Norma ISO 31000

El valor de la gestión de riesgos en las organizaciones

Índice

1. ¿De dónde viene la norma ISO 31000?

La Gestión de Riesgos en las empresas nace en la década de los 60. Ante la tecnificación y modernización de ciertos procesos que hasta ese momento se habían desarrollado de forma manual, en muchos sectores se puso de manifiesto la necesidad de realizar un mejor control de las actividades. La tecnología supuso mayor agilidad y calidad, pero a la vez nuevos retos de control y seguimiento.

A partir de esos años se publicó la primera literatura al respecto. Los sectores que más contribuyeron a la consolidación del concepto fueron el asegurador, el tecnológico, el militar y el de la ingeniería náutica y nuclear.

Sin embargo, sólo **en la segunda mitad de los años 70 la Gestión de Riesgos entró de lleno a las empresas.** Esto se debió a la aparición de las primeras normas y estándares internacionales. Quizá el más significativo fue el código de seguridad nuclear que hizo público la US Nuclear Regulatory Comission, el cual intentaba minimizar los riesgos a los que estaba expuesto el sector nuclear estadounidense.

La asimilación del término acabó de completarse gracias la difusión de otras normas al respecto, como por ejemplo el COSO, código emitido por el Comité de Organizaciones Sponsor en 1991 y que incluía prácticas para la gestión interna del riesgo. Dos años más tarde, Australia y Nueva Zelanda publicaron la norma AS/NZ 4360 sobre el riesgo en sus empresas públicas, mientras en 2002 el Insti-

tuto Británico de Gestión de Riesgos hizo público el estándar IRM. Por otro lado en el año 2002 con la finalidad de evitar fraudes y riesgo de bancarrota nace en Estados Unidos la Ley Sarbanes Oxley con el fin de monitorear a las empresas que cotizan en bolsa de valores, evitando que la valorización de las acciones de las mismas sean alteradas de manera dudosa, mientras que su valor es menor.

1.1 La norma ISO 31000: unificación de criterios

Sin embargo, estos estándares y normas internacionales tenían dos problemas en el terreno práctico: el primero, que casi todos estaban dirigidos a empresas de sectores específicos, lo cual reducía su impacto y extensión; y el segundo, que había una notoria disparidad de criterios a la hora de desarrollarlos.

Estos dos elementos motivaron a **la Organización Internacional de Normalización (ISO) a elaborar una norma que abordara la Gestión de Riesgos de forma global, necesidad que en 2009 dio origen a la norma ISO 31000.** Sin embargo, pese a su alcance genérico, es una norma no certificable; son las empresas las que se acogen voluntariamente a sus directrices en el área de Gestión de Riesgos.

Se trata de **un estándar que puede aplicarse a cualquier tipo de organización,** más allá de su naturaleza, actividad, escenario comercial o tipo de producto, entre otros factores. A través de una serie de directrices y principios, la norma busca que cada empresa implemente un Sistema de Gestión del Riesgo para reducir los obstáculos que impiden la consecución de sus objetivos, siendo compatible con cada sector.

2. Definición del riesgo empresarial y principales tipos

2.1 ¿Qué es el riesgo empresarial?

Toda actividad empresarial lleva implícito un riesgo. Algunas en mayor medida que otras, pero ninguna se encuentra exenta. El riesgo es parte de cualquier área de negocio, pues en cierta forma lo define y ayuda a ponerle límites.

En el plano corporativo, **el riesgo se define como la incertidumbre que surge durante la consecución de un objetivo.** Se trata, en esencia, circunstancias, sucesos o eventos adversos que impiden el normal desarrollo de las actividades de una empresa y que, en general, tienen repercusiones económicas para sus responsables.

Proveniente del italiano *risicare* (en español: desafiar, retar, enfrentar), de modo que al concepto también se le asocia a toda probabilidad de pérdida. Otros sinónimos con los que suele guardar una relación directa son los de peligro, amenaza, perjuicio o daño.

Esto no quiere decir que todos los elementos que enmarcan la actividad comercial de las empresas sean riesgos en sí mismos. Por el contrario, existen ciertas características esenciales que los definen como tal:

- Debe estar asociado, de alguna manera, a la actividad de la empresa.
- Son complejos, no tienen una solución inmediata.
- Su impacto debe ser significativo.
- Entorpecen, obstaculizan, dificultan o postergan procesos.

2.2. Principales tipos de riesgos empresariales

2.2.1 Según el tipo de actividad

Los riesgos están presentes en cualquier actividad. Sin embargo, algunos implican un mayor o menor nivel de incidencia sobre las actividades de las empresas. Una primera clasificación de los mismos puede hacerse en los siguientes términos:

- **Riesgo sistemático:**

  Se refiere a aquellos riesgos que estén presentes en un sistema económico o en un mercado en su conjunto. Sus consecuencias pueden aquejar a la totalidad del entramado comercial, como sucede, por ejemplo, con las crisis económicas de gran envergadura y de las cuales ninguna compañía puede sustraerse. También pueden ser originados por accidentes, guerras o desastres naturales.

- **Riesgo no sistemático:**

  Son los riesgos que se derivan de la gestión financiera y administrativa de cada empresa. Es decir, en este caso la que falla es una compañía en concreto y no el conjunto del mercado o escenario comercial. Varían en función de cada tipo de actividad y cada caso, al igual que la manera en que son gestionados. Las situaciones de crisis internas o un plan de crecimiento mal implementado son algunos ejemplos.

2.2.2 Según su naturaleza

Pero los riesgos también pueden definirse en función de su naturaleza. De hecho, es la manera más extendida a la hora de clasificarlos. Está claro que un riesgo de tipo legal o jurídico no debe tener la misma gestión que otro de tipo económico. En ese sentido, la clasificación de los riesgos quedaría de la siguiente manera:

- **Riesgos financieros:**

  Son todos aquellos relacionados con la gestión financiera de las empresas. Es decir, aquellos movimientos, transacciones y demás elementos que tienen influencia en las finanzas empresariales: inversión, diversificación, expansión, financiación, entre otros. En esta categoría es posible distinguir algunos tipos:

  - Riesgo de crédito.
  - Riesgo de tasas de interés.
  - Riesgo de mercado.
  - Riesgo gestión.
  - Riesgo de liquidez.
  - Riesgo de cambio.

- **Riesgos económicos:**

  En este caso, se refiere a los riesgos asociados a la actividad económica, ya sean de tipo interno o externo. En el primer caso, hablamos de las pérdidas que puede sufrir una organización debido a decisiones tomadas en su interior. En el segundo, son eventos cuyo origen es externo. Para diferenciarlo del ítem anterior, es preciso señalar que el riesgo económico afecta

básicamente a los beneficios monetarios de las empresas, mientras que los financieros tienen que ver con todos los bienes que tengan las organizaciones a su disposición.

- **Riesgos ambientales:**

  Son aquellos a los que están expuestas las empresas cuando el entorno en el que operan es especialmente hostil o puede llegar a serlo. Tienen dos causas básicas: naturales o sociales. En el primer grupo podemos mencionar elementos como la temperatura, la altitud, la presión atmosférica, las fallas geológicas, entre otros. En el segundo, cuestiones como los niveles de violencia y la desigualdad. Sea como sea, lo cierto es que son riesgos que no dependen de las empresas y que, por tanto, su gestión requiere de planes preventivos más eficaces.

- **Riesgos políticos:**

  Este riesgo puede derivarse de cualquier circunstancia política del entorno en el que operen las empresas. Los hay de dos tipos: gubernamentales, legales y extralegales. En el primer caso se engloban todos aquellos que son el resultado de acciones que han sido llevadas a cabo por las instituciones del lugar, por ejemplo un cambio de gobierno o una modificación en las políticas comerciales. En el segundo caso, se sitúan actos al margen de la ley como acciones terroristas, revoluciones o sabotajes.

- **Riesgos legales:**

  Se refiere a los obstáculos legales o normativos que pueden obstaculizar el rol de una empresa en un sitio determinado. Por ejemplo, en algunos países operan leyes restrictivas en el mercado que limitan la acción de ciertas compañías. Estos riesgos van generalmente ligados a los de carácter político.

Normalmente atendiendo a la naturaleza de los riesgos empresariales suele distinguirse entre riesgos puros y riesgos especulativos.

El riesgo puro se define como la incertidumbre de que acontezca un determinado suceso que ocasiona una pérdida económica. Por su parte, el riesgo especulativo se define como la incertidumbre de que ocurra un determinado suceso cuya ocurrencia produciría la materialización de una expectativa de beneficio o pérdida, indistintamente.

En consecuencia, el riesgo puro es aquél del que sólo puede derivarse un daño en caso de ocurrencia y, por tanto, una pérdida económica. Por el contrario, en el riesgo especulativo existe la incertidumbre, respecto al propio suceso, de que pudiera producirse indistintamente un beneficio o una pérdida.

En general, esta distinción es bastante significativa, ya que la cobertura financiera de los riesgos procurada por la institución aseguradora atiende generalmente a los riesgos puros. Los riesgos especulativos son asumidos habitualmente por el em-

presario en función de su conocimiento y quedan fuera del marco asegurador, si bien actualmente existe un cierto acercamiento del seguro a determinadas parcelas de riesgos especulativos. Dentro de los riesgos puros, con relación a los peligros desencadenantes de estos riesgos pueden distinguirse tres grandes áreas:

- Riesgos personales.
- Riesgos de daños materiales sobre las propiedades.
- Riesgos de responsabilidad civil.

3. ¿En qué consiste la norma ISO 31000?

La norma **ISO 31000 es una herramienta que establece una serie de principios para la implementación de un Sistema de Gestión de Riesgos en las empresas.** Como se dijo antes, puede aplicarse a cualquier tipo de organización independiente de su tamaño, razón social, mercado, fuente de capital, espectro comercial o forma de financiación. No especifica ningún área o sector en concreto.

La norma parte del hecho de que todas las empresas, en mayor o menor medida, llevan a cabo prácticas para la gestión de los riesgos. La diferencia radica en la coordinación y alineamiento de dichas prácticas.

Aunque no es certificable, el estándar busca minimizar, gestionar y controlar cualquier tipo de riesgo, más allá de su naturaleza, causa, origen o grado de incidencia. Esto se logra a través de la integración del Sistema de Gestión de Riesgos a la estrategia de cada organización, así como a sus procesos, políticas y cultura.

De hecho, no es una norma pensada para circunstancias concretas, sino que busca una aplicación continua y permanente en el tiempo. De esta manera, beneficia el grueso de las acciones, decisiones, operaciones, procesos, funciones, proyectos, servicios y activos que tengan lugar en las empresas.

3.1 Partes de la norma ISO 31000:

Para una mejor comprensión de sus principios y directrices, la norma ISO 31000: 2009 divide su contenido en tres áreas básicas:

1. Principios y directrices:

La norma ISO 31000 sirve de referencia para otros estándares sobre Gestión de Riesgos. Además, complementa la información de diversas normativas en el plano local, regional, nacional o incluso continental. En este primer apartado, se explica no sólo el alcance de la misma, sino que se detallan las prácticas básicas que debe tener en cuenta cualquier organización dispuesta a implementar un Sistema de Gestión de Riesgos. Los 11 principios expuestos son:

- La gestión crea valor a la organización.
- Debe estar integrada a los procesos.
- Forma parte de la toma de decisiones en la empresa.
- Trata de forma explícita la incertidumbre.
- Debe ser sistemática, estructurada y adecuada.
- Es necesario que esté basada en la mejor información disponible.
- Debe adaptarse a la medida de cada caso.
- Implica la inclusión de factores humanos y culturales.
- Debe ser transparente, eficaz e inclusiva.
- Es necesario que sea iterativa y sensible al cambio.
- Tiene que ir orientada a la mejora continua de la organización.

2. Gestión de riesgos:

La norma ISO 31000 define la Gestión de Riesgos como todas aquellas acciones coordinadas para dirigir y controlar los riesgos a los que puedan estar abocadas las organizaciones. En este segundo apartado, el objetivo es trazar un marco de acción para saber qué aspectos gestionar y cómo hacerlo. La gestión tiene que ver, sobre todo, con la cuantificación de los riesgos, para lo cual es fundamental definir dos elementos dentro de este proceso:

- Consecuencia:

La norma define la consecuencia como los efectos o aquellos elementos que se derivan directa o indirectamente de otros. En este caso, se trata de evaluar los riesgos que cumplen con la premisa de causa-efecto. Es cierto que no siempre se pueden prever las consecuencias de una acción o decisión, pero este solo acto es el origen de cualquier Sistema de Gestión de Riesgos. Sin un mínimo grado de consecuencia, cualquier acción en la materia resultará insuficiente.

- Probabilidad:

Este segundo término habla de la posibilidad de que un hecho se produzca. Para la Gestión de Riesgos, es fundamental que las empresas contemplen la irrupción de hechos que puedan derivarse o no de las decisiones de la empresa. Nunca se está del todo preparado para los acontecimientos, sobre todo si éstos provienen de factores externos, pero el sólo hecho de pensar en su materialización ya es un buen indicador de la Gestión de Riesgos.

3. Vocabulario de gestión:

Finalmente, en esta última parte la norma ISO 31000 plantea un conjunto de conclusiones sobre la implementación de un Sistema de Gestión de Riesgos. En este sentido, complementa la información de los dos apartados anteriores con un glosario especializado en esta materia. Si el proceso se lleva a cabo siguiendo los principios básicos, los resultados a obtener serán los siguientes:

- Mejorar la identificación de oportunidades y amenazas.
- Optimizar la gestión empresarial.
- Aumentar la confianza en los grupos de interés (stakeholders).
- Establecer una base para la toma de decisiones.
- Mejorar los controles y los métodos de seguimiento y monitoreo.
- Optimizar la prevención y la gestión de incidentes.
- Minimizar las pérdidas asociadas a los procesos empresariales.
- Fomentar el aprendizaje organizativo en todos sus niveles.

4. Metodologías de análisis de riesgos

Dado que los riesgos no tienen el mismo origen ni la misma naturaleza, existen varias estrategias para su gestión. Sin embargo, otros factores que inciden significativamente son el tamaño de las empresas, su número de integrantes, su estructura, la actividad de producción y el sector en el que operan.

Esto ha propiciado que se desarrollen **metodologías de análisis propias de un sector o especialidad.** Su objetivo es la identificación, evaluación, tratamiento y monitorización de los riesgos asociados a una actividad, función o proceso. Es decir, es lo que da forma a la implementación del sistema de gestión en sí mismo.

Sin embargo, es importante dejar claro que las metodologías de análisis de riesgos se dividen en dos grupos principales:

a) Metodologías de gestión del riesgo:

Son aquellas que están orientadas a la identificación, evaluación y el posterior tratamiento de los riesgos derivados de una actividad. Entre ellas está, como es obvio, la norma ISO 31000. También se encuentran otros estándares, como por ejemplo la norma AS/NZS 4360, que plantea un modelo de análisis centrado en los principios de la familia normativa ISO 9000.

Otras de las metodologías más reconocidas son el sistema APPCC (Análisis de Peligros y Puntos Críticos de Control) y el método del ARO (Administración del Riesgo Operacional), los cuales operan en el mismo sentido.

b) Metodologías de cuantificación:

En este caso, se trata de aquellas herramientas que se enfocan exclusivamente en la cuantificación de los riesgos. Es decir, aplican una serie de indicadores (de carácter numérico casi siempre) para medir el impacto que tienen los riesgos en las organizaciones y, a partir de ese cálculo, elaborar acciones coordinadas para su gestión, tratamiento o, incluso, eliminación.

- **Magerit:** se trata de una metodología de análisis y gestión de riesgos que ha sido elaborada por el Consejo Superior de Administración. Está específicamente diseñada para las compañías que trabajen con información digital y servicios de tipo informático. Su función principal es evaluar cuánto valor pone en juego una compañía en un proceso y cómo protegerlo. También ayuda a la planificación de tratamientos oportunos y a preparar a las organizaciones de cara a procesos de auditoría, certificación o acreditación.
- **Delphi:** es un método orientado a conocer la opinión de expertos. En un primer momento, un grupo de especialistas anónimos responde a un cuestionario que elabora una organización sobre un tema específico, en este caso la Gestión de Riesgos. Tras analizar los resultados, los responsables piden su opinión a cada uno de los integrantes del grupo. Finalmente, la empresa elabora un segundo cuestionario, aunque éste con preguntas más precisas y focalizadas. La idea es que al final se elabora un texto con las conclusiones.

Métodos Cualitativos

Es el método de análisis de riesgos más utilizado en la toma de decisiones en proyectos empresariales, los emprendedores se apoyan en su juicio, experiencia e intuición para la toma de decisiones.

Se pueden utilizar cuando el nivel de riesgo sea bajo y no justifica el tiempo y los recursos necesarios para hacer un análisis completo.

O bien porque los datos numéricos son inadecuados para un análisis mas cuantitativo que sirva de base para un análisis posterior y más detallado del riesgo global del emprendedor.

Los métodos cualitativos incluyen:

- Brainstorming
- Cuestionario y entrevistas estructuradas
- Evaluación para grupos multidisciplinarios
- Juicio de especialistas y expertos (Técnica Delphi)

Métodos Semi-cuantitativos

Se utilizan clasificaciones de palabra como alto, medio o bajo, o descripciones más detalladas de la probabilidad y la consecuencia.

Estas clasificaciones se demuestran en relación con una escala apropiada para calcular el nivel de riesgo.

Se debe poner atención en la escala utilizada a fin de evitar malos entendidos o malas interpretaciones de los resultados del cálculo.

Métodos Cuantitativos

Se consideran métodos cuantitativos a aquellos que permiten asignar valores de ocurrencia a los diferentes riesgos identificados, es decir, calcular el nivel de riesgo del proyecto.

Los métodos cuantitativos incluyen:

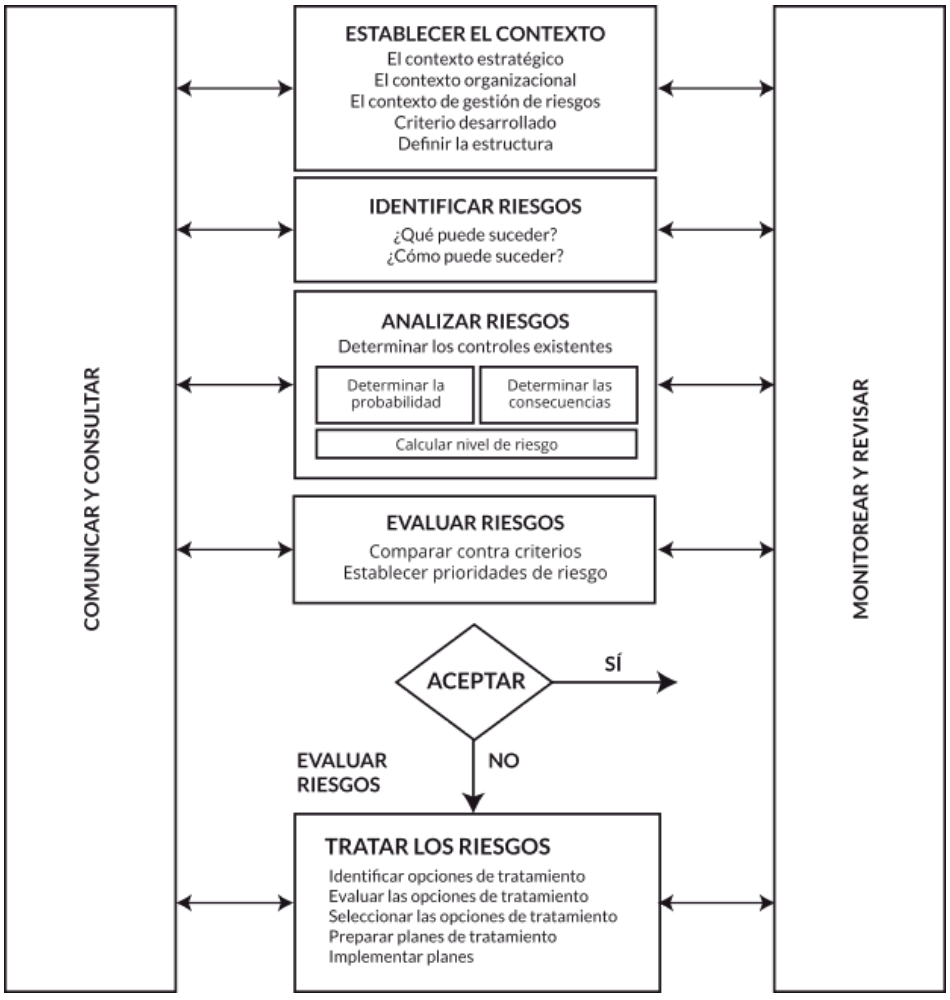
- Análisis de probabilidad
- Análisis de consecuencias
- Simulación computacional

El desarrollo de dichas medidas puede ser realizado mediante diferentes mecanismos, entre los cuales destacamos el Método Montecarlo, el cual se caracteriza por:

- Amplia visión para mostrar múltiples posibles escenarios
- Sencillez para llevarlo a la práctica
- Computerizable para la realización de simulaciones

5. Proceso de gestión de riesgos

La norma ISO 31000 tiene un enfoque de procesos. La implementación de un Sistema de Gestión de Riesgos, por tanto, debe seguir una serie de pasos para que sea eficaz y cumpla con los objetivos trazados al inicio. Los pasos básicos son:



1. Definición de objetivos:

En esta primera etapa se definen los objetivos del proceso. Es decir, se deja claro qué es lo que se busca con la implementación del Sistema de Gestión de Riesgos y cuál debe ser el alcance del mismo. La dirección de la empresa debe ser la instancia con más alto grado de implicación en la difusión de estos objetivos, pues de lo contrario no logrará que el resto de niveles se comprometan del modo deseado. Pero no sólo se apoya en una buena difusión. También es preciso definir un presupuesto y destinar los recursos necesarios para la materialización del plan de riesgos.

2. Nombramiento de responsables:

A continuación, la dirección debe delegar la coordinación de las labores de Gestión de Riesgos en uno o más responsables. Esto dependerá del tamaño de cada organización y del número de sus empleados. Sea como sea, lo único cierto es que la estrategia debe involucrar a las distintas personas en el proceso.

Aunque la empresa tenga muchos trabajadores y departamentos, lo más recomendable es que los grupos de trabajo no superen los 10 miembros. Cuando esto sucede, tienden a la descentralización excesiva de funciones y los procesos se dilatan. Para las empresas pequeñas, el grupo no debe exceder los 5 miembros.

Hay dos maneras de nombrar a los responsables de un proyecto de Gestión de Riesgos:

- **Personal interno:**

  Lo más usual en estos casos es que el personal delegado para tales tareas sea de la propia organización. Si es así, la dirección tiene la garantía de que conocen el área sobre el que se realiza la evaluación. De hecho, puede recurrir a aquellos cargos que tengan una visión más o menos global de los procesos.

- **Personal externo:**

  Cuando la empresa es demasiado pequeña o no tiene la capacidad ni la formación para llevar a cabo estas tareas, la dirección puede apoyarse en los servicios de una consultora. Sin embargo, la desventaja de esta opción es que requiere de una labor previa de empalme en la que el personal que realizará la evaluación se pone al día en todo lo relacionado a la Gestión de Riesgos.

3. Identificación de los riesgos:

A través de reuniones entre los diversos responsables, la empresa debe definir cuáles son los factores que influyen en los procesos. Y de todos esos, es preciso priorizarlos en función del impacto que tengan. Recordemos que en un proceso no todas las acciones tienen el mismo grado de importancia. Una buena manera de medir el impacto de un riesgo es a través de la siguiente tabla de valores:

a) ¿A qué área de la empresa afecta?

b) ¿Cómo la afecta?

c) ¿Qué efectos tiene sobre dicha área?

d) ¿Qué efectos tiene sobre la organización en su conjunto?

e) ¿Qué margen de maniobra otorga?

f) ¿Qué tiempo de reacción permite a la dirección?

g) ¿Qué grado de complejidad requieren sus soluciones?

h) ¿Qué consecuencias implicará el no afrontarlo?

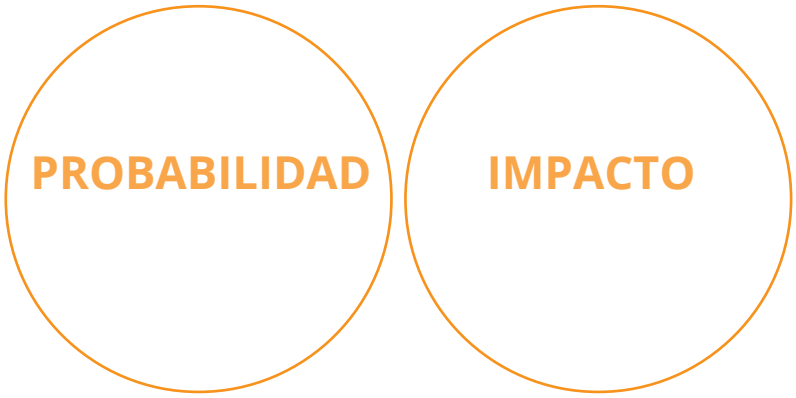
4 . Análisis de Riesgos

El objetivo es establecer una valoración y priorización de los riesgos con el fin de clasificarlos.

El análisis dependerá de la información disponible sobre el riesgo y de su origen.

Para adelantarlo es necesario diseñar escalas que pueden ser cualitativas o cuantitativas.

Se han definido dos categorías:



Esquema de priorización de riesgos

5 . Definición de las respuestas a los riesgos:

La definición obedecerá a los tres pasos anteriores, sobre todo a la identificación de los riesgos y sus efectos en los procesos. La idea es plantear las soluciones más adecuadas para poner cara a aquellos elementos que obstaculizan la consecución de los objetivos estratégicos de las empresas.

Pero así como cada organización tiene sus propios retos en esta materia, de la misma manera debe reaccionar a los riesgos que eventualmente pueden perjudicarle. Existen cinco estrategias principales a la hora de gestionar un riesgo:

- **Supresión del riesgo:**

  No es lo más habitual, pero a veces las organizaciones logran que desaparezcan los riesgos asociados a sus procesos. Esto se consigue cuando la labor de previsión se ha implementado de forma exitosa: obteniendo información adicional, adquiriendo apoyo de expertos, añadiendo recursos adicionales o modificando los elementos de la planificación, entre otros elementos.

- **Transferencia del riesgo:**

  Bajo esta figura, el riesgo es transferido a otra dependencia de la organización o, incluso, a una segunda empresa asociada. Se trata de un recurso muy común entre los grupos de compañías filiales o que comparten algún tipo de vínculo que permite esta transferencia. Por ejemplo, cuando hablamos de responsabilidad solidaria, una empresa puede asumir las deudas de otra que haga parte del conglomerado que las integra a las dos. El riesgo no se anula; sólo se redirecciona.

- **Mitigación del riesgo:**

  Es una estrategia de gestión de riesgos que consiste en reducir la probabilidad o el impacto de un riesgo sobre la organización. Es decir, que si llega a producirse, sus efectos serán mucho menores que si no se hubiesen adoptado medidas al respecto. Esta opción se usa sobre todo en aquellos casos en que los riesgos son inevitables o no dependen de la empresa en sí misma. La clave para una acertada mitigación del riesgo está en las acciones. Algunos ejemplos son:

  - Adopción de procesos más sencillos en la organización.
  - Puesta en marcha de ensayos adicionales.
  - Elección de proveedores o suministrador más fiables.
  - Adición de recursos para la labor preventiva.

- **Explotación del riesgo:**

  Recordemos que no todos los riesgos son negativos. Algunas veces, su irrupción es una oportunidad para las organizaciones. Cuando eso ocurre, en vez de mitigarla o eliminarla, la estrategia de la empresa debe centrarse en sacar el máximo provecho de la circunstancia. Un riesgo con efectos positivos se puede potenciar gracias a la designación de más personal cualificado, mayor apoyo económico o una adaptación a la planificación realizada al inicio.

- **Aceptación del riesgo:**

  En estos casos, se trata de riesgos que no suponen mayores impedimentos para la consecución de los objetivos y que, por tanto, pueden convivir con la empresa. Pero no se trata de una actitud resignada. Por el contrario, implica la elaboración de un plan de contingencia para, de este modo, adaptar el riesgo a las actividades de las empresas. Por ejemplo, las compañías que operan en zonas montañosas y con una alta probabilidad de sismos, desarrollan toda una política de emergencia en torno a la evacuación y la asistencia en casos de emergencia.

6. Plan de tratamiento

El plan de tratamiento, último paso del proceso de Gestión de Riesgos, tiene como fin la mejora de los controles para el tratamiento del riesgo. Esta etapa debe ser dinámica y flexible ante los cambios que puedan presentarse. El tratamiento de los riesgos necesita labores adicionales de registro, monitorización, actualización e intervención.

Por supuesto, este plan depende de la estrategia que se haya definido en el apartado anterior. Pensamos que muchas veces los riesgos no tienen el impacto o los efectos que en un principio habíamos creído, con lo cual es necesario modificar la estrategia y, por consiguiente, el plan de tratamiento.

Los planes de tratamiento **suelen proyectarse a corto plazo, pues con esto se evita que las condiciones iniciales se modifiquen cuando llegue el momento de la intervención.** La manera más habitual de realizar el monitoreo es través de evaluaciones periódicas o auditorías, las cuales son efectuadas por el equipo delegado.

Pero aunque todo esté previsto y las acciones se proyecten en el corto plazo, conviene contemplar alguno de los siguientes escenarios:

- La gestión de los riesgos ha sido aplicada tal como estaba previsto.
- Las respuestas a los riesgos han sido efectivas.
- Se están siguiendo las políticas y las estrategias adecuadas.
- La exposición del riesgo ha cambiado desde el último análisis.
- Se han manifestado síntomas de la aparición de riesgos.
- Han aparecido riesgos que no habían sido contemplados al inicio.

7. Problemas habituales en la gestión de riesgos

Es evidente que los procesos de Gestión de Riesgos no están exentos de problemas. Tal como hemos visto en los apartados anteriores, están compuestos por pasos complejos y que requieren de coordinación y seguimiento permanentes. En este sentido, la norma ISO 31000 ayuda a disminuir los obstáculos en dos sentidos:

7.1. En la implementación:

Se trata de aquellos obstáculos relacionados con la etapa de implementación. Es decir, cuando la empresa ha decidido dar este paso y se presta a realizar las actividades necesarias para la implementación de un Sistema de Gestión de Riesgos. En esta categoría, se pueden distinguir varios tipos de problemas:

a) **Resistencia al cambio:**

Algunas organizaciones no están lo suficientemente preparadas para llevar a la práctica un sistema de este tipo. Bien sea por falta de formación o bien porque no existe un verdadero empoderamiento del proceso, lo cierto es que la clave para atajar este asunto radica en las técnicas de grupo que la dirección ponga en marcha para aumentar el nivel de confianza de sus trabajadores.

b) **Inmediatez:**

Un buen número de organizaciones no están dispuestas a esperar los plazos que se han convenido para la implementación del sistema. Quisieran que todo fuese de una sola vez y sin que tuviesen que invertir tiempo en ello.

c) **Criterios distintos:**

Sucede sobre todo en las grandes empresas. Cuando los grupos de responsables tienen demasiados miembros o su elección no ha seguido parámetros de cierta unidad, lo más común es que entre estas personas se presenten diferencias de criterio a la hora de implementar el plan. Esto se traduce en retrasos, reuniones excesivas y, posiblemente, nombramiento de nuevos integrantes.

d) **Falta de una figura coordinadora:**

Del mismo modo, algunos grupos suelen notar la ausencia de una persona líder que direccione los procesos. De ahí la importancia de la elección de esa persona en los primeros pasos de la implementación.

e) **Incumplimiento de plazos:**

Por causa de una mala planificación, recursos insuficientes o una comunicación deficiente entre los responsables, algunas veces los procesos de implementación de Gestión de Riesgos incurren en incumplimiento de los plazos previstos. En estos casos, el perjuicio es doble: primero, porque obstaculiza la realización del proyecto en sí mismo; y segundo, porque se pierde tiempo valioso para mitigar o gestionar riesgos que, en muchos casos, tienen carácter urgente.

f) **Aplazamiento:**

Esto sucede cuando el plan ni siquiera llega a implementarse. Se han definido las directrices, las estrategias, los responsables y los recursos, pero por la razón que sea el plan acaba guardado en un archivo de la dirección.

7.2 En el mantenimiento:

En este caso, hablamos de obstáculos que surgen en la etapa de ejecución del plan de Gestión de Riesgos. Las empresas que ya han dado el paso y se encuentran en las etapas de monitorización pueden encontrarse con los siguientes problemas:

a) **Omisión de recursos:**

Llegados a esta etapa, las empresas descubren que los recursos destinados para el mantenimiento y la supervisión del plan de Gestión de Riesgos no alcanzan; son insuficientes, con lo cual se compromete la continuidad del mismo y se deja en el aire el conjunto de avances realizados hasta la fecha.

b) **Ausencia de diagnóstico previo:**

Si se han hecho cálculos errados en las primeras etapas, lo más probable es que las proyecciones también lo sean. En estos casos, los procesos requieren de un replanteamiento general.

8. Automatización del Sistema de Gestión de Riesgos según ISO 31000

Las nuevas tecnologías plantean un escenario inmejorable para la Gestión de Riesgos Corporativos. En los últimos años, los avances en ese sentido han puesto a disposición de las empresas numerosas herramientas que contribuyen a agilizar los procesos y a hacerlos más eficaces y acordes con las necesidades.

Cuando una empresa aplica este tipo de herramientas, los resultados no sólo son más precisos sino que, además, arrojan información de utilidad en el momento de aplicar las soluciones o los correctivos pertinentes.

Ni qué decir, claro, de aquellas organizaciones que trabajan con información digital y servicios informáticos. Aparte de ser una necesidad, supone también una ventaja que las diferencia de sus competidores y les sitúa un escalón por encima a la hora de iniciar la monitorización y el seguimiento de las acciones.

ISOTools como herramienta de Gestión de Riesgos

ISOTools es una excelente herramienta para la implementación de un sistema de Gestión de Riesgos. Además de automatizar y promover una monitorización eficaz del proceso, permite una mejor coordinación de las tareas entre los directivos o responsables que hayan sido delegados para tal función.

Siguiendo los principios y las directrices de la norma ISO 31000, esta herramienta aporta ventajas que merecen ser destacadas:

- Ahorra tiempo durante la ejecución de las tareas.
- Permite realizar auto evaluaciones para definir el estado actual de la organización.
- Permite un mejor registro de los datos de los diferentes procesos.
- Realiza comparativas entre análisis de riesgos.
- Permite visualizar el avance de los proyectos y las actividades.
- Relaciona actividades similares o que guarden relación.
- Ofrece cuadros de mando para ilustrar cualquier momento del proceso.
- Permite la realización de análisis de incidencias.
- Ayuda a monitorizar la ejecución de soluciones específicas.


ISOTools
EXCELLENCE