente estudio sobre la mortalidad empresarial en Galicia entre 1972 y 2008 concluye que el aseguramiento insuficiente afectó en ese período a una de cada ocho de las empresas analizadas, que en términos de empleo representaban más del 25% del total (Carmona-Badía y Dios-Vicente, 2020). Asimismo, el impacto de la pandemia por Covid-19 ha incrementado la búsqueda de una mayor seguridad por parte de usuarios, clientes y proveedores, que tratan a través de diversas alternativas de minimizar el impacto de los riesgos a los que están expuestos (Community of Insurance, 2020). Esta realidad apunta a la importancia de la gestión de riesgos como una de las actividades que puede generar valor para la empresa, tanto a través de la mejora de su imagen como de la reducción del impacto de determinados eventos. Esta relación entre gestión de riesgos y rentabilidad se ha demostrado en Otero et al. (2015), encontrándose una rentabilidad superior y más estable en las empresas que disponen de una política de gestión de riesgos, así como una relación positiva entre gestión del riesgo y rentabilidad cuando se desarrollan y se utilizan herramientas de gestión activa del riesgo.

A pesar de la importancia de la gestión del riesgo para la creación de valor, una parte muy importante del tejido empresarial está compuesto de micro, pequeñas y medianas empresas, las cuales no disponen en muchas ocasiones de un sistema de gestión normalizado. En este contexto, cabe señalar que, sin requerir grandes inversiones, esfuerzos ni modificaciones muy profundas en los procesos actuales, estas organizaciones pueden beneficiarse de una gestión del riesgo, y para ello tienen a su disposición diversas alternativas que pueden integrar como una parte más de su día a día. Entre los distintos marcos para una efectiva gestión del riesgo nos encontramos como principales exponentes con el "Committee of Sponsoring Organizations of the Treadway Commission" (COSO III) (www.coso.org), organización que está compuesta de cinco entidades estadounidenses y que se centra su marco de actuación a través de un modelo de control interno, con la «Federation of European Risk Management Associations" FERMA (www.ferma.eu), federación europea que engloba a entidades de gestión del riesgo de 21 países y con la ISO 31000:2018, que ha sustituido otros marcos (como por ejemplo el AS/NZ 4360). De estos marcos, en el presente documento se presenta una visión general de la ISO 31000:2018 debido a su flexibilidad y capacidad de adaptarse a diferentes tipos de organizaciones, particularmente a las micro, pequeñas y medianas empresas.

La ISO 31000:2018 proporciona **directrices** para gestionar el riesgo al que se enfrentan las organizaciones, que pueden ser aplicadas en cualquier entidad y permiten por tanto su adaptación a todo tipo de organizaciones, independientemente de su tamaño, su actividad o su ámbito de actuación. Por tanto, el documento proporciona un enfoque común para gestionar cualquier tipo de riesgo y no es específico de una industria o un sector.

Asimismo, se trata de una norma guía, que presenta directrices y no requisitos, por lo que no es certificable. Las directrices que emanan de la misma están encaminadas a la gestión del riesgo, justificando su finalidad por su contribución a la generación de valor. Por tanto, constituyen el punto de partida para que la organización desarrolle su propio sistema de gestión de riesgos y el objetivo perseguido, que es la creación y protección de valor. Es especialmente destacable que la norma permite su integración en los distintos sistemas de gestión de la empresa, por lo que es altamente adaptable y no requiere en la mayoría de las ocasiones de grandes modificaciones en los procesos que lleva a cabo la organización.

El foco de actuación se centra en la importancia de las personas que participan en los distintos procesos, frente a la orientación de la versión anterior centrada en los procesos. Esta modificación de la orientación tiene consecuencias importantes sobre el papel de la alta dirección y, particularmente, sobre la importancia de **comunicar** la importancia de la gestión del riesgo y de incorporar el conocimiento de las distintas partes interesadas. Junto con la ISO 31000:2018, la familia ISO 31000 incluye la ISO31010 y la guía ISO 73/2009. La ISO 31010 ofrece orientaciones para poder seleccionar y aplicar distintas técnicas de evaluación de riesgos. La guía ISO 73/2009 ofrece un compendio del vocabulario relacionado con la gestión de riesgo. Respecto a las definiciones de términos y conceptos clave debe atenderse a la ISO 31073 del comité técnico ISO/TC 262, que se encuentra en desarrollo. Finalmente, la ISO 21500 se centra en servir de guía para incorporar los postulados de la ISO 31000 en la gestión de proyectos. Esta información adicional, si bien no es necesaria para conocer la ISO 31000:2018, sí es importante como documentación de apoyo.

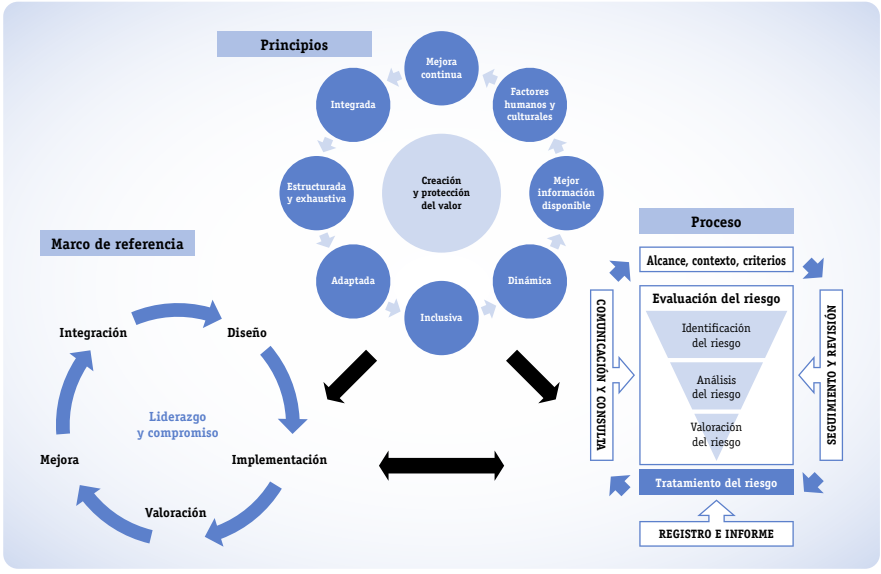
La gestión del riesgo se considera parte de la gobernanza y el liderazgo (a diferencia de otros sistemas como el sistema de gestión medioambiental o de salud laboral). Para su correcta implementación debe incorporarse en todas las actividades y a todos los niveles como un elemento adicional, complementario a los procesos y actividades.

Su objetivo es **mejorar los sistemas de gestión a través de la gestión de la incertidumbre (riesgo)**.

Esta gestión es relevante debido a que las organizaciones realizan su actividad en un marco que se ve afectado por factores externos e internos que provocan incertidumbre sobre la consecución de los objetivos propuestos. La organización debe crear valor y protegerlo y por ello la gestión del riesgo protege el sistema de generación de valor a través de la minimización de los riesgos en sus procesos. Este proceso es iterativo, de modo que la nueva información disponible para la organización, que puede tener un origen interno o externo a la organización a través de la participación de los grupos de interés, es incorporada en el proceso una vez finalizado. Esta repetición iterativa permite así establecer un ciclo de mejora continua y que el sistema se encuentre en permanente actualización.

La gestión del riesgo de acuerdo con las directrices establecidas en la norma ISO parte de nueve principios, que determinan el marco de referencia y los procesos que deben llevarse a cabo (ver figura). Los capítulos posteriores desarrollan estos tres elementos, desde la perspectiva de facilitar su compresión para un público no experto.

FIGURA 1. PRINCIPIOS, MARCO DE REFERENCIA Y PROCESO DE LA ISO 31000:2018



Fuente: Elaboración propia a partir de UNE ISO 31000 (2018)

I

Definiciones y principios

1 PRESENTACIÓN

La norma ISO 31000:2018 incorpora un total de ocho definiciones y nueve principios. Conocer las definiciones es necesario para comprender el vocabulario utilizado a lo largo del documento, así como las indicaciones establecidas en la norma y en la información adicional utilizada. Ello permite manejar un lenguaje común e identificar correctamente el aspecto señalado. De este modo, cuando se refieran términos como «riesgo», se utilizará una definición única y compartida. En relación con los principios, estos nos permiten establecer características básicas de un sistema de gestión de riesgos, al sintetizar los aspectos básicos y fundamentales sobre los que debe ser diseñado, implementado, desplegado y mejorado dicho sistema.

2 DEFINICIONES

Entre las definiciones se encuentran:

Riesgo

La norma establece una definición de riesgo como los **efectos que provoca la incertidumbre sobre los objetivos**. Esta definición amplia implica que los riesgos pueden afectar a distintos niveles de la organización, puesto que la incertidumbre puede afectar desde los objetivos estratégicos de la alta dirección al resultado de los procesos más simples. Entre otros, este motivo justifica que la norma, de manera reiterada, se centre en la importancia de lo que podríamos denominar la «cultura del riesgo» y en la importancia de que la alta dirección se comprometa con la gestión del riesgo y la comunicación de los objetivos y beneficios de esta, dado que debe abarcar a toda la organización.

Esta concepción del riesgo **incluye tanto los aspectos positivos como negativos que pueden afectar a la organización**. Así, a modo de ejemplo de una fuente de riesgo pueden surgir tanto amenazas como peligros u oportunidades. La

identificación del riesgo, su valoración y su plan de tratamiento podrían condicionar que algunas amenazas se conviertan en oportunidades si se contrapone una determinada respuesta, mientras que en relación con los peligros podría mitigarse su impacto. De ahí la importancia de identificarlos correctamente. Para su identificación, la norma indica que la definición de los riesgos a los que se enfrenta la empresa se expresa habitualmente atendiendo a cuatro dimensiones: la fuente originadora, los eventos que pueden surgir de las mismas (sean positivos o negativos), las consecuencias de los eventos (sean evitables o no) y las posibilidades o probabilidades de que ocurran los eventos anteriores.

TABLA 1. EJEMPLO DE TABLA DE DEFINICIÓN DE RIESGO

Nombre del riesgo	Fuente	Eventos que puede ocasionar	Consecuencias	Posibilidades de ocurrencia

Fuente: Elaboración propia

Gestión del riesgo

En la definición de la norma de la gestión del riesgo se destaca la necesidad de que las **actividades realizadas para dirigir y controlar la organización en relación con el riesgo estén coordinadas**, y por lo tanto no respondan a respuestas puntuales o aisladas. Ello se consigue gracias a la adaptación del sistema de gestión de riesgos a la organización y no al revés.

Parte interesada

Por parte interesada la norma entiende aquellas **personas u organizaciones internas o externas a las que afectan las decisiones de la organización. A este respecto cabe señalar que no es necesario que las decisiones tengan una consecuencia directa, puesto que es suficiente que se perciban como afectadas** para ser consideradas parte interesada. La importancia de su identificación a la hora de definir el contexto y el alcance será fundamental, puesto que en el proceso de comunicación y consulta presentarán un papel clave, tanto para ofrecer información que sirva de input o entrada para el sistema como para las decisiones de comunicación.

TABLA 2. EJEMPLO DE DEFINICIÓN DE PARTES INTERESADAS

Categoría	Parte interesada	Tipo	Motivo de su consideración	…
Cliente	Usuario	Externo		…
Cliente	Prescriptor	Externo		…
Sector Público	Gobierno local	Externo		…
Sector Público	Entidad de promoción local	Externo		…
…	…	…		…

Fuente: Elaboración propia

Fuente de riesgo

La norma entiende por fuente de riesgo **todo aquello que puede llegar a generar riesgo**. Esta definición amplia incluye todos los elementos, independientemente de que capacidad para generar riesgo esté limitada a la concurrencia de otros hechos.

Evento

Los eventos son **cambios de las circunstancias que pueden ocurrir de manera aislada o en más de una ocasión**. Este cambio puede generar riesgo, y por tanto constituir una fuente de riesgo, y puede tener varias causas y consecuencias. La definición no se limita a los hechos, puesto que también se incluyen los cambios de las circunstancias cuando se prevé una ocurrencia que finalmente no se produce y cuando se produce un cambio inesperado.

Consecuencia

Las consecuencias son el **resultado de un evento que afecta a los objetivos directa o indirectamente. Este resultado puede ser positivo o negativo** para la empresa y, en algunos casos, puede acumularse o puede desencadenar nuevas consecuencias. No necesariamente tiene que ser cierta ni poder definirse de manera cuantitativa.

Probabilidad

La definición de la norma de probabilidad es diferente de la acepción matemática. En este sentido, debe entenderse probabilidad en un sentido amplio,

como **posibilidad, sea o no cuantificable desde un punto de vista cuantitativo**. La probabilidad requiere esta posibilidad esté definida desde un punto de vista cualitativo o cuantitativo, que su determinación hubiese sido objetiva o subjetiva y debe estar descrita con la amplitud que resulte posible.

Control

De acuerdo con la norma, el control es la "medida que mantiene y/o modifica un riesgo" tenga o no el efecto esperado. Se incluyen **todas las actividades, elementos, condiciones, etc, que mantengan y/o modifiquen un riesgo**. Tras el control se mantiene el riesgo residual, como aquella parte del riesgo que permanece. Un ejemplo de control sería la instalación de un pararrayos, que reduce el riesgo de que un rayo afecte a una instalación sensible pero no se elimina por completo. Otro ejemplo sería la creación de un muro de contención o una presa para reducir el riesgo de inundación de un río, el cual mantiene el riesgo residual de que el agua supere dicho obstáculo o este se deteriore.

3 PRINCIPIOS

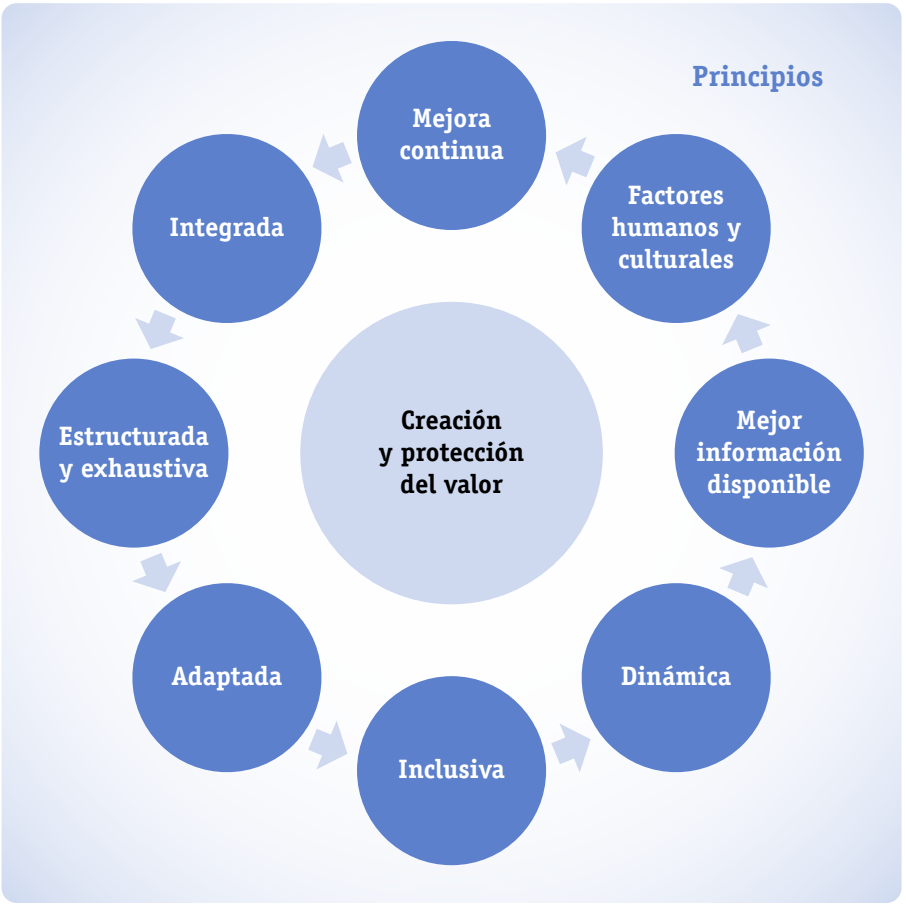
En cuanto a los principios, su **objetivo principal es que la gestión del riesgo no sea un fin en sí mismo, sino que contribuya a crear y proteger el proceso de generación de valor**. Sobre esta base, el resto de los principios buscan establecer el punto de partida de una gestión del riesgo **eficaz**, esto es, que se alcancen los resultados planificados a través de la realización de las actividades planificadas; **eficiente**, es decir, que se aprovechen los recursos disponibles; y **comunicada**, esto es, que se traslade su propósito y el valor que aporta a todos los grupos de interés. El mantenimiento de estos principios lleva implícita la importancia de incluir la gestión del riesgo en la dinámica de la empresa, así como la necesidad de comunicar su finalidad y efectos positivos.

A continuación se exponen los principios establecidos en la norma.

a) Integrada

La gestión del riesgo es parte integral de todas las actividades de la organización. Por tanto, esta actividad no debe realizarse de manera aislada, sino formar parte de todas las actividades como un elemento más de las mismas, considerando especialmente el factor humano. Por este motivo, **la dirección debe liderar la difusión de la importancia de la gestión del riesgo y de su implementación a**

FIGURA 2. PRINCIPIOS DE ACUERDO A LA ISO 31000:2018



Fuente: Elaboración propia a partir de UNE ISO 31000 (2018)

través de la cadena de mando a todos los niveles de la organización. La falta de integración de la gestión del riesgo en la organización dificulta la asunción de responsabilidad y puede reducir el compromiso de los recursos humanos.

b) Estructurada y exhaustiva

Un enfoque estructurado y exhaustivo hacia la gestión del riesgo contribuye a resultados coherentes y comparables. Es necesario planificar y realizar un control efectivo de la gestión del riesgo, adaptado a la organización. Así, para articular toda la información externa e interna de una manera **sistemática, útil y orientada al alcance previamente establecido**, la información debe estar

estructurada y ser exhaustiva, de modo que pueda ser utilizada en el proceso. Esta estructuración afecta desde la información que faciliten las partes interesadas, de distinto tipo y con diferente periodicidad (la cual debe garantizarse que, junto con el resto de información relevante esté accesible, estructurada y pueda ser utilizada por la persona responsable de tomar decisiones), hasta la información relativa a la implementación de las medidas y la elaboración de reportes que se ocasionen en las diferentes actividades de la empresa.

c) Adaptada

El marco de referencia y el proceso de la gestión del riesgo se adaptan y son proporcionales a los contextos externo e interno de la organización relacionados con sus objetivos. El sistema de gestión de riesgos no es común a todas las organizaciones, sino que se encuentra adaptado al entorno y a las características internas y externas de cada organización. De este modo, **cada organización define los riesgos que considera, así como qué cantidad de riesgo puede asumir respecto a sus objetivos**. Ello es debido a que cada organización cuenta con su propia cultura empresarial, y define sus criterios de riesgo y sus procesos. De esta forma una de las características fundamentales a adoptar por la organización es la de la flexibilidad y la capacidad de adaptación de la entidad en función de los distintos condicionantes a los que está sujeta: sector económico, tamaño, cultura, configuración y gestión organizacional, etc. Así mismo cada uno de los procesos o estructuras organizacionales debería de ser adaptado al tipo de riesgo que debe manejar. Entre ellos podría estar la gestión de riesgos relacionada con el impacto de las acciones de la competencia, con el diseño de tesorería, o con la cartera de inversiones, con la gestión de stocks, etc.

d) Inclusiva

La participación apropiada y oportuna de las partes interesadas permite que se consideren su conocimiento, puntos de vista y percepciones. Esto resulta en una mayor toma de conciencia y una gestión del riesgo informada. Todas las partes interesadas, tanto externas como internas, pueden afectar o ser afectadas por el proceso de toma de decisiones. A través de su integración en el sistema de gestión de riesgos se promueve que sus opiniones sean tenidas en cuenta, permitiendo mantener actualizada la información y promoviendo la **transversalidad del sistema, que debe implicar a todas las actividades de la organización. Por tanto, es especialmente relevante la incorporación de los responsables de tomar decisiones**. Esta inclusión debe afectar la propia consideración del entorno y la determinación de los propios criterios de riesgo. Esta participación permite que las partes puedan participar de forma acertada y constructiva, con talante

positivo a la hora de aportar elementos como el conocimiento, puntos de vista y percepciones. De esta forma se toma mayor conciencia de lo que significa pertenecer a la organización, y se establecen canales de comunicación para llevar a cabo una gestión positiva de la incertidumbre, favoreciendo no solo el conocimiento inicial sino también la retroalimentación de información.

e) Dinámica

Los riesgos pueden aparecer, cambiar o desaparecer con los cambios de los contextos externo e interno de la organización. La gestión del riesgo anticipa, detecta, reconoce y responde a esos cambios y eventos de una manera apropiada y oportuna. Así, **el proceso de gestión de riesgos no es lineal, sino iterativo, utilizando el conocimiento nuevo disponible para identificar los nuevos riesgos, los que desaparecen y los cambios y ajustes necesarios** a partir del análisis de la información disponible. Este principio parte del hecho de que todo cambio que modifique los planteamientos iniciales, tanto a nivel interno como externo, podría ser una fuente de incertidumbre que afecte a los objetivos. Por tanto, los riesgos derivados de los cambios identificados necesitan ser evaluados constantemente. A través de esta gestión continua del riesgo es posible detectar el cambio en sus etapas iniciales, para anticiparse en la respuesta y poder actuar con solvencia, minimizando el impacto negativo que el cambio detectado pueda significar. La supervisión y la revisión deben por tanto estar activas en todo momento para poder realizar una observación continua del proceso y de la estructura organizacional que permita detectar los cambios lo más rápido posible.

f) Mejor información disponible

Las entradas a la gestión del riesgo se basan en información histórica y actualizada, así como en expectativas futuras. La gestión del riesgo tiene en cuenta explícitamente cualquier limitación e incertidumbre asociada con tal información y expectativas. La información debería ser oportuna, clara y disponible para las partes interesadas pertinentes. Ello implica que **la información utilizada, sea histórica o basada en fuentes internas o externas, debe ser evaluada teniendo en cuenta sus características y sus limitaciones**, entre las que podrían encontrarse la existencia de sesgos. Los conocimientos, puntos de vista y percepciones de las distintas partes interesadas deben ser considerados por tanto con pleno conocimiento de lo que representan. Asimismo, esta información debe estar disponible y ser comprensible para las personas que toman las decisiones a todos los niveles afectados. Se pretende así que **en todo momento se disponga de la mejor información posible**. Gracias a una solvente propuesta informativa

es posible que la empresa genere expectativas futuras coherentes y ajustadas a su realidad. Por tanto, debe garantizarse la integridad y la fiabilidad de la información, considerando que la misma puede estar sujeta a sesgos, y establecer los mecanismos para su correcta actualización.

g) Factores humanos y culturales

El comportamiento humano y la cultura influyen considerablemente en todos los aspectos de la gestión del riesgo en todos los niveles y etapas. **Los comportamientos y los valores de las personas que forman parte de la organización son una parte importante a considerar en todo el sistema de gestión de riesgos**. Ello exige que la organización no sólo defina sus valores y su planteamiento de gestión del riesgo, sino que debe además tratar de que sus trabajadores y colaboradores los conozcan, los asimilen y los hagan suyos. En este sentido, la gestión del riesgo permite definir el perfil de los distintos agentes que tienen relación con la entidad y su capacidad para facilitar o dificultar la consecución de los objetivos de la organización. La organización debe ser consciente de que es necesario interpretar correctamente las opiniones que tienen los agentes internos y externos en relación con el tratamiento y la gestión del riesgo de la entidad. Conociendo e interpretando correctamente las opiniones de los agentes, y pasándolas por el tamiz de la influencia que en ellas pueda tener las propias características humanas y culturales, es posible evitar errores como una posible indiferencia a los puntos de vista de otras personas, la falta de detección del riesgo, la ausencia de respuesta ante una posible alerta o un posible sesgo a la hora de enfrentarse a temas complejos producido por el tratamiento y procesamiento de la información, entre otros.

h) Mejora continua

La gestión del riesgo mejora continuamente mediante el aprendizaje y la experiencia. Así, la incorporación de los resultados y la evaluación de los mismos debe permitir incorporar la información nueva disponible y que la organización preste atención a la posibilidad de incorporar mejoras en el sistema que aumenten su eficacia o su eficiencia. **Se trata, por tanto, de incorporar la evaluación y la mejora continua como una parte fundamental del proceso.**

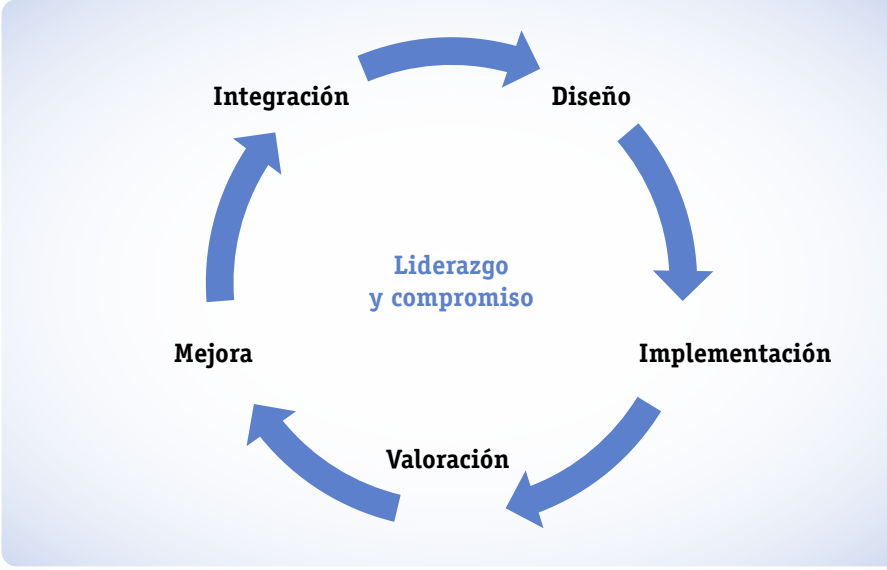
II

Marco de referencia

1 PRESENTACIÓN

El marco de referencia es el soporte del sistema, y tiene como objetivo la efectiva integración de la gestión del riesgo en todos los niveles y actividades significativas de la empresa. En particular, requiere **diseñar, implementar, valorar y mejorar el sistema de gestión del riesgo**, en línea con el proceso PDCA o PHVA (planificar, hacer, verificar y actuar), también conocido como ciclo de Deming (1989). Este proceso debe ser impulsado desde la gobernanza de la organización y como parte del proceso de toma de decisiones, por lo que debe estar alineado con los objetivos estratégicos de la organización. Además de la vinculación entre el proceso de gestión de riesgos y los objetivos estratégicos, la alta dirección y los órganos de supervisión deberán demostrar **liderazgo** y **compromiso** con la gestión del riesgo, debido a la importancia del factor humano, siendo este el pilar principal del sistema.

FIGURA 3. MARCO DE REFERENCIA



Fuente: Elaboración propia a partir de UNE ISO 31000 (2018)

2 LIDERAZGO Y COMPROMISO

El liderazgo y compromiso de la alta dirección requiere que:

- Se adapten los componentes del marco de trabajo a la organización en toda su amplitud, desde las actividades clave a las actividades que sirvan de soporte. Para ello deben considerarse las características estructurales y ponerse en práctica los principios de integración, adaptación y consideración de los factores humanos y culturales. Asimismo, la adaptación del marco de trabajo no solo debe ceñirse al diseño del sistema de gestión de riesgos, sino también a la propia implementación del mismo, a nivel de los distintos procesos.

- Se difunda adecuadamente el enfoque, plan o línea de acción a todos los niveles considerados, tanto interna como externamente, cuando corresponda. La comunicación de los objetivos es una función clave para lograr que la organización disponga de la información necesaria para alcanzar sus objetivos.

- Se demuestre el compromiso de la organización a través de la asignación de los recursos necesarios en los niveles y actividades que se requieran por parte de la alta dirección y los órganos de supervisión.

- Se asignen los roles adecuados a los diferentes niveles considerados, de modo que se establezca la autoridad, la responsabilidad y la obligación de rendir cuentas de modo que los órganos de supervisión dispongan no solo de recursos, sino de responsabilidad y autoridad.

Si bien la alta dirección es responsable de alinear el marco de referencia con los objetivos estratégicos y de las actividades de comunicación, los órganos de supervisión deben asegurar el flujo de información, así como comprender la adecuación de los riesgos identificados a las actividades realizadas y también deben velar porque la gestión del riesgo se ejecute de la manera apropiada y la comunicación sea adecuada al nivel correspondiente a su autoridad y responsabilidad. Para ello deberán rendir cuentas.

3 INTEGRACIÓN

La **integración** implica la correcta adecuación del sistema de gestión de riesgos a las diferentes particularidades de la organización y de las partes internas de

su estructura. Debido a que todos los recursos humanos deben gestionar el riesgo, el sistema debe considerar esta heterogeneidad interna. Ello exige que se asignen roles con autoridad y responsabilidades consecuentes, adaptados al contexto donde se desarrolle la actividad, teniendo en cuenta los recursos materiales y humanos. Así, la estructura de gestión, encargada de trasladar la finalidad de la gobernanza en estrategias y objetivos, puede integrar la gestión del riesgo como una parte intrínseca de sus actividades, logrando que desde la gobernanza a las operaciones de la organización se integre la cultura de gestión del riesgo y no se considere por tanto una actividad complementaria o separada del resto de actividades. Por tanto, cada organización debería definir cuáles son los riesgos que considera, que métodos aplicará para identificar y valorar los riesgos y cuales serán los criterios a seguir, siempre de acuerdo a sus particularidades. La norma no impone como debe realizarse la gestión del riesgo, pero sí destaca la importancia de que esta alcance a toda la organización y que sea adecuada al factor humano.

4 DISEÑO

El **diseño** implica, de acuerdo con la norma, un total de cinco ítems:

4.1 Comprender la organización y el contexto

Debido a la importancia de las partes interesadas y del contexto, la organización debe comprender sus redes y dependencias internas y externas, así como las percepciones, necesidades, expectativas de las partes interesadas. La ubicación de la organización respecto a las partes interesadas es un requisito previo y necesario para el proceso de comunicación y consulta. Asimismo, la organización debe establecer el entorno en términos de los factores que le afectan y que podrían agruparse en la metodología PESTEL, esto es, las variables del contexto Político, Económico, Socio-cultural, Tecnológico, Ecológico y Legal.

Es clave poder reconocer aquellos cambios que sucedan dentro del contexto, tanto externo como interno, y de ahí que sea importante su definición. Ello es debido a que en la medida en que las alteraciones sean detectadas se podrá establecer la revisión de los tratamientos del riesgo y su priorización.

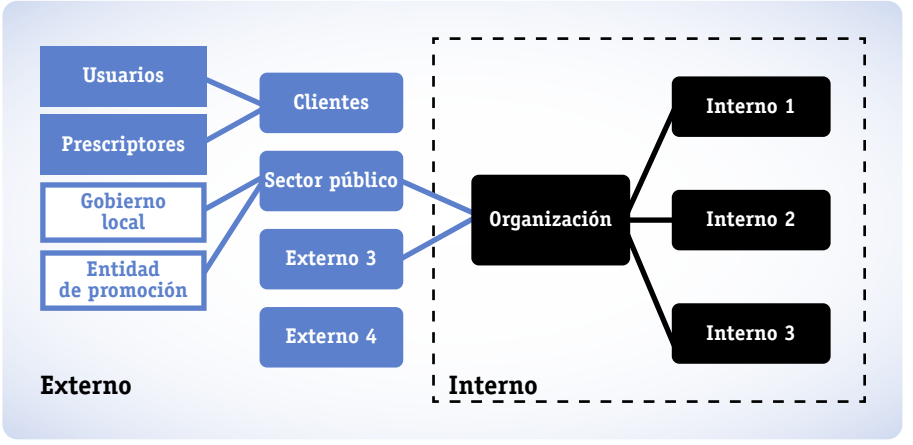
El contexto: las partes interesadas

En relación con la organización, existen partes interesadas tanto internas (propietarios, trabajadores,) como externas (clientes, proveedores, sector público, asociaciones, .). Estar partes interesadas tienen un papel relevante para el sistema de gestión de riesgos, puesto que pueden proveer información, pueden ser dueños de un riesgo, ser fuente de riesgo, etc. Por este motivo, previo al análisis de las mismas es preciso su identificación. En consecuencia, el primer paso es **identificar** las partes interesadas, esto es personas o entidades que pueden afectar a las decisiones u objetivos de la organización. La incorporación de las partes interesadas al sistema debe poner en práctica el principio relativo a que la gestión del riesgo sea inclusiva, para permitir y favorecer la participación constructiva y la toma de conciencia mediante la retroalimentación de información. Por este motivo, resultará importante su participación en el proceso de comunicación y consulta.

Una vez identificadas, es posible **clasificar** en distintos grupos a las distintas personas, agentes o entidades en función de su relación con el sistema de gestión de riesgos. Ello permitirá determinar su papel, los canales y acceso de información, así como su tratamiento.

Tras clasificar las partes interesadas es posible **evaluar** las partes interesadas en función de su influencia y de su interés, lo que permitirá establecer la relación que debe mantenerse con las mismas, tanto en términos de información a recopilar, periodicidad o comunicación de resultados.

FIGURA 4. EJEMPLO DE MAPA DE PARTES INTERESADAS



Fuente: elaboración propia

Para la elaboración del mapa de partes interesadas y su evaluación es posible utilizar el modelo disponible en el anexo de este capítulo.

El contexto: análisis pestel

Se trata de una herramienta propia del análisis estratégico empresarial que tiene en cuenta la dimensión externa de la organización, esto es, todos aquellos elementos externos que le afecten, pero sobre los que no tiene capacidad de modificación. Su función no es otra que el facilitar el análisis de las variables que afectan a la organización desde el punto de vista del entorno macroeconómico. Puede considerarse, en parte, un proceso iniciador del análisis de cuáles son las debilidades, las amenazas, las fortalezas y las oportunidades (DAFO) de la organización. Estamos, por tanto, ante el estudio pormenorizado del entorno de la organización. En síntesis, se trata de entender en qué contexto tiene que competir la empresa, qué variables externas le afectan a su actividad. Se trata, por tanto, de una herramienta que permite a la dirección ser consciente de «su realidad» en relación con el entorno en el que se mueve.

Las variables que se deben analizar, y que dan forma al nombre de este recurso son: contexto Político, Económico, Socio-cultural, Tecnológico, Ecológico y Legal. La organización debe estudiar las distintas variables y definir si afectan a la actividad (actual o futura) de forma positiva, negativa o neutra. Si lo hacen de forma positiva, estaríamos ante oportunidades, y si son negativas se tratarían de amenazas ante las que hay que cubrirse.

Ejemplo de las variables Políticas serían: situación actual de gobierno del territorio o región y las políticas aplicadas en vigor y futuras políticas (fiscales, de empleo o industriales, entre otras). En cuanto a las variables económicas podrían ser: situación macroeconómica de la economía mundial y de la región o territorio, política económica, oferta de tipos de interés nacional y/o supranacional o tasa de morosidad, etc. Las variables socio-culturales que hay que contemplar serían, entre otras: la pirámide de población del territorio, patrones de comportamiento cultural, afectación política, nivel de movilización de la población, movimientos migratorios o conciencia social ante temas que puedan afectar a la empresa. Desde el punto de vista de variables tecnológicas, se deberían analizar, entre otras: el nivel de inversión en estrategias de I+D+i del territorio, curvas de aprendizaje de las tecnologías empleadas, cambios en las formas de producción y distribución, etc. A nivel de variables ecológicas, se han de estudiar el impacto que sobre la empresa pueden tener: la concienciación de lucha contra el cambio climático, políticas ecológicas gubernamentales que afecten a la empresa, estructura del mercado energético del territorio,

conciencia social ante el cambio climático, etc. Por último, desde el punto de vista legal, se debe tener en cuenta: el cuerpo legal que rige la contratación de personal, la propiedad intelectual, la protección de la competencia y del consumidor, la salud laboral y la protección de riesgos para la salud, etc.

FIGURA 5. EJEMPLO DE VARIABLES DE ANÁLISIS PESTEL

Fuente: elaboración propia

Análisis interno

Desde el punto de vista interno es necesario que todo aquel agente que tiene relación directa o indirecta con la entidad conozca los conceptos de misión, visión y valores y de cómo la gestión del riesgo contribuye a la generación de valor. Servirán para motivar a las personas que forman parte de la organización y lograr así su bienestar, lo que redundará en la mejora de su productividad. Asimismo, pueden ayudar a la hora de conseguir la implicación de los inversores y financiadores en los nuevos proyectos, o para convencer al consumidor de las bondades de la gama de productos, entre otros.

La filosofía de una organización debe resumirse en tres conceptos ampliamente empleados como carta de presentación de la misma. A través de estos tres elementos se define su identidad corporativa y su forma de entender la realidad y lo que puede aportar a la sociedad y a la economía.

Por **misión** se entiende el para qué existe esa organización. Una correcta definición de la misión permite unificar la toma de decisiones en base a lo que

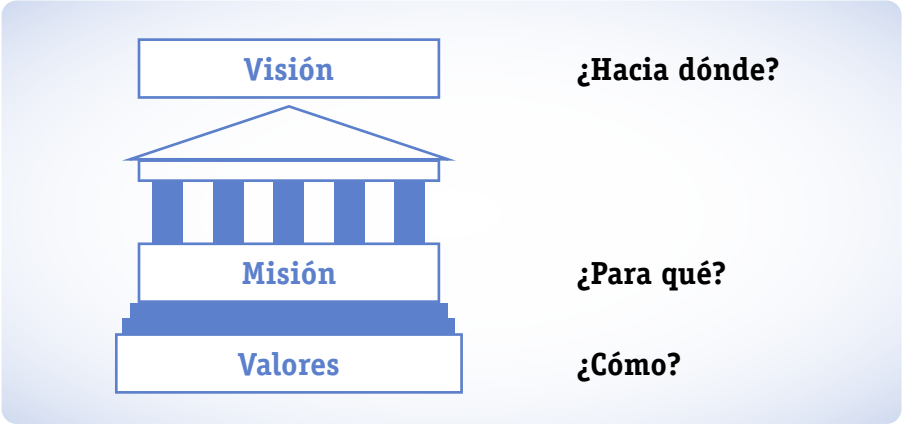
nos distingue, que tomará forma de cultura empresarial. Con la misión se debe poder responder a preguntas como: ¿a qué se dedica la organización?; ¿Qué es lo que identifica a la organización frente a los competidores?; ¿A quién está enfocada nuestra entidad como público objetivo?; ¿qué aportamos como organización?; ¿qué necesidades cubren nuestros productos?

La **visión** tiene relación con el «hacia dónde» va la empresa, qué tipo de objetivos y metas busca alcanzar con su actividad. A la hora de definir los objetivos hay que procurar que estos sean realistas y en línea con la evolución de la empresa. Éstos deben ser a corto, medio y a largo plazo. En la medida en que los objetivos se presentan como alcanzables y dentro de la línea que seguimos como entidad, servirán para motivar a todos los agentes de la organización para tratar de alcanzarlos. Se pueden distinguir cuatro tipos de categorías en relación con los objetivos:

- Estratégicos: Parten de la estrategia definida a seguir por la empresa.
- Operacionales: Busca la optimización en el uso de los recursos.
- Financieros: Pretenden respetar la imagen fiel de la gestión de los recursos económicos de la organización.
- De cumplimiento: En relación con la observancia del marco legal aplicable.

La definición de la visión parte del contexto actual y busca la activación de la organización para que esté preparada ante los retos que surjan, y pueda asumir los cambios internos necesarios para evolucionar como entidad «viva» que responde a los desafíos que se le presentan.

FIGURA 6. MISIÓN, VISIÓN Y VALORES



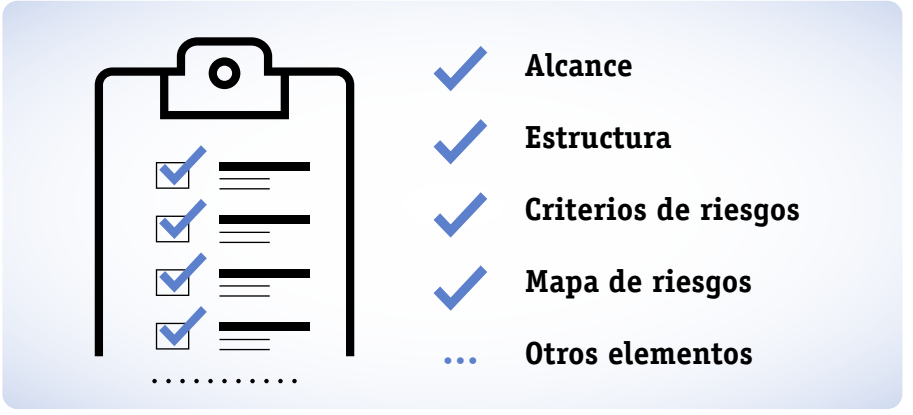
Fuente: elaboración propia

Los **valores** de la empresa son los pilares sobre los que se sustenta. Marcan su posición y la manera de relacionarse con el mundo. Su filosofía, las creencias que la mueven, los principios que busca cumplir, la cultura empresarial que está presente en la forma de organizar la entidad y de relacionarse con la sociedad. Los valores van a condicionar tanto la forma de relacionarse la entidad con sus agentes internos (trabajadores) como con los externos (proveedores, clientes, administraciones públicas o competidores, entre otros).

4.2 Articular el compromiso con la gestión del riesgo

El compromiso de la alta dirección y los órganos de supervisión debe ser explícito, a través de una comunicación clara de los objetivos y del compromiso con la gestión del riesgo a las partes interesadas. Esta explicitación del compromiso puede realizarse a través de una declaración o política. En el mismo documento debe constar la finalidad perseguida con la gestión del riesgo y la importancia de reforzar la cultura de gestión de riesgos en toda la organización. Asimismo, debe quedar clara la estructura en términos de autoridad y responsabilidad, los recursos disponibles, las prioridades y criterios para gestionar los conflictos que afecten a los objetivos, los resultados e informe de la gestión del riesgo y el proceso de revisión y mejora continua.

FIGURA 7. ASPECTOS QUE PODRÍAN INCLUIRSE EN UNA POLÍTICA DE GESTIÓN DE RIESGOS

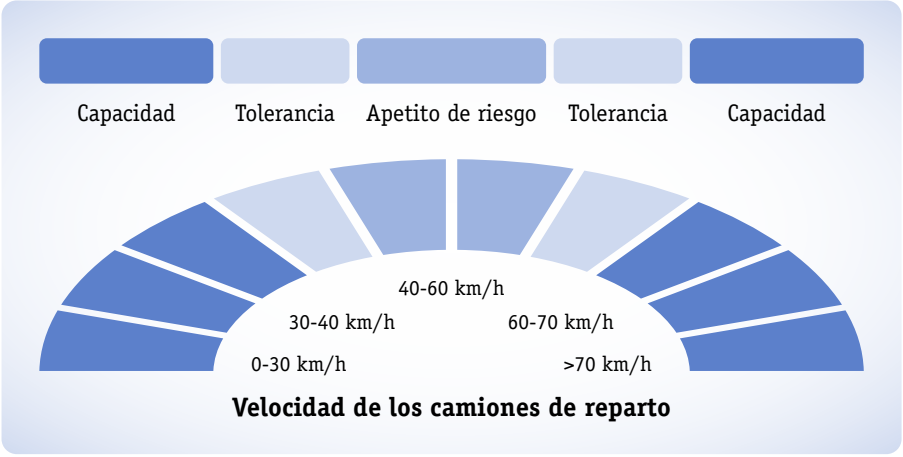


Fuente: elaboración propia

En este punto podría ser importante que la organización definiese su apetito y tolerancia al riesgo, esto es, el nivel de riesgo que está dispuesta a

asumir para alcanzar sus objetivos. Así, para calcular el nivel de riesgo deberán previamente estimarse las probabilidades, en sentido amplio, y sus consecuencias. De igual modo, la organización podría establecer sus criterios de riesgo, esto es, en base a qué aspectos se considerará la importancia de los distintos riesgos. La comparación del nivel de riesgo con los criterios establecidos en el marco del apetito y tolerancia fijado por la organización delimitarán el alcance de la gestión del riesgo, puesto que ésta podría limitarse a cumplir el marco legal o, por el contrario, ampliar su alcance incluyendo riesgos que provengan, por ejemplo, de partes interesadas que afectan a la imagen de la organización. A continuación se expone un ejemplo, relativo a la velocidad recomendada para el reparto de la mercancía. Si esta es muy baja, se correría el riesgo de demorar las entregas, y si es muy alta de multas (cumplimiento legal) o de una mala imagen frente a los clientes u otras partes interesadas (por ejemplo, por un exceso de velocidad en zonas urbanas).

FIGURA 8. APETITO, TOLERANCIA Y CAPACIDAD DE RIESGO



Fuente: elaboración propia

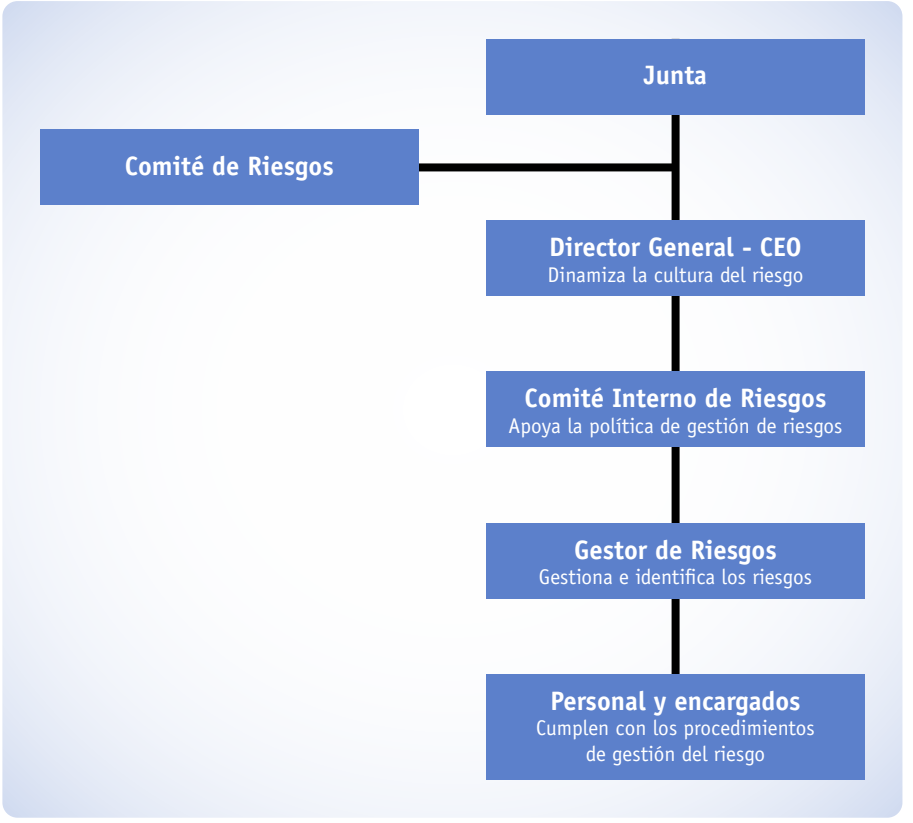
4.3 Asignar roles, autoridades, responsabilidades y obligación de rendir cuentas en la organización

La alta dirección y los órganos de gestión deben identificar a los dueños del riesgo, esto es, las personas que tienen la autoridad y responsabilidad para gestionar determinados riesgos, y que por tanto deben rendir cuentas de su gestión. A este respecto, el papel de la alta dirección, manifestado a través de liderazgo y compromiso, es que la cultura del riesgo se instaure en toda la

organización y debe asegurar, conjuntamente con los órganos de supervisión, que se asignen y comuniquen las autoridades, responsabilidades y obligaciones de rendir cuentas a todos los niveles afectados.

Los dueños del riesgo deben asegurarse de que se lleven a cabo las actuaciones que le hayan sido asignadas, y que podrían relacionarse con la recopilación de información, el análisis, la medición y valoración, la implementación de medidas de tratamiento o la comunicación y consulta, entre otras.

FIGURA 9. EJEMPLO DE ASIGNACIÓN DE ROLES: ESTRUCTURA DE GOBERNANZA DE GESTIÓN DEL RIESGO



Fuente: elaboración propia

A. Junta
   a. Asume la responsabilidad última de la gestión de riesgos.
   b. A ella le reporta el CEO y le asesora el Comité de Riesgos.

B. Comité de Riesgos
    a. Formado por técnicos especialistas en la identificación y gestión de riesgos.
    b. Asesora a los jefes de equipo sobre los procedimientos.
    c. Recibe o tiene acceso a los reportes sobre los procedimientos.
    d. Reporta a la Junta sobre el estado de la gestión de riesgos.

C. Director General-CEO
    a. Asume y dinamiza la cultura de la gestión del riesgo al conjunto de la organización
    b. Reporta directamente a la Junta sobre el estado de la gestión del riesgo.
    c. Recibe los informes del Comité Interno de Riesgos, realizados por cada parte interesada y jefes de equipo.

D. Comité Interno de Riesgos
    a. Supervisa el estado de la gestión de riesgos
    b. Se encarga de apoyar la política de implementación de la gestión de riesgos.
    c. Reporta al Director General sobre el cumplimiento de los procedimientos.
    d. Recibe los informes y reportes del gestor de riesgos.

E. Gestor de riesgos
    a. Apoya y fomenta la cultura de gestión del riesgo.
    b. Identifica y realiza la gestión de los riesgos
    c. Reporta al Comité de riesgos.
    d. Se encarga de recopilar los informes elaborados por las distintas partes interesadas.

F. Personal y encargados
    a. Realiza la aplicación de la gestión de riesgos dentro de sus funciones.
    b. Cumple con los procedimientos de gestión del riesgo
    c. Se encarga de identificar los riesgos.
    d. Reporta al gestor de riesgos.
    e. Se trata de cada una de las partes interesadas.

4.4 Asignar recursos

El primer punto dentro de la organización es evaluar sus recursos y capacidades para la gestión del riesgo, identificando las fortalezas y las debilidades detectadas. En este análisis, tanto los recursos materiales, humanos, procesos y sistemas de información, entre otros, deben ser considerados en términos de su competencia para la gestión de riesgos. Posteriormente, una vez detectadas las carencias, deberán asignarse los recursos apropiados, pues además ello refleja el compromiso y liderazgo de la alta dirección con la gestión del riesgo. Estos recursos pueden incluir desde formación hasta nuevos procesos, procedimientos, herramientas de tecnología de información y comunicación. Por tanto, los dueños del riesgo no solo dispondrán de la autoridad y responsabilidad, sino también de los recursos necesarios para realizar una efectiva gestión del riesgo asignado.

4.5 Establecer la comunicación y la consulta

Los órganos de supervisión deben dar apoyo a la alta dirección, por lo que deben encargarse de asegurar la disponibilidad de información y el correcto flujo de la misma. Asimismo, velarán por la actualización de los riesgos identificados en el contexto organizacional, de modo que participen junto con las partes interesadas de la comunicación y consulta de la empresa. A este respecto debe señalarse que las partes interesadas pueden ser receptoras de información y a la vez fuentes de la misma. Por ello, las alternativas de comunicación y el contenido de la comunicación efectuada deben responder a sus intereses, expectativas y papel que representa el destinario. El objetivo principal es que la información facilitada sea oportuna, pero además debe orientarse para que mediante la consulta sea posible recopilar información, la cual debe ser gestiona de manera eficaz y eficiente para poder ser sintetizada, evaluada y transmitida.

La utilidad de la información facilitada para la gestión del riesgo, esto es, la participación de las partes interesadas en los distintos procesos y particularmente en la identificación de riesgos, debe ser reflejada y percibida y considerada como una actividad que contribuye a tomar decisiones. La retroalimentación y la mejora continua forman así parte principal del diseño de la comunicación y consulta que realizará la organización.

5 IMPLEMENTACIÓN

La **implementación** ocurre tras la adaptación del sistema de gestión de riegos a la organización en términos de su adecuación a los objetivos perseguidos y de la difusión a todos los niveles (integración) y tras el diseño ajustado a la organización desde el punto de vista de su adecuación al contexto, el compromiso de la alta dirección, la asignación de roles y recursos y las decisiones relativas a la comunicación y consulta (diseño).

La correcta implementación requiere como aspecto principal que la gestión del riesgo sea parte de todas las actividades, esto es, se integre dentro de la cultura y de la actividad de la empresa y no constituya una actividad adicional o separada del resto. Ello implica no solo el nivel operativo (cómo se realiza la actividad) sino incluso al proceso de toma de decisiones (diseño de la misma y resto de decisiones). La implementación debe buscar, por tanto, un alcance global y conseguir, en última instancia, que la organización alcance a percibir los cambios en los contextos interno y externo como posibles fuentes de riesgo. Para ello, es necesario establecer los condicionantes de los procesos de toma de decisiones, definiendo los responsables, los plazos y estableciendo una temporalización de las actividades con una dotación adecuada de recursos. Asimismo, debe asegurarse que se comprenda y se ejecute correctamente la política de gestión de riesgos establecida, en base a los objetivos perseguidos y definidos por la organización. Como consecuencia, la implementación debe permitir que cualquier nuevo riesgo o evento sea considerado a través de la toma de conciencia de los responsables de tomar decisiones, quienes deberán disponer de un plan claro de actuación en términos de responsabilidad, autoridad, temporalización y rendición de cuentas.

6 VALORACIÓN

La **valoración** supone la evaluación constante del marco establecido, y no se refiere por tanto a la valoración de los riesgos o de las actividades realizadas, sino a la medición y valoración del conjunto del marco de referencia en sí mismo. Se pretende que a través de un proceso dinámico y en constante adaptación al contexto y a los objetivos perseguidos por la institución se evalúe la adecuación del marco de referencia y se mida de manera periódica si su implementación cumple lo esperado y si ello se orienta a al propósito establecido inicialmente. En el caso de que algún aspecto pueda ser mejorado, la organización debe actualizarlo.

7 MEJORA

La **mejora** implica adaptación y un proceso continuo de revisión y adecuación del marco de referencia. Para ello, tras la valoración la organización debe valorar la adaptación, actualización o reelaboración del marco de referencia en base a los cambios observados tanto en el contexto interno y externo como en los objetivos perseguidos. El objetivo de este aspecto es que se busque mejorar el marco de referencia, en términos de resultados, adecuación a la organización y que para ello de manera periódica se revise y se elaboren, asignen y midan los planes de mejora que surjan de las nuevas oportunidades y amenazas detectados o de las fortalezas y debilidades detectadas. Se trata así de poner en práctica y cerrar el ciclo PDCA o PHVA (planificar, hacer, verificar y actuar), también conocido como ciclo de Deming (1989). A este respecto, las políticas, los métodos que se utilicen, las plantillas y modelos se van mejorando conforme la organización adquiere experiencia en la gestión del riesgo y se adapta a los cambios del entorno.

8 MODELOS Y PLANTILLAS

TABLA 3. REVISIÓN DEL MARCO DE REFERENCIA. LIDERAZGO Y COMPROMISO E INTEGRACIÓN

Elemento	Grado de cumplimiento	Motivo	Posibles mejoras
Se han adaptado los componentes del marco de trabajo a la organización			
Se difunde adecuadamente el enfoque, plan o línea de acción a todos los niveles y todas las partes interesadas			
Se han asignado los recursos necesarios y la asignación de roles es adecuada a la autoridad, la responsabilidad y la obligación de rendir cuentas			
Se ha integrado la gestión de riesgos con las particularidades de la organización y de las partes internas de su estructura			
Se han establecido los criterios de riesgo, cuáles son los riesgos que se consideran, así como las metodologías que se utilizarán para la identificación y valoración			
.....			

Fuente: elaboración propia.

TABLA 4. EL CONTEXTO. LAS PARTES INTERESADAS

Categoría	Parte interesada	Tipo	Motivo de su consideración	Influencia	Interés	Actividad
Cliente	Usuario	Externo	…	Alta	Bajo	Comunicar
Cliente	Prescriptor	Externo	…	Alta	Alto	Involucrar
Sector Público	Gobierno local	Externo	…	Baja	Alto	Reportar
Sector Público	Entidad de promoción local	Externo	…	Baja	Bajo	Monitorizar
…	…	…	…	…	…	…

Fuente: elaboración propia.

TABLA 5. EL CONTEXTO. ANÁLISIS PESTEL

Categoría	Elemento	Plazo	Probabilidad de ocurrencia	Impacto esperado
Político	Cambio gobierno local	1 mes	Alta	Muy positivo
	Rebaja fiscal	2 años	Media	Positivo
	…	…	…	…
	…	…	…	…
Económico	…	…	…	…
	…	…	…	…
	…	…	…	…
	…	…	…	…
	…	…	…	…
Social	…	…	…	…
	…	…	…	…
…	…	…	…	…

TABLA 6. DEFINICIÓN DE MISIÓN, VISIÓN Y VALORES

Elemento	Definición
Misión	[Define que es la empresa, para qué existe. Es importante aclarar las diferencias frente a la competencia. Por ejemplo, no es adecuado «una empresa de café» sino que debe establecerse lo que la hace diferente: el mejor café en grano a granel, el mejor café molido monodosis, el café más rápido para familias, el café óptimo para canal horeca por su rendimiento, el mejor café listo para tomar en tres segundos, el mejor café servido en la playa, etc]
Visión	[Define «hacia dónde» va la empresa, qué tipo de objetivos y metas busca alcanzar. Por ejemplo: liderazgo en el noroeste peninsular en la calidad del servicio postventa de un determinado producto]
Valores	[Define cómo?, esto es, que rige la actividad de la empresa. Por ejemplo: honradez, rapidez, hacer las cosas como las ha hecho la organización desde hace años, etc.]

TABLA 7. REVISIÓN DEL MARCO DE REFERENCIA. EL DISEÑO, INTEGRACIÓN, VALORACIÓN Y MEJORA

Elemento	Grado de cumplimiento	Motivo	Posibles mejoras
Se ha analizado el contexto interno y externo			
Se ha elaborado la política de gestión de riesgos			
Se han asignado roles, responsabilidades, autoridades y obligación de rendir cuentas			
Se han asignado los recursos necesarios, incluyendo formación			
Se han establecido los medios y contenidos de la comunicación y consulta con las partes interesadas			

Fuente: elaboración propia.

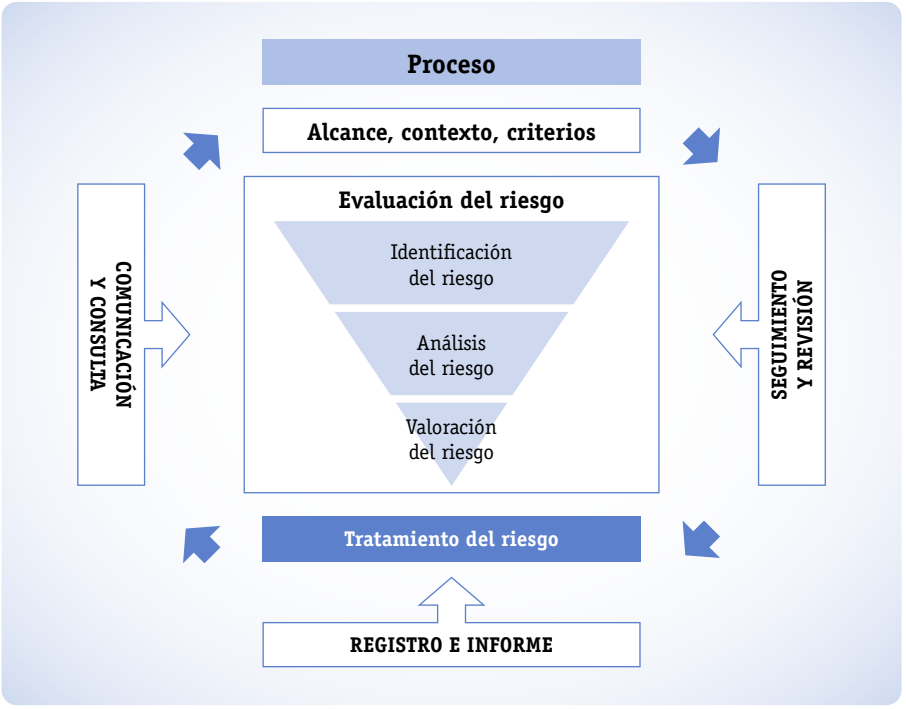
III

Proceso

1 PRESENTACIÓN

A continuación se detallan los puntos relativos al proceso. El proceso debe ser principalmente iterativo y dinámico, puesto que debe estar adaptado a los cambios en el contexto interno y externo. La integración de la gestión del riesgo en las actividades y operaciones debe hacerse atendiendo al alcance y a los factores humanos y culturales que se hubiesen incluido en el contexto externo e interno. Por ello, el proceso comienza con la comunicación y consulta a las partes interesadas, tanto externas como internas para obtener la información inicial necesaria.

FIGURA 10. ETAPAS DEL PROCESO DE GESTIÓN DE RIESGOS



Fuente: Elaboración propia a partir de UNE ISO 31000 (2018)

2 COMUNICACIÓN Y CONSULTA

El primer paso para poder identificar los riesgos a los que se enfrenta la empresa es recopilar información del contexto externo e interno para disponer de conocimiento sobre su situación. Asimismo, la organización debe informar a estas partes interesadas, de modo que se genere una relación bilateral y de manera iterativa. Dicha relación afecta a todas las fases del proceso de gestión de riesgo si bien las distintas partes interesadas demandarán y ofrecerán información de distinta naturaleza. El mapa de partes interesadas nos informará sobre los requerimientos de información de cada parte interesada y la actividad que debe realizarse en relación a la misma.

En el caso de las partes interesadas externas, éstas deberán conocer el planteamiento que realiza la realiza la organización para gestionar el riesgo, la efectividad de dicha gestión y la importancia de la misma para apoyar el proceso de creación de valor. Por tanto, la comunicación estará encaminada principalmente a la toma de conciencia y a transmitir las justificaciones, los motivos y las acciones necesarias que la organización lleva a cabo para gestionar su riesgo.

En cuanto a las partes interesadas internas, éstas deberán conocer el proceso de gestión de riesgos, así como sus responsabilidades y la importancia de gestionar el riesgo para apoyar el proceso de creación de valor. El hecho de que el factor humano sea el elemento principal de la gestión del riesgo provoca que este punto sea especialmente relevante, no solo para demostrar así el compromiso e integración de la dirección, sino también para involucrar todas las actividades y procesos en la gestión del riesgo.

La implementación correcta de la comunicación y consulta permitirá que la organización reciba información útil e íntegra, que podrá ser utilizada para el proceso de gestión de riesgos, contribuyendo a identificar riesgos, valorarlos y tratarlos. Mediante esta relación se favorece la obtención de perspectivas y conocimiento multidisciplinar, permitiendo incorporar distintas percepciones y sensibilidades y contribuyendo a la generación de la cultura de gestión responsable del riesgo, lo que redundará en la mejora de la confianza.

> Para apoyar esta actividad, la organización podría diseñar un plan de comunicación interna y externa que podrá ir acompañado de un plan de reportes de SQRF (sugerencias, quejas, reclamaciones y felicitaciones).

3 ALCANCE, CONTEXTO Y CRITERIOS

3.1 Alcance

El alcance debe definirlo la propia organización, para lo que debe tener claro el objetivo perseguido, entre los cuales podría encontrarse limitarse a cumplir con la legislación, mejorar la gestión del riesgo en un área específica, como por ejemplo la medioambiental, mejorar un área de la empresa que presenta alta volatilidad en sus resultados, etc.). Una vez establecido el objetivo que se persigue, deberá explicitarse el alcance, dado que se puede limitar a determinadas plantas de la organización, áreas o incluso niveles (estratégico, operacional, de programa, de actividad). Posteriormente deberán definirse los riesgos que se analizarán y cuáles serán los criterios a considerar. Para ello, la organización puede obtener información de diferentes clasificaciones de riesgos. A la hora de clasificar los tipos de riesgos debemos señalar que se pueden establecer diversas categorías de riesgo. Nos basaremos en lo recogido en Otero et al. (2015), en el que se puede encontrar una revisión completa y muy ilustrativa de las mismas. Para clasificar los distintos tipos de riesgo podemos preguntarnos:

— **¿Se puede definir el riesgo correctamente y de forma objetiva, o es difícil su objetivación?**

- Riesgo objetivo: Podría definirse como riesgo explícito y correctamente definido en términos de gestión de riesgo a partir de su composición, características y condicionantes extrínsecos e intrínsecos objetivables.
    - » Es útil a la hora de definir correctamente el continente o contenido a asegurar.
    - » Suele hacer referencia a condicionantes generales y característicos del sujeto u objeto a asegurar.
    - » Es posible incluir los distintos riesgos objetivos en forma de preguntas fáciles de responder (con números, afirmativa o negativamente, etc.) en un cuestionario a cubrir por el interesado.
- Riesgo subjetivo: Sería aquel tipo de riesgo implícito y propio del individuo u organización analizada. No es fácil definir el riesgo de forma objetiva y afecta al individuo por sus propias circunstancias específicas. Incluso puede suceder que el propio sujeto no sea consciente del mismo, y por lo tanto no sea explicitado como riesgo.

» Este tipo de condicionantes que afectan al riesgo del objeto/sujeto tienen que ver con aspectos difícilmente medibles (honestidad, moralidad, coherencia, responsabilidad, etc.)

» Adicionalmente, se trata de elementos potenciadores del riesgo que el propio sujeto/objeto de valoración puede desconocer u ocultar porque no son visibles o no son fácilmente explicitables.

» En muchos casos se intenta caracterizar al sujeto/objeto a través de variables cualitativas que incluyan cierto grado de objetivación a través de escalas en las que poder incluir al sujeto/objeto.

— **El riesgo que se analiza, ¿forma parte de la operativa normal del sujeto/objeto o es fruto de un accidente o fatalidad?:**

- Riesgo ordinario: Obedecen a situaciones previsibles con efectos previamente definidos.

  » Pueden ser riesgos habituales o no, pero en todo caso es posible la medición de su impacto a partir de la experiencia previa en situaciones similares.

  » Se puede objetivar el impacto o daño y su medición y graduación en función de las variables que lo definen.

- Riesgo extraordinario: Aquel que sucede de forma atípica o imprevista. No se alcanzan a definir de forma previa las causas que lo provocan.

  » No debe definirse como extraordinario un riesgo que, conociéndose las causas que lo pueden provocar (un incendio en una fábrica de explosivos), puede provocar más daños que los inicialmente considerados (afectación de vidas y viviendas del entorno de la empresa).

— **El riesgo considerado, ¿a qué afecta, a un sujeto o a un objeto?:**

- Riesgos personales: Propios de la integridad física de las personas.
- Riesgos sobre objetos: Aquellos que afectan a los bienes.
- Riesgos patrimoniales: Tienen que ver con el conjunto de bienes de las personas físicas o jurídicas.

— El riesgo que se trata, ¿a qué sección organizacional/empresarial afecta?:

- Riesgos sobre la estrategia: Aquellos que tienen que ver con el cumplimiento de la misión, visión y valores de la empresa, con la consecución o no de los objetivos marcados, con la aplicación de las políticas empresariales establecidas desde la dirección, etc.

- Riesgos relacionados con la gestión del conocimiento: Los que afectan al tratamiento y utilización de patentes, ideas empresariales legalmente definidas, uso incorrecto o fraudulento de licencias, etc.

- Riesgos que afectan a la marca o a la imagen de la organización: Derivados de posibles cambios en cómo es percibida y valorada la compañía por sus *stakeholders* y el resto del mercado. Relacionada con la pérdida de confianza o con valoraciones negativas de la organización.

- Riesgos tecnológicos: Aquellos que tienen que ver con la posible obsolescencia tecnológica de los bienes y equipos empleados por la organización. Tanto actuales como futuros. El riesgo se vincularía con la imposibilidad de la empresa de cumplir sus objetivos por motivos derivados del uso de la tecnología.

- Riesgos relacionados con el cumplimiento o de conformidad: Los que se relacionan con la capacidad de observar y cumplir con lo establecido en materia legal, contractual y demás corpus jurídico. Las afectaciones son diversas, como el ámbito de salud y seguridad laboral, cumplimiento de normas medioambientales, fiscales, laborales, administrativas, etc.

- Riesgos financieros: Aquellos riesgos que tienen que ver con la gestión financiera y de los recursos monetarios. Entre otros, estarían los derivados de la ejecución del presupuesto, de la realización de pagos, o la gestión de excedentes de tesorería, ejemplos todos ellos del ámbito interno de la empresa, a los que habría que añadir además los relativos a la financiación externa (líneas de crédito, préstamos, descuento de efectos, etc.), como la volatilidad de los tipos de cambio de las divisas o de los tipos de interés.

- Riesgos operacionales: Serían los riesgos derivados del día a día de la empresa, aquellos relacionados con la gestión de proveedores, la custodia, tratamiento y mantenimiento de las mercancías, productos en curso y terminados, el funcionamiento de los sistemas de información internos (intranet, ERPs, etc.) así como de la página web y/o plataforma de venta por internet, etc.

En la siguiente tabla se propone una posible plantilla a emplear para la clasificación de los riesgos:

TABLA 8. DEFINICIÓN Y CLASIFICACIÓN DE RIESGOS

A la hora de definir los riesgos y clasificarlos se debe tener en cuenta los siguientes elementos:		
Objetivación	Se trata de un tipo de riesgo objetivo?	
	o se trata de un tipo de riesgo subjetivo?	
Operativa	Se trata de un tipo de riesgo propio de la operativa?	
	o se trata de un tipo de riesgo extraordinario?	
Sujeto/ Objeto	El riesgo tiene que ver con una persona o trabajador	
	El riesgo tiene que ver con un objeto concreto de la empresa	
	El riesgo tiene que ver con el patrimonio de la empresa en su conjunto?	
Por sección o área empresarial	La empresa no se adapta a las demandas del mercado (producto, precio, tecnología, etc.)	Estratégicos
	La organización no está al día en el uso de la tecnología, no está en el camino de la "digitalización"	
	La compañía no es capaz de competir, no responde correctamente a los ataques de la competencia	
	No se está cubierto ante posibles cambios políticos, normativos, regulatorios, financieros derivados de la internacionalización	
	Los trabajadores, internamente en los equipos de trabajo, con los clientes, proveedores y demás stakeholders se comportan con educación, ofrecen un buen trato y transmiten correctamente la imagen de marca de la empresa? Si no es así, estamos ante un riesgo de deterioro de imagen o pérdida de confianza	
	Cómo son percibidos los productos o servicios de la empresa? Cumplen las expectativas de los clientes en términos de calidad y precio? Incumplir las expectativas en este sentido implica riesgo de deterioro de imagen o pérdida de confianza	
	Corremos el riesgo de ser absorbidos por la competencia?	
	Es previsible una caída de los ingresos de ventas o de los beneficios?	Operativos
	Hasta qué punto está cubierta la empresa ante posibles rupturas de suministro?	
	Cómo gestiona la organización el clima laboral? Hace algún control o seguimiento de las nuevas incorporaciones? Cómo está funcionando el plan de seguridad laboral? Los trabajadores "sienten" los valores de la empresa, están identificados con la imagen de la empresa?	
	Funciona correctamente la plataforma digital de venta por internet? Es ágil y de fácil acceso y navegación la página web? Qué tipo de noticias relacionadas con la empresa se publican en medios digitales y en las redes sociales? El encargado de la gestión de las redes sociales mantiene activa la página web y las redes sociales en las que está presente la empresa?	
	Cómo funciona el transporte de nuestras mercancías? Y el de nuestras ventas? Los clientes están satisfechos con los plazos y el trato de sus productos entregados en domicilio?	

Por sección o área empresarial	Si la empresa necesita financiación, sería fácil que nos la concedieran (proveedores, entidades financieras, socios, etc.)	Financieros
	Estamos al tanto de cumplir con nuestras obligaciones financieras (pagos) para con terceros? Se producen retrasos? Se producen impagos? Podemos sufrir nosotros impagos de nuestros clientes o deudores?	
	Trabajamos con divisas extranjeras? Estamos cubiertos ante posibles variaciones en los tipos de cambio?	
	Estamos cubiertos ante posibles cambios en los tipos de interés de nuestras operaciones financieras?	
	Consideramos posibles denuncias o reclamaciones a los directivos de nuestra organización por su gestión?	Regulatorios
	Estamos cubiertos ante posibles reclamaciones comerciales relacionadas con el comportamiento o satisfacción de los productos o servicios que ofrecemos?	
	Consideramos el entorno ambiental y respetamos la legislación en cuanto a afectaciones medioambientales derivadas de nuestros procesos y gestión de residuos?	
	La Responsabilidad Social Corporativa (RSC) forma parte de la misión, visión y valores de la empresa? Qué actuaciones realiza la empresa en este ámbito? Tiene suficiente impacto social las actuaciones en RSC que realiza la empresa?	
	Está cubierta la empresa en términos de ciberdelincuencia, globalización, actos terroristas, pandemias?	Gobales

Fuente: elaboración propia y elaboración propia a partir de Otero et al. (2015)

En la siguiente tabla se muestra el Listado de los 10 riesgos principales identificados para España en 2020 según se recoge en el Allianz Risk Barometer (2020:a y b). Además de todos ellos, el informe recoge también un nuevo tipo de riesgo, el relacionado con desarrollos macroeconómicos, como por ejemplo los derivados con las políticas monetarias, programas de austeridad, incremento de los precios de materias primas, deflación o inflación, entre otros.

TABLA 9. PRINCIPALES RIESGOS IDENTIFICADOS PARA ESPAÑA POR EL ALLIANZ RISK BAROMETER

Posición	Tipo de riesgo
1	Incidentes relacionados con la ciberseguridad
2	Interrupciones en el negocio, como en la cadena de suministro
3	Catástrofes naturales (lluvias torrenciales, mareas vivas, tormentas, terremotos, etc.)
4	Cambios en la legislación-regulación (inseguridad normativa, guerras comerciales, sanciones económicas, proteccionismo, aranceles, Brexit, desintegración de la Eurozona, etc.)
5	Fuego, explosiones
6	Riesgos ambientales (por ejemplo, polución)
7	Cambio climático e incremento de la volatilidad en cuanto al tiempo atmosférico
8	Pérdida de reputación o de valor de la marca
9	Cambios en el mercado (volatilidad, competencia, barreras de entrada, fluctuaciones, etc.)
10	Nuevas tecnologías (inteligencia artificial, vehículos autónomos, impresión 3D, internet de las cosas, nanotecnologia, blockchain, etc.)

Fuente: Elaboración propia a partir de Allianz Risk Barometer (2020:a y b)

Posteriormente, la organización puede establecer los resultados esperados y las herramientas y técnicas de evaluación que se aplicarán. Finalmente, resulta procedente que la organización señale como será la medición y que requisitos son necesarios para que la gestión del riesgo se considere que se ha realizado de manera satisfactoria, señalando qué registros deberán obtenerse y estableciendo los recursos y las responsabilidades.

3.2 Contexto

De acuerdo con lo planteado en el marco de referencia, en este punto deberá analizarse el contexto externo e interno definido previamente. Este análisis tiene como finalidad identificar las fuentes de riesgo, por lo que puede resultar útil comparar los recursos y capacidades de la empresa frente al resultado del análisis PESTEL con el objetivo de identificar la complejidad en las redes de relaciones y poder así sintetizar la información. Para ello puede resultar de utilidad plasmar el resultado en una matriz de Debilidades, Amenazas, Fortalezas y Oportunidades (DAFO) y plantear para las distintas partes interesadas cuáles pueden constituir fuentes de riesgo y así además poder anticipar eventos.

FIGURA 11. EJEMPLO RESUMIDO DE MATRIZ DAFO

Fuente: elaboración propia

3.3 Criterios

La organización deberá identificar las áreas principales de riesgo que afectan a los objetivos, y definir para cada una de ellas cual es el nivel de riesgo asumible y deseable. Debido a la heterogeneidad de las mismas y de las distintas mediciones, es aconsejable definir para cada una de ellas las causas y consecuencias posibles, la medición, así como el apetito y la tolerancia por el riesgo de la organización, esto es, la cantidad de riesgo que desea y puede asumir. Para dicha definición no es necesario utilizar en todos los casos herramientas cuantitativas, pues en ocasiones es suficiente con valorar qué áreas de la organización se podrían ver afectadas y si dicha consecuencia tendría un impacto bajo, medio o elevado.

Los criterios para decidir si un riesgo es aceptable o no, teniendo en cuenta su probabilidad y su impacto, así como el riesgo residual que existe tras la aplicación de un potencial control, dependerán del contexto externo e interno de la

empresa, puesto que debe alinearse con los objetivos, recursos y capacidades de la organización teniendo en cuenta la importancia de las partes interesadas. Cabe destacar que debido a que el proceso de gestión de riegos es dinámico, los criterios de riesgo están sujetos a una revisión periódica, lo que permite su adaptación al contexto.

IV
Evaluación

1 PRESENTACIÓN

Para la evaluación del riesgo se pueden emplear diversas técnicas y metodologías, y entre ellas es posible utilizar las que pueden encontrarse en la ISO 31010. A continuación se expone en qué consiste cada una de ellas.

2 TÉCNICAS Y METODOLOGÍAS

Tormenta de ideas

Método de trabajo grupal encaminado a la aportación nuevas ideas o planteamientos ante el enunciado de un problema. El ambiente debe ser lo suficientemente relajado como para que el participante se sienta motivado a opinar con libertad. Las aportaciones no deben cuestionarse, sólo recogerse. Debe motivarse la generación suficiente de aportaciones como para poder seleccionar las más relevantes o innovadoras. Una vez definido el grupo de personas participantes, el responsable debe plantear una pregunta abierta partiendo de la motivación de un supuesto o situación. Por ejemplo: «Acaba de suceder esto en la empresa, cómo debemos proceder », o «Qué deberíamos hacer si».

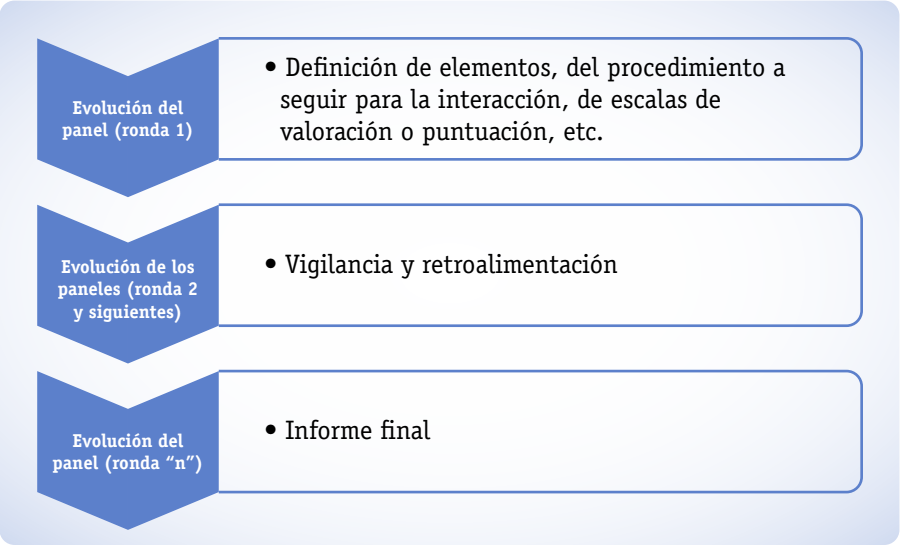
Entrevistas estructuradas o semiestructuradas

Las entrevistas permiten recoger información de los entrevistados. Si éstas son estructuradas implican definir de antemano las cuestiones a realizar, debiendo establecer el grado de concreción que se quiere obtener. Para este tipo de entrevistas no se contempla la posibilidad de que el entrevistador se «salga del guión», sino que se limita a poner voz a las preguntas preestablecidas. Las entrevistas semiestructuradas permiten cierto grado de libertad al entrevistador, que sí tiene una guía del tipo de respuestas que desea obtener, pero que a la vez tiene la posibilidad de salirse del guión y emplear sus recursos en forma de nuevas preguntas que le permitan llegar al nivel de profundidad buscado o al objetivo marcado inicialmente.

Técnica Delphi

Se trata de una metodología de comunicación sistemática, estructurada e interactiva que se basa de un proceso de panel de expertos sucesivo. A partir del diseño de encuestas o formularios específicos, se van analizando las respuestas, que sirven como base para la siguiente ronda. Hay una retroalimentación guiada o estructurada.

FIGURA 12. TÉCNICA DELPHI



Fuente: elaboración propia

Lista de verificación

Es una herramienta sencilla y objetiva que permite analizar las propiedades de un elemento, sistema u organización. A partir de una lista de cuestiones que se responden con un «sí» o con un «no» se comprueba si los atributos examinados de la entidad cumplen o no los requisitos objeto de análisis. Bien es cierto que al tratarse de una respuesta objetiva, sin posibilidad de justificación, el proceso pierde capacidad informativa, ya que dejan de incluirse en el análisis los matices y detalles, que pueden ser relevantes para la toma de decisiones.

Con ella es posible hacer un control de calidad de los productos, evaluar a proveedores o al personal, entre otros. La finalidad puede ser de control, de evaluación, de análisis o de verificación, entre otros.

Análisis preliminar de peligros (PHA)

Empleado en entornos donde no se dispone de mucha información. Se trata de una herramienta interesante para identificar peligros o situaciones que presenten vulnerabilidad. Como resultados proporciona sugerencias para poder aminorar el riesgo derivado de los peligros analizados. Se trata de resultados cualitativos. Es necesario disponer de los criterios de diseño, definición de los equipos y materiales. Los pasos para realizarlo serían: Selección del proceso a analizar, identificación de los riesgos/peligros potenciales, evaluación de las causas de estos peligros, definición de los efectos derivados de los peligros, agrupación de los peligros en función de su naturaleza y establecimiento de los controles para reducir los peligros detectados.

Análisis funcional de riesgos y de operatividad o HAZOP «Hazard and Operability Study»

Se trata de una herramienta de análisis de riesgo de proceso o PHA. Se puede aplicar tanto en una etapa de diseño inicial de proceso como en fase de operación. Está basada en la idea de que los riesgos o problemas de operatividad derivan de una desviación de las variables que definen el proceso en relación con los indicadores normales de operación. A partir del análisis sistemático de las desviaciones que se producen en las variables principales, se persigue definir las causas y consecuencias de las mismas. De esta forma es posible mejorar la seguridad del proceso o instalación, además de evidenciar los problemas en diseño y operatividad en fase inicial de proyecto.

Análisis de peligros y de puntos críticos de control (HACCP)

Se trata de una técnica sistemática y preventiva, basada en la objetividad y la lógica. Tiene su aplicación en industrias que fabriquen productos o materiales que van a estar en contacto con alimentos. Se pretende identificar todos aquellos riesgos de contaminación que pueden suceder en la cadena de producción en relación con los productos y los distintos componentes de los mismos: físicos, químicos y biológicos. Una vez identificados los riesgos, se busca establecer medidas de prevención y de control para garantizar la integridad del proceso y la seguridad del producto.

Evaluación de los riegos ambientales

La evaluación de los riesgos ambientales se basa en el análisis de los riesgos en los que puede incurrir una empresa desde el punto de vista ambiental, y

en la emisión de un juicio sobre el nivel de tolerancia de la empresa ante esos riesgos. A la hora de realizar la evaluación de los riesgos son numerosos los condicionantes que pueden influir en la misma: factores económicos, financieros, sociales y/o normativos; factores identitarios relacionados con la misión, visión y valores de la entidad; la disponibilidad de la tecnología que permita minorar el impacto de los riesgos; la estrategia de la empresa.

Técnica estructurada «y si» (en inglés, SWIFT: Structured «What-if» Technique)

Técnica simple que consiste en que el sujeto se pregunte (o un entrevistador consulte al entrevistado) «qué entiende que pasaría si sucede tal acontecimiento. ¿Cómo se debería de actuar?». Puede plantearse este formato de pregunta de forma directa en entrevista personal o en dinámica de grupo empleando la técnica de la «lluvia de ideas» o «Delphi 66».

Análisis de escenarios

Se trata de una metodología que se basa en la definición de los distintos escenarios o situaciones que se pueden dar ante distintos estados de la naturaleza. La definición de distintos escenarios permite contemplar y abarcar la mayor parte de las situaciones que se pueden suceder junto con sus consecuencias. Se pueden incluir así eventos tanto hipotéticos como extraordinarios y extremos, relacionados estos últimos con los tests de estrés. Es fundamental la correcta definición de las variables clave que permiten establecer distintos escenarios. El análisis de escenarios se suele aplicar en teoría de la decisión o teoría de juegos, y se busca asignar probabilidades a los distintos escenarios contemplados.

Análisis de impacto en el negocio (en inglés, Business Impact Analysis, BIA)

Se basa en el análisis del impacto que tendrían posibles situaciones que lleven a la ruptura de los procesos de negocio de la entidad. Mediante este análisis se busca identificar qué procesos son críticos para la entidad, por cuanto un fallo en ellos conduciría a la organización a registrar un impacto negativo no asumible ni deseable desde el punto de vista operacional, económico, social, de reputación, etc.

Análisis de la causa raíz (ACR)

Técnica expost que busca encontrar las causas que provocaron cierto problema o error para así tratar de evitar que suceda de nuevo. Con ello se pretende

prevenir y pronosticar eventos antes de que se produzcan. Son numerosas las herramientas que se pueden emplear para acometer un ACR, del mismo modo que se pueden encontrar distintos campos de aplicación de esta técnica, como los relativos al control de calidad, seguridad y salud laboral y análisis de fallas, entre otros.

Análisis de modos y efectos de fallos (en inglés, FMEA, Failure Mode and Effect Analysis)

Como su nombre indica se trata de un método empleado para prevenir los fallos y analizar los riesgos de un proceso. Es fundamental identificar las causas, los efectos y el proceso de detección para determinar las acciones que se emplearán para no incurrir en fallos. Según lo comentado la causa es el motivo por el que se produjo el error, el efecto define las consecuencias que el fallo tiene para nuestro cliente y el proceso de detección será aquel que permite evitar nuevos fallos. Con el FMEA se busca reducir los riesgos de los errores en los procesos y de la probabilidad de los fallos que se pueden producir. Entre los objetivos de esta herramienta se encuentran la priorización de los fallos en función del nivel de riesgo, poder actuar con medidas preventivas y definir el responsable y plazo para acometer una medida de este.

FIGURA 13. ANÁLISIS DE MODO Y EFECTOS DE FALLA

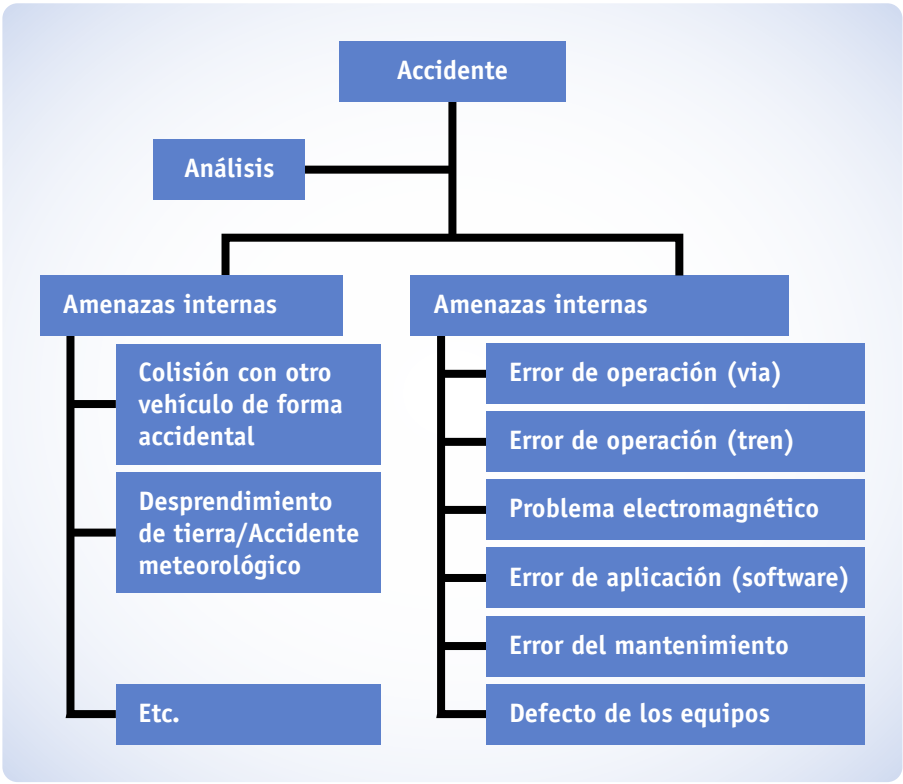
Función del proceso	Posible fallo	Efecto potencial	Severidad	Ocurrencia	Causa	Medio de detección
Limpieza de pieza	Limpieza insuficiente	Devolución entrega	Alta	2%	Falta de presión de agua	Verificar conexión de agua
					Falta de jabón	Verificar existencia de jabón antes del inicio

Fuente: elaboración propia

Análisis del árbol de fallas (en inglés, Fault tree analysis, FTA)

Método empleado en la ingeniería de seguridad y fiabilidad consistente en un análisis de fallas de tipo deductivo con estructura de arriba hacia abajo. Se busca definir el proceso de fallo o error que sufren los procesos y la probabilidad de suceso de un accidente o una falla funcional de un sistema o de un nivel.

FIGURA 14. ANÁLISIS DE ÁRBOL DE FALLOS

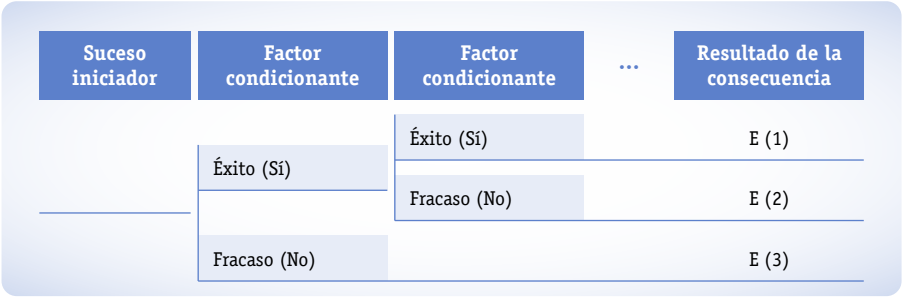


Fuente: elaboración propia

Análisis del árbol de eventos (en inglés, Event Tree Analysis, ETA)

Método inductivo que se basa en la descripción paso a paso del proceso generado a partir de un evento. Se parte así de un suceso que detona un proceso. Es necesario definir los distintos factores que condicionan el devenir de ese proceso. A través del dibujo de las ramas del árbol se recogen las posibles situaciones que se pueden ir generando a partir del motivo iniciador. Para establecer los distintos tramos por los que puede avanzar el proceso es necesario definir los factores que condicionan la evolución de la situación. A partir del evento detonador del proceso, normalmente la rama inferior del árbol conduce al fallo o a la no ocurrencia, y la rama superior es indicativa del éxito o la ocurrencia del suceso. En caso de tener información sobre las probabilidades de los diferentes éxitos o fracasos a asignar para cada factor condicionante, la técnica puede pasar de cualitativa a cuantitativa.

FIGURA 15. ANÁLISIS DEL ÁRBOL DE EVENTOS



Fuente: elaboración propia

Análisis de causa-consecuencia

Técnica basada en la agrupación de árboles de eventos. Su componente gráfica la convierten en una herramienta con una gran capacidad comunicativa que permiten observar desde las causas que provocan cierto evento hasta las posibles consecuencias que puede generar. De nuevo, poder asignar probabilidades a los sucesos permite definirla como técnica cuantitativa. Si no es posible, se propone como herramienta cualitativa.

Análisis de causa y efecto o diagrama de Ishikawa

Se trata de un planteamiento con el que la organización puede llegar a conocer las causas que conducen a una situación negativa. Un ejemplo de ello puede ser llegar a conocer los motivos que llevan a que sus objetivos se desvíen. Se busca llegar a la razón o a la raíz que provoca esa desviación del objetivo. Una vez se define el problema a tratar se establecen las categorías a partir de las que enfocar el análisis, y así tratar de descomponer en varios elementos característicos el proceso objeto de análisis. Ejemplos de estas categorías podrían ser en una empresa: materias primas, maquinaria, procedimientos establecidos o estándares de medición, mano de obra o entorno físico de trabajo, entre otras. Una vez se explicitan para estas categorías las causas que conducen al problema, el responsable debe seleccionar qué causas son las más relevantes a la hora de generar el problema.

Análisis de capas de protección (LOPA)

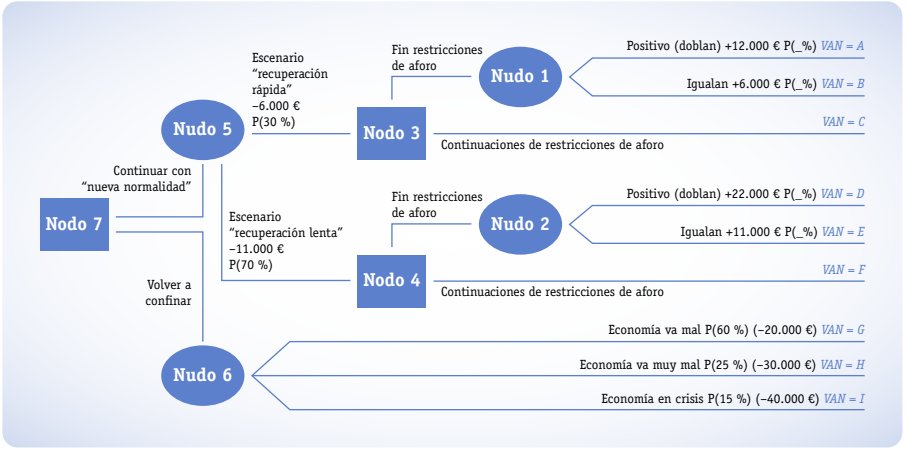
Herramienta cualitativa para la evaluación de peligros y riesgos, en línea con la técnica estructurada «y si », el análisis funcional de riesgos y de operatividad o

HAZOP «Hazard and Operability Study» y los árboles de eventos. Puede realizarse en cualquier momento de desarrollo del proceso, pero se recomienda en la fase inicial de diseño de organigramas de procesos. Mediante reglas rigurosas se estandarizan las capas de protección que son independientes y los eventos que conducen a la generación de riesgos. A través de las reglas se podrá definir el riesgo de cada causa-efecto. Se busca definir una serie de situaciones de peligro, con las consecuencias que cada situación puede generar y las medidas de protección a aplicar para cada una de ellas.

Análisis del árbol de decisiones (Diagrama de árbol de decisiones)

Técnica que se basa en la representación gráfica de los posibles efectos o resultados derivados de la toma de una serie de decisiones. Suele dibujarse partiendo de un único nodo, a la izquierda, indicativo de la decisión inicial a tomar. A partir de este nodo inicial el problema se «ramifica» para representar los efectos o resultados que derivan de esta decisión. A su vez, nuevos nodos dan lugar a nuevas ramificaciones expresivas de los resultados o efectos. Entre los nodos que se pueden encontrar están los de probabilidad (que se dibujan en forma de círculo e incluyen información sobre la probabilidad de suceso de los efectos que se derivan de un mismo nodo), de decisión (con forma de un cuadrado y representan una toma de decisiones vinculada con las distintas opciones existentes) y el nodo terminal que indica la sucesión de decisiones y eventos por los que se opta en forma de ruta a partir de las sucesivas ramas y nodos seleccionados.

FIGURA 16. EJEMPLO DE ÁRBOL DE DECISIONES



Fuente: elaboración propia

Análisis de la fiabilidad humana (en inglés, HRA: Human Reliability Analysis)

Técnicas basadas en el estudio de aspectos psicológicos y propios de las organizaciones que se pueden encuadrar dentro de la fiabilidad de sistemas. Se pueden categorizar en dos ramas: las relativas al análisis probabilístico de los riesgos y las propias relacionadas con el control del cognitivo. El análisis probabilístico de los riesgos se basa en la idea de que las personas, al igual que las máquinas, pueden fallar o cometer errores. El planteamiento pasa por asignar probabilidades de ocurrencia del fallo en las distintas fases del proceso. Las propias del control cognitivo trata de modelizar el comportamiento humano a partir de una sucesión de modos de control.

Análisis bow tie

Esta herramienta permite definir el riesgo a partir de las causas y las consecuencias que se derivan de él. Se propone así el estudio de las rutas de un riesgo, que es representado en forma de nudo central de la corbata (bow tie). A partir de este nudo central se definen las causas del mismo, así como los eventos críticos a los que pueden derivar de este riesgo. Para generar este tipo de diagramas se puede partir de los de árboles de fallos y eventos, así como de una lluvia de ideas.

Mantenimiento centrado de la fiabilidad o Reliability Centred Maintenance, RCM en inglés

Técnica empleada para definir planes de mantenimiento con el objetivo último de aumentar la fiabilidad del proceso de la instalación. La fiabilidad se vehicula a través de la disminución del tiempo de parada o de ruptura de suministro, provocado bien por la ruptura del stock o por averías imprevistas. Si esto se consigue, un efecto positivo añadido es el incremento de tiempo de disposición o de utilización de la instalación y otro, la posible reducción de los costes derivados del mantenimiento de la misma y del número de averías. En cuanto al tratamiento de la información relativa a los fallos o averías hay que tener en cuenta: por un lado la explicitación del fallo —si este es evidente o no, visible o no, detectable fácilmente o no—, los efectos que ese fallo o avería provoca, y por último la probabilidad de que suceda ese fallo.

Análisis de fugas (SA) y análisis del circuito de fugas (SCA)

Se trata de una técnica que permite detectar problemas en el hardware y en el software mediante el empleo de distintas tecnologías. Estas herramientas pueden incluir además otras técnicas como las de árboles de fallo y el análisis del modo de fallo y de los efectos (FMEA). Para realizar un análisis de fugas es necesario: preparar y/u obtener los datos, construir el árbol de red, evaluar los distintos caminos que ofrece la red, y la elaboración del informe final. En cuanto a los caminos de la red, pueden estar formados por materiales, acciones del operador, o códigos o enunciados lógicos. El circuito de fuga se caracteriza por dar lugar bien a funciones no deseadas, o bien por frustrar o invalidar funciones deseadas del sistema.

Análisis de Markov

Técnica cuantitativa empleada en aquellos casos en los que, ante una sucesión de posibles eventos, la probabilidad de que uno tenga lugar depende de que el anterior se realice. Se trata de cadenas de memoria, en las que los sucesos pasados condicionan los futuros. Con ello se pretende definir probabilidades de éxito ante sucesos que se pueden dar para cada estado o situación. Se busca predecir así cómo se va a comportar un sistema

Simulación de Monte Carlo

Herramienta cuantitativa estadística basada en la generación de variables aleatorias a partir de un patrón para resolver problemas numéricos. Mediante la sucesiva iteración de los comportamientos de un sistema real se busca la imitación del mismo, para llegar a predecir cómo va a evolucionar. Es fundamental definir correctamente las variables del sistema para llegar a reproducir su comportamiento y tratar de conseguir predecir cómo se comportaría ante los supuestos estudiados.

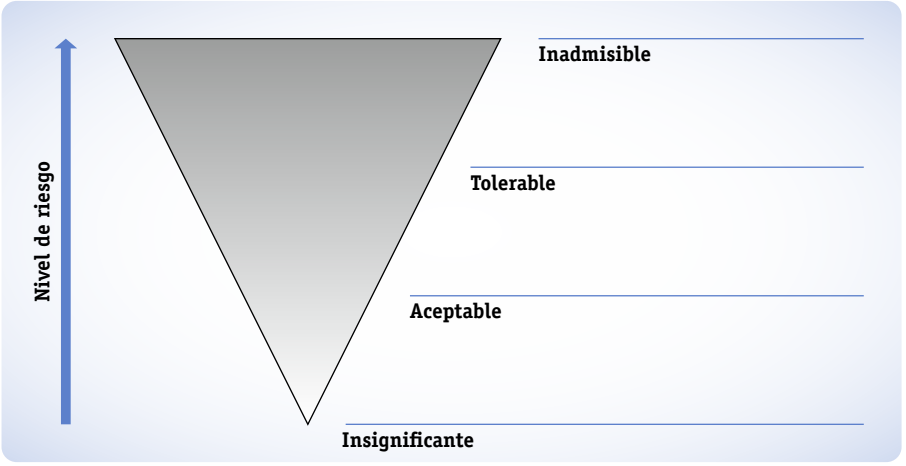
Estadística y redes Bayesianas

Los modelos probabilísticos de tipo bayesiano permiten clasificar, diagnosticar, o tomar decisiones a partir de la definición de las variables que conforman un sistema, y de las relaciones de dependencia que se pueden establecer entre dichas variables. Sería posible, incluso, inferir cómo se comportarían las variables desconocidas a partir del comportamiento de las que sí se conocen. Es fundamental el conocimiento previo que pueden aportar los expertos a la hora de definir tanto el sistema como las variables.

Curvas FN

Se trata de representaciones gráficas de la probabilidad de que una población se vea afectada por los efectos no deseados de un evento en concreto. Se basan en el diseño de curvas o «zanahorias ALARP (del inglés As Low As Reasonable Practicable», en las que se establece un modelo que contempla todo lo reducido que sea asumible razonadamente. Al aplicarse a riesgos que provocan daño a las personas, suelen definirse en forma de número de víctimas que provoca el suceso.

FIGURA 17. CURVAS FN



Fuente: elaboración propia

Índices de riesgo

Se trata de indicadores calculados a partir de datos históricos. Se busca definir cómo de posible es que suceda un evento, junto con los efectos que este evento pueda tener, y que supere el nivel de asunción de riesgo que proponga o acepte la entidad. Se pretende poner límite al impacto negativo que un evento tenga en el éxito de una organización. Un ejemplo podría ser el número de quejas telefónicas por un mal servicio en compras por internet. En la medida en que se supere el número de devoluciones previsto, quizás está fallando el empaquetado o el servicio de reparto. En todo caso, el número que se establece como límite a partir del cual se debe activar la revisión del proceso debe ser establecido con precisión, además de calcular el impacto negativo que tendría sobre la organización alcanzar este límite.

Matriz de consecuencia/probabilidad

También denominada matriz de probabilidad-impacto. Técnica analítica de carácter cualitativo que permite establecer los distintos niveles de riesgo que se pueden dar ante un cierto evento, junto con las probabilidades de que se den estos niveles y los efectos que éstos tengan sobre nuestra organización. La matriz está compuesta en un eje por los valores de probabilidad, y en el otro eje por los valores de impacto del riesgo sobre los objetivos de nuestra organización. Se trata de una herramienta visual y que permite establecer las prioridades en función del riesgo y el impacto que tendría para la organización.

Análisis de coste/beneficio (Cost Benefit Analysis, CBA, en inglés)

Técnica basada en el cálculo monetario de los beneficios y los costes que implica para la sociedad llevar a cabo un proyecto a lo largo de un período determinado. Se estudian sus alternativas posibles, para así poder compararlas, y poder tomar una decisión sobre qué proyecto de los analizados debe ser acometido. Este análisis incluye el VAN de acometer cada proyecto, descontando la inversión inicial y los rendimientos mínimo requeridos. Incluye, además de los costes propios imputables de forma directa al proyecto, aquellos costes y beneficios de carácter ambiental y social, debidamente cuantificados.

Análisis de decisión multicriterio (e inglés, Multi-Criteria Decision Analysis)

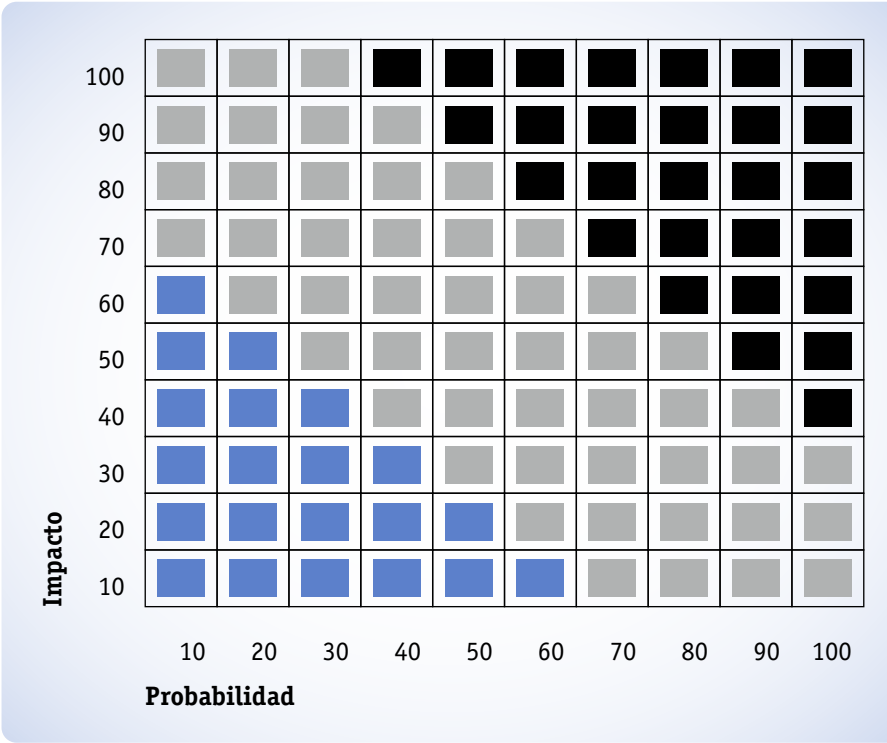
Herramienta que posibilita la evaluación y el estudio comparado de proyectos de forma estándar, con objetividad, sistemática y ponderaciones. Permite tener en cuenta diversos criterios individuales de tal forma que la solución propuesta final sea una opción satisfaciente, pero no óptima. Es decir, no se busca la optimización de todos los criterios a la vez

3 EL MAPA DE RIESGOS

La evaluación de los riesgos permite que los mismos sean finalmente clasificados o agrupados a través de herramientas tales como el mapa de riesgos. El mapa de riesgos es una herramienta que expone los distintos riesgos junto con su probabilidad de ocurrencia (cuantitativa o cualitativamente) y el daño potencial que puede ocasionar. Por tanto, al sintetizar esta información permite evaluar el nivel global de exposición de la organización a los distintos

riesgos. Habitualmente se representa de manera interactiva, de modo que al seleccionar cada uno de los riesgos se despliegue más información sobre los mismos (por ejemplo fuente que lo ocasiona, fuente de información, fecha de la última actualización, etc). La intersección del mapa de riesgos con la definición de apetito, tolerancia y capacidad de riesgo permite establecer y priorizar las áreas de actuación.

FIGURA 18. MAPA DE RIESGOS



Leyenda: Los colores (mapa de calor) azul, gris y negro representan respectivamente los niveles de apetito, tolerancia y capacidad de riesgo.
Fuente: elaboración propia.

El mapa de riesgos puede, por tanto, constituir el resumen global de los riesgos identificados tras su análisis. A continuación, es necesario establecer un tratamiento de los distintos riesgos, especialmente los que sean más relevantes. En la norma ISO 31000:2018 se establecen cinco alternativas: 1. No hacer nada, 2. Evaluar las opciones de tratamiento, 3. Analizar en mayor profundidad el riesgo, 4. Continuar con los mismos controles que se habían establecido o 5. Reconsiderar los objetivos que se persiguen.

4 TRATAMIENTO

4.1 Presentación

El proceso de gestión del riesgo tiene en el tratamiento del riesgo uno de los pasos clave: la toma de decisiones relativas al control del riesgo. En este punto, a la hora de acometer correctamente la toma de decisiones, será fundamental una correcta gestión de la información. Esto se logra a través de la definición y establecimiento de canales de comunicación entre los agentes implicados, de mecanismos de consulta ágiles y ajustados a los tiempos del proceso que se quiere controlar y de herramientas que permitan la monitorización de las actuaciones que se quieren revisar de forma continuada. Será, pues, a partir del análisis de la situación derivada de la información obtenida cuando se puedan determinar qué riesgos necesitan ser tratados, cuáles no, y el nivel de urgencia o prioridad que se les da a cada uno de ellos.

En el proceso de tratamiento del riesgo se incluye el diseño, la evaluación, la selección y la implementación de acciones con las que actuar sobre los riesgos existentes en la organización.

Para analizar y gestionar el riesgo de forma correcta y eficaz es necesario conocer de qué tipo de riesgo se trata, de dónde procede. Este es un aspecto clave para poder realizar el tratamiento de ese riesgo, así como para poder establecer los controles que lo acotarán a través de la definición de límites de variación para las variables consideradas relevantes.

Además, se deberá lograr un nivel de comunicación adecuado entre los agentes implicados en su gestión: el tratamiento del riesgo alcanzará sus objetivos si la información a analizar es relevante y pertinente, además de ser actualizada de forma constante en aquellos períodos de tiempo establecidos por los agentes.

La definición de los agentes responsables de ejecutar estas acciones de tratamiento y control del riesgo es otro de los elementos más importantes.

> Para definir correctamente los perfiles de las personas que ejecutarán el control de las medidas establecidas es necesario tener en cuenta no sólo el puesto que ocupa cada persona en la organización, sino también el tipo de información que maneja y los canales de información que tiene a su disposición.

Será clave, pues, que las personas responsables tengan acceso directo a la información que tienen que evaluar, así como canales de información por los que transmitir correctamente la toma de decisiones que derivan de los controles establecidos. Gracias al tratamiento del riesgo se estará en línea de mejora continua del modelo de gestión del riesgo.

El tratamiento de los riesgos implica las siguientes etapas: formulación de iniciativas para gestionar el riesgo; selección de las medidas adecuadas; programación, planificación e implementación de medidas; evaluación del éxito de las medidas llevadas a cabo; calificación del riesgo residual que no es posible eliminar como asumible o no asumible y propuesta de medidas a acometer para reducir el riesgo residual.

A la hora de optar por una de las distintas alternativas para el tratamiento del riesgo será fundamental analizar correctamente los aspectos positivos que tiene el llevar a cabo la estrategia seleccionada, junto con los costes, penalizaciones y aspectos negativos de la misma. Asimismo, no deben considerarse solamente los condicionantes económicos derivados de la decisión en la toma de decisiones, sino también deben incluirse los impactos que tenga la alternativa seleccionada sobre la propia estructura de la organización, en clave de alteración en las obligaciones o en los objetivos organizacionales. La ISO 31000:2018 indica que se debe consultar a los agentes interesados en la toma de decisiones y proponer las distintas alternativas que se están manejando, para tener en consideración el feedback generado a la hora de acometer la mejor estrategia en la organización para el tratamiento del riesgo en cuestión.

Las alternativas que se recogen en la ISO 31000:2018 para el tratamiento del riesgo se encuentran:

- Evitar aquellos riesgos que sea posible a través del cese de la actividad que lo origina o bien mediante el no acometimiento de un proceso o actividad que lo generaría.
- Actuar contra la fuente que origina el riesgo
- Mitigar los efectos negativos que genera el riesgo
- Actuar para minorar la probabilidad de que suceda el riesgo
- Asumir el riesgo porque se trata de una oportunidad para la organización, que está preparada para asumir sus efectos y éstos están debidamente estudiados. Se podría incluso asumir un aumento del riesgo para potenciar la señalada oportunidad.

- Transferir la gestión del riesgo a un agente externo a la organización (contratos/pólizas de seguros). Con ello se logra compartir el riesgo con un agente que nos da la cobertura necesaria para reducir el impacto negativo en caso de producirse.

- No hacer nada y aceptarlo. En este caso es clave disponer de una información correcta y ajustada a la realidad que vive la organización.

El resultado obtenido tras la selección de la mejor alternativa para el tratamiento del riesgo analizado puede no ser satisfactorio o lo suficientemente eficaz para la organización en su conjunto o para alguno de los agentes implicados en su gestión. Es por ello que para tratar de asegurar la efectividad de las medidas implementadas es necesario implementar un proceso de monitorización, control y revisión continuados.

La organización debe marcar de cerca el riesgo que quiere gestionar. Ello se consigue con una vigilancia constante de los indicadores establecidos para mantener el riesgo controlado. A través del control continuado se estará posibilitando el éxito del proceso de tratamiento del riesgo. La detección de un comportamiento anómalo de un indicador generará una alerta en el sistema de detección que conducirá a un escenario de alerta y de posible toma de decisiones por los agentes seleccionados.

Puede suceder que la implementación de las medidas no conduzca a una minoración del riesgo. En ese caso, es necesario un replanteamiento de las medidas acometidas, así como un análisis más profundo de las variables que definen ese riesgo.

4.2 Plan de tratamiento de riesgos

Para aplicar el plan de tratamiento del riesgo es necesario establecer o definir los distintos tipos de riesgos que pueden suceder en la organización, así como los indicadores que permitirán su control, el nivel de impacto que provocan estos riesgos en la organización en caso de suceder, la probabilidad de que éstos tengan lugar, el nivel de riesgo y el responsable de llevar a cabo la recepción de la información y su análisis, para la posterior toma de decisiones.

Todos estos datos se podrían incluir en una tabla de este tipo:

TABLA 10. PLAN DE TRATAMIENTO DE RIESGOS

Código identificativo del riesgo	Descripción del riesgo	Indicador	Área de Impacto	Impacto	Probabilidad de ocurrencia	Nivel de riesgo	Responsable o propietario	Controles
Se trata de un código interno de la organización que permite identificar el tipo de riesgo considerado	Breve definición del riesgo que se está considerando	Tipo de medida o valor que identifica el riesgo considerado.	Área de impacto en la que se puede encuadrar el tipo de riesgo considerado. Por ejemplo: Financiero, Contable, Reputacional, legal, salud y seguridad laboral, Ley de Protección de datos, etc.	El impacto podría definirse como la materialización del riesgo. Pueden establecerse diversos niveles en función de la afectación a la organización: Crítico, Alto, Medio o Bajo.	Definición de la posibilidad de ocurrencia. Ésta puede ser: Alta, Media y Baja. Es posible que la estimación de la probabilidad de ocurrencia se gestione a través de una metodología cualitativa, a partir de la consulta con los encargados o jefes de equipo	En función del impacto que tiene el riesgo considerado y la probabilidad de que suceda, es posible establecer el nivel que tiene para la organización. Éste puede ser considerado: Crítico, Alto, Medio o Bajo.	Cada tipo de riesgo debe tener un responsable que ejecute el control y las medidas establecidas relacionadas con la toma de decisiones. El propietario debe velar por el cumplimiento de la implementación de las medidas. El responsable debe tener acceso directo a la información y ésta debe ser de calidad, y en la medida de lo posible estar lo más actualizada posible.	Si una vez analizado el riesgo, se concluye que debe ser tratado por superar el nivel de riesgo aceptable previamente establecido

Fuente: elaboración propia

Una vez se establecen los controles a implementar, conviene elaborar una tabla resumen del plan de tratamiento del riesgo donde se recojan los responsables, el plazo concedido y los recursos asignados para llevar a cabo dichos controles.

TABLA 11. RESUMEN DEL PLAN DE TRATAMIENTO DE RIESGOS

Control a implementar	Actuación sobre los distintos tipos de riesgos	Responsable de la ejecución del control	Plazo de tiempo concedido para su implementación	Recursos asignados
Medida de control que busca corregir la situación de riesgo generada. Puede establecerse la misma medida para distintos tipos de riesgo que pueden estar relacionados.	Agrupación de los distintos riesgos en función de la medida de control definida en la columna anterior.	Persona sobre la que recae la responsabilidad de llevar a cabo la medida correctora o actuación correspondiente	Período de tiempo concedido para llevar a cabo la implementación de la medida correctora. Se relaciona con el tiempo con el que cuenta el responsable para transmitir la información referente al control a los agentes interesados o implicados.	Período de tiempo aproximado que es necesario para que los responsables de la implementación lleven a cabo la medida correctora.

Fuente: elaboración propia

El plan de tratamiento de riesgos permite definir: los controles a aplicar para tratar de contener el riesgo de la organización; el riesgo sobre el que se actúa; el responsable asignado, el plazo de implementación establecido para llevarlo a cabo, y los recursos necesarios para garantizar la gestión del riesgo.

5 SEGUIMIENTO Y REVISIÓN

El **seguimiento** y la **revisión** continua del plan del tratamiento del riesgo son la base para conseguir la efectividad del mismo.

Por **seguimiento** se entiende la consulta constante y actualizada del conjunto del plan de tratamiento del riesgo, centrándose sobre todo en el estado del criterio aplicado para el control del riesgo. El responsable de cada una de las fases por las que pasa la aplicación del criterio de control sobre el riesgo debe comprometerse con la resolución de la fase o realización de la tarea encomendada. Debe señalarse que la aplicación del criterio de control puede

implicar a más de un responsable, en función del organigrama de la organización o de la asignación de los procesos inmersos en el control. Podría tratarse de una asignación de responsabilidades en cadena, donde un objetivo de control general desencadena una serie de encomiendas en función de la estructura establecida en la empresa o propia del proceso. Pues bien, es clave que cada uno de los responsables asignados complete con éxito la tarea encomendada a su persona o cargo para que se pueda dar por exitosa y eficaz la aplicación del plan de tratamiento del riesgo.

La **revisión** continuada va de la mano del seguimiento y hace referencia a la comprobación exhaustiva del cumplimiento o no de lo establecido dentro del plan de tratamiento del riesgo. De nuevo, la revisión constante del proceso depende de la voluntad y compromiso para con la tarea del responsable asignado. En la medida en que el encargado realiza una revisión explícita y basada en criterios claros y definidos a través de una plantilla física o digital, se estará llevando a cabo una revisión correcta. Paralelamente es necesario definir el período temporal en el que se debe realizar la revisión (horas, días o semanas, por ejemplo). El aspecto temporal es uno de los elementos clave, ya que el cumplimiento de la tarea de revisión lleva implícito el hecho de realizarlo ajustándose a los tiempos marcados, tiempos que fueron definidos en base al correcto funcionamiento del proceso y al éxito del criterio de control establecido.

Mediante la aplicación de ambos, de forma planificada, es posible alcanzar la calidad en cuanto a la organización y a los distintos procesos que se llevan a cabo en la institución. Asimismo, se consigue una mayor eficacia en las tres fases de los procesos: diseño, implementación y alcance de los resultados.

El seguimiento y la revisión deben llevarse a cabo a lo largo de la totalidad de las etapas del proceso de gestión del riesgo. En todas ellas los responsables encargados de su aplicación están llamados a realizar tareas relacionadas tanto con la planificación y definición de procesos y personas encargadas de los mismos; con la recopilación, gestión y análisis de la información —que debe ser relevante y presentada en tiempo, además de ser actualizada—; con el registro de los resultados obtenidos —y que serán comparados con la puntuación objetivo— y con la generación de la debida retroalimentación dentro del proceso de gestión de riesgos —y que es clave para el sistema funcione y pueda mejorar constantemente gracias a la toma de decisiones relacionadas con la señalada gestión del riesgo—.

Los resultados derivados del seguimiento y la revisión están llamados a ser incorporados a la totalidad de las actividades relacionadas con la gestión del desempeño, medición e informe de la organización.

6 REGISTRO E INFORME

Registro e informe

La gestión del riesgo sólo tiene sentido y es efectiva si la organización la asume como propia e inherente a sus principios y procesos. Para lograr una gestión útil del riesgo es necesario que esté correctamente definida y **documentada**, en lo referente a los procesos, responsables y resultados. A ello hay que sumarle la importancia de **registrar** los hitos en términos de procedimiento y la **comunicación** de los resultados a través de los mecanismos y canales correspondientes.

Entre los objetivos que se buscan mediante el registro e informe, estarían:

- La comunicación de las actividades llevadas a cabo dentro de la gestión del riesgo
- La comunicación e información de los resultados del proceso de gestión del riesgo
- La generación de información relevante y en tiempo para favorecer la toma de decisiones
- La mejora continua de las actividades relacionadas con la gestión del riesgo
- Servir de apoyo a los responsables y a las partes interesadas, para la toma de decisiones y la posterior rendición de cuentas derivada de sus obligaciones

A la hora de crear, conservar y tratar la información, se debe hacer un esfuerzo por registrar aquella que sea relevante, permitiendo su acceso tanto en tiempo de toma de decisiones, para facilitarla, como posteriormente.

En este contexto, es clave establecer quién tiene acceso y cuándo lo tiene a la información, en función del grado de confidencialidad de la misma. El propio tratamiento del riesgo incluye una serie de controles y tareas a revisar con responsables asignados. Se pueden establecer al menos dos niveles de acceso: uno de ellos relacionado con la coyuntura, relacionado claramente con la toma de decisiones cuando procede, y un segundo instante relacionado con la revisión o el análisis de la estrategia llevada a cabo una vez se tomaron las decisiones.

A la hora de definir los **perfiles de acceso a la información documentada** es clave tener en cuenta el contexto interno de la propia empresa y el contexto externo.

Desde el punto de vista **interno** la comunicación de la información relativa a la gestión del riesgo entraña una cierta sensibilidad, por cuanto están siendo analizados o examinados distintos procesos internos de la organización que tienen sus responsables organizacionales que están viendo examinadas sus tareas o sus responsabilidades. Esto puede generar tensión entre la persona llamada a revisar el proceso en términos de gestión del riesgo y el trabajador/a de la organización. Por ello parece clave mantener la confidencialidad del registro de los datos objeto de análisis, así como la gestión que pueda derivar de la toma de decisiones al respecto. El acceso a esta información debe ser controlado en función del tipo de información que se maneje en cada procedimiento. Asimismo, el propio tratamiento del riesgo debe de ser concebido dentro la misión, visión y valores corporativos u organizacionales. En la medida en que el control del riesgo se asume como propio dentro del objetivo y valores de la propia organización se estará garantizando la utilidad y el éxito de la estrategia de control del riesgo. Ello permite, además, que la gestión del riesgo vaya empapando de forma transversal a todos los procesos y personas y partes interesadas de la compañía, y se perciba la propia gestión del riesgo como uno de los pilares de la organización. En la medida en que esto se consigue, el diseño de los modelos y procesos con los que se trabaja en la empresa llevarán incorporada la perspectiva del control del riesgo, y la cultura empresarial que se transmite a los trabajadores/as incluirá un compromiso con la gestión del riesgo de la entidad que será clave para alcanzar los objetivos empresariales fijados.

Desde el punto de vista **externo**, la comunicación derivada de la gestión del riesgo es un activo con el que se puede potenciar la imagen de la compañía. Para ello hay que considerar lo que pueden estar esperando de la organización los distintos *stakeholders* en materia de riesgos. La compañía debe ser consciente que el hecho de comunicar al exterior algo que tenga que ver con el concepto de «riesgo» es algo muy sensible. Cualquier error de comunicación en este sentido puede afectar a su imagen de marca muy negativamente. El error puede derivar tanto de una comunicación por exceso de información, por defecto o por una redacción incorrecta o improcedente. Por ello, la compañía debe prestar especial atención a qué es lo que comunica, cómo lo presenta al exterior y para qué lo comunica (el objetivo que busca con ello).

La correcta y exitosa gestión del riesgo reside en la generación en tiempo y forma de los informes correspondientes desde los responsables a las partes interesadas. El informe se puede entender como uno de los pilares de la

gobernanza de la organización. Disponer de informes relevantes contribuye a la mejora de la calidad del diálogo con las partes intervinientes o interesadas. Facilita las tareas de la alta dirección y de los distintos órganos de supervisión y control a cumplir con las tareas encomendadas y responsabilidades. A la hora de elaborar los informes se deben tener en cuenta distintos elementos, entre otros:

- A quién va dirigido el informe y qué información contiene. Se debe tener en cuenta las partes interesadas a quienes va dirigido, en cuanto al origen y destino de la información, para ajustar su contenido a lo realmente relevante. Eliminar información superflua permite la concentración en el problema a resolver y eliminar distracciones que puedan interferir en la toma de decisiones. Pero es fundamental que el informe contenga toda la información necesaria. La ausencia de información sensible puede condicionar muy negativamente la toma de decisiones.

- El coste del informe. La organización debe valorar el coste de realización de cada informe. Para ello se debe incluir la dedicación en horas, de personas intervinientes y de recursos materiales que implique la generación del informe. Habría que incluir además el coste de oportunidad de no realizarlo: qué impacto tendría en la organización no contar con ese informe. En función de todo ello habría que decidir si llevar a cabo ese informe o no.

- La frecuencia del informe. Como se comentó anteriormente, hay que tratar de centrar la atención del responsable y de las partes interesadas en la información clave o fundamental. La ausencia de «ruido» es uno de los elementos más importantes a tener en cuenta a la hora de la toma de decisiones. En este sentido, limitar el número de informes a los realmente necesarios, ni por exceso ni por defecto, resulta clave para facilitar la tarea de las partes interesadas y de la gobernanza.

- Tiempos del informe. El «cuándo» disponer de los informes condiciona positiva o negativamente no sólo el proceso de gestión del riesgo en lo relativo a la toma de decisiones y aplicación correcta de los controles establecidos, sino que también en cuanto a la buena gobernanza de la entidad y a la mejora continua de la organización en su conjunto. Para que el «engranaje» funcione correctamente tanto las personas encargadas de realizar el informe como aquellas encargadas de recibirlo y analizarlo deben cumplir con los tiempos asignados para cada una de las tareas. En la medida en que los informes son elaborados y recibidos en tiempo, las partes interesadas pueden tomar las decisiones oportunas a la vista de la

información generada por el procedimiento: información que fue definida como clave, relevante y necesaria a la hora de poder gestionar oportunamente los riesgos de la organización.

- Método del informe: Cada organización definirá el método elegido para la realización de los informes. La definición del tipo de información que debe contener cada informe condicionará el método aplicado. Puede haber informes objetivos, cuyo análisis o contenido se basa en el establecimiento de una serie de reglas objetivas. También pueden elaborarse informes subjetivos, que incluyen la valoración subjetiva del responsable a la vista de la información analizada y que puede/debe estar contenida en el propio informe para servir de apoyo a la parte interesada en materia de gobernanza.

- Pertinencia de la información con respecto a los objetivos de la organización: Si bien los objetivos empresariales estratégicos son los propios que marca el consejo de dirección, como el control del riesgo debería de estar incluido en las propias políticas internas de la organización y en su ideario (misión, visión y valores), se podría afirmar que los informes deben incluir la referencia al cumplimiento de aquellas secciones o tareas al que dicho informe responda. En la medida en que el informe facilita la tarea del responsable de la sección asignada, se estará contribuyendo al cumplimiento de los objetivos de la sección, y con ellos, al de la organización.

- Pertinencia de la información con respecto a la toma de decisiones: La información que contiene cada informe vendrá condicionada por el destinatario del mismo. De esta forma probablemente no se necesite el mismo informe si se trata de un jefe de equipo o controlador de proceso que si se trata de un encargado de gobernanza. En la medida en que cada informe se ajuste al perfil del puesto llamado a tomar decisiones, se estará contribuyendo a la gestión eficiente del riesgo.

La comunicación de la gestión del riesgo es clave de cara al exterior de la empresa. Los *stakeholders* y partes interesadas valoran positivamente toda información relativa a cómo gestiona los riesgos la entidad. Como ya se apuntó la información a transmitir debe ser exacta, se debe cuidar la redacción, se deben evitar posibles interpretaciones incorrectas derivadas de expresiones no acertadas y el lenguaje ha de ser claro y conciso. Esta comunicación se puede vehicular a través de un documento corporativo denominado «Política de control y gestión de riesgos». A través de este documento, la organización debe transmitir una imagen positiva en lo referente a la identificación de los riesgos que le afectan, cómo los gestiona para reducir su posible impacto, cuáles son sus

principios básicos para una correcta gestión del binomio riesgo-oportunidad aceptando un nivel de riesgo tal que haga posible el cumplimiento de los objetivos de la entidad, junto con la definición de las distintas políticas específicas para los riesgos que afecten a su actividad.

Con el documento en el que se recoge la «Política de control y gestión de riesgos» se busca proponer los principios básicos junto con el marco de actuación encaminado para el control y la gestión de los distintos riesgos a los que se enfrenta la entidad, y que deberán aplicarse atendiendo a la identidad corporativa de la organización

La mejora continua

Una vez alcanzado este punto, se habrán incorporado en la organización los distintos procesos necesarios para una correcta gestión del riesgo, y es momento de replantear todo el sistema propuesto. Tras el proceso realizado se dispone de un mayor conocimiento de la organización, así como de los procesos y el sistema que se ha puesto en práctica. El objetivo de este punto es mejorarlo. Es más, el sistema de gestión de riesgo sólo es útil, eficaz y eficiente si cumple su función y se revisa con cierta periodicidad, replanteándose lo previamente establecido y prestando atención a los cambios que hayan podido suceder y que puedan condicionar a la organización.

La actualización y mejora del sistema de gestión de riesgos permite eliminar o mejorar aquellos elementos que no estén funcionando correctamente o que necesiten una de una actualización, por haberse modificado las condiciones iniciales, los supuestos y definiciones de partida o los objetivos de la empresa. Asimismo, es fundamental y clave continuar identificando (proactivamente) los nuevos riesgos o peligros que puedan ir surgiendo con el desarrollo y continuación de la actividad empresarial.

No se trata de comenzar desde cero, ni mucho menos! El sistema ya está creado y está funcionando. Se trata de aprovechar la propia experiencia y el aprendizaje que se genera tras la implantación del sistema de gestión de riesgos para que sea más eficaz y alcance sus objetivos de manera más eficiente. De esta forma, podemos replantearnos si tras un primer período de funcionamiento:

- la organización y sus equipos están comprometidos, formados y satisfechos en la gestión de riesgos,

- se continúan evaluando los riesgos, buscando la identificación de nuevos riesgos y fuentes de los mismos,
- el plan de tratamiento necesita de incluir o modificar algún elemento para acomodarse mejor a la realidad de la organización
- los riesgos se tratan conforme a lo establecido en el plan de tratamiento,
- los procesos funcionan correctamente y sus funciones son eficaces,
- se cumplen los procedimientos e instrucciones definidos
- las partes interesadas contribuyen al sistema de la gestión de riesgos, si cumplen con sus tareas, si ha habido algún cambio en ellas, si se ha incorporado alguna nueva parte interesada
- la revisión y el seguimiento se realizan correctamente, o necesitan de alguna corrección para acomodarlo mejor a la organización,
- el registro e informe cumplen su función y recogen lo que sucede en la empresa en cuanto a gestión de riesgos, o es necesaria alguna mejora para adaptarlo mejor a la organización.

En la medida en que la organización y su personal interiorizan la gestión del riesgo como una parte más de su día a día, y entienden la necesidad de actualización y mejora continua del mismo se estará protegiendo correctamente el sistema de generación de valor. Se debe motivar a todo el personal, sean directivos, encargados de equipos y/o trabajadores, a que verbalice y explicite a través de los canales apropiados aquellos posibles cambios que detecten en la realidad de la empresa y su entorno en cuanto a los riesgos percibidos. De esta forma se estará consiguiendo la mejora continua del sistema de gestión de riesgos, y con ello, la protección de la organización para hacerla más fuerte, viable y sostenible.

7 MODELOS Y PLANTILLAS

TABLA 12. EJEMPLO DE PLANTILLA DE PLAN DE TRATAMIENTO DE RIESGOS

Código identificativo del riesgo	Descripción del riesgo	Indicador	Área de Impacto	Impacto	Probabilidad de ocurrencia	Nivel de riesgo	Responsable o propietario	Control	Responsable de la ejecución del control	Plazo de tiempo concedido para su implementación	Recursos asignados	Otra información

Fuente: elaboración propia

TABLA 13. EJEMPO DE TABLA DAFO

Fuente	Tipo	Ítem
Análisis interno	Fortalezas	Fortaleza 1.
	Fortalezas	Fortaleza 2.
	…….	……
	Debilidades	Debilidad 1
	Debilidades	Debilidad 2
	…….	……
Análisis externo	Oportunidades	Oportunidad 1
	Oportunidades	Oportunidad 2
	……	
	Amenazas	Amenaza 1
	Amenazas	Amenaza 2
	……	

Fuente: elaboración propia

TABLA 14. EJEMPLO DE TABLA DE APOYO PARA LA ELABORACIÓN DEL MAPA DE RIESGOS

Riesgo	Impacto	Probabilidad	Otra información (control, responsable, área, código identificativo)
……	……	……	……

Bibliografía

Allianz Risk Barometer (2020a). Identifying the major business risks for 2020. Allianz Global Corporate & Specialty.

— (2020b). Results Appendix 2020. Allianz Global Corporate & Specialty.

Carmona-Badía, X. y Dios-Vicente, A. (2020). Mortalidad empresarial en galicia 1972-2008. Factores de impacto y gestión del riesgo. 1.ª edición. ISBN: 978-84-09-23870-5. Fundación INADE, Instituto Atlántico del Seguro (Vigo).

Community of Insurance. (2020). INFORME Covid-19: Impacto y perspectivas para la industria aseguradora. Recuperado de: https://communityofinsurance.es/2020/04/19/covid-19-impacto-y-perspectivas-para-el-seguro/

Edwards, D. W. (1989). Calidad, productividad y competitividad: la salida de la crisis. *Ediciones Diaz Santos*, *412*.

Otero et al. (2015). La gestión del riesgo y el seguro en la empresa gallega. ISBN: 978-84-608-2136-6. Fundación INADE, Instituto Atlántico del Seguro (Vigo).

Más información

Casares-San José-Martí, I. y Lizarzaburo-Bolaños, E.R. (2016). Introducción a la Gestión Integral de Riesgos Empresariales Enfoque: ISO 31000. ISBN: 978-612-47172-2-2. Platinum editorial S.A. (Lima, Perú).

Dallas, M., (2013). Management of Risk: Guidance for Practitioners and the international standard on risk management, ISO 31000: 2009. White Paper, http://www. best-management-practice. com/gempdf/management_of_risk_guidance_for_practitioners_and_the_international_standard_on_risk_management_iso31000_2009. pdf, accesat la, 5, 2015.

Para la búsqueda de normas ISO es posible utilizar el buscador https://www.aenor.com/Buscador