agers

Asociación Española
de Gerencia de
Riesgos y Seguros

VOCES DE GESTIÓN DE RIESGOS

Comentarios a los términos empleados en la UNE-ISO Guía 73:2009 para su aplicación en ISO 31000

UNE
NormalizaciónEspañola

Voces de Gestión de Riesgos

Comentarios a los términos empleados en la UNE-ISO Guía 73:2009 para su aplicación en ISO 31000

Miembros de la comisión técnica de ISO

Coordinadores:

Gonzalo Iturmendi Morales	BUFETE G. ITURMENDI Y ASOCIADOS S.L.P.
Ángel Escorial	RISKIA
Toni Teixidó	ETVALIA
Cristina Gutiérrez Pérez	RISK TO RISK
Julio López García	WILLIS TOWERS WATSON
Isabel Casares San José-Martí	CASARES ASESORÍA ACTUARIAL Y DE RIESGOS
Mariano Blanco Gema	CHUBB
Javier Álvarez	CACUMEN

agers | Asociación Española de Gerencia de Riesgos y Seguros

ISBN: 978-84-697-9959-8
Depósito Legal: M-5633-2018
Copyright: DEP636543042456424153

PRÓLOGO

Las organizaciones de todo tipo y tamaño se enfrentan a factores e influencias externas e internas que hacen incierto saber si alcanzarán sus objetivos. En este contexto caracterizado por la incertidumbre la gestión del riesgo, como parte de la gobernanza en las organizaciones, es una pieza fundamental a todos sus niveles que contribuye, asimismo, a la mejora de sus sistemas de gestión.

En esta línea la actividad de estandarización, de la que la Asociación Española de Normalización, UNE, es responsable tanto a nivel nacional como internacional, se ha convertido en una herramienta de gran potencia para las organizaciones. Además de haber conseguido un consenso internacional a la hora de abordar todo el proceso de evaluación del riesgo, pone en valor y da difusión a las buenas prácticas existentes en la disciplina. De esta forma, consigue un mismo idioma técnico entre los profesionales del riesgo desde el punto de vista internacional.

La actividad de normalización internacional en riesgos, cimentada en los trabajos del Comité internacional ISO TC 262 "Risk Management", tiene su espejo nacional en el comité técnico de normalización de UNE, CTN 307 "Gestión del riesgo". En este órgano se realiza el seguimiento técnico del ISO TC 262, al tiempo que permite la participación activa de sus miembros en el mismo. El ISO TC 262 "Risk Management," es el responsable de la elaboración de los estándares de gestión del riesgo a nivel internacional, entre los que se encuentra la norma ISO 31000:2009 "Gestión del riesgo. Principios y directrices", estándar en el que se cimenta el resto de las normas internacionales y nacionales sobre riesgos.

Esta norma, incorporada al cuerpo normativo nacional como UNE ISO 31000:2010, proporciona directrices para gestionar el riesgo al que se enfrentan las organizaciones, independientemente de su tamaño, sector de actividad y contexto en el que operen. Proporciona un enfoque común para gestionar cualquier tipo de riesgo, aplicándose a todo tipo de actividades, incluyendo la toma de decisiones a todos los niveles. La norma proporciona orientación sobre los beneficios y valores de la gestión del riesgo eficaz y eficiente y ayuda a organizaciones a una mayor comprensión y trato de las incertidumbres a las que hacen frente para lograr sus objetivos.

En este entorno normativo, la Asociación Española de Gerencia de Riesgos y Seguros (AGERS), como miembro del comité nacional CTN 307, trabaja activamente y colabora con UNE en las labores de normalización, lo que le permite elevar la experiencia nacional de sus profesionales a los diferentes foros internacionales de normalización.

Es por ello que el trabajo realizado en este libro "voces de riesgo" por los profesionales de AGERS cobra un especial sentido, ya que se ha realizado un esfuerzo importante a la hora de comentar y desgranar, desde el punto de vista práctico, toda la terminología existente en la norma internacional ISO 31000. Es importante destacar

que la terminología íntegra de este pilar normativo en riesgos está extractada en la Guía UNE ISO 73:2010 IN "Gestión del riesgo. Vocabulario", documento sobre el que ha trabajado AGERS para poner a disposición de la comunidad de riesgos este libro.

Asimismo, me es grato destacar que esta obra ve la luz en un momento importante desde el punto de vista de la actualidad normativa, ya que la nueva versión de la Norma ISO 31000 se ha publicado muy recientemente. Esta nueva versión va a suponer un punto de inflexión, no sólo desde el punto de vista técnico, presentando una versión más madura que el texto anterior, sino desde el punto de vista del lenguaje ya que se ha trabajado con términos más claros y precisos, con la expectativa de que al lector le resulte más simple de entender

A esto se le añade el hecho de que la nueva versión de la ISO 31000 se va a convertir en un potente vector de diseminación de un léxico en español en la disciplina del riesgo que traspasará nuestras fronteras. En ISO se está trabajando en una versión oficial en español consensuada por toda la comunidad de habla hispana en la que están representados más de 13 países. En estos trabajos liderados por UNE, AGERS está colaborando de una forma muy activa, poniendo a disposición de la comunidad hispanohablante toda su experiencia no sólo técnica, sino sobre terminología de riesgos en nuestro idioma.

Esto va a suponer que la nueva versión de la Norma ISO 31000 y la futura guía ISO 74 de vocabulario, que deberán ser leídas en conjunto, se vayan a convertir en vectores de diseminación de una terminología consensuada en español entre la comunidad iberoamericana lo que va a redundar en un crecimiento del conocimiento técnico.

Las páginas que siguen son de gran interés para los profesionales de la gestión de riesgos y seguros, así como para aquellos interesados en iniciarse en la materia. La información que contiene, es una aportación a la extensión de las buenas prácticas en una función cada vez más valorada por las empresas.

Javier García Diaz

Director General de UNE

ÍNDICE

INTRODUCCIÓN

La estandarización de procesos de gestión de riesgos facilita la labor de esta actividad decisiva en las organizaciones, al tiempo que ofrece ventajas competitivas a quienes las implementan, al optimizar la política y procedimientos de identificación, análisis, evaluación, control y financiación de los riesgos soportados en cada organización.

La Asociación Española de Gerencia de Riesgos y Seguros (AGERS) ha tenido la satisfacción de participar en el proceso de elaboración de las normas UNE-ISO Guía 73 IN de vocabulario de gestión del riesgo, UNE-ISO 31000, Gestión del riesgo, principios y directrices, norma UNE ISO31010 sobre las técnicas de apreciación del riesgo y el Informe Técnico ISO 31004 de orientaciones para la implementación de la norma ISO 31000. Actualmente AGERS sigue trabajando activamente en la revisión de dichas normas en el seno del grupo internacional encargado de su actualización. La comisión ISO 31000 creada dentro de la Asociación para llevar a cabo estos trabajos, decidió que merecía la pena analizar y explicar en profundidad los términos que sirvieron de base para la elaboración de las normas internacionales de gestión de riesgos, ante la necesidad de clarificar la terminología empleada, una labor elemental, que no deja de ser la base del proceso de gestión de riesgos que se aplicará en cada organización de acuerdo con su estilo propio y sus necesidades específicas.

Las normas claras a la hora de ejecutar un proceso de gestión de riesgos concreto, permiten la anticipación a los problemas que plantean las amenazas e incertidumbres y trazan la forma de analizarlas y abordarlas, planteando sus posibles soluciones mediante pautas de actuación ante los retos que plantean la propia actividad de la organización. La estandarización basada en el consenso empírico de las mejores prácticas de gestión de riesgos, no solo ayuda a comprender la forma de abordar esta actividad de manera eficiente, sino que también previene errores humanos, fallos de procesos, produce ahorro de tiempo de trabajo, así como de recursos económicos propios y ajenos.

Para que la estandarización sea posible, se requiere el empleo de términos cuyo significado sea claro, preciso y comúnmente aceptado por la comunidad científica y profesional implicada en su utilización, todo lo cual supone el empleo de términos unívocos que -a la postre- facilitan la comunicación interna y externa de la organización. Bajo estos parámetros nació la idea de crear la presente publicación en la que, siguiendo las definiciones contenidas en la norma UNE-ISO Guía 73 IN, se explica el alcance y significado de los términos empleados en dicha norma por medio de la opinión de los distintos autores participantes en el libro.

La importancia del léxico es vital, ya que nos permite interactuar con el entorno y la sociedad de manera sistematizada y comprensible, mediante un lenguaje internacional alineado a los términos consensuados, cuyo uso pretende ser lo más universal posible para posibilitar y potenciar la comunicación en la prevención, control y tratamiento de los riesgos.

Este libro es algo más que una aportación para la mejora del empleo de los términos científicos y profesionales de la gestión de riesgos. Pretende que las palabras y las expresiones de los estándares no queden congeladas en los textos normalizados. Ciertamente todos necesitamos un estilo comprensible sencillo, claro, conciso y directo de comunicación, que permita optimizar la política y procedimientos de gestión de riesgos. Sin embargo, pretendemos que este trabajo sea algo más que el análisis de una guía de actuación, para ello necesitamos contar con su colaboración como lectores inquietos e inteligentes capaces de ejercer el pensamiento crítico para evolucionar hacia un enfoque estructurado que ayude a la gerencia a entender y manejar las incertidumbres, abarcando todos los riesgos y así maximizar el valor de la organización.

Somos conscientes de que las palabras que abordamos en esta publicación están cargadas de un significado primario que necesariamente debe evolucionar, porque –a buen seguro- se transfigurará y cambiará en función de la experiencia que nazca de los distintos escenarios de riesgos y las necesidades de cada organización, alcanzando una expresividad nueva que desbordará el primer dibujo aquí esbozado. Por eso resulta necesaria la implicación del lector inteligente que haga posible la transfiguración del significado inicial de las voces aquí analizadas, de forma que evolucionen, cobren vida propia e independencia, gracias a la tenacidad en el compromiso de la aplicación de las mejores prácticas de gestión de riesgos.

Si el lector consigue integrar las voces abordadas, si descubre nuevos matices y significados desde la perspectiva que proporciona la experiencia, si consigue integrar las voces aquí analizadas en una gestión eficaz de los riesgos, oportunidades y eventos esperados e inesperados, entonces estaremos todos de enhorabuena.

Gonzalo Iturmendi Morales

Secretario General de AGERS

1. TÉRMINOS RELATIVOS AL RIESGO[1]

1.1. Riesgo.

Efecto de la incertidumbre sobre la consecución de los objetivos.[2]

I.- Definición.

Existen varias definiciones del término riesgo. Todas ellas coinciden en la combinación de la probabilidad de ocurrencia de un suceso y sus consecuencias. O bien en la posibilidad de acaecimiento de un suceso que tendrá un impacto sobre los objetivos.

El riesgo implica la exposición a una posibilidad de pérdida para la organización.

Veamos algunas definiciones de riesgo:

- Federation of European Risk Management Associations (FERMA) (2003: 3)
- La combinación de la probabilidad de un suceso y sus consecuencias.
- ISO 31000 (2009):

Efecto de la incertidumbre sobre la consecución de los objetivos.

---

1 Los comentarios a los apartados 1 Términos relativos al riesgo y 2 Términos relativos a la gestión de riesgos fueron elaborados por **D. Gonzalo Iturmendi Morales**.

2 A propósito del término riesgo, la UNE-ISO Guía 73:2009 contiene las siguientes notas:
"NOTA 1 Un efecto es una desviación, positiva y/o negativa, respecto a lo previsto. NOTA 2 Los objetivos pueden tener diferentes aspectos (tales como financieros, de salud y seguridad, o ambientales) y se pueden aplicar a diferentes niveles (tales como, nivel estratégico, nivel de un proyecto, de un producto, de un proceso o de una organización completa). NOTA 3 Con frecuencia, el riesgo se caracteriza por referencia a sucesos potenciales (3.5.1.3) y a sus consecuencias (3.6.1.3), o a una combinación de ambos. NOTA 4 Con frecuencia, el riesgo se expresa en términos de combinación de las consecuencias de un suceso (incluyendo los cambios en las circunstancias) y de su probabilidad (3.6.1.1). NOTA 5 La incertidumbre es el estado, incluso parcial, de deficiencia en la información relativa a la comprensión o al conocimiento de un suceso, de sus consecuencias o de su probabilidad."

- Diccionario Mapfre de Seguros. Antonio Guardiola Lozano y Julio Castelo Matrán.

Combinación de la probabilidad de ocurrencia de un suceso y sus consecuencias. Puede tener carácter negativo (en caso de ocurrir se producen pérdidas) o positivo (en caso de ocurrir se producen ganancias). En la terminología aseguradora, se emplea este concepto para expresar indistintamente dos ideas diferentes: de un lado, riesgo como objeto asegurado; de otro, riesgo como posible ocurrencia por azar de un acontecimiento que produce una necesidad económica y cuya aparición real o existencia se previene y garantiza en la póliza y obliga al asegurador a efectuar la prestación, normalmente indemnización, que le corresponde. Este último criterio es el técnicamente correcto, y en tal sentido se habla del riesgo de incendio o muerte para aludir a la posibilidad de que el objeto o persona asegurados sufran un daño material o fallecimiento, respectivamente; o se habla de riesgos de mayor o menor gravedad, para referirse a la probabilidad más o menos grande de que el siniestro pueda ocurrir.

- Diccionario de Términos de Seguros, Reaseguros y Financieros.
  Francisco Mochón Morcillo, Rafael Isidro Aparicio y Gonzalo Fernández Isla.
  Incertidumbre sobre el futuro.

- AGERS, en “Curso de introducción a la Gerencia de Riesgos”.

Incertidumbre de ocurrencia de un suceso con efectos negativos, considerando, también incierta, la magnitud de dichos efectos.

Sea cual fuere la definición que se emplee, la incertidumbre (o el riesgo) es la esencia de todo contrato de seguro. De acuerdo con el Reglamento (CE) nº 1126/2008 de la Comisión, de 3 de noviembre de 2008, por el que se adoptan determinadas normas internacionales de contabilidad, al menos uno de los siguientes factores tendrá que ser incierto al comienzo de un contrato de seguro:

a) si se producirá o no el evento asegurado;

b) cuándo se producirá, o

c) cuánto tendría que pagar la entidad aseguradora si se produjese.

En algunos contratos de seguro, el evento asegurado es el descubrimiento de una pérdida durante el período de duración del contrato, incluso si la pérdida en cuestión procediese de un evento ocurrido antes del inicio del contrato, siempre y cuando el siniestro no fuera conocido por el asegurado o que este no tuviera conocimiento de la existencia de una reclamación relacionada con el siniestro. En otros contratos de seguro, el evento asegurado debe tener lugar dentro del período de duración del contrato, incluso si la pérdida que resulte fuera descubierta después de la finalización del plazo del contrato.

Existen contratos de seguro cubren eventos que ya han ocurrido, pero cuyos efectos financieros son todavía inciertos. Un ejemplo es un contrato de reaseguro que cubre a la entidad aseguradora directa contra la evolución desfavorable de la siniestralidad

ya declarada por los tomadores de las pólizas. En estos contratos, el evento asegurado es el descubrimiento del coste final de dichas prestaciones.

II.- Tipos de riesgos.

La actividad, la vida misma, comporta exposición al riesgo. Los riesgos de la vida comportan riesgos ligados a la propia existencia del hombre en sociedad.[3] Sin embargo podemos realizar clasificaciones de riesgos de forma agrupada, como veremos a continuación.

A.- Por su contenido troncal.

Existen múltiples formas de clasificar los riesgos en función de distintos criterios de especialidad; por ejemplo, durante años se les ha clasificado según el objeto sobre el que recaen, en este sentido la clasificación pivotaba entre riesgo patrimoniales (daño material que implica una disminución o pérdida, total o parcial, de patrimonio), riesgos personales (salud, integridad física o mental, capacidad para el trabajo, vejez o sobrevivencia) y riesgos de responsabilidad civil (obligación legal que tiene una persona física o jurídica de indemnizar los daños causados a terceros siempre que concurran los requisitos necesarios para tener que reparar el daño causado).

B.- Por la regularidad estadística.

Otras clasificaciones se han hecho en función de su probabilidad de ocurrencia y la regularidad estadística. Se distingue entre riesgo ordinario, cuya ocurrencia es susceptible de medición estadística conforme a pautas de efectos previsibles del sector asegurados; y riesgos extraordinarios o también llamados consorciables, que son asumidos por el Consorcio de Compensación de Seguros, organismo que cubre los daños producidos a las personas y en los bienes por determinados fenómenos de la naturaleza y por algunos acontecimientos derivados de determinados hechos de incidencia política o social, siempre y cuando exista un contrato de seguro de los ramos respecto de los que la legislación vigente establece la obligación de incluir en sus correspondientes coberturas la garantía de estos riesgos. Su marco regulador se encuentra en el Estatuto Legal del Consorcio, aprobado por la Ley 21/1990, de 19 de diciembre, y que, tras sucesivas modificaciones, ha quedado recogido en el texto refundido aprobado por el Real Decreto Legislativo 7/2004, de 29 de octubre, con diversas modificaciones posteriores.

---

3 MONTOYA MELGAR, ANTONIO. Definición de "riesgos de la vida", Diccionario Jurídico [Real Academia de Jurisprudencia y Legislación]. 1ª ed.; diciembre 2016: "Fórmula de la imputación objetiva que entiende que la vida comporta riesgos ligados a la propia existencia del hombre en sociedad, de modo que, por ejemplo, no se pueden imputar a quien causó heridas leves a otro, los daños que éste haya sufrido en un accidente de circulación en que se vio envuelto el taxi que le llevaba al hospital".

En todo caso los caracteres esenciales del riesgo implican la incertidumbre o aleatoriedad, la posibilidad de ocurrencia, su concreción, licitud y existencia de un contenido económico.

C.- Por su especialidad.

Los riesgos también se pueden clasificar en función agrupándolos en función de su especialidad en riesgos estratégicos, operacionales, de cumplimiento o responsabilidad jurídica, financieros y medioambientales.

1. Riesgos estratégicos: son los riesgos que nacen de la dirección tomado por la organización, de sus disciplinas de trabajo, de los mercados a los que pretenden acceder, las relaciones sociales y societarias, así como las personas relevantes y la gestión de la imagen y marca.

2. Riesgos operacionales: son los riesgos que componen todas las actividades diarias, así como los medios tanto personales como materiales puestos a disposición de la organización, tanto internos como externos.

3. Riesgos cumplimiento o jurídicos: son los riesgos que nacen del régimen jurídico o de las consecuencias de las desviaciones en las actividades operacionales de la organización, así como los riesgos por incumplimiento de las normas empresariales y de convivencia o los que nacen del azar y que son generadores de perjuicios.

4. Riesgos financieros: son los riesgos que nacen de las desviaciones sobre los objetivos financieros y económicos de la organización bien por situaciones operacionales, de mercado o de incumplimiento.

5. Riesgos medioambientales: son los riesgos que nacen en la convivencia con el entorno y el medioambiente al que está sometida la organización y en especial sus actividades.

ESTRATÉGICOS

- Riesgo de desarrollo estratégico

- Riesgo de estructura societaria

- Riesgo de fusiones y adquisiciones

- Riesgo de I+D+i

- Riesgo de las personas relevantes en la estrategia

- Riesgo de mercados

- Riesgo de sostenibilidad

- Riesgo en la responsabilidad social corporativa y en el buen gobierno.

- Riesgos reputacionales.[4]

OPERACIONALES

- Riesgos de la naturaleza
- Riesgos biológicos
- Riesgos tecnológicos
- Riesgos de las actividades sociales
- Riesgos de las actividades antisociales
- Riesgos sobre las personas

CUMPLIMIENTO

- Riesgo contractual
- Riesgo extracontractual
- Riesgo de cumplimiento de obligaciones normativas
- Riesgo penal

FINANCIEROS

- Riesgo de aprovisionamiento
- Riesgo de crédito
- Riesgo de explotación
- Riesgo de financiación corporativa
- Riesgo de financiación crediticia
- Riesgo de financiación operacional
- Riesgo de inmovilizado material

---

4 Los riesgos reputacionales, dada su relevancia decisiva, son considerados en ocasiones como una categoría troncal junto con los riesgos estratégicos, operacionales, de cumplimiento, financieros y medioambientales. La reputación es la posibilidad de afectación del prestigio de una entidad por cualquier evento externo, fallas internas hechas públicas, o al estar involucrada en transacciones o relaciones con negocios ilícitos, que puedan generar pérdidas y ocasionar un deterioro de la situación de la entidad. Sin embargo, hemos considerado más apropiado clasificarlos como una categoría más dentro de los riesgos estratégicos.

- Riesgo de intangibles
- Riesgo de inversiones financieras
- Riesgo de mercado
- Riesgo de otros deudores
- Riesgo de solvencia corporativa
- Riesgo sobre existencias
- Riesgo de liquidez

MEDIOAMBIENTALES

- Riesgos graduales
- Riesgos accidentales

D.-Riesgos asegurables voluntariamente y no asegurables.

Muchos de los riesgos referenciados anteriormente son asegurables, es decir, aquellos que por su naturaleza son susceptible de ser asegurados porque encuentran encaje en el mercado asegurador y cumplen los caracteres esenciales del riesgo asegurable.

Pero también encontramos muchos de los riesgos no asegurables o con grandes dificultades de aseguramiento porque o bien carecen de alguno de los elementos o caracteres del riesgo que impiden su aseguramiento o bien porque no existe capacidad suficiente en el mercado asegurador como para asumir financieramente las transferencias económicas del riesgo.

El riesgo asegurado es el "elemento esencial del contrato de seguro, consistente en la posibilidad de que se produzca un evento o suceso que genere un daño o una necesidad pecuniaria para el asegurado".[5] De manera que el contrato seguro es nulo si, cuando se celebra, carece de riesgo.

El Reglamento (CE) nº 1126/2008 de la Comisión, de 3 de noviembre de 2008, por el que se adoptan determinadas normas internacionales de contabilidad distingue entre riesgo de seguro y otros riesgos distintos de seguros.

---

5 MONTOYA MELGAR, ANTONIO. Definición de "Riesgo asegurado", Diccionario Jurídico [Real Academia de Jurisprudencia y Legislación]. 1ª ed.; diciembre 2016: "El riesgo debe describirse con exactitud en la póliza, y han de comunicarse al asegurador las circunstancias que pueden incidir en su valoración, en el momento de celebración del contrato y con posterioridad, durante la vigencia del mismo."

Entre los riesgos distintos de seguros distingue:

En mora. Un activo financiero está en mora en el momento en que la contraparte deje de efectuar un pago cuando contractualmente deba hacerlo.

Otros riesgos de precio. El riesgo de que el valor razonable o los flujos de efectivo futuros de un instrumento financiero puedan fluctuar como consecuencia de variaciones en los precios de mercado (diferentes de las que provienen del riesgo de tipo de interés o del riesgo de tipo de cambio), ya estén causadas dichas variaciones por factores específicos al instrumento financiero en concreto o a su emisor, o por factores que afecten a todos los instrumentos financieros similares negociados en el mercado.

Préstamos a pagar. Préstamos a pagar son los pasivos financieros, diferentes de las cuentas comerciales a pagar a corto plazo en condiciones normales de crédito.

Riesgo de crédito. El riesgo de que una de las partes del instrumento financiero pueda causar una pérdida financiera a la otra parte si incumple una obligación.

Riesgo de liquidez. El riesgo de que una entidad encuentre alguna dificultad para cumplir con obligaciones asociadas con pasivos financieros que se liquiden mediante la entrega de efectivo u otro activo financiero.

Riesgo de mercado. El riesgo de que el valor razonable o los flujos de efectivo futuros de un instrumento financiero puedan fluctuar como consecuencia de variaciones en los precios de mercado. El riesgo de mercado comprende tres tipos de riesgo: riesgo de tipo de cambio, riesgo de tipo de interés y otros riesgos de precio.

Riesgo de tipo de cambio. El riesgo de que el valor razonable o los flujos de efectivo futuros de un instrumento financiero puedan fluctuar como consecuencia de variaciones en los tipos de cambio de una moneda extranjera.

Riesgo de tipo de interés. El riesgo de que el valor razonable o los flujos de efectivo futuros de un instrumento financiero puedan fluctuar como consecuencia de variaciones en los tipos de interés de mercado.

Riesgo de seguro. En la definición de contrato de seguro se hace referencia al riesgo de seguro, que es todo riesgo, distinto del riesgo financiero, transferido por el tomador de un contrato al emisor del mismo. Un contrato que exponga al emisor a un riesgo financiero, pero que no tenga un componente significativo de riesgo de seguro, no es un contrato de seguro. La definición de riesgo de seguro hace referencia al riesgo que la entidad aseguradora acepta del tomador. En otras palabras, el riesgo de seguro es un riesgo preexistente, transferido del tomador del seguro a la aseguradora. Por ello, un nuevo riesgo creado por el contrato no podrá ser un riesgo de seguro.

Riesgo financiero es aquel que representa un posible cambio futuro en una o más de las siguientes variables: un tipo de interés especificado, el precio de un instrumento financiero, el precio de una materia prima cotizada, un tipo de cambio, un índice de precios o de intereses, una clasificación o un índice crediticio u otra variable. Si se

trata de una variable no financiera, es necesario que la misma no sea específica de una de las partes en el contrato. Se trata de variables financieras y no financieras. La lista contiene variables no financieras que no son específicas para ninguna de las partes del contrato, tales como un índice de pérdidas causadas por terremotos en una región particular o un índice de temperaturas en una ciudad concreta. La lista excluye variables no financieras que son específicas para una de las partes, tal como la ocurrencia o no de un incendio que dañe o destruya un activo de la misma. Además, el riesgo de variaciones en el valor razonable de un activo no financiero no será un riesgo de tipo financiero si el valor razonable refleja no sólo cambios en los precios de mercado para dichos activos (una variable financiera), sino también el estado o condición de un activo no financiero específico perteneciente a una de las partes del contrato (una variable no financiera). Por ejemplo, si una garantía del valor residual de un automóvil específico expone al garante al riesgo de cambios en el estado físico del mismo, el riesgo será un riesgo de seguro, no un riesgo financiero.

Algunos contratos exponen al emisor a un riesgo financiero, además de a un riesgo de seguro significativo. Por ejemplo, muchos contratos de seguro de vida garantizan una tasa mínima de rentabilidad a los tomadores (lo cual crea riesgo financiero), y a la vez prometen una indemnización por fallecimiento que excede varias veces el saldo de la cuenta del tomador (lo que crea un riesgo de seguro en la modalidad de riesgo de fallecimiento). Estos contratos son contratos de seguro.

En algunos contratos, la ocurrencia del evento asegurado provoca el pago de un importe ligado a un índice de precios. Estos contratos serán contratos de seguro, siempre que el pago que dependa del evento asegurado pueda ser significativo. Por ejemplo, una renta vitalicia vinculada a un índice del coste de la vida transfiere riesgo de seguro, puesto que el pago es provocado por un suceso incierto, la supervivencia del perceptor de la renta. La vinculación al índice de precios es un derivado implícito, pero también transfiere riesgo de seguro. Si la transferencia de riesgo resultante es significativa, el derivado implícito cumple la definición de contrato de seguro, en cuyo caso no será necesario separarlo y medirlo por su valor razonable.

La definición de contrato de seguro hace referencia a que un evento pueda afectar de forma adversa al tomador de la póliza. Esta definición no limita el pago, por parte de la entidad aseguradora, a un importe que tenga que ser igual al impacto financiero del evento adverso. Por ejemplo, la definición no excluye una indemnización del tipo «nuevo por-viejo», en la que se paga al tomador del seguro un importe suficiente para permitir la reposición de un activo viejo dañado por un activo nuevo. De forma similar, la definición no limita el pago, en un contrato de seguro de vida temporal, a las pérdidas financieras sufridas por los dependientes del fallecido, ni impide el pago de importes predeterminados para cuantificar la pérdida causada por muerte o por un accidente.

Algunos contratos requieren un pago si ocurre un evento incierto especificado, pero no exigen que haya originado un efecto adverso al tomador como condición previa para dicho pago. Tal contrato no será un contrato de seguro, incluso si el tomador lo utilizase para reducir una exposición al riesgo subyacente. Por ejemplo, si el tomador utiliza un derivado para cubrir una variable subyacente no financiera, que está corre-

lacionada con los flujos de efectivo de otro activo de la entidad, el derivado no será un contrato de seguro puesto que el pago no está condicionado a que el tomador se vea afectado adversamente por una reducción en los flujos de efectivo del otro activo. Por el contrario, la definición de contrato de seguro hace referencia a un evento incierto, tras el cual el efecto adverso sobre el tomador del seguro es una precondición contractual para el pago. Esta precondición contractual no obliga a la entidad aseguradora a investigar si el evento ha causado realmente un efecto adverso, pero le permite denegar el pago si no se cumple la condición de que el evento haya provocado dicho efecto adverso.

El riesgo de interrupción o persistencia (es decir, el riesgo de que la otra parte cancele el contrato antes o después del momento esperado por la entidad aseguradora al fijar el precio) no será un riesgo de seguro, puesto que el pago a la otra parte no depende de un evento futuro incierto que afecte de forma adversa a la misma. De forma similar, el riesgo de gasto (es decir, el riesgo de aumentos inesperados de los costes administrativos asociados con la gestión del contrato, que no tenga relación con costes asociados con los eventos asegurados) no será un riesgo de seguro, puesto que un aumento inesperado en los gastos no afecta de forma adversa a la contraparte del contrato.

Por tanto, un contrato que exponga a la entidad aseguradora a riesgos de interrupción, persistencia o gasto, no será un contrato de seguro, salvo que también exponga a la entidad aseguradora a un riesgo de seguro. No obstante, si el emisor de ese contrato redujese dicho riesgo utilizando un segundo contrato, para transferir parte de ese riesgo a un tercero, ese nuevo contrato expondrá a la otra parte a un riesgo de seguro.

Una entidad aseguradora podrá aceptar un riesgo significativo del tomador de un seguro sólo si la aseguradora es una entidad distinta del tomador. En el caso de que la entidad aseguradora sea una mutua, la mutua acepta el riesgo procedente de cada tomador de la póliza y lo concentra. Aunque los tomadores de las pólizas asumen este riesgo concentrado de forma colectiva, en su condición de socios propietarios, la mutua también ha aceptado el riesgo, lo que constituye la esencia de un contrato de seguro.

El Reglamento (CE) nº. 1126/2008 de la Comisión, de 3 de noviembre de 2008 establece una serie de ejemplos de contratos de seguro siempre que la transferencia de riesgo de seguro resulte significativa, así como ejemplos de contratos que no son de seguro, entre los que se encuentra el autoseguro:

Ejemplos de contratos de seguro.

a) seguro contra el robo o los daños en la propiedad;

b) seguro de responsabilidad derivada de garantía de productos, responsabilidad profesional, responsabilidad civil o gastos de defensa jurídica;

c) seguro de vida y de decesos (aunque la muerte sea cierta, es incierto el momento de ocurrencia o, para algunos tipos de seguro de vida, si ocurre o no en el período cubierto por el seguro);

d) seguro de rentas vitalicias y pensiones (es decir, contratos que prevén indemnización por un evento futuro incierto -la supervivencia del que percibe las rentas o del pensionista- para ayudar al rentista o al pensionista a mantener un nivel de vida determinado, que podría verse en otro caso afectado adversamente por el hecho de su supervivencia);

e) discapacidad y asistencia sanitaria;

f) bonos de caución, bonos de fidelidad, bonos de rendimiento y bonos de aval para licitaciones (esto es, contratos que prevén indemnizaciones si la otra parte incumple un compromiso contractual, por ejemplo, la obligación de construir un edificio);

g) seguro de crédito, que prevé la realización de pagos específicos para reembolsar al tomador por una pérdida en la que incurre porque un deudor específico incumple su obligación de pago en los plazos, originales o modificados, establecidos por un instrumento de deuda. Estos contratos pueden revestir diferentes formas legales, tales como la de un aval, algunos tipos de cartas de crédito, un contrato de derivado de crédito para caso de impago o un contrato de seguro.

h) garantías de productos. Las garantías de productos, emitidas por un tercero, que cubran los bienes vendidos por un fabricante, mayorista o minorista entran dentro del alcance de esta NIIF. No obstante, las garantías de productos emitidas directamente por el fabricante, mayorista o minorista no entran dentro de su alcance, ya que están cubiertas por la NIC 18 y la NIC 37;

i) seguros por vicios ocultos en los títulos de propiedad (es decir, seguros contra el descubrimiento de defectos en los títulos de propiedad de la tierra que no son aparentes cuando se suscribe el contrato de seguro). En este caso, el efecto asegurado es el descubrimiento de un defecto en el título, no el defecto en sí;

j) asistencia en viaje (es decir, indemnización, en efectivo o en especie al tomador de la póliza por las pérdidas sufridas durante un viaje).

k) bonos de catástrofe, en los que se prevén reducciones en los pagos del principal, de los intereses o de ambos en caso de que un evento adverso específico afecte al emisor del bono (salvo en el caso de que el evento específico no cree un riesgo de seguro que sea significativo, por ejemplo, si se trata del cambio en un tipo de interés o de cambio de moneda extranjera);

l) permutas de seguro y otros contratos que establecen pagos basados en cambios climáticos, geológicos u otras variables de tipo físico que sean específicas para una de las partes del contrato;

m) contratos de reaseguro.

Los siguientes son ejemplos de contratos que **no constituyen contratos de seguro**:

a) contratos de inversión, que tienen la forma legal de un contrato de seguro pero que no exponen a la entidad aseguradora a un riesgo de seguro significativo, por ejemplo,

los contratos de seguro de vida en que la aseguradora no soporta un riesgo de mortalidad significativo (estos contratos son instrumentos financieros distintos del seguro, o son contratos de servicios, véanse los párrafos B20 y B21);

b) contratos que tienen la forma legal de un seguro, pero transmiten todo el riesgo significativo de seguro al tomador, mediante mecanismos, que son directamente ejecutables y no prevén posibilidad de cancelación, por los que se ajustan los pagos futuros del tomador como resultado directo de las pérdidas aseguradas, por ejemplo algunos contratos de reaseguro financiero o ciertos contratos sobre colectivos (estos contratos son instrumentos financieros distintos del seguro, o son contratos de servicios, véanse los párrafos B20 y B21);

c) autoseguro, en otras palabras, la retención de un riesgo que podría haber estado cubierto por un seguro (en este caso no hay contrato de seguro porque no existe un acuerdo con otra parte);

d) contratos (como los de apuestas) que obligan a realizar pagos si ocurre un evento futuro incierto, pero no requieren, como precondición contractual, que el evento afecte de forma adversa al tenedor. No obstante, esto no impide la estipulación de un desembolso predeterminado con el fin de cuantificar la pérdida causada por eventos tales como la muerte o un accidente);

e) derivados que exponen a una de las partes a un riesgo financiero, pero no a un riesgo de seguro, porque obligan a la misma a realizar pagos basados exclusivamente en los cambios experimentados por una o más variables como las siguientes: un tipo de interés específico, el precio de un instrumento financiero determinado, el precio de una materia prima concreta, el tipo de cambio de una divisa particular, un índice de precios o de tipos de interés específico, una calificación crediticia o un índice crediticio determinado, o bien otra variable similar, suponiendo, en el caso de las variables no financieras, que no se trate de una variable específica para una de las partes del contrato (véase la NIC 39)

f) una garantía relacionada con un crédito (o bien una carta de crédito, un contrato de derivado de crédito para caso de impago o un contrato de seguro de crédito) que obligue a realizar pagos, aunque el tenedor no haya incurrido en pérdidas a consecuencia de que el deudor no haya efectuado los pagos al vencimiento (véase la NIC 39);

g) contratos que requieren pagos basados en variables climáticas, geológicas u otras magnitudes físicas que no son específicas para una de las partes del contrato (denominados comúnmente derivados climáticos);

h) bonos de catástrofe, en los que se prevean reducciones en los pagos del principal, de los intereses o de ambos, basadas en variables climáticas, geológicas u otras magnitudes físicas que no son específicas para una de las partes del contrato.

E.- Riesgos asegurables en España y clasificación por ramos de seguro.

Dado que el marco legal de la actividad aseguradora regula tanto las actividades de seguro directo de vida y de seguro directo distinto del seguro de vida y las actividades de reaseguro, como las operaciones preparatorias o complementarias de las de seguro que practiquen las entidades aseguradoras y reaseguradoras, las actividades de prevención de daños vinculadas a la actividad aseguradora y cualesquiera otras actividades cuando se establezca expresamente en una norma con rango de ley, resulta necesario distinguir las siguientes figuras que operan en el mercado asegurador, así como los ramos en los que pueden operar:

1. Entidad aseguradora: Una entidad autorizada para realizar, conforme a lo dispuesto por esta Ley o por la legislación de otro Estado miembro, actividades de seguro directo de vida o de seguro directo distinto del seguro de vida.

2. Entidad aseguradora cautiva: Entidad aseguradora propiedad de una entidad no financiera, o de una entidad financiera que no sea una entidad aseguradora o reaseguradora o forme parte de un grupo de entidades aseguradoras o reaseguradoras, que tiene por objeto ofrecer cobertura de seguro exclusivamente para los riesgos de la entidad o entidades a las que pertenece o de una o varias entidades del grupo del que forma parte. La LOSSEAR define la expresión grupo como todo conjunto de entidades que está integrado por una entidad participante, sus filiales y las entidades en las que la participante o sus filiales posean una participación, así como las entidades vinculadas entre sí por hallarse sujetas a una dirección única o porque sus órganos de administración, de dirección o de control, se compongan mayoritariamente de las mismas personas; o se base en un reconocimiento, contractual o de otro tipo, de vínculos financieros sólidos y sostenibles entre esas entidades (artículo 131.1.f).

3. Entidad aseguradora domiciliada en un tercer país: Una entidad aseguradora que, si tuviera su domicilio social en algún Estado miembro, estaría obligada, con arreglo a las disposiciones de ese Estado, a obtener una autorización para realizar la actividad aseguradora.

4. Entidad reaseguradora: Una entidad que haya recibido autorización con arreglo a lo dispuesto en esta Ley, o conforme a la legislación de otro Estado miembro, para realizar actividades de reaseguro.

5. Entidad reaseguradora cautiva: Entidad reaseguradora propiedad de una entidad no financiera, o de una entidad financiera que no sea una entidad aseguradora o reaseguradora o forme parte de un grupo de entidades aseguradoras o reaseguradoras, definido en el artículo 131.1.f), y que tiene por objeto ofrecer cobertura de reaseguro exclusivamente para los riesgos de la entidad o entidades a las que pertenece o de una o varias entidades del grupo del que forma parte.

6. Entidad reaseguradora domiciliada en un tercer país: Una entidad que, si tuviera su domicilio social en un Estado miembro, estaría obligada, con arreglo a las disposiciones de ese Estado, a obtener una autorización para realizar la actividad reaseguradora.

7. Reaseguro: La actividad consistente en la aceptación de riesgos cedidos por una entidad aseguradora o por una entidad reaseguradora, incluidas las entidades aseguradoras o reaseguradoras domiciliadas en terceros países.

8. Reaseguro limitado: Reaseguro en el que el potencial máximo de pérdida explícito, expresado en términos de riesgo económico máximo transferido, derivado tanto de un riesgo de suscripción significativo como de la transferencia de un riesgo temporal, supera la prima durante la totalidad del período de vigencia del contrato por una cuantía limitada pero significativa, junto con, al menos, una de las siguientes características:

a) Consideración explícita y material del valor temporal del dinero.

b) Disposiciones contractuales que moderen el equilibrio de la experiencia económica entre las partes en el tiempo, con el fin de lograr la transferencia de riesgo prevista.

En el caso de España la Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras establece los siguientes ramos de riesgos asegurables, todos ellos considerados riesgos de seguro.

A) Ramos de seguro distintos del seguro de vida y riesgos accesorios.

a) En el seguro directo distinto del seguro de vida la clasificación de los riesgos por ramos se ajustará a lo siguiente:

1. Accidentes.

Las prestaciones en este ramo pueden ser: a tanto alzado, de indemnización, mixta de ambos y de cobertura de ocupantes de vehículos.

2. Enfermedad (comprendida la asistencia sanitaria y la dependencia).

Las prestaciones en este ramo pueden ser a tanto alzado, de reparación, bien mediante el reembolso de los gastos ocasionados, bien mediante la garantía de la prestación del servicio, o mixta de ambos.

3. Vehículos terrestres (no ferroviarios).

Incluye todo daño sufrido por vehículos terrestres, sean o no automóviles, salvo los ferroviarios.

4. Vehículos ferroviarios.

5. Vehículos aéreos.

6. Vehículos marítimos, lacustres y fluviales.

7. Mercancías transportadas (comprendidos los equipajes y demás bienes transportados).

8. Incendio y elementos naturales.

Incluye todo daño sufrido por los bienes (distinto de los comprendidos en los ramos 3, 4, 5, 6 y 7) causado por incendio, explosión, tormenta, elementos naturales distintos de la tempestad, energía nuclear y hundimiento de terreno.

9. Otros daños a los bienes. Incluye todo daño sufrido por los bienes (distinto de los comprendidos en los ramos 3, 4, 5, 6 y 7) causado por el granizo o la helada, así como por robo u otros sucesos distintos de los incluidos en el ramo 8.

10. Responsabilidad civil en vehículos terrestres automóviles (comprendida la responsabilidad del transportista).

11. Responsabilidad civil en vehículos aéreos (comprendida la responsabilidad del transportista).

12. Responsabilidad civil en vehículos marítimos, lacustres y fluviales (comprendida la responsabilidad del transportista).

13. Responsabilidad civil en general.

Comprende toda responsabilidad distinta de las mencionadas en los ramos 10, 11 y 12.

14. Crédito.

Comprende insolvencia general, venta a plazos, crédito a la exportación, crédito hipotecario y crédito agrícola.

15. Caución (directa e indirecta).

16. Pérdidas pecuniarias diversas.

Incluye riesgos del empleo, insuficiencia de ingresos (en general), mal tiempo, pérdida de beneficios, subsidio por privación temporal del permiso de conducir, persistencia de gastos generales, gastos comerciales imprevistos, pérdida del valor venal, pérdidas de alquileres o rentas, pérdidas comerciales indirectas distintas de las anteriormente mencionadas, pérdidas pecuniarias no comerciales y otras pérdidas pecuniarias.

17. Defensa jurídica.

Las entidades aseguradoras habrán de optar por alguna de las siguientes modalidades de gestión:

a) Confiar la gestión de los siniestros del ramo de defensa jurídica a una entidad jurídicamente distinta, que habrá de mencionarse en el contrato. Si dicha entidad se hallase vinculada a otra que practique algún ramo de seguro distinto del de vida, los miembros del personal de la primera que se ocupen de la gestión de si-

niestros o del asesoramiento jurídico relativo a dicha gestión no podrán ejercer simultáneamente la misma o parecida actividad en la segunda. Tampoco podrán ser comunes las personas que desempeñen cargos de dirección de ambas entidades.

b) Garantizar en el contrato de seguro que ningún miembro del personal que se ocupe de la gestión de asesoramiento jurídico relativo a dicha gestión ejerza al tiempo una actividad parecida en otro ramo si la entidad aseguradora opera en varios o para otra entidad que opere en algún ramo distinto del de vida y que tenga con la aseguradora de defensa jurídica vínculos financieros, comerciales o administrativos con independencia de que esté o no especializada en dicho ramo.

c) Prever en el contrato el derecho del asegurado a confiar la defensa de sus intereses, a partir del momento en que tenga derecho a reclamar la intervención del asegurador según lo dispuesto en la póliza, a un abogado de su elección.

18. Asistencia.

Asistencia a las personas que se encuentren en dificultades durante desplazamientos o ausencias de su domicilio o de su lugar de residencia permanente. Comprenderá también la asistencia a las personas que se encuentren en dificultades en circunstancias distintas, determinadas reglamentariamente, siempre que no sean objeto de cobertura en otros ramos de seguro.

19. Decesos.

Incluye operaciones de seguro que garanticen la prestación de servicios funerarios para el caso de que se produzca el fallecimiento, o bien subsidiariamente, cuando no se pueda realizar la prestación, por causa de fuerza mayor o por haberse realizado el servicio a través de otros medios, distintos de los dispuestos por la aseguradora, a satisfacer a los herederos legales del asegurado fallecido la suma asegurada, que no debe exceder del valor medio de los gastos funerarios por un fallecimiento.

Los riesgos comprendidos en un ramo no podrán ser clasificados en otro ramo, sin perjuicio de lo dispuesto respecto de los riesgos accesorios en el apartado 4.

Cuando la autorización se conceda simultáneamente para varios ramos, se otorgará con las siguientes denominaciones:

1.º «Accidentes y enfermedad»: Cuando se autoricen los ramos 1 y 2.

2.º «Seguro de automóvil»: Cuando la autorización comprenda la cobertura de ocupantes de vehículos del ramo 1 y los ramos 3, 7 y 10.

3.º «Seguro marítimo y de transporte»: Cuando la autorización comprenda la cobertura de ocupantes de vehículos del ramo 1 y los ramos 4, 6, 7 y 12.

4.º «Seguro de aviación»: Cuando la autorización comprenda la cobertura de ocupantes de vehículos del ramo 1 y los ramos 5, 7 y 11.

5.º «Incendio y otros daños a los bienes»: Cuando se autoricen los ramos 8 y 9.

6.º «Responsabilidad civil»: Cuando se autoricen los ramos 10, 11, 12 y 13.

7.º «Crédito y caución»: Cuando se autoricen los ramos 14 y 15.

8.º «Seguros generales»: Cuando se autoricen todos los ramos de seguro directo distinto del seguro de vida enumerados en este artículo.

b) Riesgos accesorios.

La entidad aseguradora que obtenga una autorización para un riesgo principal perteneciente a un ramo de seguro distinto del de vida o a un grupo de ramos podrá, asimismo, cubrir los riesgos comprendidos en otro ramo sin necesidad de obtener autorización para dichos riesgos, siempre que concurran los siguientes requisitos:

1.º Que estén vinculados al riesgo principal.

2.º Que se refieran al objeto cubierto contra el riesgo principal.

3.º Que estén cubiertos por el contrato que cubre el riesgo principal.

4.º Que para la autorización en el ramo al que pertenezca el riesgo accesorio no se requieran mayores garantías financieras previas que para el principal, salvo, en cuanto a este último requisito, que el riesgo accesorio sea el de responsabilidad civil cuya cobertura no supere los límites que reglamentariamente se determinen.

Cuando el ramo accesorio sea el 2 (enfermedad), éste no comprenderá prestaciones de asistencia sanitaria o prestaciones de asistencia por dependencia.

Los riesgos comprendidos en los ramos 14 (crédito), 15 (caución) y 17 (defensa jurídica), no podrán ser considerados accesorios de otros ramos, salvo el ramo 17 (defensa jurídica), que, cuando se cumplan las condiciones exigidas en el párrafo anterior, podrá ser considerado como riesgo accesorio del ramo 18 (asistencia), si el riesgo principal sólo se refiere a la asistencia facilitada a las personas en dificultades con motivo de desplazamientos o de ausencias del domicilio o del lugar de residencia permanente, y como riesgo accesorio del ramo 6 (vehículos marítimos, lacustres y fluviales), cuando se refiera a litigios o riesgos que resulten de la utilización de embarcaciones marítimas o que estén relacionados con dicha utilización.

B) Ramo de vida y riesgos complementarios.

a) El seguro directo sobre la vida se incluye en un solo ramo, el ramo de vida, que comprenderá:

1. El seguro sobre la vida, tanto para caso de muerte como de supervivencia, o ambos conjuntamente, incluido en el de supervivencia el seguro de renta; el seguro sobre la vida con contraseguro; el seguro de nupcialidad, y el seguro de natalidad. Asimismo, comprende cualquiera de estos seguros cuando estén vinculados con

fondos de inversión u otros activos a los que se refiere el artículo 73. Igualmente, podrá comprender el seguro de dependencia.

2. Las operaciones de capitalización basadas en técnica actuarial, que consistan en obtener compromisos determinados en cuanto a su duración y a su importe a cambio de desembolsos únicos o periódicos previamente fijados.

3. Las operaciones de gestión de fondos colectivos de jubilación, entendiendo por tales aquellas que supongan para la entidad aseguradora administrar las inversiones y, particularmente, los activos representativos de las reservas de las entidades que otorgan prestaciones en caso de muerte, en caso de vida o en caso de cese o reducción de actividades. También estarán comprendidas tales operaciones cuando lleven una garantía de seguro, sea sobre la conservación del capital, sea sobre la percepción de un interés mínimo.

4. Las operaciones tontinas, entendiendo por tales aquellas que lleven consigo la constitución de asociaciones que reúnan partícipes para capitalizar en común sus aportaciones y para repartir el activo así constituido entre los supervivientes o entre sus herederos.

b) Riesgos complementarios.

Las entidades autorizadas para operar en el ramo de vida podrán cubrir como riesgos complementarios los comprendidos en el ramo 1 (accidentes) y en el ramo 2 (enfermedad), sin necesidad de obtener autorización para dichos ramos, siempre que concurran los siguientes requisitos:

1.º Que estén vinculados con el riesgo principal.

2.º Que se refieran al objeto cubierto contra el riesgo principal.

3.º Que estén garantizados en un mismo contrato con éste.

4.º Cuando el ramo complementario sea el 2 (enfermedad), que éste no comprenda prestaciones de asistencia sanitaria o prestaciones de asistencia por dependencia.

F.- Por el sometimiento a normas del contrato. Grandes Riesgos.

Otra forma de clasificar los riesgos por su magnitud y sometimiento a la normativa de seguros se refiere a los denominados grandes riesgos susceptibles de no estar sometido a la normativa de contratación de la Ley de Contrato de seguro y riesgos sometidos necesariamente a los imperativos legales del marco contractual del contrato de seguro.

En los contratos de seguro por grandes riesgos las partes tendrán libre elección de la ley aplicable. La definición de grandes riesgos del número 2 del artículo 107 de la LCS fue derogada por la letra a) de la disposición derogatoria de la Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras («B.O.E.» 15 julio) que entró en vigor el 1 enero 2016, sin embargo

podemos encontrar la definición legal precisamente en la LOSSEAR (artículo 11); así, a efectos de lo establecido en la normativa española de control y supervisión de seguros privados y de contratos de seguro, se entiende por grandes riesgos los siguientes:

a) Los de vehículos ferroviarios, vehículos aéreos, vehículos marítimos, lacustres y fluviales, mercancías transportadas (comprendidos los equipajes y demás bienes transportados), la responsabilidad civil en vehículos aéreos (comprendida la responsabilidad del transportista) y la responsabilidad civil de vehículos marítimos, lacustres y fluviales (comprendida la responsabilidad civil del transportista).

b) Los de crédito y de caución cuando el tomador y el asegurado ejerzan a título profesional una actividad industrial, comercial o liberal y el riesgo se refiera a dicha actividad.

c) Los de vehículos terrestres (no ferroviarios), incendio y elementos naturales, otros daños a los bienes, responsabilidad civil en vehículos terrestres automóviles (comprendida la responsabilidad del transportista), responsabilidad civil en general y pérdidas pecuniarias diversas, siempre que el tomador supere los límites de, al menos, dos de los tres criterios siguientes:

Activo total del balance: 6.200.000 euros.

Importe neto del volumen de negocios: 12.800.000 euros.

Número medio de empleados durante el ejercicio: 250 empleados.

Si el tomador del seguro formara parte de un grupo de sociedades cuyas cuentas consolidadas se establezcan con arreglo a lo dispuesto en los artículos 42 a 49 del Código de Comercio, los criterios mencionados.

La ley española sobre el contrato de seguro es de aplicación al seguro contra daños en los siguientes casos:

a) Cuando se refiera a riesgos que estén localizados en territorio español y el tomador del seguro tenga en él su residencia habitual, si se trata de persona física, o su domicilio social o sede de gestión administrativa y dirección de los negocios, si se trata de persona jurídica.

b) Cuando el contrato se concluya en cumplimiento de una obligación de asegurarse impuesta por la ley española.

En los contratos de seguro por grandes riesgos las partes tendrán libre elección de la ley aplicable. Fuera de los anteriores casos, regirán las siguientes normas para determinar la ley aplicable al contrato de seguro contra daños:

a) Cuando se refiera a riesgos que estén localizados en territorio español y el tomador del seguro no tenga en él su residencia habitual, domicilio social o sede de gestión administrativa y dirección de los negocios, las partes podrán elegir entre la aplicación de la ley española o la ley del Estado en que el tomador del seguro tenga dicha residencia, domicilio social o dirección efectiva.

b) Cuando el tomador del seguro sea un empresario o un profesional y el contrato cubra riesgos relativos a sus actividades realizadas en distintos Estados del Espacio Económico Europeo, las partes podrán elegir entre la ley de cualquiera de los Estados en que los riesgos estén localizados o la de aquél en que el tomador tenga su residencia, domicilio social o sede de gestión administrativa y dirección de sus negocios.

c) Cuando la garantía de los riesgos que estén localizados en territorio español se limite a los siniestros que puedan ocurrir en un Estado miembro del Espacio Económico Europeo distinto de España, las partes pueden elegir la ley de dicho Estado.

La localización del riesgo se determinará conforme a lo previsto en la LOSSEAR. Se entiende por Estado miembro de localización del riesgo:

a) El Estado miembro en que se hallen los bienes, cuando el seguro se refiera a inmuebles, o bien a éstos y a su contenido, si este último está cubierto por la misma póliza de seguro.

Cuando el seguro se refiera a bienes muebles que se encuentren en un inmueble, y a efectos de los tributos y recargos legalmente exigibles, el Estado miembro en el que se encuentre situado el inmueble, incluso si éste y su contenido no estuvieran cubiertos por la misma póliza de seguro, con excepción de los bienes en tránsito comercial.

b) El Estado miembro de matriculación, cuando el seguro se refiera a vehículos de cualquier naturaleza.

c) El Estado miembro en que el tomador del seguro haya firmado el contrato, si su duración es inferior o igual a cuatro meses y se refiere a riesgos que sobrevengan durante un viaje o fuera del domicilio habitual del tomador del seguro, cualquiera que sea el ramo afectado.

d) En todos los casos no expresamente contemplados anteriormente, aquel en que el tomador del seguro tenga su residencia habitual o, si fuera una persona jurídica, aquel en el que se encuentre su domicilio social o la sucursal a que se refiere el contrato.

La elección por las partes de la ley aplicable, cuando sea posible, deberá expresarse en el contrato o desprenderse claramente de su contenido.

A efectos de lo establecido en la LOSSEAR, se entiende por operaciones de coaseguro comunitario, las que reúnan las siguientes condiciones:

1. Que den lugar a la cobertura de uno o más riesgos que puedan calificarse como grandes riesgos.

2. Que participen en la cobertura del riesgo varias entidades aseguradoras, una de las cuales será la entidad aseguradora abridora, de forma no solidaria, en calidad de coaseguradoras, por medio de un contrato único, mediante una prima global y para una misma duración.

3. Que cubran riesgos localizados en la Unión Europea.

4. Que a los efectos de la cobertura del riesgo, la entidad aseguradora abridora se encuentre habilitada para cubrir la totalidad del riesgo.

5. Que al menos una de las entidades coaseguradoras participe en el contrato por medio de su domicilio social o de una sucursal establecida en un Estado miembro distinto del estado de la entidad aseguradora abridora.

6. Que la entidad aseguradora abridora asuma plenamente las funciones que le corresponden en el coaseguro y, en particular, determine las condiciones de seguro y de tarificación.

Las entidades aseguradoras que participen en España en una operación de coaseguro comunitario en calidad de abridoras, así como sus actividades como tales coaseguradoras, se regirán por las disposiciones aplicables al contrato de seguro de grandes riesgos.

Cuando un contrato de seguro pueda calificarse de coaseguro comunitario, las obligaciones que se imponen a las entidades aseguradoras que operen en régimen de libre prestación de servicios según lo dispuesto en los artículos 57 a 59 de la LOSSEAR se aplicarán únicamente a la entidad abridora de la operación. Las entidades aseguradoras españolas que participen en operaciones de coaseguro comunitario deben disponer de datos estadísticos suficientes sobre las operaciones en las que participen en cada uno de los Estados miembros. Si una entidad aseguradora española participa en una operación de coaseguro comunitario calculará las provisiones técnicas correspondientes a su participación en la operación de acuerdo con las disposiciones de la LOSSEAR y las normas que la desarrollen, si bien el importe de las citadas provisiones técnicas habrá de ser como mínimo igual al importe calculado de acuerdo con las normas a las que estuviera sometida la entidad abridora de la operación.

G.- Riesgos asegurables obligatoriamente.

Finalmente existen riesgos cuyo aseguramiento es obligatorio que van desde las operaciones aseguradas por el Consorcio de Compensación de Seguros en relación con los riesgos extraordinarios, riesgos nucleares, seguros agrarios, seguro obligatorio de automóviles, seguros medioambientales, seguro de crédito a la exportación y seguro de crédito y caución, pasando por los seguros deportivos, universitarios, de colegios profesionales (Abogados, Fisioterapeutas, Aparejadores, Arquitectos, Médicos) y los seguros obligatorios propiamente dichos de caza, pesca, construcción (seguros de viviendas, en su construcción, de viviendas turísticas en copropiedad, seguros de edificios), el amplio elenco de la circulación y el transporte (seguro obligatorio de automóviles, seguro de pasajeros de aeronaves, seguro de las aeronaves ligeras, seguros de buques y embarcaciones, buques mercantes, embarcaciones de recreo o deportivas, embarcaciones de alta velocidad, motos náuticas, otros vehículos náuticos, de pasajeros marítimos, transporte de mercancías y de logística, transportes ordinarios, transportes especiales y logística).

También hay actividades sujetas a la necesidad de aseguramiento en cooperantes, de estudiantes, de espectáculos (seguro de fuegos artificiales, seguros taurinos, de festejos taurinos, de encierros, de demostraciones aéreas civiles) de actividades peligrosas con productos tóxicos (con productos químicos, con productos derivados del petróleo e hidrocarburos, de hidrocarburos, de gas, con explosivos), de actividades con impacto en el medio ambiente y responsabilidad ambiental de la Ley 26/2007 de Responsabilidad Medioambiental, seguro de traslados transfronterizos de residuos, seguro de vertederos y seguro de contaminación por hidrocarburos.

Actividades variopintas han de ser necesariamente aseguradas, como los cambistas profesionales, los intermediarios de mercado de valores, mediadores de seguros, administradores concursales, sociedades de tasación de inmuebles, agencias de viajes, entidades colaboradoras de las Administraciones Públicas (en la realización de inspecciones y pruebas de vuelo, en el control de productos alimentarios, en el control de productos de construcción, en el control de calidad de la edificación, en Comprobación de barcos de recreo y motos náuticas, en control de aguas vertidas a dominio público hidráulico, de equipos a presión transportables con mercancías peligrosas, de verificación aparatos a usar en atmósferas explosivas, de control de aparatos de gas, en el sector minero, en la verificación de juguetes y en las estaciones ITV).

El mundo de los seguros obligatorios de responsabilidad civil profesional y otros oficios regulados es especialmente promiscuo a la hora de su aseguramiento. Entre ellos encontramos los seguros como el de los Notarios, los Agentes de seguros, los Agentes de la Propiedad Industrial, el seguro de los Sanitarios (los sanitarios de la sanidad privada, centros de fecundación in vitro, ensayos clínicos), Auditores de Cuentas, Mediadores de Conflictos, Instaladores y Reparadores (Instaladores de equipos contra incendios, Instaladores de gas, Instaladores de suministro y evacuación de agua, Instaladores y conservadores de ascensores), seguros de instalaciones (instalaciones de productos petrolíferos y gas, instalaciones de antenas radíoeléctricas de aficionados e instalaciones de telecomunicación. Significativo es el mundo de la seguridad privada con sus seguros de instaladores, Vigilantes Jurados, Centrales de seguridad, etc.).

Muchos son seguros obligatorios existentes en España y aún más las actividades sujetas a la necesidad de aseguramiento, como requisito para el ejercicio de las mismas. Tal es la cantidad y variedad de seguros que no siempre responden a las exigencias técnicas que de ellos se espera.

Los recientes cambios legislativos tendentes a registrar y armonizar este marco jurídico son útiles para los ciudadanos, para las empresas y para las administraciones públicas, ya algunos anduvieron que en esta materia un poco despistados. Tan importante es registrar la información relativa a los seguros establecidos por norma con rango de ley, como aquellos otros seguros exigidos por otras disposiciones de rango inferior.

La Directiva 2009/38/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, sobre el acceso a la actividad de seguro y de reaseguro y su ejercicio, conocida como Directiva Solvencia II, prevé que cada estado comunicará a la Comisión los riesgos para los cuales su legislación impone la obligatoriedad de un seguro.

La disposición adicional segunda de la Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras (LOSSEAR), señala que la Dirección General de Seguros y Fondos de Pensiones comunicará a la Comisión Europea, de acuerdo con el registro que se desarrolle reglamentariamente y que gestionará el Consorcio de Compensación de Seguros, los seguros obligatorios existentes en España, indicando las disposiciones específicas que regulan el seguro obligatorio.

Los órganos competentes de las Comunidades Autónomas informarán a la Dirección General de Seguros y Fondos de Pensiones de los seguros obligatorios existentes de acuerdo con su normativa. Así mismo, recabarán y comunicarán la información sobre los seguros de suscripción obligatoria aprobados por las entidades que integran la administración local de su ámbito territorial de competencia.

El registro público de Seguros Obligatorios (RSO) ofrece transparencia y garantía a todos los operadores de este sector, pero también a los asegurados que podrán verificar con facilidad el cumplimiento de las exigencias normativas de aseguramiento en cada caso. Contiene la información actualizada relativa a los seguros obligatorios existentes en España, ya sean de ámbito estatal o de una determinada Comunidad autónoma, y las disposiciones legales específicas que los regulan.

La información que recoge el RSO en cada momento, en cuanto a los seguros obligatorios que constan inscritos en el mismo y a la información que sobre cada uno de ellos se encuentra reflejada, es estrictamente la remitida al RSO hasta dicho momento por los distintos órganos correspondientes de la administración estatal o autonómica.

El acceso a la información del RSO favorecerá la dificultad que plantea la enorme cantidad de normas de todo tipo que exigen la necesidad de aseguramiento para llevar realizar determinadas actividades sobre bases técnicas que no siempre se ajustan a la realidad del mercado asegurador. [6]

---

6 El Consorcio de Compensación de Seguros (CCS) *http://www.consorseguros.es/web/inicio* tiene legalmente encomendada la gestión de este registro de Seguros Obligatorios (RSO). En su condición de gestor del mismo, el CCS elaborará cada año un informe sobre el contenido del RSO que incluirá, por una parte, listados de los seguros obligatorios ordenados por distintos criterios (fecha de entrada en vigor; actividades para las que se exigen los seguros obligatorios; rango legal de las normas que los regulan; y ámbito estatal o autonómico) y, por otra, los cambios producidos durante el año (nuevos seguros; seguros modificados; y seguros suprimidos). El CCS tiene legalmente encomendada la gestión de este RSO. En su condición de gestor del mismo. La información del RSO es pública, se refiere a seguros obligatorios vigentes en cada momento, y puede consultarse en su Web. La normativa legal que regula el RSO está constituida por la disposición adicional segunda de la Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras; por la disposición adicional primera del Real Decreto 1060/2015, de 20 de noviembre, que desarrolla dicha Ley; y por la Resolución de 18 de diciembre de 2015 de la Dirección General de Seguros y Fondos de Pensiones (DGSFP), por la que se concreta el contenido del RSO, el procedimiento y las especificaciones de la información a remitir a la DGSFP. Para consultas V. *http://www.consorseguros.es/web/registro-seguros-obligatorios*.

2. TÉRMINOS RELATIVOS A LA GESTIÓN DEL RIESGO

2.1.- Gestión del riesgo.

"Declaración de las intenciones y orientaciones generales de una organización en relación con la gestión del riesgo."

La **gestión de riesgos** es la acción directa de instituciones, empresas, organizaciones y profesionales ante el riesgo, utilizando una metodología científica como nuevo paradigma de atención al riesgo.

La gestión de riesgos de una organización es el conjunto de métodos que permite identificar, analizar y evaluar los riesgos a los que está sometida la misma, cuantificando las pérdidas derivadas de su acaecimiento, determinando las pérdidas para su eliminación y/o reducción, optimizándolas en términos económicos, a fin de preservar y/o mantener sus activos materiales, personales e inmateriales de la organización en la posición óptima para el desempeño de sus objetivos.

Se entiende por **gerencia de riesgos**, la actividad profesional directiva, de carácter estratégico, que tiene por objetivo identificar, evaluar, intervenir, prevenir, proteger, tomar decisiones de actuación e informar, las situaciones de riesgo implícito y/o explícito en una organización, mediante una metodología científica y directiva, cuya finalidad es conseguir el cumplimiento de los objetivos estratégicos de la misma y la atención de todos sus grupos de interés

Se entiende por **administración del riesgo**, la actividad ordenada y organizativa de instituciones públicas y privadas con o sin ánimo de lucro, con carácter integrador e integrado, para intervenir en situaciones de riesgo implícito y/o explícito, vinculando la actividad de la financiación de los programas de atención al riesgo, a la retención y/o transferencia del mismo.

La gestión de riesgo operativo persigue que la organización identifique, evalúe, controle y haga un tratamiento adecuado de los riesgos soportados de la forma más eficaz posible, para proteger sus activos y optimizar la exposición a los mismos.

Históricamente, conforme se recogía en el informe consultivo del Comité de Supervisión Bancaria de Basilea II[7], no existía hasta aquel momento una definición generalmente aceptada de riesgo operacional. La definición más extendida de riesgo operacional era aquel riesgo que no era riesgo de mercado o riesgo de crédito.

---

7 Comité de Supervisión Bancaria de Basilea II, "Operational Risk, Consultative Document: Supporting Document to the New Basel Capital Accord", Basel Committee on Banking Supervision, Basilea, 2001.

Sin embargo, más recientemente se ha vendido relacionando este concepto como el riesgo de pérdida proveniente de varios tipos de errores humanos o técnicos, y otras lo han asociado con la interrupción del negocio, y con los riesgos legales y administrativos; en suma, el riesgo de sufrir pérdidas debido a la inadecuación o fallos que los procesos, personas o sistemas internos o bien a causa de acontecimientos externos.

En la Enciclopedia de Economía y Negocios se define el riesgo operativo equiparándolo al operacional, afirmando que puede manifestarse de diversas formas: "errores, fraudes, caída de la performance de la entidad, eventos y desastres no controlados y esperados, que afecten al desarrollo de la actividad; pérdida de información, problemas en los sistemas tecnológicos de control e información, etcétera."[8] Dentro del riesgo operativo distingue entre:

a) Riesgo de control o técnico[9].

b) Riesgo de transacción por los siguientes motivos.

- Error en la ejecución
- Complejidad del producto
- Error en el registro
- Error en la liquidación
- Riesgo de la opción de entregable
- Falta de documentación e incumplimiento de las normas de contratación

c) Riesgo de sistema[10] por las siguientes causas:

- Error del modelo o programa empleado en la medición y control de riesgos.
- Error en la valoración de las posiciones.
- Fallo del sistema
- Fallo de las telecomunicaciones.
- En un mercado organizado por falta de medidas y garantías oportunas.

---

8 LÓPEZ DOMÍNGUE, IGNACIO, Enciclopedia de Economía y Negocios Vol. 17, pág.: 9.403.

9 "La complejidad de la operativa del mercado, que puede llevar consigo errores, fallos de control interno, malos sistemas de valoración del riesgo y de información y fraude, constituiría el riesgo de control o técnico, que se intenta solucionar mediante la separación de la actividad negociadora, la auditora o controladora y la registradora." LÓPEZ DOMÍNGUE, IGNACIO. ***Ob. cit.*** Pág.: 9.404.

10 Entendiendo como tal: "el diferente resultado que se obtendría aplicando una misma metodología de medición de riesgos sobre una determinada cartera, en empresas distintas, pero dentro de la misma actividad", ***ob. cit.*** pág.: 9.405.

Frost desglosa dos componentes de los riesgos operativos, distinguiendo por un lado la integridad operativa (idoneidad de los controles operativos y el gobierno empresarial) y por otro la materialización o prestación de servicios (capacidad de implementar los procesos empresariales de forma constante). En el primer caso se refiere a la gestión de riesgos operativos que tienen su origen en entornos inadecuados, tales como fraude, errores u omisiones, hechos dolosos, ***moobing***, deficientes políticas de protección de los derechos de los trabajadores, inexistencia de sistemas de control y protección del medioambiente, etc. En el segundo supuesto se está refiriendo a la gestión de riesgos de orígenes imprevistos en las actividades de la empresa, procesos, gestión de proyecto, gestión de proveedores, gestión de capacidad y servicio, gestión de crisis, personal, etc.[11]

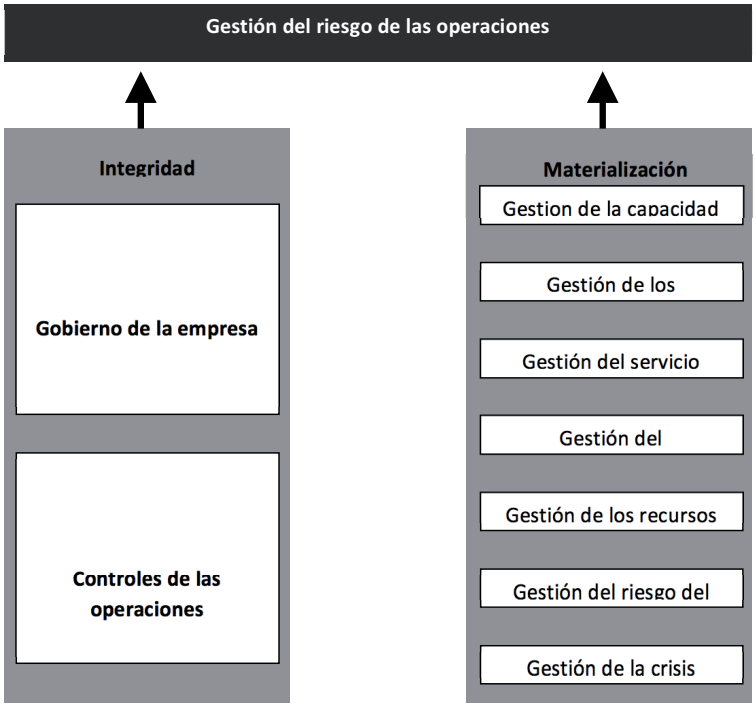

Gráfico 1. Esquema de los elementos de la gestión de riesgos operativos seguido por CRIST FROST.[12]

En el año 2005 se apuntaba la necesidad de avanzar en la metodología de gestión de riesgos hacia un nuevo modelo en el que esta actividad formará parte esencial de la gestión estratégica de cualquier empresa. Por medio de este proceso las empresas se enfrentan, dirigen y coordinan los riesgos relacionados con sus actividades, con el fin de obtener un beneficio sostenido en cada una de dichas actividades y en el conjunto

---

11 Véase al respecto CRIST FROST y otros. Manual de gestión de riesgos operativos, pág. 14: Ediciones Deusto, Bilbao 2002.

12 CRIST FROST. y otros ***ob. cit.*** Pág.: 15.

de todas. Decíamos entonces que la gestión de riesgos constituye una actividad funcional, en ocasiones operacional de la organización que permite reforzar los objetivos estratégicos de la misma, actuando en todas sus áreas para lograr ir hacia una meta común: el aumento del valor para los ***stakeholders*** en sus ámbitos económico, social y medioambiental y un adecuado gobierno de la organización. El proceso de gerencia estratégica de los riesgos, consiste en la integración de la política de riesgos en todas las áreas de la empresa: planificación estratégica, proyectos, desarrollo, procesos de toma de decisiones, etc., con el fin de reforzar los objetivos estratégicos de la entidad y la obtención de ventajas competitivas a través del conocimiento del nivel global de riesgo de la organización y su posible incidencia en los objetivos estratégicos de la misma.[13]

Como vemos con el paso del tiempo las organizaciones han venido adoptando sus propias definiciones de lo que es el riesgo operacional, sin embargo, podemos afirmar que hay un consenso general sobre lo que establece el Nuevo Acuerdo de Capital de Basilea II[14], que es el riesgo de pérdida, directo o indirecto, causado por unos procesos internos inadecuados y/o erróneos, personas y sistemas o por sucesos externos.[15]

En el sector asegurador, el riesgo operacional es, según los estándares de Solvencia II, el riesgo de pérdida debido a unos inadecuados o fallos internos de procesos, empleados, sistemas o eventos externos.[16]

El término gestión del riesgo operacional (ORM) se define como un proceso cíclico continuo que incluye la evaluación de riesgos, toma de decisiones de riesgo, y la aplicación de controles de riesgo, lo que resulta en la aceptación, la mitigación o prevención de riesgos. ORM es la supervisión de los riesgos operativos, incluyendo el riesgo de pérdidas resultantes de los procesos internos no o inadecuada y sistemas de los factores humanos, o eventos externos.

Los principios básicos del ORM pivotan sobre distintas actitudes ante los problemas detectados que van desde la aceptación el riesgo cuando los beneficios superan a los costos o bien su no aceptación cuando se considera que los riesgos son innecesarios. En cualquier caso y sea cual fuere la opción que se adopte, se precisa una gestión de los riesgos soportados mediante una política y procedimientos adecuados que permitan tomar decisiones para controlar, minimizar y tratar los riesgos soportados.

---

13 FERNÁNDEZ ISLA, GONZALO - ITURMENDI MORALES, GONZALO, Cambios en el proceso de gerencia de riesgos, Barcelona septiembre de 2005.

14 Los acuerdos de Basilea II consisten en recomendaciones sobre la legislación y regulación bancaria y son emitidos por el Comité de supervisión bancaria de Basilea. El propósito de Basilea II, publicado inicialmente en junio de 2004, es la creación de un estándar internacional que sirva de referencia a los reguladores bancarios, con objeto de establecer los requerimientos de capital necesarios, para asegurar la protección de las entidades frente a los riesgos financieros y operativos.

15 Comité de Supervisión Bancaria de Basilea II, "Operational Risk, Consultative Document: Supporting Document to the New Basel Capital Accord", Basel Committee on Banking Supervision, Basilea, 2001.

16 Véase Ceiops, "Quantitative Impact Study 2 - Technical Specification", CEIOPS, Bruselas, 2006, pág. 57. "SCRop operational risk module. 5.189 Operational risk is the risk of loss arising from inadequate or failed internal processes, people, systems or from external events."
http://www.dgsfp.meh.es/sector/qis2/QIS2TechnicalSpecification.pdf

El riesgo más relevante en el ámbito bancario es el riesgo de crédito. Sin embargo, el riesgo operacional está altamente considerado por su importancia, junto con los riesgos de cambio, de tipo de interés, de liquidez y riesgo-país. Para las entidades bancarias se acepta la definición apuntada anteriormente como el riesgo de pérdida para una entidad financiera derivado de una incidencia en sus procesos, sistemas o en la actuación de su personal o por un hecho causado por un acontecimiento externo. Esta apreciación del riesgo no se basa por tanto en el riesgo de insolvencia o impago de las deudas, sino como que por determinados fallos (en procesos internos, del personal, informáticos) de los distintos sistemas la entidad financiera por cuya causa se originen pérdidas económicas.

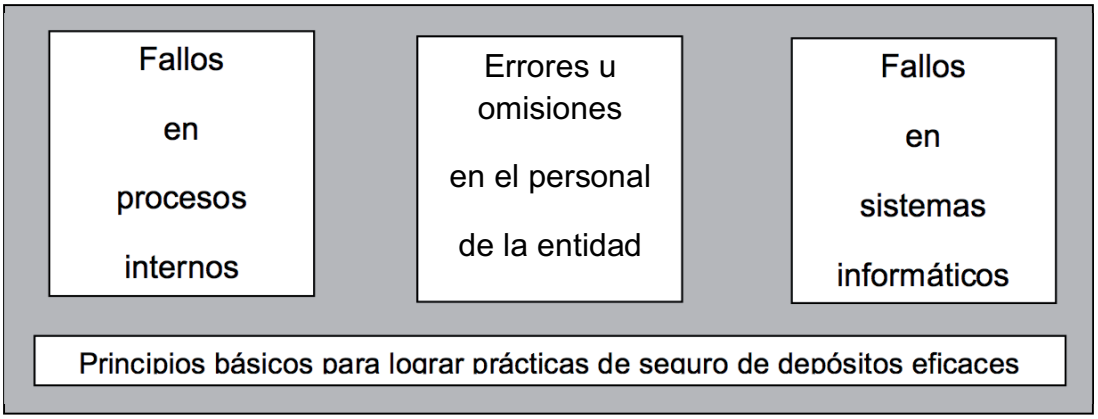

Gráfico 2.

El Comité de Supervisión Bancaria de Basilea, Asociación Internacional de Aseguradores de Depósitos, estableció en el año 2009 una serie de Principios Básicos que suponen un esquema voluntario para lograr prácticas de seguro de depósitos eficaces; siendo las autoridades nacionales libres de implementar las medidas adicionales que consideren necesarias para obtener un seguro de depósitos efectivo dentro de sus respectivas jurisdicciones. Los Principios Básicos no están diseñados para abarcar todas las necesidades y circunstancias de todos los sistemas bancarios. Las circunstancias particulares de cada país deben tomarse en cuenta en el contexto de las leyes y los poderes existentes para satisfacer los objetivos de interés público y el mandato del sistema de seguro de depósitos. Advierte el Comité que un sistema de seguro de depósitos eficaz debe basarse en diversos elementos externos o precondiciones que incluyen la valoración continua de la economía y del sistema bancario, el buen gobierno de las agencias que integran la red de seguridad del sistema financiero, una intensa regulación y supervisión prudencial; un marco legal y un régimen de transparencia y rendición de cuentas bien desarrollados.

La gestión de riesgos corporativos puede ayudar a asegurar que la alta dirección de la organización sea consciente en forma oportuna sólo del grado de progreso de la entidad hacia la consecución de sus objetivos estratégicos y operativos. Pero esto no es una garantía de seguridad razonable de que los objetivos en sí mismos se alcancen.

El Informe COSO sobre gestión de riesgos corporativos distingue entre objetivos **estratégicos** y objetivos **operativos**. Los primeros se refieren a la "misión", "visión" o "finalidad", que la alta dirección establece, configurando en gran medida la razón de ser de la entidad en términos generales. "A partir de esto, la dirección fija los objetivos estratégicos, formula la estrategia y establece los correspondientes objetivos operativos, de información y de cumplimiento para la organización. Aunque la misión de una entidad y sus objetivos estratégicos sean generalmente estables, su estrategia y muchos objetivos relacionados con ella son más dinámicos y se adecuan mejor a las cambiantes condiciones internas y externas. A medida que éstas cambian, la estrategia y los objetivos conexos deben volver a situarse en línea con los objetivos estratégicos."[17]

Aunque el Informe COSO no habla en ningún momento de riesgos operativos, admite tres categorías amplias de objetivos que al mismo tiempo que suponen metas a alcanzar, también son susceptibles de vulnerabilidad. En primer lugar, los **objetivos operativos** propiamente dichos, que se corresponden con la eficacia y eficiencia de las operaciones de la organización, incluyendo los objetivos de rendimiento y rentabilidad y de salvaguarda de recursos frente a pérdidas. Seguidamente diferencia los denominados **objetivos de información**, que son los relativos a la fiabilidad de la información. Incluyen información interna y externa e implican la financiera y no financiera; y, finalmente establece una última categoría en los denominados **objetivos de cumplimiento**, que se refieren a la verificación de cumplimiento normativo o "compliance".[18]

La norma para la gestión eficaz de los riesgos. (ISO 31010), contempla la herramienta de gestión de riesgos denominada *Business impact analysis* (BIA)[19] dentro de una serie de normas ISO31000 publicadas en 2009 y 2011 por AENOR, como es la norma UNEISO31010 sobre las técnicas de evaluación del riesgo. La norma recopila más de treinta técnicas de identificación, análisis y evaluación que pueden ser aplicadas para la gestión eficaz de los riesgos entre cuyas herramientas se encuentra el análisis de

---

17 Gestión de Riesgos Corporativos. Marco Integrado. Resumen Ejecutivo Marco. Committee of Sponsoring Organizations of the Treadway Commission (COSO), revisión de septiembre de 2004. Edic. mayo 2005, ISBN: 84-933856-1-3. Pág. 50.

18 El Informe COSO afirma al respecto de los objetivos operativos, en ob. cit. Págs. 51 y 52: "Los objetivos operativos se refieren a la eficacia y eficiencia de las operaciones de la entidad e incluyen otros subobjetivos orientados a mejorar ambas características mediante la movilización de la empresa hacia sus metas finales. Los objetivos operativos deben reflejar los entornos empresarial, sectorial y económico en los que actúa la entidad. Necesitan, por ejemplo, ser relevantes respecto a las presiones competitivas hacia la calidad, una menor duración del ciclo de puesta a disposición del producto en el mercado o hacia los cambios tecnológicos. La dirección debe asegurar que los objetivos reflejan la realidad y las exigencias del mercado y que están expresados en términos que permitan conocer las principales medidas del rendimiento. Un conjunto claro de objetivos operativos, vinculados a sub-objetivos, es esencial para el éxito. Los objetivos operativos proporcionan un punto de focalización para orientar la asignación de recursos. Si los objetivos no son claros o no están bien concebidos, dicha asignación puede resultar desenfocada"s. Marco Integrado. Resumen Ejecutivo Marco. Committee of Sponsoring Organizations of the Treadway Commission (COSO), revisión de septiembre de 2004. Edic. mayo 2005, ISBN: 84-933856-1-3. Pág. 50.

19 Análisis de impacto en el negocio (BIA).

impacto en el negocio (BIA). Notemos que el abanico de técnicas de la norma ISO 31010 es amplio, pero no excluye otras más específicas y adaptadas a cada caso.

En cualquier caso, resulta necesario que tanto en la política, como el diseño y la estructura de gestión del riesgo operacional esté implicados los miembros de los órganos de administración y representación de la organización que deberán definir, mantener y retroalimentar con claridad y precisión la política, metodología y normativa sobre gestión de riesgos. A su vez, el equipo profesional encargado de ejecutar el plan deberá asesorar a la dirección sobre la forma de realizar evaluaciones de riesgo operacional, sobre las mejoras en los controles y su supervisión, analizar los informes específicos sobre riesgos y sobre los incidentes más importantes que se produzcan, supervisar los acontecimientos que pudieran tener un efecto importante sobre la empresa y su repercusión sobre el área de riesgos operacionales, supervisar las técnicas de gestión de riesgos y su influencia sobre la estructura general de la misma y finalmente revisar la eficacia del área organizativa de gestión de riesgos.

Podemos afirmar que verdaderamente el riesgo operacional afecta a todo tipo de organizaciones, no siendo –por tanto- exclusivo del sector financiero. En consecuencia, tanto el tamaño como la actividad de la organización no son elementos determinantes para apreciar la existencia de estos riesgos, los cuales están íntimamente ligados los objetivos operativos propiamente dichos, coincidentes con la eficacia y eficiencia de las operaciones de la entidad, incluyendo los objetivos de rendimiento y rentabilidad y de salvaguarda de recursos frente a pérdidas. Así entendido, el riesgo se refiere a la probabilidad de ocurrencia de pérdidas directas o indirectas como consecuencia de fallos en los procesos internos o externos de la entidad, que produzcan la indisponibilidad operativa de la misma, pérdidas económicas, pérdida de valor del patrimonio neto, incrementos de costos, pérdida de oportunidades de negocio, daños de reputación, pérdida de clientes, gastos adicionales, pérdida de beneficios, vulneración de datos, responsabilidades pecuniarias con grupos de interés afectados por la actividad de la organización, sanciones administrativas y penales por incumplimientos normativos, entre otros.

La gestión de los riesgos corporativos, también llamada gestión del riesgo empresarial, que viene de la expresión anglosajona **Enterprise Risk Management (ERM)**, nació como metodología a final del siglo pasado, a raíz de la gestión de riesgos desarrollada desde la perspectiva de su aseguramiento frente a riesgos operacionales. Con posterioridad, como indica DOPAZO y CANDELARIO, “este fenómeno ha evolucionado hasta relacionar la gestión del riesgo con otras áreas de la empresa como producción, seguridad, asesoría jurídica, auditoría, innovación, calidad, medioambiente, Responsabilidad Social Empresarial, entre otras. Esta evolución responde a la búsqueda de un enfoque multidisciplinar de la gestión de los riesgos inherentes a una empresa u organización, admitiendo que la gestión de dichos riesgos bajo un enfoque integral permite obtener beneficios a través de la evaluación y la supervisión de la interrelación existente entre ellos. Nadie parece dudar que gestionar de forma aislada cada riesgo, sin considerar la correlación habida entre riesgos, introduce ineficiencias porque la organización (empresa) no conoce realmente su exposición al riesgo real, ni el efecto de la volatilidad, la frecuencia y la severidad de cada riesgo. Es decir, la

organización no dispone de toda la información adecuada (fenómeno de asimetrías de la información) para asignar sus recursos de forma eficiente."[20]

La nueva visión del ERM que cambia el enfoque de gestión de riesgos fragmentados y *ad hoc*, a un enfoque integrado, continuo y amplio, implica abordar de forma sistemática e integrada la gestión de los riesgos totales a los que se enfrenta una organización, proceso por la cual la misma determina, controla, explota, financia, y supervisa todas las fuentes de riesgos con el fin de aumentar el valor a corto y a largo plazo de la organización para sus grupos de interés.

2.1.1.- Marco de trabajo de la gestión del riesgo.

"Esquema incluido en el marco de trabajo de la gestión del riesgo (2.1.1) que especifica el enfoque, los componentes de gestión y los recursos a aplicar para la gestión del riesgo (1.1)."

El marco de trabajo de la gestión del riesgo supone el conjunto de elementos que proporcionan los fundamentos y las disposiciones de la organización para el diseño, la implantación, el seguimiento, la revisión y mejora continua de la gestión del riesgo soportado o bien por la organización o bien por la sociedad en su conjunto.

Es posible y conveniente reducir el riesgo de consecuencias negativas, en particular para la salud y la vida humana, el medio ambiente, el patrimonio material y cultural, la actividad económica y las infraestructuras asociadas tanto en las organizaciones, como en la sociedad en general. Para que las medidas dirigidas a reducir los riesgos sean efectivas, tienen que coordinarse en la medida de lo posible por medio de la Política de gestión del riesgo y el Plan de gestión del riesgo.

El significado del riesgo tiene relevancia en tanto en cuanto sea estimado y valorado dentro del marco de un contexto y entorno determinados, conforme a un conjunto de objetivos y resultados esperados.

La gestión de riesgos implica una actividad trasversal sobre toda la organización para poder determinar el "apetito al riesgo" de la misma, es decir, la cantidad y tipo de riesgo que una organización está dispuesta a tomar en orden de alcanzar sus objetivos estratégicos.

Considerando la actitud ante los riesgos y los factores asociados a esta actitud, podemos concluir que cuanto mayor es el grado de conocimiento del riesgo, mayor es el apetito al mismo basado precisamente en su conocimiento sobre el impacto total de riesgo que una organización está preparada para aceptar en la consecución de sus objetivos, mayor es la consciencia y la profesionalidad ante los riesgos.

---

20 DOPAZO FRANGUÍO, Mª PILAR y CANDELARIO MACÍAS, Mª ISABEL, "Gerencia de Riesgos sostenible y Responsabilidad Social Empresarial en la actividad aseguradora". V. capítulo I Generalidades y Marco legal de referencia. Premio Internacional de Investigación Julio Sáez Castillo, 23 mayo 2011. Asociación española de gerencia de riesgos y seguros, AGERS.

La contratación de un seguro se presenta como una conducta adecuada frente al riesgo y aparece de forma programada como consecuencia de la fase de financiación del riesgo, si bien, existe un porcentaje elevado de organizaciones que señala que lo que hay que hacer es «asumir lo que puede ocurrir», lo que pone de manifiesto una postura conformista o arriesgada ante las connotaciones negativas de una situación, mientras que un porcentaje mucho mayor tiene una posición más profesional, que parte de identificar, analizar, evaluar, controlar los riesgos y proceder a su aseguramiento solamente después de haber completado todas las fases de la gestión de riesgos para evitar las posibles pérdidas de los siniestros.

El mero hecho de que puedan ocurrir siniestros que afecten a las personas, a su familia o a sus bienes, crea en los individuos la necesidad de estar preparado ante esas eventualidades negativas. El seguro es percibido en los ciudadanos como algo paradójico, lo ideal para el consumidor es no llegar a usarlo.

La implantación de la gestión del riesgo es imprescindible para cualquier organización que quiera estar bien y eficientemente gestionada, supone una actividad transversal a todas las áreas de la organización, quienes no la implanten, perderán una ventaja competitiva, será exigida, cada vez más, a través de la cadena de valor; en suma, implantar la gestión del riesgo, además de eficiencia y de administración adecuada de los recursos disponibles, es hoy más que nunca una verdadera palanca de competitividad.

Todos los agentes implicados en la gestión de riesgos deben analizar sus resultados, adaptar sus estrategias y tomar decisiones -en suma- partiendo de la eficacia de la gestión en beneficio propio. El objetivo común de hacerse más fuertes con una gestión de riesgos es acorde con los tiempos que corren, sin olvidar que la clave ante los riesgos está más en una disposición interna de las organizaciones ante sus decisiones, que en una condición de las circunstancias concretas que concurren en cada organización.

2.1.2.- Política de gestión del riesgo.

La política de gestión del riesgo debe establecer un el nivel mínimo de controles en el seno de la organización necesario para una gestión de riesgos eficaz, aumentándolo cuando sea necesario, o reduciéndolo al mínimo cuando los sistemas de gestión y control funcionen correctamente y los porcentajes de error se mantengan en un nivel aceptable.

La política de gestión del riesgo establece la misión, objetivos y funciones, aspectos todos ellos que serán recogidos en el plan de gestión de riesgos.

Para que la política de gestión de riesgos sea eficaz se requiere el apoyo de la alta dirección de la organización que demuestre liderazgo, compromiso y acciones concretas con respecto al sistema de gestión de riesgos que garantice:

a) que el sistema de gestión de riesgos se implemente de forma adecuada para conseguir los objetivos propuestos;

b) que las exigencias derivadas del sistema de gestión de riesgos se incorporan a los procesos y procedimientos operativos de la organización;

c) que se disponga de recursos adecuados y suficientes para la ejecución eficaz del sistema de gestión de riesgos;

d) que se cumpla la política de gestión de riesgos;

e) que se comunique internamente la importancia de una gestión eficaz de riesgos, coherente con los objetivos y requisitos definidos en la política de gestión de riesgos, así como del sistema de gestión de riesgos;

f) que se dirija y apoye al personal de la organización para lograr el cumplimiento de los requisitos y la eficacia del sistema de gestión de riesgos de acuerdo con su rol en la organización;

g) que se promueva la mejora continua;

La política de gestión del riesgo se puede aplicar a un producto, un proceso o un proyecto particular, y a una parte o a la totalidad de la organización. A modo de ejemplo,

I.- En el ámbito financiero estas políticas se referirán como mínimo a:

a) las actividades que la organización considere de negociación e integrantes de la cartera de negociación a efectos de los requisitos de fondos propios;

b) la medida en que una posición puede valorarse diariamente a precios de mercado por referencia a un mercado líquido activo tanto para la oferta como para la demanda;

c) respecto de las posiciones valoradas con arreglo a un modelo, la medida en que la entidad puede:

i) determinar todos los riesgos importantes de la posición,

ii) cubrir todos los riesgos importantes de la posición con instrumentos para los que existe un mercado líquido activo tanto para la oferta como para la demanda,

iii) calcular estimaciones fiables relativas a las hipótesis y los parámetros clave utilizados en el modelo;

d) la medida en que la entidad puede y debe generar para la posición valoraciones del riesgo que puedan validarse externamente de manera coherente;

e) la medida en que limitaciones legales u otros requisitos operativos podrían menoscabar la capacidad de la entidad para efectuar una liquidación o cubrir la posición a corto plazo;

f) la medida en que la entidad puede y debe gestionar activamente los riesgos de las posiciones de su actividad de negociación;

g) la medida en que la entidad puede transferir riesgos o posiciones entre la cartera de negociación y lo excluido de la cartera de negociación, y los criterios para estas transferencias.[21]

II.- En el ámbito de la **prevención de riesgos graves**. Existen también políticas específicas para la prevención de accidentes graves que parten del modelo europeo regulado en la Directiva 2012/18/UE del Parlamento Europeo y del Consejo de 4 de julio de 2012, relativa al control de los riesgos inherentes a los accidentes graves en los que intervengan sustancias peligrosas y por la que se modifica y ulteriormente deroga la Directiva 96/82/CE. En estos casos el plan se basa en:

1. Los Estados miembros velarán por que los industriales estén obligados a redactar un documento por escrito en el que se defina su política de prevención de accidentes graves y deberán asegurarse de su correcta aplicación. La política de prevención de accidentes graves tendrá por objeto garantizar un alto grado de protección de la salud humana y del medio ambiente. Será proporcionada a los peligros de accidente grave. Incluirá los objetivos generales y los principios de actuación del industrial, el reparto de tareas y responsabilidades de gestión, así como el compromiso de mejorar de forma permanente el control de los riesgos de accidente grave y de garantizar un elevado nivel de protección.

2. La política de prevención de accidentes graves se elaborará y, cuando así lo exija la legislación nacional, se enviará a la autoridad competente en los siguientes plazos:

a) en el caso de los establecimientos nuevos, en un plazo razonable antes de comenzar la construcción o la explotación, o antes de las modificaciones que den lugar a un cambio en el inventario de sustancias peligrosas;

b) en todos los demás casos, en el plazo de un año a partir de la fecha en que la presente Directiva se aplique al establecimiento en cuestión.

3. Los apartados 1 y 2 no se aplicarán si el industrial ya ha establecido la política de prevención de accidentes graves y, de exigirlo la legislación nacional, la ha transmitido a la autoridad competente antes del 1 de junio de 2015, y la información contenida en ella cumple lo dispuesto en el apartado 1 y no ha cambiado.

4. El industrial revisará periódicamente la política de prevención de accidentes graves, al menos cada cinco años, y la actualizará cuando sea necesario. Cuando

---

21 V. El Reglamento (UE) No 575/2013 del Parlamento Europeo y del Consejo de 26 de junio de 2013, sobre los requisitos prudenciales de las entidades de crédito y las empresas de inversión, y por el que se modifica el Reglamento (UE) no 648/2012.

así lo exija la legislación nacional, la dicha política de prevención actualizada se enviará sin demora a la autoridad competente.

5. La política de prevención de accidentes graves se aplicará mediante medios y estructuras adecuados y mediante un sistema de gestión de la seguridad, de conformidad con el anexo III de la Directiva y de forma proporcionada a los peligros de accidente grave y a la complejidad de la organización o las actividades del establecimiento En el caso de establecimientos de nivel inferior, la obligación de aplicar dicha política de prevención podrá cumplirse por otros medios, estructuras y sistemas de gestión adecuados, que sean proporcionados a los peligros de accidente grave, habida cuenta de los principios establecidos en el anexo III de la Directiva.[22]

III.- En el ámbito de los **riesgos excesivos dentro del sistema financiero.** La estabilidad financiera es una condición previa para que el sistema financiero[23] funcione y para que la economía real proporcione puestos de trabajo, crédito y crecimiento. La crisis financiera ha puesto de manifiesto importantes carencias en la supervisión de las entidades financieras[24] -y de los riesgos sistémicos[25]- que no ha podido anticipar una evolución macroprudencial adversa ni impedir la acumulación de **riesgos excesivos dentro del sistema financiero**.

El Reglamento (UE) No 1092/2010 del Parlamento Europeo y del Consejo de 24 de noviembre de 2010, relativo a la supervisión macroprudencial del sistema financiero en la Unión Europea y por el que se crea una Junta Europea de Riesgo Sistémico (JER), con la siguiente política ante la posible aparición de este tipo de riesgo:

1. La JERS asumirá la supervisión macroprudencial del sistema financiero en la Unión a fin de contribuir a la prevención o mitigación del riesgo sistémico para la estabilidad financiera en la Unión que surge de la evolución del sistema financiero, y teniendo en cuenta la evolución macroeconómica, de modo que se eviten episodios de perturbaciones financieras generalizadas. Contribuirá al buen funcionamiento del mercado interior y garantizará así una contribución sostenible del sector financiero al crecimiento económico.

2. A efectos de lo dispuesto en el apartado 1, la JERS desempeñará las siguientes funciones:

---

22 DIRECTIVA 2012/18/UE DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 4 de julio de 2012, relativa al control de los riesgos inherentes a los accidentes graves en los que intervengan sustancias peligrosas y por la que se modifica y ulteriormente deroga la Directiva 96/82/CE.

23 Entendido el «sistema financiero» como el conjunto de entidades y mercados financieros, los productos y las infraestructuras de mercado.

24 Entendida la «entidad financiera» como toda empresa comprendida en el ámbito de aplicación de la legislación a que se refiere el artículo 1, apartado 2, del Reglamento (UE) no 1093/2010, del Reglamento (UE) no 1094/2010 y del Reglamento (UE) no 1095/2010, así como cualquier otra empresa o entidad que opere en la Unión y cuya principal actividad sea de índole similar.

25 Entendido el «riesgo sistémico» como un riesgo de perturbación del sistema financiero, que puede tener repercusiones negativas graves sobre el mercado interior y la economía real. Todos los tipos de intermediarios, mercados e infraestructuras financieros pueden ser sistémicamente importantes en cierto grado.

a) determinar y/o recopilar, y analizar toda la información pertinente y necesaria, a efectos de alcanzar los objetivos descritos en el apartado 1;

b) identificar y priorizar los riesgos sistémicos;

c) emitir avisos cuando dichos riesgos sistémicos se consideren significativos, y, en caso necesario, hacer públicos dichos avisos;

d) formular recomendaciones para la adopción de medidas correctoras en respuesta a los riesgos detectados, y, en su caso, hacer públicas dichas recomendaciones;

e) emitir un aviso confidencial dirigido al Consejo cuando decida que podría plantearse una situación de emergencia tal como se define en el artículo 18 del Reglamento (UE) nº 1093/2010, del Reglamento (UE) nº 1094/2010 y del Reglamento (UE) nº 1095/2010 y proporcionar al Consejo una evaluación de la situación para que este considere la necesidad de adoptar una decisión dirigida a las AES determinando la existencia de una situación de emergencia;

f) vigilar que se adopten medidas en respuesta a los avisos y recomendaciones;

g) colaborar estrechamente con todas las demás partes en el SESF y, en su caso, proporcionar a las AES la información sobre riesgos sistémicos necesaria para el desempeño de su cometido; y, en particular, en cooperación con las AES, desarrollar, un conjunto de indicadores cuantitativos y cualitativos (cuadro de riesgos) para determinar y medir el riesgo sistémico;

h) participar, en caso necesario, en el Comité Mixto;

i) coordinar sus acciones con las de las organizaciones financieras internacionales, en particular el FMI y el JEF, así como con los organismos pertinentes de terceros países, en cuanto se refiere a la supervisión macroprudencial;

j) realizar otras tareas conexas, conforme a lo especificado en la legislación de la Unión.

2.1.3.- Plan de gestión del riesgo.

"Esquema incluido en el marco de trabajo de la gestión del riesgo (2.1.1) que especifica el enfoque, los componentes de gestión y los recursos a aplicar para la gestión del riesgo (1.1)."[26]

---

26 A propósito del término "Plan de gestión de riesgos", la UNE-ISO Guía 73:2009 incluye las siguientes notas: "NOTA 1 Por lo general, los componentes de gestión incluyen los procedimientos, las prácticas, la asignación de responsabilidades, la secuencia y la cronología de las actividades. NOTA 2 El plan de gestión del riesgo se puede aplicar a un producto, un proceso o un proyecto particular, y a una parte o a la totalidad de la organización."

El plan de gestión de riesgos debe determinar de forma clara, precisa y congruente los componentes de gestión incluyen los procedimientos, las prácticas, la asignación de responsabilidades, la secuencia y la cronología de las actividades.

Al igual que en la política de gestión de riesgos, el plan de gestión del riesgo se puede aplicar a un producto, un proceso o un proyecto particular, y a una parte o a la totalidad de la organización.

Para que tanto la política como el plan de gestión de riesgos sea sostenible se requiere que todo el proceso del plan se retroalimente mediante la administración del riesgo. La administración de riesgo de la organización implica la puesta en marcha del plan de gestión de riesgos que es un proceso que debe diseñarse y ser aprobado por los administradores y directivos de la organización y puesto en conocimiento de su personal. Forma parte de la estrategia de la organización, respondiendo a la política previamente diseñada de la misma y las expectativas ante los eventos potenciales que puedan afectarla para proporcionar una seguridad e integridad razonable referente al logro de objetivos.

El conocimiento del comportamiento de los riesgos redunda en una visión global de los mismos y en su gestión estratégica, con el fin de proteger el patrimonio y recursos de las organizaciones, ante las posibles pérdidas a las que están expuestas y de aprovechar las oportunidades que pueden obtenerse al gestionar los riesgos eficientemente.

El plan de gestión del riesgo debe establecer los objetivos y acciones concretas para conseguir su correcta administración, profundizando en el análisis científico del comportamiento de los riesgos, en sus vertientes técnica, jurídica y económica, que posibilite la identificación, evaluación y control de aquellos riesgos de las organizaciones que permita reforzar los objetivos estratégicos de quienes conviven con los riesgos, actuando en todas sus áreas, para alcanzar una meta común, la minimización de los riesgos soportados, el correcto tratamiento de los mismos, así como su financiación mediante la suscripción de seguros o la retención total o parcial de los riesgos y finalmente el aumento del valor para los stakeholders en sus ámbitos económico, social y medioambiental y un adecuado gobierno de la empresa.

El estudio y conocimiento de del comportamiento de los riesgos y la solución a los problemas planteados supone una mejora en la gestión, desde el nivel de anteproyecto, incorporando mejoras para eliminar o controlar/mitigar pérdidas potenciales y aprovechar las oportunidades de mejora competitiva, fomentando el desarrollo de una sociedad más justa y con sólidos valores, así como el establecimiento y la divulgación de principios de información y formación en el ámbito profesional de los riesgos y seguros con instituciones públicas y privadas, empresas y organizaciones en general.

3. TÉRMINOS RELATIVOS AL PROCESO DE GESTIÓN DEL RIESGO[27]

3.1 Proceso de gestión del riesgo:

"Aplicación sistemática de políticas, procedimientos y prácticas de gestión a las actividades de comunicación, consulta, establecimiento del contexto, e identificación, análisis, evaluación, tratamiento, seguimiento (3.8.2.1) y revisión del riesgo (1.1)."

Puesto que la gestión de riesgo como tal, ocupa con su propia voz un importante espacio a lo largo de este recopilatorio de definiciones comentadas. Comenzaremos centrándonos en el propio significado de Proceso y lo que implica en cuanto a la gestión del riesgo se refiere.

Proceso según el Diccionario de la lengua española de la Real Academia Española, proviene del sustantivo latino "*processum*", y del verbo "*procederé*", ambos términos a su vez incorporan el prefijo "*pro*" (hacia adelante) y la partícula sintáctica "*cere*" (de caer, encaminar), dando lugar a un vocablo con varias acepciones, entre otras y a nuestros efectos, significados como progreso, avance, marchar, ir adelante, hacia un determinado fin.

---

27 Los comentarios sobre los términos siguientes han sido desarrollados por **Dña. Cristina Gutiérrez Pérez y D. Mariano Blanco Gema**: 3. Términos relativos al proceso de gestión de riesgos. 3.1. Proceso de gestión del riesgo; 3.2 Términos relativos a la comunicación y la consulta; 3.2.1 comunicación y consulta; 3.2.1.1 parte interesada; 3.2.1.2 percepción del riesgo; 3.3 Términos relativos al contexto; 3.3.1 establecimiento del contexto; 3.2.1.1 parte interesada; 3.2.1.2 percepción del riesgo. 3.3 Términos relativos al contexto; 3.3.1 establecimiento del contexto; 3.3.1.1 contexto externo: 3.3.1.2 contexto interno; 3.3.1.3 criterio de riesgo.

Por ende, *proceso* está definido como "*la sucesión de actos o acciones realizados con cierto orden, que se dirigen a un punto o finalidad, así como también al conjunto de fenómenos activos y organizados en el tiempo*".

Entre sus diferentes significados nos interesa a estos efectos de una manera especial la acepción como "*el conjunto de las fases sucesivas de un fenómeno natural o de una operación artificial*". Un proceso se puede definir por tanto como una serie de actividades, acciones o pasos organizados e interrelacionados, orientados a obtener un resultado específico, concreto y predeterminado, como consecuencia del valor agregado que aporta cada una de las fases que se llevan a cabo en las diferentes etapas por los responsables que desarrollan las funciones de acuerdo con su estructura orgánica. Donde incluso se podría mencionar, por la naturaleza propia de la gestión de riesgos, que el proceso es desarrollado en un ente "Vivo" como es en este caso, la empresa u organizaciones en continua evolución, desarrollo y actualización de la propia gestión de riesgos, para adaptarse en cada momento a las situaciones cambiantes, nuevos intervinientes, amenazas y en general a la evolución de la propia dinámica empresarial.

Detenernos en la duración implícita que engloba la palabra Proceso, tendente al infinito, ya que teóricamente sería la acción de efectuar una serie de actividades sin momento final definido. Por lo que se plantea que el Proceso de gestión de riesgos podría ser un proceso infinito o alternativamente que su fin se dé, sólo cuando la empresa deje de existir.

Según la norma UNE-ISO Guía 73:2009*, "El Proceso de gestión del riesgos es una aplicación sistemática de políticas, procedimientos y prácticas de gestión a las actividades de comunicación, consulta, establecimiento del contexto, e identificación, análisis, evaluación, tratamiento, seguimiento y riesgo."*

La traducción al inglés de esta voz sería "*Risk Management Process",* y en lengua francesa "*Processus de Gestion des Risques*".

La norma ISO 31000:2009 específica que el Proceso de gestión de riesgos debería: ser una parte de la gestión, integrarse en la cultura e imbricarse en las prácticas de la organización, así como adaptarse a los procesos propios del negocio. El proceso de gestión del riesgo comprende, entre otras, las actividades de:[28]

- Comunicación y consulta.
- Establecimiento del Contexto (interno y externo).
- Apreciación del riesgo que incluye identificación, análisis y evaluación de los riesgos.
- Tratamiento de los diversos riesgos.
- Seguimiento, revisión y actualización periódica.

Esquema: Proceso de gestión de riesgos basado en la ISO 31000:2009

---

28 Prácticamente todas las actividades que comprende el proceso de gestión del riesgo son desarrolladas y comentadas de manera separada a lo largo del documento "Voces del riesgo".

La Guía de Implementación ISO/TR 31004 señala que la implementación del proceso de gestión del riesgo se puede adaptar proporcionalmente al tamaño y requisitos de cada organización. No hay que olvidar que el proceso como tal, se encuentra presente a lo largo de los 11 principios a satisfacer, que se establecen en la norma ISO 31000 para que se logre una eficiente gestión de riesgos. Es por esto que tan sólo nos detendremos en el principio que consideramos de mayor relevancia, en la confianza de que el amable y avisado lector profundice en cada uno de los mencionados principios que se plasman cada uno con su voz o entrada propia.

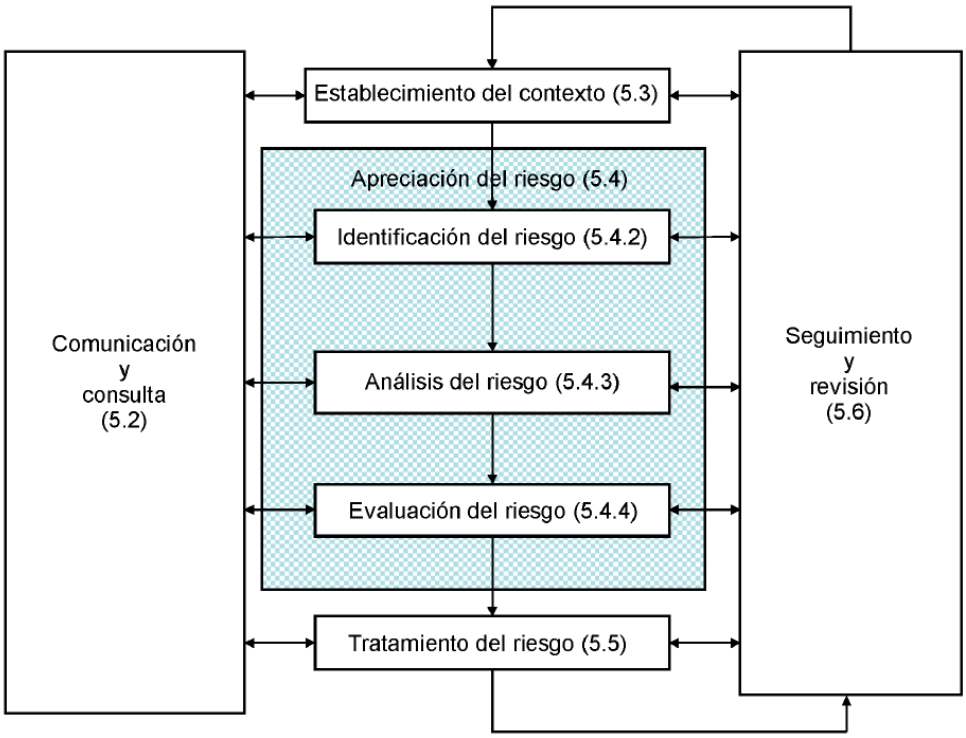

Gráfico 3.

En referencia al Principio 2 de la ISO 31000:2009: *La gestión del riesgo es una parte integral de todos los procesos de la organización,* la ISO/TR 31004 en su aplicación detalla, entre otros elementos y relativo al proceso de gestión del riesgo, lo siguiente:

1. *El proceso para gestionar el riesgo debe ser parte integrante de las actividades que generan el riesgo; de lo contrario, la organización deberá modificar la toma de decisiones cuando se detecten los riesgos asociados.*

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

3. *Si no existe un sistema de gestión formal, el marco de trabajo puede servir para este propósito.*

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

Por otra parte, los estándares de gestión de riesgos publicados por FERMA, muestran que el Proceso de gestión de riesgo engloba, a su vez, las etapas siguientes:

Gráfico 4.

El proceso de gestión de riesgos puede ser tipificado como una lista de actividades coordinadas, tendentes a ordenar debidamente la gerencia de esos riesgos. Existen descripciones alternativas de este proceso, pero siempre encontramos los diferentes componentes que representan de forma nemotécnica "*las 7Rs y las 4Ts*" de la gestión del riesgo, estos son:

- **R**econocimiento o identificación de riesgos
- "**R***anking*" Clasificación o evaluación de riesgos

- Respuesta a riesgos significativos
    - **T**olerar
    - **T**ratar
    - **T**ransferir
    - **T**erminar
- **R**ecursos Controlados
- **R**eacción Planificada Previamente
- **R**eportar y monitorear el desempeño del riesgo
- **R**evisión del marco de gestión de riesgos

Gráfico 5.

Las organizaciones deben poner énfasis en la mejora continua de la gestión de riesgos, entre otros, mediante la revisión y consiguiente adaptación de los procesos de gestión del riesgo, al menos una vez al año.

Cabe mencionar la importancia que se otorga al *proceso de gestión del riesgo* en cada una de las voces incluidas en este trabajo.

Tras comentar los procesos de gestión de riesgos propuestos por las diferentes normas y guías, consideramos de interés para el lector, ampliar con aportaciones realizadas a la comunidad científica e investigadora, dada su gran relevancia y calado internacional,

específicamente por lo que supone para el significado del propio proceso de gestión de riesgos como eje central de los componentes y principios de la gerencia de riesgos que plantea COSO (Committee of Sponsoring Organizations of the Treadway Commission):

- 1992 COSO I - Marco de Control Interno
- 2004 COSO II - ERM 2004
- 2013 COSO III basado en COSO I
- 2017 COSO *ERM—Integrating with Strategy and Performance*

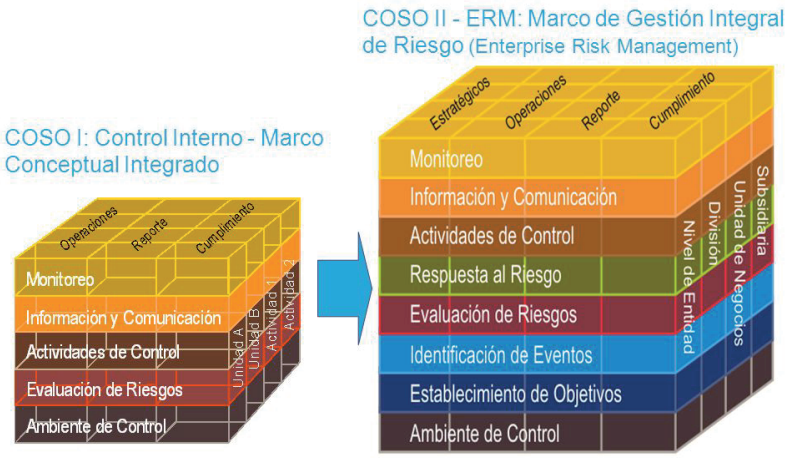

Gráfico 6: COSO I – COSO II ERM

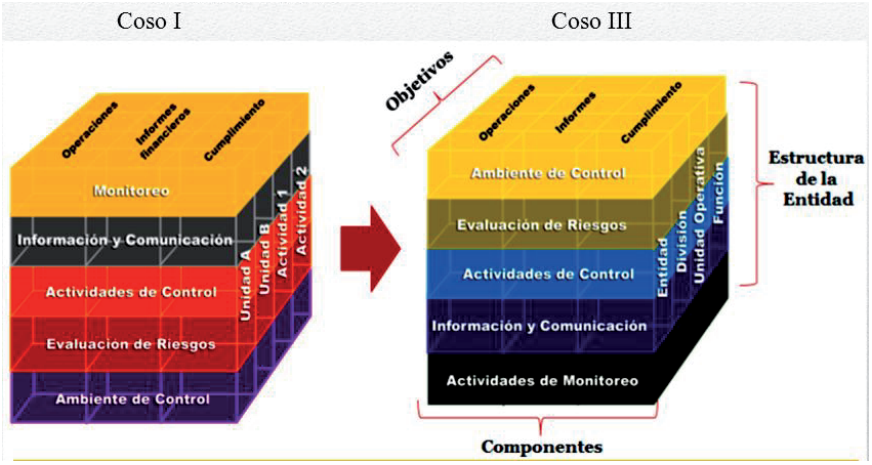

Gráfico 7: COSO I – COSO III (regreso a la estructura inicial)

La última versión ofrecida por el comité COSO, basada en Gestión de riesgos empresarial integrada con la estrategia y el desempeño, muestra la gestión de riesgos como un conjunto de principios sobre los cuales los procesos pueden ser construidos y/o integrados por una organización, continuados con un sistema de monitoreo, aprendizaje y mejora continuada del desempeño.[29]

Gráfico 8: COSO ERM 2017 - Estrategia

El Marco en sí es un conjunto de principios organizados en cinco componentes interrelacionados: 1) Gobierno y cultura, 2) estrategia y fijación de objetivos, 3) desempeño, 4) comprobación y revisión, y 5) comunicación información y reporte. La representación gráfica muestra el avance hacia el incremento de valor, y como se entrelaza cada componente influyendo en las diversas áreas. Dichos componentes se apoyan en 20 principios que cubren todo el proceso y lo hacen viable mediante prácticas que pueden ser utilizadas de diferentes maneras y por cualquier tipo de organización independientemente de su tamaño.

---

29 Como colofón, en los gráficos hemos querido ilustrar la imbricación del "Proceso de gestión de riesgos" con COSO, aun siendo un tema fuera del ámbito de la propia "Voz", hemos decidido resaltarlo dada la transversalidad tanto del "proceso de gestión de riesgos" como del propio esquema COSO.

Gráfico 9: COSO 2017 ERM Integración con la estrategia y el cumplimiento.

3.2 Términos relativos a la comunicación y la consulta.

3.2.1 Comunicación y consulta.

Procesos iterativos y continuos que realiza una organización para proporcionar, compartir u obtener información y para establecer el diálogo con las partes interesadas (3.2.1.1), en relación con la gestión del riesgo (1.1).[30]

Comunicación es la acción y efecto de expresarse para ser entendido por otros, o para divulgar a otros un determinado saber o conocimiento es decir descubrir, manifestar o hacer saber a alguien algo, en nuestro caso en relación con la empresa y su desarrollo.

Consulta es la acción y efecto de interpelar, preguntar o solicitar información sobre determinado asunto, tema o situación; además de referirse a la búsqueda de la documentación o datos sobre algún asunto o materia; cabe señalar que con esta acepción se refiere también a examinar o tratar un asunto intercambiando pareceres con una o varias personas que conozcan y puedan aportar datos o información de utilidad para la organización.

La comunicación y consulta forman parte de las actividades del proceso de Gestión del Riesgo. La norma UNE-ISO Guía 73:2009 define La comunicación y consulta, como procesos iterativos y continuos que realiza una organización para proporcionar,

---

30 A propósito de la expresión comunicación y consulta, la UNE-ISO Guía 73:2009 contiene las siguientes notas: "NOTA 1 La información puede corresponder a la existencia, la naturaleza, la forma, la probabilidad (3.6.1.1) la importancia, la evaluación, la aceptabilidad y el tratamiento de la gestión del riesgo. NOTA 2 La consulta constituye un proceso de comunicación informada de doble sentido entre una organización y sus partes interesadas, sobre una cuestión antes de tomar una decisión o determinar una orientación sobre dicha cuestión. La consulta es:

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

compartir u obtener información y para establecer el dialogo con las partes interesadas en relación con la gestión del riesgo.

Si nos centramos en las palabras que no han sido descritas a lo largo de estas voces, la comunicación y consulta constituye un conjunto de fases sucesivas de una operación organizada y jerarquizada, tendente a un determinado fin, como es la actividad empresarial, que se efectúa y repite o se extiende sin interrupción a lo largo del tiempo. Tales funciones son realizadas en una organización para poner a disposición de las partes interesadas información, así como repartir, dividir, distribuir o alcanzar, conseguir y lograr dicha información. Además, permite entre las partes interesadas, establecer discusiones o conversaciones, donde alternativamente manifiesten sus ideas, análisis o comparaciones de los resultados o condiciones de una investigación, en relación a la gestión del riesgo.

La norma UNE-ISO Guía 73:2009 a su vez señala que la información puede corresponder a la existencia, la naturaleza, la forma, la probabilidad, la importancia, la evaluación, la aceptabilidad y el tratamiento de la gestión del riesgo.

Por su parte la Consulta constituye un proceso de comunicación informada bidireccional o de doble sentido entre una organización y sus partes interesadas, sobre una cuestión antes de tomar una decisión o determinar una orientación sobre dicha cuestión.

En esta línea la Consulta es un proceso que impacta sobre una decisión a través de la influencia más que por la autoridad; y una contribución para una toma de decisión, y no una toma de decisión conjunta. La Consulta, se constituye como un paso para la elaboración de una determinada decisión siendo parta de las bases sobre las que se asentará la decisión o la línea de actuación.

Cabe resaltar por su gran importancia el concepto de bidireccionalidad o “doble sentido” puesto que muestran la fluidez y el necesario trasvase de información en ambas direcciones, intercomunicando los diversos estamentos de la organización y ayudando a que se integren unos con otros (del alto nivel a nivel inferior u operacional y viceversa).

Volviendo a la Información, elemento central y pieza clave de esta voz, se refiere a acción y efecto de informar en el sentido de explicar y aportar sentido y entendimiento a una situación, proceso o evento. Completándose con la comunicación y la consulta o adquisición de conocimientos que una vez reunidos en conjunto y procesados, permiten ampliar o delimitar los datos que se poseen sobre una materia determinada y sobre esa base establecer las acciones subsiguientes y darles la secuencia temporal requerida para que la organización alcance sus fines.

En el mundo de los negocios presenta connotaciones especiales la denominada “información privilegiada”: constituida por una información de tal tipo y condición que, por referirse a hechos o circunstancias desconocidos para otros, puede generar ventajas, normalmente ilícitas, a quien dispone de ella. Sin duda la información privilegiada puede aportar mucho a la búsqueda de una ventaja competitiva, al margen de la catalogación moral que le demos a su uso. En el ámbito de los mercados de valores, aunque poderosa, la información privilegiada no suele estar bien considerada, puesto que se refiere a la que se ha tenido acceso reservadamente, usualmente con ocasión

del desempeño de un cargo o del ejercicio de una actividad empresarial o profesional, y que, por su relevancia para la cotización de los valores, es susceptible de ser utilizada en provecho propio o ajeno ocasionando una acción desleal, de hecho para la mayor parte de legislaciones occidentales se considera delito punible y son abundantes los casos de su persecución en la literatura y práctica jurídicas.

Su traducción al inglés sería *Communication and Query* y al francés *Communication et Consultation*.

Las organizaciones deberían desarrollar un plan de comunicaciones que recogiese las políticas, estrategias, recursos, objetivos y acciones de comunicación, tanto internas como externas, implicando a las partes interesadas, generando confianza en la empresa, lo que redundaría en una mejor preparación para situaciones de crisis y/o emergencias. Tal mejora en la preparación constituye un elemento capital del abordaje de la gerencia de riesgos.

A través de la comunicación adecuadamente canalizada de la propia gestión del riesgo, informes, disponibilidad de información al alcance de todos y otros mecanismos como desarrollo de consultas, se apoyará y fomentará en la organización el cumplimiento normativo y un mayor control sobre los riesgos.

Como acertadamente hace hincapié la norma ISO 31000:2009 las comunicaciones y consultas con las partes interesadas externas e internas, se deberían realizar en todas las etapas del proceso de gestión del riesgo. Además, deberían facilitar intercambios de información que sean veraces, pertinentes, exactos y entendibles, teniendo en cuenta los aspectos confidenciales y de integridad personal.

Una gestión de riesgos optimizada incluye comunicaciones y consultas continuas o al menos periódicas con las partes interesadas en la empresa y en su contorno próximo.

Como hemos visto la comunicación y consulta influye en todos los procesos de la gestión del riesgo y forma parte de manera directa o indirecta de cada uno de los principios de la norma ISO 31000:2009, aunque por su especial relevancia nos detendremos en el Principio 9: La gestión de riesgo es transparente y participativa, y su aplicación según la ISO/TR 31004, donde detalla que la consulta con las partes involucradas, como parte de la aplicación del proceso de gestión del riesgo, necesita una planificación cuidadosa. Siendo aquí donde se puede construir confianza, o destruirla.

En la ISO/TR 31004, guía para la implementación de la gestión del riesgo en el anexo C sobre Mandato y Compromiso, indica que para que ambos sean eficaces, la alta dirección y el órgano de supervisión de la organización deberían expresar de forma clara a las partes involucradas el enfoque para gestionar el riesgo, documentar y comunicar sus decisiones, según sea apropiado.

Un modo de expresar y comunicar el mandato de una manera explícita, es por medio del establecimiento de la política y su posterior comunicación. La ISO 31000:2009, especifica que la organización debería no solamente hacer que su política acerca de la gestión del riesgo sea clara, sino también que sea conocida, esto es comunicarla interna y externamente.

Las organizaciones deben informar regularmente a sus grupos de interés explicando sus políticas de gestión de riesgos y la efectividad con la que se están consiguiendo los objetivos planeados. Las medidas relativas a los informes a cumplimentar sobre la gestión de riesgos deben quedar establecidas claramente y ser puestas a disposición de los interesados.

Cada vez más, los interesados esperan que las empresas den muestras de una gestión eficaz en cuanto al rendimiento no financiero de la empresa en áreas tales como asuntos comunitarios, derechos humanos, prácticas laborales, salud, seguridad en el trabajo, deber de cuidado, medioambiente y responsabilidad social corporativa.

3.2.1.1 Parte interesada.

"Persona u organización que puede afectar, estar afectada, o percibir que está afectada por una decisión o actividad."[31]

Definimos como "parte interesada" a cualquier organización, grupo o individuo que pueda afectar o ser afectado por las actividades de una empresa u organización de referencia.

Es bastante común que para referirse a Parte Interesada se emplee terminología anglosajona *"Stakeholder"*.

En el ámbito de la gerencia de riesgos, como detalla la norma UNE-ISO Guía 73:2009, la parte interesada hace referencia a la persona u organización que puede afectar, estar afectada, o percibir que está afectada por una decisión o actividad. Incluyendo la propia persona que toma las decisiones. Así en el medio empresarial y en el tráfico económico a menudo, suele hablarse de partes interesadas para referirse de manera genérica y global a cualquier persona o entidad que sea o pueda ser afectada/perjudicada por las actividades o la marcha de una organización determinada.

Así cada organización dispone de sus partes interesadas, también denominadas grupos de interés, públicos de interés, corresponsables u otros.

Cabe mencionar por su gran utilización a nivel técnico, (e implantación en la sociedad hispanohablante), que "Parte interesada" ha sido la traducción buscada que mejor definía todo lo que engloba el término *"Stakeholder"* al que ya nos hemos referido; a día de hoy podemos observar su utilización muy común en ingles en diferentes documentos escritos es castellano. Por su parte, la traducción más acertada al francés sería *"Partie Prenante"*.

Clasificación de Partes Interesadas en función de su relación con la empresa.

Partes Interesadas Internas:

- Empleados y colaboradores
- Subcontratistas y sus empleados

---

31 A propósito de la expresión "parte interesada", la UNE-ISO Guía 73:2009 contiene la siguiente: NOTA Una persona que toma decisiones puede ser una parte interesada."

- Dueños /Propietarios /Accionistas
- Directivos

Partes Interesadas Externas:

- Clientes
- Proveedores
- Accionistas
- Gobiernos Nacional / Local/ Provincial/ Autonómico
- Sociedad, (Asociaciones empresariales, industriales, o profesionales)
- Medios de comunicación; sindicatos, ONG
- Competidores
- Proveedores/Acreedores

La clasificación anterior, ilustra con claridad a que universo hacemos referencia al hablar de grupos de interés. Colectivos que ejercen una influencia (o potencialmente pueden ejercerla) sobre la capacidad de la empresa para conseguir sus objetivos, una de las máximas de la gerencia de riesgos.

Por último, resaltar como mención especial la referencia a las partes interesadas incluida en la Guía de Implementación ISO/TR 31004 en el sentido del "Principio 8: La gestión del riesgo integra los factores humanos y culturales" La gestión del riesgo permite identificar las aptitudes, las percepciones y las intenciones de las personas externas e internas que pueden facilitar u obstruir el logro de los objetivos de la organización.

La guía de implementación de la Gestión del riesgo 31004 en su aplicación plantea que éste principio consiste en obtener las opiniones de las partes interesadas, así como entender que esas opiniones pueden estar influenciadas por las respectivas características humanas y culturales. Los factores a considerar incluyen conceptos políticos y sociales, al igual que conceptos de ámbito temporal y geográfico.

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

El diseño del marco de referencia y la comunicación acerca del riesgo debería tener en cuenta las características culturales, sociológicas y los niveles de conocimiento de los diversos destinatarios o partes interesadas.

3.2.1.2 Percepción del riesgo.

"Punto de vista de una **parte interesada** (3.2.1.1) sobre un **riesgo** (1.1)."[32]

Generalmente se considera, la Percepción del Riesgo, como la habilidad o capacidad para detectar, identificar y reaccionar ante una situación de riesgo, peligro o amenaza. Por tanto, la Percepción del Riesgo sería la que lleva a ser consciente del hecho de riesgo y consecuentemente estar alerta ante los fenómenos imprevistos que puedan obligar a tomar decisiones que conduzcan a la adecuada gestión de tal riesgo, siempre en el ánimo de eliminar sus consecuencias dañinas o minimizarlas lo máximo posible.

Por otra parte, en Gerencia de Riesgos la definición utilizada es la que marca la norma UNE-ISO Guía 73:2009 señalando que la Percepción del Riesgo, es el punto de vista de una parte interesada sobre un determinado riesgo. Detallando que ha captado el hecho potencialmente dañino y mediante la percepción del riesgo refleja las necesidades, las cuestiones, los conocimientos, las opiniones y los valores de la parte interesada, de cara a ese riesgo.

En otras voces o entradas de este trabajo, serán comentadas las definiciones de "Parte Interesada" y "Riesgos" nos centraremos en el propio significado de la palabra percepción, siendo ésta la acción y efecto de percibir, notar, observar de manera interpretativa, es decir y en nuestro caso, la acción y efecto de comprender o conocer algo.

Si nos detenemos en la Nota ofrecida por la norma UNE-ISO Guía 73:2009 y la derivación de sus significados. La percepción del riesgo refleja el impulso irresistible que hace que las causas obren infaliblemente en cierto sentido, los asuntos, el entendimiento, el juicio o valoración que se forma una persona respecto de algo o de alguien, y el grado de utilidad o aptitud de las cosas para satisfacer las necesidades o proporcionar bienestar, o causar otros efectos (positivos o negativos) en la parte interesada.

Los términos utilizados de manera recurrente en el ámbito internacional son *"Risk Perception"* (inglés) y *"Perception du Risque"* (francés), siendo las connotaciones de dichas acepciones las mismas que en lengua española.

Por otra parte, cabe destacar que la percepción del riesgo, aunque es nombrada a lo largo de toda la ISO 31000, hace un mayor hincapié en lo relativo al proceso de gestión del riesgo, deteniéndose en los apartados de Comunicaciones y Establecimiento del Contexto, citando textualmente.

Las comunicaciones y consultas con las partes interesadas son importantes ya que estas pueden emitir juicios sobre el riesgo basados en sus percepciones de riesgos. Estas percepciones pueden variar debido a diferencias en los valores, las necesidades, las hipótesis, los conceptos y las inquietudes de cada una de las partes interesadas.

---

32 A propósito de la expresión "percepción del riesgo", la UNE-ISO Guía 73:2009 incluye la siguiente: "NOTA La percepción del riesgo refleja las necesidades, las cuestiones, los conocimientos, las opiniones y los valores de la parte interesada."

Por obvio que resulte, conviene recordar aquí que cada una de las partes interesadas puede tener unos intereses diferentes, contrapuestos e incluso antagónicos, precisamente esa diversidad hace que las percepciones también puedan ser muy distintas ante un mismo fenómeno o riesgo.

La gestión de riesgos nos ayuda a tomar decisiones, para lo cual es importante poder contar con las opiniones de las partes interesadas, así como contrastar sus respectivas percepciones de los riesgos. Por lo tanto, en el proceso de toma de decisiones se debería identificar y registrar todas las percepciones del riesgo, o cuantas más posibles mejor.

En referencia al establecimiento del contexto, por su parte, en el contexto externo puede incluir, sin limitarse, las relaciones con las partes interesadas externas, sus valores y sus percepciones. En cuanto al contexto interno puede incluir las relaciones con los valores y las percepciones de cada una de las partes internas.

Así mismo la 31004, detalla, la incertidumbre que, junto con los objetivos, da lugar al riesgo, puede ser que, entre otras consecuencias, se produzca por la percepción de incertidumbre que puede variar entre partes de la organización y sus partes involucradas.

Abundemos un poco más en la interacción con la incertidumbre; en todo lo relacionado con los riesgos y su manejo, la incertidumbre juega un rol principal, ya que siempre nos estaremos enfrentando a fenómenos aleatorios cuya manifestación u ocurrencia serán inciertos. De hecho, para la mayor parte de los casos podemos afirmar que la transformación del riesgo en hechos dañosos es muy poco frecuente, aunque su intensidad cuando sucede pueda ser severa y poner en peligro la continuidad de la actividad. Todo esto nos conduce a la incertidumbre tanto en si algo sucederá y en caso de que acontezca al impacto económico de sus efectos, esa falta de certezas es la que permite la enorme elasticidad en las percepciones de los actores, que pueden enfocar los temas de modo pesimista, optimista o neutro, en diferentes gradaciones para cada categoría y sin que sea fácil armonizar los grados o consensuarlos entre los diferentes intervinientes.

Por ilustrar esta idea el propietario de la industria siempre estará más proclive a considerar que sus riesgos son limitados y de transferencia sencilla, mientras que para el asegurador que ha de tarificarlos, suscribirlos y cobrar una prima por esa transferencia de riesgos, siempre le parecerá que el nivel de riesgo es más alto y tendera a cobrar una prima superior.

3.3 Términos relativos al contexto.

3.3.1 Establecimiento del contexto.

“Definición de los parámetros externos e internos a tener en cuenta cuando se gestiona el riesgo, y se establecen el alcance y los **criterios de riesgo** (3.3.1.3) para la **política de gestión del riesgo** (2.1.2).”

Según el diccionario de la Real Academia Española en una de sus entradas para este término, señala que "contexto" es "el entorno físico o de situación, político, histórico, cultural o de cualquier otra índole, en el que se considera un hecho". Siendo también posible definirlo como "el conjunto de circunstancias que rodean una situación y sin las cuales no se puede analizar ni comprender correctamente".

Acercándose al uso común que hace el público en general, descubrimos que el Establecimiento, "es la acción y el efecto de iniciar, radicar, establecer, ordenar, mandar, decretar, o dejar demostrado y firme un principio, teoría, idea, hecho, situación, cosa o empresa, etc."

La norma UNE-ISO Guía 73:2009 establece en conjunto el "Establecimiento del Contexto" como la definición de los parámetros externos e internos a tener en cuenta cuando se gestiona el riesgo, y se establece el alcance y los criterios de riesgo, de cada actividad, acción o aspectos, para la debida interpretación y análisis de la política de gestión de riesgos.

Tras observar y racionalizar las diferentes acepciones y definiciones no incluidas en las descritas más arriba, podríamos afirmar que el Establecimiento del Contexto consiste la exposición con claridad, concreción y precisión de los datos o factores que se toman como necesarios para analizar o valorar adecuadamente una situación externa y/o interna, digna de ser tenida en cuenta cuando se aborda la gerencia del riesgo, y se establecen el alcance, los parámetros y criterios de cada riesgo para la diseñar de manera apropiada la política de gestión de tales riesgos.

Su traducción a la lengua inglesa podría ser *"Setting the context"* y para la documentación en francés *"Mise en Contexte"* o *"Etablissement du Contexte"*.

Como indica la ISO 31000:2009 Mediante el Establecimiento del Contexto, la organización articula sus objetivos, define los parámetros externos e internos a tener en cuenta en la gestión del riesgo, y establece el alcance el alcance y los criterios de riesgos para los procesos sucesivos de gestión del riesgo/s. Hay que tener en cuenta que, aunque las características del Establecimiento del Contexto puedan ser similares a las acciones de diseño del propio marco de trabajo del proceso de gestión del riesgo, los incluidos en el Contexto deberán ser más detallados, fidedignos y ajustados a la realidad de cada caso, ya que son la base sobre la que se irán asentando los pasos y acciones siguientes en el proceso científico de la gerencia de riesgos.

Diferenciemos a continuación entre el contexto externo y el interno.

El establecimiento del contexto del proceso de gestión del riesgo debería establecer los objetivos, las estrategias, el alcance y los parámetros de cada una de las actividades subsiguientes, el siguiente esquema ilustra este punto:

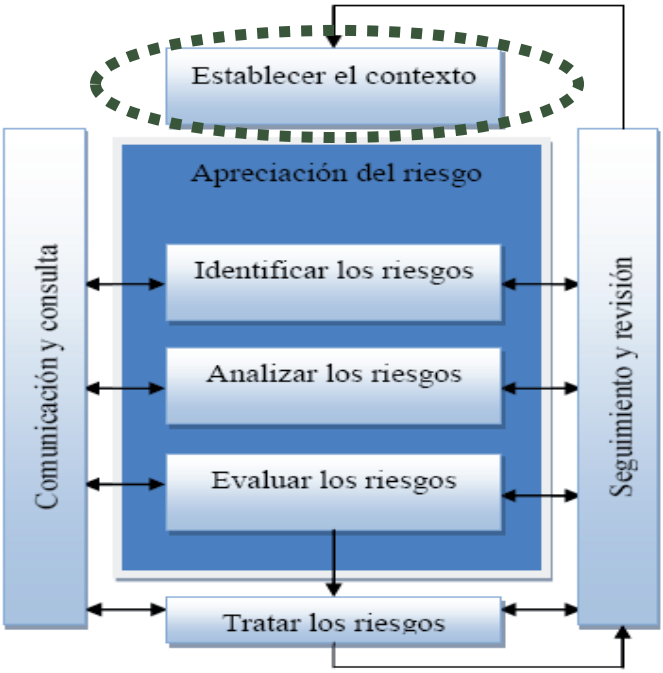

Gráfico 10. Esquema del Proceso de Gestión del Riesgo ISO 31000:2009.

En la ISO 31000:2009, el Establecimiento del Contexto, además de ser pieza clave en el proceso de Gestión de Riesgos, encuentra una mención literal en el Principio séptimo: "La gestión del riesgo está adaptada, detallando: La gestión del riesgo se alinea con el contexto externo e interno de la organización y con el perfil del riesgo".

Como sabemos la gestión del riesgo debe adaptarse a cada organización, la norma ISO 31000 proporciona un enfoque genérico para la gestión del riesgo, que es aplicable a todo tipo de organizaciones y a todo tipo de riesgo. Ahora bien, todas las organizaciones tienen su propia cultura, características, criterios de riesgo y contextos de operación. No se pueden comparar linealmente las circunstancias y situaciones que particularizan cada organización o cada uno de los riesgos a los que se ve confrontada, de hecho, incluso si consideramos una misma organización, a lo largo del tiempo tendrá cambios contextuales, en función de su evolución y experiencias previas, por lo que el establecimiento del contexto cobra también una visión temporal, al ir evolucionando a lo largo de los años.

Como el propio esquema de proceso indica, el establecimiento del contexto debe mantener un continuo seguimiento y revisión y por supuesto Evaluar si las características y el contexto de la información han cambiado, tal y como se indica en el apartado 5.4 del Anexo D de la ISO 31004.

Se debe determinar si el contexto interno o externo de la organización ha experimentado cambios significativos desde que se desarrolló. Y en tal caso, reevaluar y alinearlo, para mejor comprender y explicar los cambios acaecidos y actuar de manera

consecuente. Confirmando así que el marco de trabajo y los procesos son adecuados para su propósito y coherentes con los objetivos y prioridades de la organización.

Para mejor comprensión de lo expuesto en los párrafos inmediatamente anteriores, se adjunta grafico en el que se consideran los principales aspectos que afectan a la organización, señalando una selección de los que se pueden catalogar como Internos y de aquellos clasificables como Externos.

Es interesante resaltar que en ocasiones los contextos externos e internos se entrecruzan y existen zonas de coincidencia en las que se pueden considerar "mixtos", son las áreas de intersección que se muestran en el gráfico.

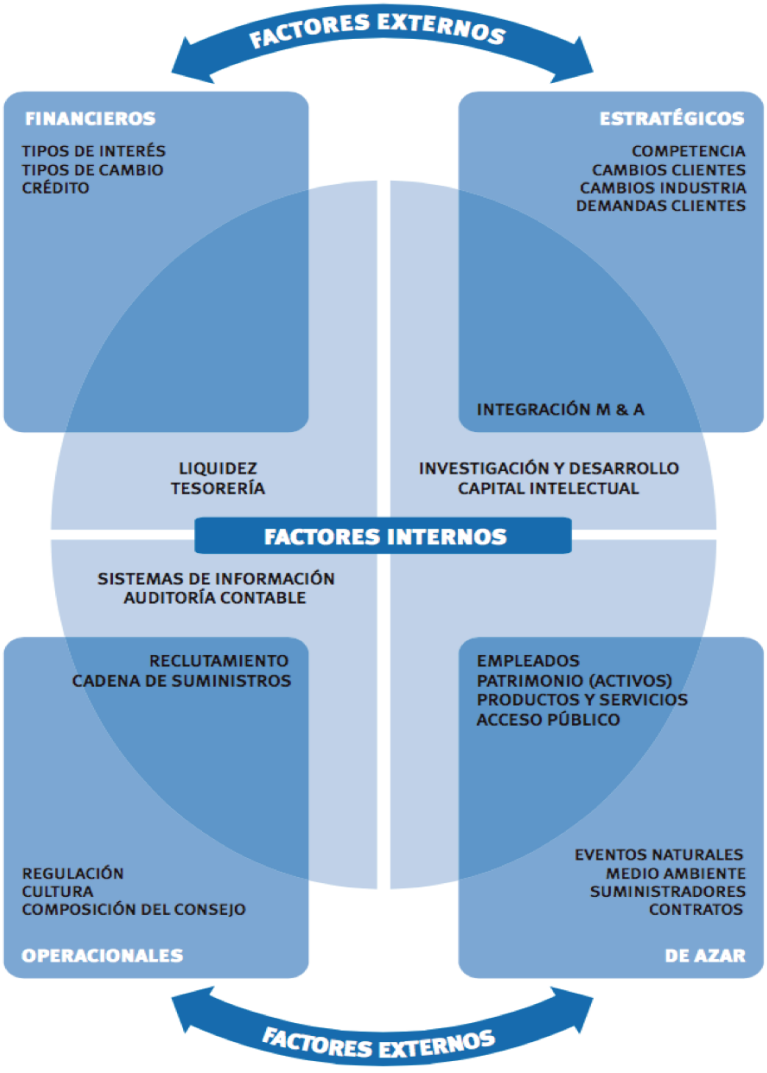

Gráfico 11. Diagrama de factores externos, internos y su intersección. Fuente: FERMA.

Conviene aclarar que este gráfico no constituye un catálogo exhaustivo de todos los factores que han de ser considerados, también ha de tenerse en cuenta la evolución temporal de los factores que evolucionaran con la organización de que se trate.

3.3.1.1 Contexto externo:

"Entorno externo en el que la organización busca alcanzar sus objetivos."[33]

Es un término que deriva del vocablo latino *"contextus"* y que se refiere a todo aquello que rodea a un algo (persona, ente, organismo, situación, etc.) y que produce algún tipo de efecto sobre ese algo; en nuestro caso el "Contexto Externo" se manifiesta en el ámbito exterior de una corporación y por tanto incluye en su definición las condiciones locales, nacionales e internacionales, que se interrelacionan con una determinada organización en un momento concreto del tiempo.

La definición que nos ofrece la norma UNE-ISO Guía 73:2009 en referencia al contexto externo, es: entorno externo en el que la organización busca alcanzar sus objetivos, identificando que, el entorno externo puede incluir:

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

- Los factores, elementos y tendencias que tengan o puedan tener un potencial impacto sobre los objetivos de la organización; y

- Las relaciones con las partes interesadas externas sus percepciones y sus valores.

El contexto interno, por el contrario, constituye todo aquello que en el seno de la propia organización (en su interior) pueda influir en cómo afronta, evalúa y gestiona esa organización sus riesgos.

Es más fácil la comprensión del contexto externo si se tienen en cuenta ejemplos concretos, como son el entorno legal, tecnológico, competitivo, de mercado, cultural, social y económico, ya sea internacional, regional o local.

La traducción del contexto externo al inglés sería *"External context"* y al francés *"Contexte Externe"*.

---

33 La UNE-ISO Guía 73:2009 contiene las siguientes notas en relación con la expresión contexto externo: "NOTA El entorno externo puede incluir el entorno cultural, social, político, legal, reglamentario, financiero, tecnológico, económico, natural y competitivo, a nivel internacional, nacional, regional o local; los factores y las tendencias que tengan impacto sobre los objetivos de la organización; y las relaciones con las partes interesadas externas (3.2.1.1), sus percepciones y sus valores."

Según el Anexo D Seguimiento y Revisión de la ISO/TR 31004 apartado 2.4 Los indicadores anticipados,[34] que podrían reflejar cambios en el contexto externo, se encuentran con frecuencia en fuentes de acceso común como informes, artículos de opinión, reportajes y encuestas, que reflejan los cambios y tendencias en la industria en la que opera la organización o en sus temas de intervención cotidiana.

Por ilustrar mejor esta definición podemos reseñar algunos ejemplos de elementos que forman parte del contexto externo, como son:

- El Precio de las 'mercancías' o materias primas, tasas de interés, rendimientos de bonos, tasas de cambio, índices bursátiles, índice de precios al consumidor (en cada ocasión que mencionamos índice nos estamos refiriendo a su tendencia);

- Nivel de incidentes, siniestros o fraude en organizaciones similares o relacionadas;

- Cifras de tamaño y crecimiento del mercado, y cambios repentinos en el volumen de órdenes o pedidos; cambios en las necesidades de los consumidores y/o clientes;

- Grado de estabilidad política y/o social, malestar social y activismo político, tasas de desempleo;

- Deuda pública del país. Saldo de la balanza de pagos. Competidores de otros países que puedan estar accediendo al mercado local;

- Políticas arancelarias o sistemas proteccionistas de otros países en el área de actividad de nuestra organización y factores similares.

- Subsidios y/o subvenciones estatales que puedan afectar a nuestros productos o a nuestras materias primas.

Según se indica en la ISO/TR 31004, la aplicación del segundo principio de la ISO 31000:2009, la gestión del riesgo es una parte integral de todos los procesos de la organización. Los cambios en el contexto externo van más allá de la influencia y el control de la organización, lo que potencialmente puede dar lugar a nuevos riesgos.

Los factores externos en ocasiones se convierten en internos cuando el grado de afectación que comportan para nuestra organización les hace adquirir una gran importancia o influencia respecto a los riesgos o el futuro desarrollo de nuestra organización, es decir, encontramos con frecuencia una mutación de factores externos en internos y viceversa, dependiendo de las condiciones que afecten a nuestra actividad.

Las organizaciones cualquiera que sea su actividad, tienen un componente de relaciones con el entorno, el mercado, las autoridades y otros tipos de entes que les rodean, de esta interacción nace la importancia del "contexto externo", puesto que en

---

34 También conocidos como indicadores adelantados.

el mundo globalizado en que vivimos, el desarrollo de cualquier entidad puede verse afectado de múltiples maneras por elementos externos, a veces sin que lo hayamos previsto o anticipado, de esto se deriva, la fenomenal importancia de vigilar y evaluar correctamente y de forma continuada el "contexto externo", para una adecuada gestión de riesgos.

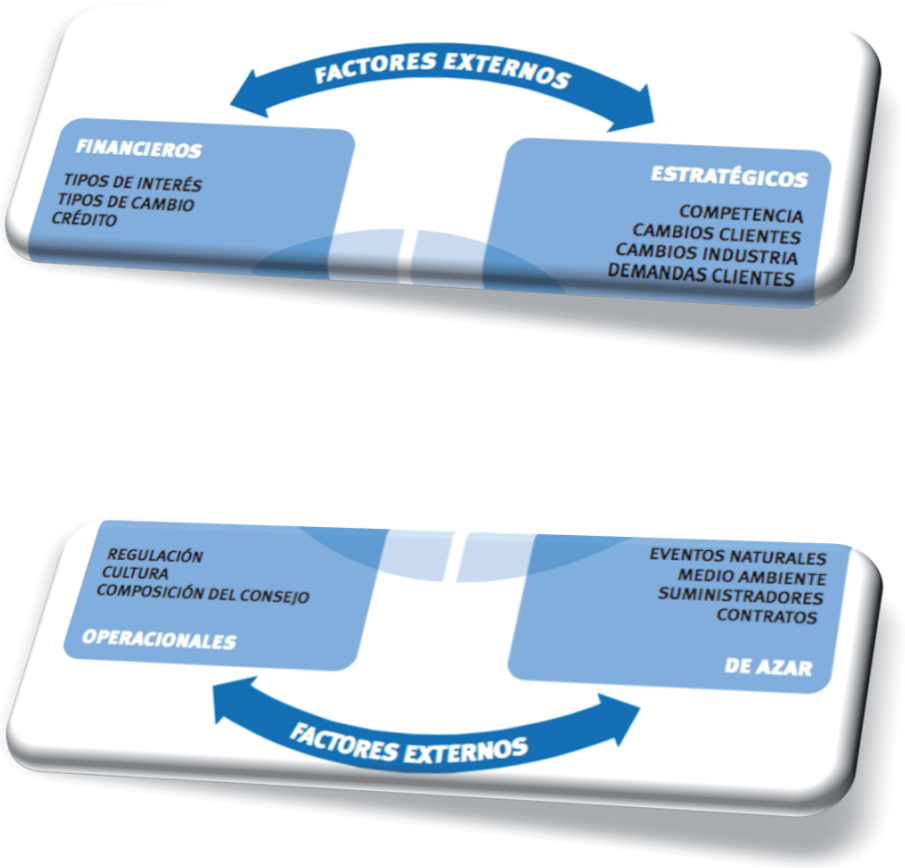

Gráfico 12.

3.3.1.2 Contexto interno:

"Entorno interno en el que la organización busca alcanzar sus objetivos."[35]

El contexto interno, se refiere a las condiciones dentro de la propia organización, que se está definido en el vocabulario de la norma UNE-ISO Guía 73:2009 como el entorno más cercano, intrínseco y propio (Interno) en el que la organización busca y se apoya para alcanzar sus objetivos.

Por lo general se detalla, que el entorno interno puede incluir:

- El gobierno corporativo, la estructura de la organización, los miembros de toda clase y jerarquía, las funciones y las obligaciones.
- Las políticas, objetivos y estrategias,
- Los recursos, conocimientos, patentes, sistemas y procedimientos
- Los sistemas de información, los flujos de información y los procesos de toma de decisiones de cualquier ámbito, formal o informal.
- Las relaciones con, y las percepciones y los valores de las partes interesadas internas.
- La cultura, las normas, las directrices de la organización; y las relaciones contractuales.

Es importante definir y vigilar el contexto interno puesto que la gestión del riesgo se realiza en gran medida dentro de la propia organización o entidad, por lo cual los objetivos ya sean de un proyecto o de toda la organización en su conjunto. Esto implica que deberemos considerar todas las actividades o procesos que tienen lugar en el interior, sin dejar de lado los efectos y reacciones que desde el exterior puedan venir (por supuesto estas reacciones serán "contexto externo", pero pueden venir derivadas de una acción interna previa).

Las consecuencias de no establecer correctamente el contexto interno pueden acarrear efectos adversos para la organización, ya que podremos pasar por alto elementos o dejaremos de reconocer todas las oportunidades o amenazas para lograr los objetivos de la empresa e incluso que poner en peligro su continuidad.

---

35 A propósito del término contexto interno, la UNE-ISO Guía 73:2009 contiene las siguientes notas: "El contexto interno puede incluir:

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

Debemos tener muy presente el considerar todo aquello relacionado con los valores, la cultura, los conocimientos y el desempeño de la organización, ya que nos puede facilitar la comprensión del contexto interno y por ende la mejor valoración de todos los riesgos y una más acertada toma de decisiones.

La traducción al inglés es *"Internal context"* y al francés *"Contexte Interne"*.

Del Anexo D Seguimiento y Revisión de la ISO/TR 31004 apartado 2.4 obtenemos las características internas que pueden dar lugar a cambios en una organización, nos influirían en el contexto interno y por tanto en la consecución de objetivos.

Es importante registrar los cambios que se producen en:

- Estructura;
- prácticas y requisitos de gobierno corporativo;
- políticas, normas internas y modelos;
- requisitos contractuales;
- sistemas estratégicos y operacionales afectados por factores internos;
- capacidades y recursos;
- conocimiento, habilidades y propiedad intelectual;
- sistemas y flujos de información;
- comportamiento social, ambiental y cultural;

Los factores a tener en cuenta a la hora de evaluar el contexto interno son, entre otros, los que se enuncian en el gráfico siguiente:

Gráfico 13.

3.3.1.3 Criterio de riesgo:

"Término de referencia respecto a los que se evalúa la importancia del riesgo"[36]

Criterios de Riesgo:

Puesto que en las primeras páginas de este documento se ha desarrollado todo lo relativo al significado más amplio de la palabra Riesgo a través de la propia "Voz del Riesgo" nos centraremos en el "Criterio" y todo lo que entraña dentro de una organización.

El Criterio proviene del latín tardío *critérium*, y este a su vez del griego. *κριτήριον kritḗrion*, derivado de la palabra *κρίνειν krínein* 'juzgar', hace referencia al juicio o, acción y efecto, de distinguir algo de otra cosa, señalando la diferencia que hay entre ellas. Los criterios de riesgo son reglas que se deben seguir o a las cuales se deben ajustar las conductas, tareas, actividades, para mejor conocer la verdad e identificar la verdadera naturaleza de dicho/s riesgo/s.

La norma UNE-ISO Guía 73:2009 define los Criterios de Riesgo, como los términos de referencia respecto a los que se evalúa la importancia de un riesgo. Los criterios de riesgo se basan en los objetivos de la organización, y en el contexto externo e interno. Apuntando que los criterios de riesgo se pueden obtener de normas, leyes, políticas y otros requisitos o regulaciones.

Su traducción al inglés sería *"Risk Criteria"* y al francés *"Critères de Risque"*.

La norma ISO 31000:2009, plantea dentro del apartado dedicado al establecimiento del contexto de la organización, la definición de los criterios de riesgo. La organización debería definir los criterios de riesgo que se aplican para evaluar la importancia del riesgo. Los criterios deberían reflejar los valores, los objetivos y los recursos de la organización. Algunos criterios pueden estar impuestos o derivarse de requisitos legales o reglamentarios, o de otros requisitos suscritos por la organización. Los criterios de riesgos deberían ser coherentes con la política de gestión de riesgo de la organización, definirse al comienzo de cualquier proceso de gestión de riesgo y revisarse continuamente.

Factores para definir los criterios de riesgo:

- Naturaleza y tipo de las causas y de las consecuencias que se puedan producir, y como se deben medir
- El método de definición de la probabilidad o periodos de recurrencia
- Los plazos de la probabilidad y/o de las consecuencias dañosas

---

36 A propósito del término criterio de riesgos, la UNE-ISO Guía 73:2009 contiene las siguientes notas: "NOTA 1: Los criterios de riesgo se basan en los objetivos de la organización, y en el contexto externo e interno. NOTA 2: Los criterios de riesgo se pueden obtener de normas, leyes, políticas y otros requisitos".

- El método para determinar el nivel de riesgo
- Las opiniones de las partes interesadas
- El nivel al que el riesgo comienza a ser aceptable o tolerable
- Combinaciones múltiples de riesgo existentes, y como se deberían considerar.

Para una gestión de riesgos optimizada, es clave que los riesgos de la organización se encuentren en los límites de sus criterios de riesgo.

Por su parte la propia ISO/TR 31004 hace referencia expresa a los criterios del riesgo diciéndonos que son los parámetros definidos por la organización que le permiten describir los riesgos y tomar decisiones acerca de la importancia de los mismos, reflejando por tanto la actitud de la organización frente al riesgo. Estas decisiones posibilitan evaluar el riesgo y seleccionar el tratamiento más adecuado.

La integración de la gestión de riesgos en la organización ocurre dentro de un contexto dinámico. La organización debería monitorear los cambios provocados por el proceso de implementación, y por los cambios en el contexto interno y externo. Con el transcurso del tiempo y la evolución de las circunstancias se puede producir la necesidad de alteraciones o cambios en sus criterios de riesgo.

Por último, mencionar la capacidad organizadora de los criterios, puesto que para cada ámbito concreto los criterios establecidos por la organización serán la fuente de otras decisiones o procesos dentro de la cadena de la gerencia de riesgos.

3.4.- Términos relativos a la apreciación del riesgo.[37]

3.4.1.- Apreciación del riesgo.

3.5.1. Identificación de los Riesgos

3.5.1.1. Descripción del Riesgo.

3.5.1.2. Fuentes de riesgo.

3.5.1.3. Suceso.

3.5.1.4. Peligro.

3.5.1.5. Dueños del Riesgo

3.4.1.- Apreciación del riesgo. Proceso global que comprende la identificación del riesgo (3.5.1.), el análisis del riesgo (3.6.1.) y la evaluación del riesgo (3.7.1.)

Toda entidad se enfrenta a una variedad de riesgos de fuentes externas o internas que deben ser apreciados. Una pre-condición para la apreciación del riesgo es establecer objetivos ligados a los distintos niveles e internamente consistentes.

Apreciación del riesgo es: la identificación y análisis de los riesgos pertinentes al logro de los objetivos, formando una base para determinar cómo los riesgos deben ser manejados. Debido a que las condiciones económicas y asociadas al ramo de la actividad, las regulaciones y las operaciones se encuentran en constante evolución, se necesitan mecanismos para identificar y tratar los riesgos especiales asociados al cambio.

Se trata del proceso mediante el cual se establece la probabilidad de que ocurran daños personales o pérdidas materiales y la cuantificación de los mismos. Se conocen las variables del riesgo y existe una relación probabilística entre las acciones y sus consecuencias.

Tradicionalmente, desde sus inicios, los recursos tendentes a destinar para apreciar el riesgo se veían como un gasto para la empresa, en el transcurso de los años se ha podido constatar la importancia de analizar los riesgos, lo que ha resultado en considerar no un gasto sino un coste que previene riesgos, pérdidas económicas, deterioros de reputación e imagen y se ha transformado en un elemento estratégico para conseguir y garantizar el éxito empresarial.

En la apreciación del riesgo, es complejo establecer unos patrones de actuación, pues existen numerosos factores que condicionan el cumplimiento de las fases de identificación del riesgo, análisis del riesgo y evaluación del riesgo.

---

37 Los comentarios a los siguientes fueron elaborados por fueron elaborador por **D. Toni Teixidó**: 3.4. Términos relativos a la identificación del riesgo; 3.5.1. Identificación de los riesgos; 3.5.1.2. Fuentes de riesgo; 3.5.1.3. Suceso; 3.5.1.4. Peligro; 3.5.1.5. Dueños del riesgo.

El objetivo de dotar de los recursos para apreciar el riesgo, es el de minimizar los gastos y maximizar los resultados para dotar a la empresa de una mayor estabilidad y aportar recursos que deriven en ventajas competitivas en su sector.

Cada empresa u organización, en base al conocimiento propio del riesgo, debe liderar el diseño de los mecanismos necesarios que permitan identificar los siguientes parámetros que se representan en el diagrama.

Gráfico 14.

Tanto en COSO II como en la norma ISO 31000, la "apreciación del riesgo" se refiere al proceso de evaluación cualitativa y cuantitativa de la exposición al riesgo en las diferentes actividades o procedimientos de la empresa.

Red Herremann afirma "Conocer a los otros es signo de inteligencia, conocerse a si mismo de sabiduría".[38]

38 Ned Herremann *"The Whole Brain Business Book"*. Mac Graw-Hill, Nueva York, 1996.

3.5.- Términos relativos a la identificación del riesgo.

3.5.1. Identificación de los Riesgos

Proceso que comprende la búsqueda, el reconocimiento y la descripción de los riesgos.

Actualmente la gerencia de riesgos es un campo de máxima importancia en las empresas, para liderar y como pilar fundamental, para determinar la "Identidad Corporativa", lo que la empresa es y quiere ser, que constituye un elemento básico de su estrategia.

"La identidad juega un papel clave, proporciona significado, estabilidad y diferenciación" (Moingeon, B. and Soenen, G. 2002)[39]. Otro aspecto fundamental en el que aporta la gerencia de riesgos, es en la "Reputación Corporativa", la imagen ética de la empresa al exterior y al interior, que está siendo una demanda inevitable hoy en día, por parte de accionistas, socios, empleados, clientes, proveedores, ...

Se produce un riesgo cuando existe la posibilidad de que un hecho negativo ocurra o no ocurra o que, suponga un hecho positivo, lo cual plantea dos análisis de riesgo o binomial "Riesgo Positivo" y "Riesgo Negativo".

- **Riesgo Negativo:** Comúnmente su significado se ha asociado a aspectos negativos, citando, por ejemplo: riesgo de incendio, de inundación, de muerte, de contaminación, de paralización de la actividad, …

- **Riesgo Positivo**: Considerando el riesgo, dentro de un marco de incertidumbre, como una oportunidad de generar beneficios, mejoras en los procesos o estabilidad en la empresa.

En la gerencia de riesgos, un aspecto determinante y fundamental es "**la identificación de los riesgos a los que está sometida una empresa**".

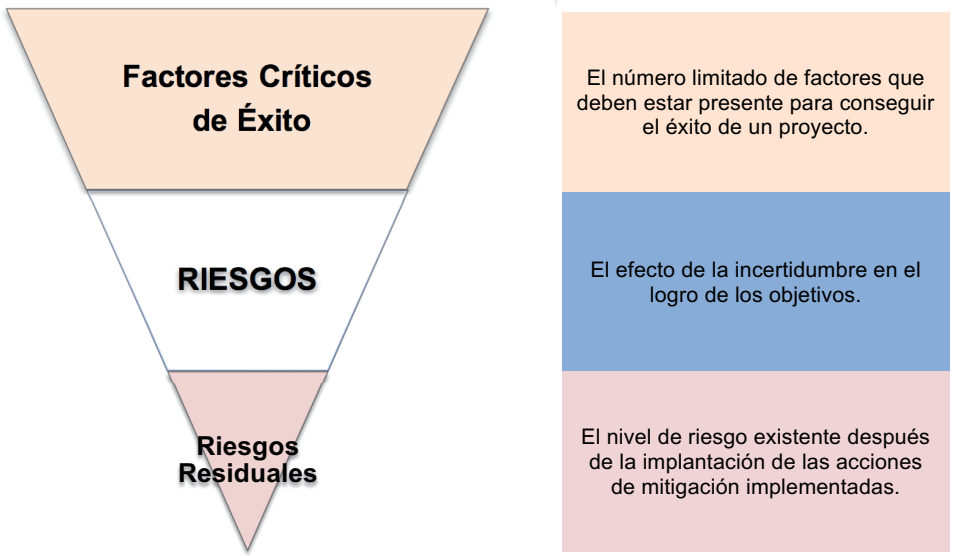

Gráfico 15.

39 Moingen, B, and Soenen, G. (Eds). "Organizational identity and corporate identity". Routledge, London. 2002.

El primer paso del análisis debe consistir siempre en la búsqueda de las fuentes, orígenes o causas de los riesgos, así como los sujetos que pueden verse afectados por los mismos, sus consecuencias potenciales, las áreas de afectación y el impacto global que puede suponer en la evolución de la empresa.

Es importante, generar las bases de conocimiento y de datos históricos que alimenten la base de conocimiento sobre el propio riesgo. La información histórica permitirá generar patrones de conducta o de funcionamiento que podrán desarrollarse con modelos de análisis teóricos.

En las organizaciones es necesario contar con un panel de expertos, bien de la propia empresa bien externos con suficiente experiencia y conocimiento, siempre con el objetivo de liderar la identificación de los riesgos, y por ende dotar de los recursos necesarios a la empresa para minimizar las consecuencias negativas y maximizar las positivas si se producen.

Es habitual utilizar como herramienta de trabajo, la generación de una "checklist" o relación detallada de riesgos, basada en aquellos sucesos que podrían afectar directa o indirectamente a conseguir los objetivos de la empresa.

No hay una especificación en la norma ISO sobre las "herramientas y técnicas de identificación del riesgo" que pueden ser utilizadas, pero si propone que en cada caso se adecuen a los objetivos, aptitudes y riesgos a los que la empresa esté expuesta.

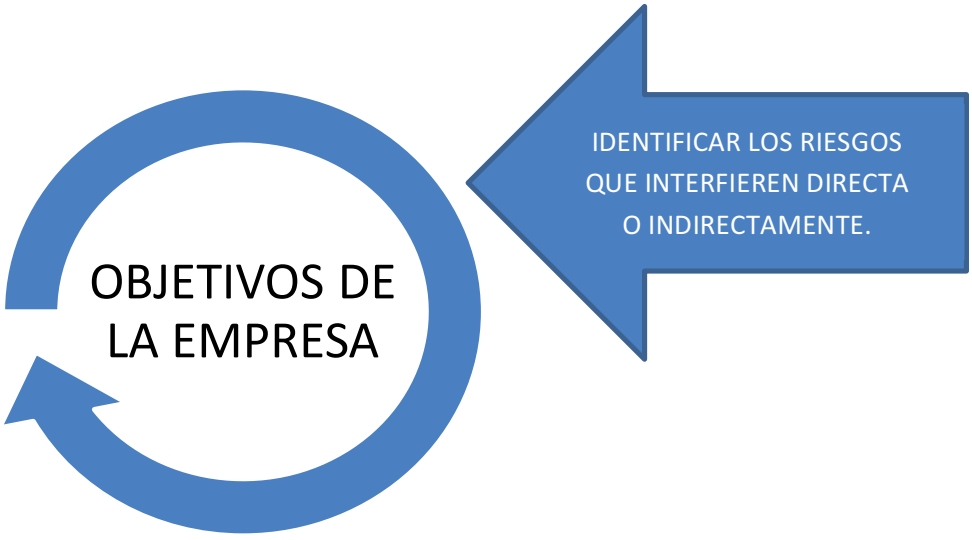

Gráfico 16.

3.5.1.1. Descripción del riesgo.

Representación estructurada del riesgo que contiene generalmente cuatro elementos, las fuentes, los sucesos (3.5.1.3.), las causas y las consecuencias (3.6.1.3.).

El término riesgo en inglés *"Risk"* y *"Hazard"*, según el autor Kaplan and Garrick (1981), definen el término "Risk" como la posibilidad de daño o grado de probabilidad de ese daño, mientras que *"Hazard"* de definiría como la fuente de daño.[40]

Es importante la enumeración de las particularidades de un riesgo, con objeto de su aceptación y tarificación por parte de la entidad aseguradora.

En esta primera fase de la metodología se identifican de forma sistemática las posibles causas concretas de los riesgos empresariales, así como los diversos y posibles efectos que debe afrontar gerencia.

Una correcta descripción del riesgo requiere un conocimiento detallado de la empresa:

- mercado en el que opera,
- entorno legal,
- social,
- político,
- cultural que le rodea.

La identificación del riesgo debe ser sistemática, y empezar por identificar los objetivos clave de éxito y las amenazas que puedan perturbar el logro de dichos objetivos.

Descripción del riesgo como amenaza es el sistema más utilizado para identificarlo. En este contexto, **gestionar el riesgo** significa liderar e instalar sistemas de control que minimicen tanto la probabilidad de que ocurran sucesos negativos como su severidad (la pérdida económica que supondría para el empresario), es decir el objetivo sería asignar recursos para reducir la probabilidad de sufrir efectos negativos.

Procedimientos para identificar y describir los riesgos:

- Análisis de procesos.
- Brainstorming.
- Entrevistas.
- Workshops o talleres de trabajo.
- Comparación con otras organizaciones.
- Cuestionarios.

---

40 Ref. Kaplan, S., and Garrick, B. J. (1981). On the quantitative definition of Risk. Risk Analysis.

Descripción del riesgo como oportunidad, la gestión significa utilizar técnicas que maximicen los resultados, limitando los posibles perjuicios y costes.

3.5.1.2. Fuentes de riesgo.

Elementos que, por si solos o en combinación con otros, presentan el potencial intrínseco de engendrar un riesgo (1).[41]

Fuentes de riesgo son todos aquellos ámbitos de la empresa, internos o externos, que pueden generar amenazas de pérdidas o impedimentos para alcanzar los objetivos.

Un procedimiento que facilita la identificación de los riesgos es el preguntarse, para cada una de las fuentes, si existen debilidades o amenazas en cada una de las fuentes.

Las fuentes de riesgo fueron analizadas en el apartado 1.1, donde puede apreciarse la diversidad de formas de calificar los riesgos. Por ejemplo, según su origen, podrían establecerse los siguientes:

1. **SECTOR:** Riesgo de que factores externos e independientes de la gestión del emprendedor puedan influir directa o indirectamente de manera significativa en el logro de sus objetivos y estrategias.

2. **OPERATIVO:** Relacionado con la habilidad del empresario o el ejecutivo para convertir la estrategia elegida en planes concretos, mediante la asignación eficaz de recursos.

3. **TECNOLOGÍA:** Mide cual es la exposición de la empresa a los riesgos tecnológicos, derivados de la necesidad de acometer fuertes inversiones para asegurar la viabilidad de su proyecto empresarial, en un plazo determinado de tiempo o la necesidad de formar a sus empleados en el uso de la tecnología.

4. **PROVEEDORES:** El papel que jueguen los proveedores en el sector podría generar riesgos para la empresa, debido a las variaciones en el precio de las materias primas, a disponer de variedad en la oferta y durante un periodo de tiempo continuo, así como su grado de concentración que determinará la forma de pago tradicionalmente aceptada en el sector.

5. **CLIENTES:** Los clientes podrían ser un foco importante de riesgo para la empresa, puesto que son los generadores de ingresos y barómetro para suministrar capacidad de liquidez económica. El riesgo puede proceder de cambios en sus gustos y necesidades, de generar presiones a la baja en los precios o de dilatar el periodo de pago entre otros, de modo que la propuesta del valor de la empresa ha de estar siempre orientada al cliente.

6. **COMPETIDORES:** El tamaño, la capacidad financiera y operativa de los agentes de un sector determinan el grado de rivalidad del mismo y establecen las reglas

---

41 A propósito del término fuentes de riesgo, la UNE-ISO Guía 73:2009 aclara en NOTA: "Una fuente de riesgo puede ser tangible o intangible".

de juego que cualquier nuevo agente tiene que considerar para operar en ese mercado, esto puede suponer riesgos para el emprendedor.

7. **FINANCIERO:** La incertidumbre asociada a la gestión efectiva y al control de las finanzas que lleve a cabo el emprendedor, así como a los efectos de factores externos como la disponibilidad de crédito, tipos de cambio, movimientos de los tipos de interés, etc.

8. **SOCIOPOLITICO:** Asociado a factores que no son propios del mercado como políticas sociales (empleo, políticas fiscales, políticas monetarias, políticas de desarrollo, etc.) o eventos relacionados con inestabilidad política (ataques terroristas, guerras civiles, revueltas populares, etc.).

Es necesario liderar la búsqueda y reconocimiento del riesgo, que debe ser sistemática y debe comenzar por definir los objetivos planteados, analizar los factores que son clave en su empresa o el cometido para alcanzar el éxito y revisar cuales son las debilidades del proyecto y las amenazas a las que se enfrenta.

Es habitual, generar un análisis DAFO (Debilidades, Amenazas, Fortalezas y Oportunidades), en particular los puntos débiles y las amenazas, ofrecerán una visión de los riesgos a los que se enfrenta la empresa.

Gráfico 17.

3.5.1.3. Suceso.

Según el Diccionario de la Real Academia Española de la lengua, Suceso se define como:

1. Cosa que sucede, especialmente cuando es de alguna importancia.

2. Éxito, resultado, término de un negocio.

3. Hecho delictivo.

4. Accidente desgraciado.

La expresión proviene del latín "*successus*" llegada, éxito.

En el análisis de riesgos consideraríamos que un **Suceso** es una ocurrencia o cambio de un conjunto particular de circunstancias.

Un suceso puede ser único o repetitivo, y se debe a varias causas.

a. Único. Su ocurrencia se produce en una sola ocasión.

b. Repetitivo. Su ocurrencia se produce en varias ocasiones en el tiempo, y su periodicidad depende en cada circunstancia.

Un suceso, la primera ocasión que ocurre es único, cuando se produce en otra ocasión ya es repetitivo, puede darse dos o más veces.

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

Por ejemplo: La erupción de un volcán, los estudios y la ciencia determinan que es probable que un volcán entre en erupción, pero no es posible determinar cuándo se producirá el suceso.

Un suceso se puede calificar como un "incidente" o "accidente"

a. **Incidente**: es aquello que se interpone en el transcurso normal de una situación o evento. Es un hecho puntual, por ejemplo, en un acto público, surge un altercado de protesta que obliga a posponer dicho acto.

El incidente, es importante analizarlo y liderar la toma de las medidas necesarias, para restaurar la situación anterior a la ocurrencia del mismo.

b. **Accidente**: hecho imprevisto que altera la marcha normal o prevista de las cosas, especialmente al causar un daño o perjuicio a la persona, bien o derecho.

Ejemplos: accidente de tráfico, accidente industrial, incendio, explosión, inundación, …

Un suceso sin consecuencias también se puede citar como "cuasi accidente", o "incidente" en el que la consecuencia sea igual al resultado de un suceso que afecta a los objetivos.

Un cuasi accidente: es un incidente donde no ha ocurrido ningún efecto negativo como, por ejemplo:

- El fallo en la línea de anclaje de una carga en un barco portacontenedores antes de zarpar en el que no se arriesga la estabilidad del buque, pero es necesario restaurar el sistema de anclaje para garantizar la estabilidad y la seguridad de la carga y del buque.

Otro ejemplo explicativo de un "quasi accidente", es en el supuesto que dos vehículos en circulación, están a punto de colisionar por la maniobra imprevista que realiza uno de los vehículos al aparecer un animal en la carretera. Son situaciones que no resultaron lesiones personales o daños materiales, pero tenían el potencial de hacerlo.

Accidente, sería la colisión de los vehículos, con resultado de daños materiales y/o personales.

3.5.1.4. Peligro.[42]

Fuente de daños potencial.

Situación en la que existe la posibilidad de amenaza u ocasión de que ocurra una desgracia o contratiempo. En términos de lesiones o efectos negativos para la salud, daños a la propiedad, daños al entorno o una combinación de todos.

Proviene del latín "*periculum*".

- Factores que Causan el Peligro, según su naturaleza.

  a. Factores **Naturales**:
  Origen: Si son de la mano de la naturaleza.
  Ejemplo: Una avalancha de nieve.

  b. Factores **Antropomórficos:**
  Origen: No son de la mano de la naturaleza.
  Ejemplo: El vertido de un producto tóxico.

- Un peligro puede ser una fuente de riesgo, que puede materializarse de forma Latente o Potencial:

  a. **Fuente de Riesgo Latente.** La situación es potencialmente peligrosa pero todavía las cosas, las personas, el medio ambiente o la propiedad no fueron afectadas.

---

42 A propósito del término peligro, la UNE-ISO Guía 73:2009 contiene la siguiente nota: "Un peligro puede ser una fuente de riesgo (3.5.1.2.)."

Como, por ejemplo: «un puente que en su estructura presenta algunas debilidades, será un peligro latente».

b. **Fuente de Riesgo Potencial**. La situación está en condiciones para afectar a las personas, cosas o propiedades y requiere una evaluación para determinar concretamente las posibilidades de que se convierta en una emergencia.

Como, por ejemplo: «un puente que en su estructura se aprecian grietas evidentes que suponen un peligro inmediato que pone en duda su estabilidad».

Es importante calcular la probabilidad de que un peligro provoque daños concretos, para ello existen varios métodos para analizar cada situación y determinar la posibilidad de la ocurrencia y la magnitud de los daños que pudiera ocasionar.

- Clasificación del Peligro

El peligro se ha clasificado por numerosos organismos oficiales con la finalidad de liderar la aportación de una nomenclatura y simbología que permita unificar los criterios de identificación del peligro, como por ejemplo la OMS (Organización Mundial de la Salud), que ha establecido una clasificación del peligro según su naturaleza.[43]

- Peligros Biológicos: bacterias, virus, parásitos, …
- Peligros Químicos: pesticidas, mico toxinas, aditivos alimentarios tóxicos, …
- Peligros Físicos: objetos que puedan causar daños físicos al consumidor.

Las Naciones Unidas (ONU), en el año 2011 publicó la 4ª Edición Revisada, del "Sistema Globalmente Armonizado de Clasificación y Etiquetado de Productos Químicos" (S.G.A.), según las consecuencias del peligro.[44]

- Peligros al Medio Ambiente.
- Peligros Físicos.
- Peligros para la Salud.

---

43 OMS (Organización Mundial de la Salud).

44 Las Naciones Unidas (ONU), 4ª Edición Revisada, del "Sistema Globalmente Armonizado de Clasificación y Etiquetado de Productos Químicos" (S.G.A.), según las consecuencias del peligro (2011).

3.5.1.5. Dueños del Riesgo

Persona o entidad que tiene responsabilidad y autoridad para liderar la gestión de un riesgo (1.1.).

El riesgo es siempre del dueño (*"res Perit domino"*).

El dueño es el responsable de la gestión del riesgo, y debe tener los conocimientos, los recursos y la autoridad para hacer frente al riesgo.

El dueño del riesgo es posible analizarlo desde dos ángulos:

A) En calidad de Propietario o Especialista del Riesgo:

• En calidad de propietario del activo que genera el riesgo, o que es el propietario del riesgo (RISK OWNER).

• En calidad de especialista en identificar, evaluar y liderar las medidas necesarias para mitigar o acotar el riesgo. Lo que se conoce como la figura del GESTOR DE RIESGOS.

B) La importancia del Riesgo

A menudo el propietario del riesgo no es el gestor del riesgo, es importante determinar claramente las responsabilidades personales según sus conocimientos y su eficiencia.

A) El dueño del riesgo "**PARCIAL**", solamente tiene responsabilidad sobre una parte del proceso y del riesgo.

B) El dueño del riesgo "**TOTAL**". tiene responsabilidad sobre la globalidad del proceso y del riesgo.

Las funciones del dueño del riesgo son:

Gráfico 18.

3.6. Términos relativos al análisis del riesgo.[45]

3.6.1. Análisis del riesgo.

3.6.1.1. Probabilidad *(likehood)*.

3.6.1.2. Exposición.

3.6.1.3. Consecuencia.

3.6.1.4. Probabilidad *(probability)*.

3.6.1.5. Frecuencia.

3.6.1.6. Vulnerabilidad.

3.6.1.7. Matriz de riesgo.

3.6.1.8. Nivel de riesgo.

3.6.1. Análisis del riesgo.

La guía ISO 73:2009 define el análisis del Riesgo como el Proceso que permite comprender la naturaleza del riesgo (1.1) y determinar el nivel de riesgo (3.6.1.8).

Podríamos definir también el análisis del riesgo como el estudio sistemático[46] de la incertidumbre que permite conocer, categorizar y clasificar los distintos riesgos y su impacto en una organización facilitando la toma de decisiones para su mitigación.

Se trata por tanto de un proceso en el que a través de la recopilación de datos e información de diversa naturaleza se asignan valores a los riesgos a través de su evaluación y estimación, permitiendo a la organización determinar sus prioridades, plantear una estrategia y facilitar la toma de decisiones a la gerencia involucrada.

De acuerdo con la normativa ISO 31000 el análisis de riesgo es una de las actividades incluidas en el proceso de gestión del riesgo, actividad inmediatamente posterior a la identificación del riesgo y anterior a la evaluación de riesgo. El análisis ahonda en el conocimiento del riesgo y para ello se toma en consideración la fuente del riesgo, la consecuencia y la probabilidad *(likehood)* para poder estimar el riesgo inherente.

---

45 Los comentarios a los apartados 3.6.- Términos relativos al análisis del riesgo. 3.6.1, Análisis del riesgo. 3.6.1.1. Probabilidad *(likehood)*, 3.6.1.2. Exposición, 3.6.1.3. Consecuencia, 3.6.1.4. Probabilidad *(probability)*, 3.6.1.5. Frecuencia, 3.6.1.6. Vulnerabilidad, 3.6.1.7. Matriz de riesgo y 3.6.1.8. Nivel de riesgo, fueron elaborados por D. **Julio López García**.

46 RISK STEERING COMMITTEE "Department of Homeland Risk Lexicon." Página27, 2008.Ed. Us Department of Homeland Security.

Este riesgo es definido por COSO[47] como el riesgo al que se somete una entidad sin que se haya tomado ninguna medida por parte de la gerencia que pudiera alterar la probabilidad y el impacto.

El análisis de riesgo se lleva a cabo a través de técnicas cualitativas, cuantitativas o semi-cuantitativas, la utilización de una u otra técnica es indiferente y dependerá del riesgo, del propósito del análisis, así como de la información y los datos disponibles. Mientras que el uso de medidas cualitativas o semi-cuantitativas se utiliza para visualizar un riesgo la valorización cuantitativa es más costosa y por lo tanto se utiliza en aquellos riesgos en los que se requiere un análisis de mayor profundidad. Las herramientas disponibles son amplías como las monografías, gráficos de riesgo, pero la más extendida es la matriz de riesgo[48] que nos permite visualizar el riesgo.

Es importante resaltar que no existe un modelo estándar para la gerencia de riesgos, sino que será cada organización quien determine el proceso que desea adoptar, algunas organizaciones distribuyen el análisis en dos etapas (COSO) mientras que otras como FERMA lo distribuyen en tres fases, lo importante es que el análisis esté correctamente realizado.

Podemos mencionar como ejemplo el los estándares de gerencia de riesgos establecidos por la organización FERMA[49] el proceso de gerencia de riesgos incluye la valoración de riesgos y dentro de la misma el Análisis de los Riesgos que se compone de tres fases, la identificación de riesgos, la descripción de riesgos y la estimación de riesgos.

Fase primera (identificación de riesgos):

La primera fase permite conocer dentro de las actividades más importantes que desarrolla una empresa cuales son los riesgos que llevan aparejadas el ejercicio de las mismas. Es de gran importancia que se identifiquen muy bien que actividades desarrolla la empresa, ya que el análisis de riesgo de riesgo pretende conocer cuál es la exposición de una organización y ello conlleva tener el mayor conocimiento posible de muchos aspectos tales como el mercado en el que se desenvuelve, su estrategia, sus objetivos, etc.

Podemos distinguir dos sub-fases dentro de esta primera fase de identificación del riesgo:

Identificación Inicial de riesgos: afecta a aquellas organizaciones que previamente no han identificado sus riesgos de una forma ordenada o estructurada, a una nueva organización, o a un nuevo proyecto o actividad llevado a cabo por una organización.

---

47 CURTIS PATCHIN, CAREY MARK "Risk Assesment in Practice." Página7, 2012.Ed. Committee of Sponsoring Organizations of the Treadway Commission (COSO).
48 Ver definición 3.6.1.7.
49 FEDERATION OF EUROPEAN RISK MANAGEMENT ASSOCIATIONS (FERMA) "Estándares de Gerencia de Riesgos." Página 6, Bruselas 2003.Ed. FERMA.

Identificación contínua de riesgos: debe formar parte de la rutina habitual de una organización que previamente ya ha realizado la identificación inicial de riesgos. Se trata de identificar riesgos que no habían sido previamente identificados, cambios en los actuales riesgos o riesgos que anteriormente eran relevantes para una organización pero que ya no lo son. Las organizaciones y el entorno en el que se mueven son cambiantes e imprevisibles. Un claro ejemplo sería el crecimiento experimentado por el seguro de ciberriesgo durante los últimos quince años. Antes considerado como un ramo residual pero que en la actualidad forma parte de la cartera de riesgos transferidos de cualquier organización que se precie.

Existen muchos modos de identificar los riesgos, algunos ejemplos podrían ser las siguientes:

- Analizar los procesos y procedimientos llevados a cabo en cada actividad productiva de la organización.
- Consultar a los trabajadores y supervisores aprovechando la experiencia interna.
- Analizar los accidentes, incidentes y enfermedades a través de los registros y datos de la organización.
- Consultar con especialistas en prevención de riesgos laborales (por ejemplo).

Algunos ejemplos sencillos de posibles riesgos comunes en una fábrica podrían ser los siguientes:

Riesgo	Daño potencial
Trabajo manual	El movimiento repetitivo de ciertas actividades puede generar distensiones musculares y por lo tanto bajas laborales.
Gravedad	La gravedad puede provocar caídas, resbalones que pueden derivar en posibles lesiones.
Electricidad	Posibles muertes por electrocución en caso de trabajar con elementos de alta tensión.
Maquinaria y equipos	Posibles atropellos por la maquinaria móvil que trabaja en la nave (carretillas).
Ruido	La exposición prolongada a sonidos elevados puede provocar problemas auditivos.
Radiación	La utilización de maquinaria con rayos laser o luz
Psicológicos	Efectos causados por estrés (fatiga), bullying que puedan derivar en bajas de los trabajadores.

Tabla 1.

Fase Segunda: descripción de los riesgos

La segunda fase (descripción) dota de estructura a los riesgos identificados. Esto nos permite poder visualizar de forma individual las características de cada riesgo y nos permitirá una vez efectuado el análisis priorizar en aquellos riesgos que la organización considere que tienen que ser tratados o a los que se debe dotar de mecanismos de control. Tomando en consideración los ejemplos anteriormente mencionados un ejemplo podría ser el siguiente:

Riesgo	Maquinaria y equipos
Naturaleza del riesgo	Operacional
Actores afectados	Empleados y terceros que trabajen en la nave
Probabilidad de ocurrencia	Baja
Importancia	Alta
Tratamiento del riesgo	Personal cualificado conduciendo las carretillas, señalización optima de las zonas de paso, transferencia adecuada del riesgo
Posibles mejoras	Realización de cursos en materia de prevención laboral avanzados, futuro protocolo en caso de accidente personal

Tabla 2.

Tal y como podemos observar en el ejemplo descrito, en este caso el riesgo es de carácter operacional e involucra a los empleados y terceros que trabajen habitualmente con esta maquinaria. Debido al tratamiento del riesgo llevado a cabo las probabilidades de que se materialice un evento de estas características son escasas, no obstante, en caso de producirse las consecuencias podrían ser graves debido a las altas indemnizaciones que judicialmente se suelen dictar a favor del afectado. Independientemente que se hayan tomado medidas de control tales como una adecuada señalización o la contratación de un seguro obligatorio de responsabilidad civil la gravedad de las consecuencias derivadas de este tipo de eventos aconseja tomar medidas de control adicionales como un protocolo para accidentes personales o impartir cursos de prevención laboral avanzados al personal que trabaje en las instalaciones.

Fase tercera: estimación de los riesgos

La última fase (estimación) permite medir cual es la probabilidad de ocurrencia de un riesgo, así como sus posibles consecuencias. Dado que se han identificado anteriormente los riesgos, se procede a la diferenciación entre los distintos riesgos tomando en consideración sus consecuencias (positivas o negativas) así como la probabilidad de ocurrencia.

La estimación del riesgo se realiza a través del análisis cualitativo y cuantitativo mencionado al principio de este epígrafe. El análisis cualitativo se basa en el uso de escalas descriptivas mientras que el análisis cuantitativo requiere valores numéricos para estimar probabilidad (likehood) y el impacto utilizando datos

de muy diversas fuentes. Entre las ventajas que ofrecen las técnicas cualitativas podemos destacar que estas son más sencillas de elaborar, y que pueden ofrecer valiosa información en ámbitos tales como la vulnerabilidad, impacto, seguridad o la reputación. Por el contrario, son más imprecisas dado que dentro de un mismo nivel de riesgo puede haber grandes diferencias en la cuantía del riesgo. En cuanto a las técnicas cuantitativas podemos destacar que permiten realizar el análisis del coste-beneficio a la hora de tomar decisiones por parte de la gerencia para controlar o mitigar un riesgo, aunque ello suponga una asignación de recursos importante para la organización.

La gran mayoría de organizaciones utilizan técnicas cualitativas en un primer momento para posteriormente apostar por el uso de técnicas cuantitativas más complejas para el tratamiento de aquellos riesgos más relevantes y que influyen en la toma de decisiones.

Algunos ejemplos de análisis cualitativos serían los siguientes: entrevistas, encuestas, benchmarking, o el análisis de escenarios. Respecto al análisis cuantitativo un modelo habitual es el probabilístico.

Como se ha mencionado anteriormente el análisis de riesgo se realiza siempre respecto del riesgo inherente (antes de las medidas de mitigación). Una vez se han desarrollado las respuestas al riesgo, se volverá a analizar el riesgo residual definido por COSO como el riesgo remanente una vez la gerencia ha tomado medidas de respuesta sobre el riesgo.

3.6.1.1 Probabilidad *(Likehood)*.

La Guía ISO 73:2009 define la probabilidad *(likehood)* como la posibilidad de que algún hecho se produzca.

En primer lugar, debemos diferenciar la probabilidad *(likehood)* de la probabilidad *(probability)*. Tal y como se indica en la Nota 2 de la Guia 73:2009 la palabra likehood no tiene equivalente en otras lenguas y es por ello que se utilizar la palabra probabilidad *(probability)*. Este término como veremos en la definición 3.6.1.4 tiene un significado relacionado con el ámbito matemático. En el ámbito de la gerencia de riesgos el término probabilidad *(likehood)* será interpretado de igual forma que el término probabilidad *(probability)* en otros idiomas.

La probabilidad es una de las tres dimensiones del riesgo junto con su dirección (positiva o negativa) y sus consecuencias. Todo riesgo tiene un grado de probabilidad, aunque esta sea muy pequeña si existe probabilidad entonces hay riesgo. Tal y como se ha mencionado la probabilidad representa la posibilidad de que un acontecimiento dado ocurra y por ello se trata de un término relacionado con la exposición que depende a su vez de la duración y frecuencia de esa exposición. Imaginemos por ejemplo el siguiente caso: exponer ocho personas ante un mismo riesgo durante una hora es equivalente a exponer cuatro personas ante ese mismo riesgo durante dos horas.

Para poder estimar la probabilidad las organizaciones se sirven de eventos pasados que puedan ser observables. Los datos se pueden basar en información obtenida internamente o externamente. Los datos internos suelen proveer mejores resultados, aunque los datos externos nos permiten mejorar el análisis realizado. Así por ejemplo si una organización quiere analizar las paradas en su producción como consecuencia del fallo de cierta clase maquinaria lo primero que hará será analizar las paradas que ha sufrido en el pasado, y el impacto que estas paradas tuvieron en su actividad. Posteriormente y si es posible llevará a cabo un estudio de *Benchmarking*.[50] Se trata de un proceso de colaboración entre distintas entidades de un mismo sector basado en procesos o eventos específicos, y en donde se comparan medidas y resultados de tal forma que se puedan identificar oportunidades de mejora. La información disponible en materia de eventos o procesos permite comparar el rendimiento con el de otras organizaciones. Habitualmente se realiza el proceso de Benchmark para medir la probabilidad y el impacto de ciertos eventos potenciales en un determinado sector. Una vez conocidos los resultados de este estudio la gerencia de la organización dispondrá de información suficiente para analizar si las medidas de prevención que actualmente están llevando a cabo son suficientes, si estas son las adecuadas, o si por el contrario tienen que adoptar medidas adicionales a las ya implantadas.

A la hora de realizar predicciones sobre el futuro las organizaciones deben ser cautelosas ya que no solo se deben tomar en consideraciones aquellos hechos pasados observables sino también en los distintos factores ya que influyen en el transcurso del tiempo.

Para poder apreciar el riesgo las organizaciones habitualmente recurren una combinación entre las técnicas cualitativas y cualitativas dependiendo de las circunstancias. Así por ejemplo se recurrirá a las técnicas de apreciación cualitativa cuando los datos con los que cuenta la organización no sean confiables o bien sean insuficientes para poder realizar una apreciación cuantitativa en garantías. Puede darse también el caso que aun teniendo suficientes datos confiables el análisis de datos requiera un esfuerzo tal que el coste-beneficio no compense. Las técnicas cuantitativas son más precisas y se utilizan en actividades más complejas y sofisticadas por lo que lo habitual es que complementen a las técnicas cualitativas.

Para poder visualizar la probabilidad adecuadamente se recurre a las de matrices de riesgo. Se puede expresar mediante términos cualitativos (frecuente, probable, posible, improbable…) así también se puede expresar como un porcentaje de probabilidad o dentro de una frecuencia temporal. En el caso de utilizar valores numéricos (frecuencia o porcentaje) debemos hacer referencia al periodo de tiempo relevante por ejemplo anual, o si hacemos referencia a un proyecto el tiempo de duración que vaya a tener ese proyecto. Un ejemplo de escala ilustrativo para la probabilidad *(Likehood)* podría ser el siguiente:

---

50 AM BEST “Glossary of Insurance Terms” Letra B www.ambest.com.

Escala	Frecuencia	Definición
5	Frecuente	Una vez o más cada 2 años
4	Probable	Una vez cada 2 años hasta 25 años
3	Posible	Una vez cada 25 años hasta 50
2	Improbable	Una vez cada 50 años
1	Raro	Una vez cada 100 años

Escala	Frecuencia	Definición
5	Frecuente	Más de un 90% de posibilidades de que ocurra
4	Probable	65% a 90% de posibilidades de que ocurra.
3	Posible	35% a 65% de probabilidades de que ocurra.
2	Improbable	De 10% a 35% de posibilidades de que ocurra.
1	Raro	Menos de 10% de posibilidad de que ocurra.

Tabla 3.

3.6.1.2. Exposición.

La Guía ISO 73:2009 define la exposición como el grado al que se somete una organización y/o una parte interesada (3.2.1.1) en caso de un suceso (3.5.1.3).

Podemos definir también como expresión que mide[51] la vulnerabilidad de una organización frente a la ocurrencia de un evento.

La exposición a un riesgo viene determinada por la combinación entre el impacto y la probabilidad (likehood).

Por ello cualquier organización que quiera gestionar correctamente sus riesgos primero procederá a identificar cuáles son los riesgos a los que se expone y posteriormente analizará individualmente cada uno de esos riesgos identificados.

Desde el punto de vista de la industria aseguradora resulta muy interesante tomar en consideración los cada vez más habituales riesgos catastróficos y como estos sucesos afectan gravemente desde un punto de vista económico y social a los países y organizaciones que sufren sus consecuencias.

Una organización de carácter multinacional que tenga operaciones en todo el mundo estará siempre expuesta a riesgos catastróficos (inundaciones, Terremotos, tsunamis, ciclones o incluso huracanes) que tendrá que identificar (según la región geográfica) y analizar de forma independiente si quiere gestionar adecuadamente sus riesgos. Este análisis se realizará a través de la evaluación de la probabilidad *(likehood)* y el

51 AM BEST "Glossary of Insurance Terms" Letra E www.ambest.com.

impacto permitiendo a la organización articular una respuesta basada en la gerencia de riesgos.

En el caso de un riesgo catastrófico por ejemplo se tendrá que considerar donde se encuentran situados los activos de la organización (si se trata de zonas sísmicas o no), si existe acumulación de activos en una determinada zona geográfica, o donde se encuentra situado el activo de mayor suma asegurada, o de mayor importancia operativa para la organización. Todos estos factores condicionarán el impacto sufrido por la organización en caso que se materialice el evento. Una elevada concentración de activos en una zona sísmica puede elevar la exposición de una organización a niveles de riesgo[52] inaceptables que podrían comprometer no solo su actividad sino también el cumplimiento de sus objetivos futuros o incluso en el caso que el impacto fuera muy grave podría comprometer la viabilidad futura de la organización. Una correcta política de gerencia de riesgos aconsejaría realizar un análisis cuantitativo de tal forma que la organización pudiera obtener información precisa sobre el impacto que pudiera generar un riesgo catastrófico como el comentado. Si los resultados no son positivos es posible que la gerencia de riesgos aconseje deslocalizar ciertos activos a otras zonas de menor actividad sísmica de tal forma que el impacto y la probabilidad de ocurrencia disminuyan reduciendo la exposición de la organización.

Para poder visualizar la exposición a un riesgo la herramienta más adecuada (y la más común) es la matriz de Riesgo[53]. Las matrices de riesgo utilizan diferentes escalas en función del objetivo pretendido. No existe ningún parámetro que establezca el uso de una u otra escala en una matriz de riesgo, sino que será cada organización la que determine cuál es el estándar de Escala que mejor se ajuste a sus necesidades, y por tanto a sus objetivos. Si buscáramos obtener un nivel mínimo de categorización entonces optaríamos por una Escala 3x3[54] mientras que si nuestro objetivo es realizar una evaluación cuantitativa para un riesgo Particular entonces utilizaríamos una Matriz de Riesgo con Escala 5x5.[55]

Entendemos que la exposición a un riesgo es aceptable cuando el impacto sufrido como consecuencia de un evento es tolerable y la frecuencia de ocurrencia permite a la organización seguir alcanzando los objetivos pretendidos. Si por el contrario la exposición ante un riesgo no es aceptable se deberán implantar medidas de control en el caso de que ese riesgo no hubiera sido tratado con anterioridad, y se revisarán los mecanismos de control actuales en el caso que estuviéramos ante un riesgo residual[56] y que por tanto hubiera sido objeto de un tratamiento de riesgo anterior.

---

52 Ver definición 3.1.6.7 “nivel de riesgo”.
53 Ver definición 3.1.6.7 “Matriz de riesgo”.
54 Ver ejemplo Gráfico dentro de la definición matriz de riesgo.
55 Ver ejemplo Gráfico dentro de la definición matriz de riesgo.
56 Ver definición de riesgo residual 3.8.1.6.

3.6.1.3 Consecuencia.

La Guía 73:2009 define consecuencia como: "Resultado de un suceso (3.5.1.3) que afecta a los objetivos".

Podríamos también considerar la consecuencia como "el efecto [57] derivado de la materialización [58] de un riesgo".

Un ejemplo de consecuencia podrían ser los numerosos Daños Materiales sufridos por un centro comercial como consecuencia de una Explosión súbita y accidental. A través del análisis de la consecuencia podemos identificar y evaluar aquellos efectos actuales y potenciales de un evento.

Existen diversos resultados asociados a un evento y estos son siempre tomados en consideración durante el proceso de gerencia de riesgos. Las consecuencias de un evento pueden ser positivas, negativas o una mezcla de ambas, aunque normalmente en gerencia de riesgos se suelen tomar en consideración las negativas. Los acontecimientos cuyas consecuencias son negativas son analizados para posteriormente decidir si se deben tomar medidas para su control o mitigación. Los eventos con consecuencias positivas por el contrario son una oportunidad para reducir las consecuencias negativas causadas por otros acontecimientos, y se toman en consideración durante el proceso de gerencia de riesgos para que la organización pueda tomar futuras decisiones en relación con su estrategia y objetivos. Así por ejemplo una correcta Política de gestión de riesgos puede derivar en la implantación de un sistema integral de protección contra incendios cuya consecuencia positiva sería la reducción de los potenciales daños causados por un incendio que previsiblemente tendría (consecuencias negativas) para la consecución de los objetivos de la organización.

Existen diversos rangos de posibles resultados asociados a un acontecimiento y se toman en consideración para dar una respuesta al riesgo en fases posteriores del análisis de riesgo. Las consecuencias positivas y negativas de un riesgo son tomadas en consideración se estructuran de forma individual o por categoría. Para poder visualizar mejor las consecuencias se puede recurrir a una tabla de estimación. Así, por ejemplo, podemos tomar en consideración las consecuencias en términos de amenazas y oportunidades clasificándolas en altas, medias y bajas. La gran mayoría de organizaciones pueden trabajar con esta clasificación no obstante otras querrán utilizar tablas más complejas que la aquí expuesta:

---

57 RISK STEERING COMMITTEE. "Department of Homeland Risk Lexicon." Página 10, 2008.Ed. Us Department of Homeland Security.

58 GUARDIOLA LOZANO ANTONIO, CASTELO MATRAN JULIO "Diccionario Mapfre de Seguros." Página 114, Madrid 2009.Ed. Fundación Mapfre.

Tabla de estimación:

Altas	Fuerte impacto financiero en los resultados de la organización. Afectación importante en la estrategia operativa de la empresa
Medias	Impacto financiero moderado en los resultados de la organización. Afectación moderada en la estrategia operativa de la empresa
Bajas	Impacto financiero mínimo en los resultados de la organización. Afectación baja en la estrategia operativa de la empresa

Tabla 4.

Así también podemos clasificar las consecuencias por ejemplo según su gravedad. Tomando en consideración los daños materiales sufridos en una fábrica como consecuencia de un incendio, podríamos establecer la siguiente clasificación que considera cinco niveles de riesgo según las consecuencias generadas por el evento (severa, grave, moderada, menor y baja). La utilización de clasificaciones con más o menos niveles depende exclusivamente de la organización, y del tipo de riesgo que se tome en consideración. No siempre utilizar una clasificación con más niveles es garantía de un mejor resultado. Hay que tomar en consideración que la diferencia entre uno y otro nivel puede ser prácticamente inexistente provocando que su interpretación por parte de los trabajadores de la organización se dificulte. Pensemos que dependiendo de la gravedad de las consecuencias se activara un determinado tipo de protocolo u otro y no quedara claro si las consecuencias fueran severas o graves. En este caso una clasificación que utilizara solamente tres calificaciones (severa, moderada, baja) facilitaría la aplicación del protocolo ya que las consecuencias quedarían dentro de la calificación severa y por tanto se aplicaría el protocolo habilitado a tal efecto.

Tabla Clasificación Consecuencias según gravedad

Clasificación	Consecuencia
Severa	Daños materiales y personales muy graves (muertes). Parada total de la producción.
Grave	Daños materiales muy graves. Parada parcial de la producción.
Moderada	Daños Materiales importantes. No se observa parada en la producción.
Menor	Daños Materiales menores.
Baja	Daños Materiales prácticamente inexistentes. Actividad normal.

Tabla 5.

Finalmente, una organización puede quedar afectada por cadenas de acontecimientos que se combinan e interactúan entre si dando lugar a consecuencias distintas entre sí. Un acontecimiento aislado puede tener consecuencias limitadas mientras que una secuencia de acontecimientos podría tener consecuencias mucho más graves. Un cho-

que entre dos vehículos tiene consecuencias negativas pero limitadas mientras que el descarrilamiento de un tren puede provocar la muerte de pasajeros, daños a otros trenes, a las vías, a las propiedades colindantes e incluso la interrupción de la Línea Férrea. Un solo evento inicial ha dado lugar a multitud de consecuencias negativas.

3.6.1.4 Probabilidad *(Probability)*.

La Guía 73:2009 define probabilidad como medición de la posibilidad de que algo se produzca, expresada como un número comprendido entre 0 y 1, donde o es la imposibilidad y 1 es la certeza absoluta.

Otra definición podría ser la de Collins (1979): "medida de la frecuencia y probabilidad *(likehood)* relativas de la ocurrencia de un evento cuyos valores se encuentran entre cero (imposibilidad) y uno (certeza) derivada de la distribución teórica realizada a través de la observación". Quizás el primer intento para definir los principios de la probabilidad vino a través del Libro Liber de Ludo Alea[59] *(Book on Games of chance)* en el que Cardano, su autor definió la probabilidad como el número de resultados favorables dividido entre el número total de resultados posibles, hoy en día esta definición sigue siendo utilizada. Como ejemplo de la importancia de la probabilidad mencionaremos que la fundación del Sector Asegurador se encuentra fundamentada en la probabilidad y la estadística. Las Compañía Aseguradoras pueden predecir con cierto grado de precisión la ocurrencia de un siniestro a través de la inclusión de un gran número de riesgos homogéneos dentro de un *pool*.

Es común el uso del término probabilidad para referirse a una de las dimensiones del riesgo (incertidumbre), las otras dimensiones serían el impacto (efecto) y la dirección (positivo o negativo). También es habitual que se confunda el riesgo (chance) con la probabilidad generando cierta confusión a la hora de emplear un término u otro.

Todo evento es susceptible de ocurrir en un rango entre o y 1. Un evento con probabilidad 0 es imposible que ocurra mientras que un evento con probabilidad 1 ciertamente ocurrirá. Un ejemplo muy sencillo sería tirar una moneda al aire, en principio las probabilidades de que salga cara o cruz estarían repartidas (0,5) por cada opción (contando que no es posible que la moneda caiga sobre su propio canto). En este experimento la distribución de la probabilidad actúa, ya que no importa el número de veces que se repita el experimento que la distribución de la probabilidad será la misma.

La probabilidad se encuentra ligada al riesgo como la posibilidad de ocurrencia de un evento (positivo o negativo)[60]. Para el proceso de gerencia de riesgos nos interesarán aquellos eventos que son susceptibles de ocurrir, ya que un evento que es imposible que ocurra o que es ciertamente ocurrirá no conlleva riesgo alguno.

---

59 Dr. Chao "Financial Risk Management Course. Concept and Applications" Página 16, 2009.
60 HEAD L.GEORGE "Risk Management –Why and How. An illustrative introduction to risk management for Business Executives." Página 11, Dallas 2009. Ed. International Risk Management Institute, Inc.

El proceso de gerencia de riesgos siempre tomará en consideración aquellos eventos cuya probabilidad es mayor de 1 y menor de 0. Imaginemos el proceso de gerencia de riesgos de un Hotel, en el mismo se identificaran tanto eventos cuya probabilidad de ocurrencia alta (más de 0,75) como podrían ser las caídas registradas, como los eventos cuya ocurrencia es muy improbables (menos de 0,1) pero cuya ocurrencia puede tener unas consecuencias graves para la consecución de los objetivos, como podría ser un incendio en el que se produjeran muertes. Ambos casos son susceptibles de ocurrir, pero cuanto mayor es la probabilidad menor es el riesgo ya que la organización está acostumbrada a la ocurrencia de ciertos acontecimientos y por lo tanto puede establecer las medidas de control oportunas. En el caso de un Hotel se tendrán en cuentas aquellas zonas donde se hayan producido más caídas para señalizarlas adecuadamente. Dado que el objetivo principal del proceso de gerencia de riesgos de una organización es siempre en la medida de lo posible eliminar el riesgo, y si no es posible mitigarlo se tendrá en consideración la posibilidad de utilizar una vía alternativa de paso. De esta forma que eliminaremos completamente el riesgo existente, aunque se tendrá que tomar en consideración que surgirán nuevos riesgos con la apertura de la nueva vía. Si la organización realiza correctamente el proceso de análisis de riesgos tendrá implantado dentro de su rutina habitual la identificación continua de riesgos[61] que le permitirá analizar este nuevo riesgo.

Respecto a aquellos eventos de ocurrencia improbable, se tomarán las medidas de control suficientes para que estos sigan siendo de ocurrencia improbable, siguiendo con el ejemplo de un grave incendio se tomaran en consideración medidas de control enfocadas a la prevención (*sprinklers*, sistemas de protección o contra incendios) así como a la prevención a través de la implantación de medidas de protocolo.

3.6.1.5 Frecuencia.

En la guía ISO 73:2009 el término frecuencia se define como número de sucesos (3.5.1.3) o de efectos en una unidad de tiempo definida.

No obstante, también podría definirse como “expresión que indica el número de veces[62] que tiene lugar un evento durante un periodo determinado”.

La frecuencia es un término susceptible de ser categorizado y cuantificado y se puede aplicar tanto a sucesos ocurridos en el pasado, como a sucesos que ocurrirán en el futuro y esto nos permite utilizarlo como una medida de probabilidad. Podemos clasificar los eventos de la siguiente manera:

Eventos de baja frecuencia: se trata de aquellos eventos cuya ocurrencia es posible, pero que en el pasado rara vez se han producido y cuya ocurrencia será también excepcional en el futuro. Un evento de baja frecuencia podría ser un accidente aéreo,

---

61 Ver definición Análisis del Riesgo 3.6.1.
62 RUBIN W. HARVEY “Dictionary of Insurance Terms.” Página 200, Nueva York 2013. Ed. Barrons.

los cálculos estadísticos nos permiten afirmar que el avión sigue siendo a día de hoy el medio de transporte más seguro que existe. La ocurrencia de un evento de este tipo es muy improbable en relación al número de vuelos que hay programados en todo el mundo.

Eventos de frecuencia moderada: son eventos que se han producido cada cierto tiempo en el pasado y cuya ocurrencia se espera que suceda en algún momento concreto del futuro. En el ámbito asegurador podríamos establecer un símil con los siniestros de responsabilidad civil patronal.

Eventos de alta frecuencia: finalmente este tipo de eventos son aquellos que se han producido frecuentemente en el pasado y que se espera sigan sucediendo en el futuro con la misma regularidad. Podríamos considerar eventos de alta frecuencia las reclamaciones que se producen en los establecimientos hoteleros o centros comerciales como consecuencia de los resbalones y caídas.

Uno de los objetivos de categorizar y cuantificar la frecuencia es permitir que una organización pueda tratar de forma adecuada su exposición[63] a un determinado riesgo. Cuando se realiza un análisis del riesgo[64] se toman en consideración diferentes factores siendo uno de ellos la frecuencia. A través del estudio de la frecuencia la organización obtiene una valiosa información que le permitirá comprobar si está llevando a cabo todas las medidas de control necesarias o por el contrario es necesario modificar las actuales o incluso implantar otras medidas de control alternativas.

Para poder visualizar mejor lo comentado anteriormente vamos a poner el ejemplo de una estación de esquí y en concreto una de sus pistas negras más demandadas. Imaginemos que tomando en consideración el histórico de atenciones médicas de los últimos diez años en esa pista se han realizado una media de unas 15 atenciones médicas al año, y en los últimos tres años este número ha sufrido un incremento hasta 25 las atenciones médicas anuales. Si un evento se repite habitualmente o su ocurrencia se ha visto incrementada durante los últimos años es muy posible que una organización decida establecer procedimientos de control adicionales o modificar los existentes. En este caso es posible que las caídas se hayan estado produciendo por una mala señalización de las placas de hielo, una mejor señalización de la pista, evitará que los esquiadores se precipiten a las placas de hielo reduciendo la exposición al riesgo. También se podría optar por implementar nuevas medidas. El aumento en las atenciones médicas también podría deberse a un aumento en los esquiadores que bajan esa pista, y es muy probable que muchos de ellos no tengan el nivel requerido para descender una pista de esa dificultad. Establecer un control que solamente permita el acceso a los esquiadores de cierto nivel podría ser una medida alternativa para evitar más accidentes.

---

63 Ver definición 3.6.1.2 Exposición.
64 Ver definición análisis del riesgo 3.6.1.

Si las medidas de control llevadas a cabo son las correctas el resultado será una menor frecuencia en la materialización de los eventos y por lo tanto una reducción de los mismos.

Un evento que ocurra regularmente (alta frecuencia) puede ser perfectamente tolerable para una organización debido a que su impacto sea mínimo, mientras que ciertos eventos muy improbables (baja frecuencia) pueden tener un serio impacto para la consecución de los resultados. Continuando con el Símil de la Pista de Esquí, un volumen elevado de caídas puede constituir un riesgo tolerable ya que en la mayoría de casos no requieren mayor atención que la médica. Además, la propia estación podría repercutir una pequeña prima en concepto de asistencia, evitando que ningún esquiador tenga que pagar para ser atendido, es decir podría transferir el riesgo.

Los eventos de alta frecuencia suelen estar muy bien identificados y por lo tanto establecer medidas de control adecuadas no supone un problema para la organización. Sin embargo, serán aquellos eventos de baja frecuencia, pero de impacto elevado aquellos a los que una organización tenga que prestar atención, dado que su identificación es compleja (debido a su baja frecuencia) y las consecuencias de los mismos imprevisibles.

Continuando con el ejemplo de la estación de esquí, imaginemos que se produce la muerte de un esquiador. Evidentemente este evento es extraordinario (baja frecuencia) pero las consecuencias del mismo son extraordinarias. A la posible compensación económica habría que añadir riesgos adicionales como el reputacional que agravaría el impacto de este evento, cuya gravedad puede incluso afectar a la consecución de los objetivos de la organización. Es muy importante que se identifiquen todos los riesgos aun cuando estos no se hayan materializado ya que permitirán tomar las medidas de control adecuadas que impidan que se pueda materializar este evento.

3.6.1.6. Vulnerabilidad.

La Guia ISO 73:2009 define vulnerabilidad como propiedades intrínsecas de que algo se produzca como resultado una sensibilidad a una fuente de riesgo (3.5.1.2) que puede conducir a un suceso con una consecuencia. (3.6.1.3).

La vulnerabilidad se puede considerar también como una característica[65] que afecta a una organización y que la hace ser susceptible de sufrir un impacto como consecuencia de un evento.

La vulnerabilidad está directamente relacionada con la probabilidad *(likelihood)* y también con el impacto. Cuanto mayor sea la vulnerabilidad de una organización mayor será el impacto que sufra en caso de que un evento se materialice, de ahí la importancia de analizar correctamente la vulnerabilidad.

---

65 CLUB DE LA SECURITÉ DE L, INFORMATION FRANCAIS (CLUSIF) “Risk Management Concept and Methods.” Página 10, Paris 2008.Ed. CLUSIF.

El análisis de la vulnerabilidad comienza con la identificación de los riesgos a los que se expone una organización. Dado que no todos los riesgos son iguales, deberemos prestar especial atención a la naturaleza de los mismos.

Cuando se materializa un evento el impacto sufrido puede ser de carácter material, financiero, medioambiental, personal, o político. Cabe incluso la posibilidad de que un evento provoque daños de diversa naturaleza. Así por ejemplo un siniestro grave ocurrido en una central nuclear generará un impacto de naturaleza material, financiera, medioambiental y personal.

Una vez se ha cumplido con la primera fase relativa a la identificación del riesgo se deberán tomar en consideración aquellos factores, procesos o condiciones que determinen cual será el alcance de la vulnerabilidad en caso de que se produzca un evento. Dada la amplia variedad que puede haber podemos proceder a su clasificación en dimensiones para una mayor comodidad.

Para poder ver de forma práctica esta clasificación, vamos a tomar en consideración el ejemplo de una organización multinacional con actividad y activos en Latinoamérica podríamos poner como ejemplo la siguiente clasificación:

Dimensión Física: calidad en los materiales de construcción, estándares de construcción seguidos, medidas de protección contra incendios, protocolos de seguridad, etc.

Dimensión Geográfica: inestabilidad Política, conflictos armados, corrupción.

Dimensión Financiera: estado financiero de la organización, transferencia adecuada de riesgos, implantación de planes de continuidad.

Dimensión Medioambiental: Calidad del aire y suelo, legislación local en materia medioambiental.

Las dimensiones anteriormente mencionadas permiten clasificar las condiciones, procesos y factores que determinarán el alcance del impacto y por tanto la vulnerabilidad de la organización frente a un posible evento.

Imaginemos que esta misma organización tiene activos en un país con actividad sísmica y sufre un riesgo catastrófico de magnitud baja (terremoto) en una de sus instalaciones. La utilización de materiales de materiales de construcción inadecuados, o el no seguimiento de los estándares más avanzados en materia de construcción pueden provocar que este evento que en condiciones normales causaría una pérdida parcial termine causando una pérdida total o casi total. La imposibilidad de que la organización continúe con su actividad debido a esta pérdida total no solo provoca un daño económico considerable, sino también un daño social o incluso medioambiental.

Si por el contrario se hubieran utilizado materiales de construcción adecuados, o si se hubieran seguido los estándares más avanzados en materia sísmica posiblemente

el impacto del terremoto hubiera sido menor y por lo tanto las pérdidas sufridas al permitir que la organización continuara con su actividad, aunque fuera de forma parcial.

No solo es importante analizar los factores y condiciones que determinan la vulnerabilidad sino también evaluar el grado de la misma. Para poder evaluar el grado de vulnerabilidad al que nos exponemos se deberá analizar el potencial impacto de un evento y para ello, lo mejor es recurrir a su cuantificación siempre y cuando sea posible. La cuantificación del impacto nos permite conocer mejor la gama de posibles daños y pérdidas derivados de un evento y todo ello dentro de un horizonte de tiempo estimado.

Una vez identificados los factores y condiciones que determinan la vulnerabilidad la organización deben comprobar si efectivamente está aplicando una política de riesgos adecuada o por el contrario debe introducir cambios en la misma. Siguiendo el anterior ejemplo (Multinacional implantada en Latinoamérica) se deberían plantear las siguientes preguntas:

- Disponemos de planes de contingencia adecuados.
- Qué capacidad de adaptación, agilidad y adaptabilidad (resiliencia) tiene la organización.
- Puedo afrontar financieramente un evento catastrófico, o debo transferir el riesgo.

Todas estas preguntas tienen como objetivo analizar y cuantificar un riesgo para poder después visualizarlo. El método más habitual es a través de una escala.

3.6.1.7 Matriz de Riesgo.

La Guía ISO 73:2009 define matriz de riesgo como "herramienta que permite clasificar y visualizar los riesgos (1.1), mediante la definición de categorías de consecuencias (3.6.1.1) y probabilidad (3.6.1.4).

Podríamos definir Matriz de Riesgo como método[66] que permite evaluar y clasificar un riesgo de forma gráfica a través de la combinación de distintos componentes de un riesgo tales como la consecuencia y la probabilidad. Esta información permite a la organización tomar decisiones con el objetivo de que estas puedan evitar ciertas combinaciones y se reduzca la exposición.

La matriz de riesgo es ante todo una herramienta de control y gestión. Las organizaciones la utilizan para identificar dentro de las actividades más importantes que

---

66 DUMBRAVA VASILE "Using Probability-Impact Matrix in Analysis and Risk Assesment projects" Página 91, Rumania 2013.Ed. Journal of Knowledge Management, Economics and Information Technology.

desarrollan el tipo y el nivel de riesgo inherentes a estas, tomando también en consideración los factores de riesgo. Los riesgos a los que se enfrenta una organización pueden estar afectados por factores de riesgo que pueden ser de distinta índole tales como operacionales, estratégicos, etc. Estos factores pueden alterar el nivel de riesgo y por tanto la consecución de sus objetivos. Ejemplos de factores externos podrían ser los tipos de cambio, cambios en la legislación mientras que factores internos pueden obedecer a cambios de estructura.

Como se ha mencionado la matriz permite visualizar los riesgos, y esto se realiza a través de su graficación en un plano cartesiano. En el eje x se incluye la probabilidad de ocurrencia mientras que en el eje y se identifica el impacto, se determina el riesgo mediante la valoración de escalas. La matriz se puede evaluar de forma cuantitativa y de forma cualitativa. La valorización en términos cuantitativos o cualitativos dependerá de la disponibilidad de información, los medios y el tiempo disponible. La valorización cualitativa es más sencilla que la cuantitativa, pero esta última aporta una mejor información si el uso de datos ha sido el adecuado. Cabe mencionar que es posible incluir dentro de una misma matriz la valorización cualitativa y cuantitativa y esto nos permitirá evaluar la ocurrencia del evento con una mayor precisión.

Dependiendo del nivel de información que obtengamos de la organización respecto a su perfil de riesgos, utilizaremos una matriz con menor o mayor escala. Así para un mínimo nivel de categorización se puede utilizar una Matriz 3x3 mientras que si pretendemos analizar un riesgo particular utilizaremos una matriz 5x5. La matriz 3x3 como hemos mencionado categoriza los riesgos de manera sencilla (bajo/medio/alta) y la matriz con escala 5x5 posee una escala mucho más precisa (muy bajo/bajo/medio/alto/muy alto). Como ejemplo podríamos incluir el siguiente:

Gráfico 19.

Rango del perfil de riesgos: (1, insignificante) (2, Bajo) - Apetito al riesgo (3, medio), (4, moderado) - Tolerancia al riesgo (6, alto) (9, catastrófico) - Capacidad al riesgo.

Como se puede apreciar en la matriz, se incluyen calificaciones dentro de cada cuadrante combinando la probabilidad y el impacto.

Estas calificaciones se encuentran dentro de un rango y dependen la combinación entre el impacto y la probabilidad. Se pueden añadir colores a los cuadrantes, permitiendo una mejor visualización de la matriz.

A modo de conclusión podemos asignar a la matriz de riesgo las siguientes utilidades.

1) Representa de forma gráfica la probabilidad y el impacto de un riesgo.

2) Evalúa de forma independiente un riesgo tomando en consideración su probabilidad de ocurrencia y su impacto.

3) Permite elegir los riesgos que tienen que ser tratados a fin de establecer prioridades para su tratamiento y control.

4) Finalmente es una herramienta cuya utilidad es facilitar la toma de decisiones en aquellos riesgos que se han analizado.

3.6.1.8 Nivel de Riesgo.

La Guía ISO 73:2009 define el nivel de riesgo como la Magnitud de un riesgo (1.1) o combinación de riesgos, expresados en términos de la combinación de las consecuencias (3.6.1.3) y de su probabilidad.

También podemos definirlo como exposición a la que se somete una organización tomando en consideración la probabilidad de que se produzca un suceso y el impacto que pudiera generar el mismo para la consecución de sus objetivos.

Todas las organizaciones están expuestas a un determinado nivel de riesgo, no obstante, es cada organización quién de forma individual debe determinar cuál es el nivel de riesgo que está dispuesta a tolerar y que le permita seguir creando valor. La tolerancia al riesgo es el nivel de incertidumbre que una organización está dispuesta a aceptar como organización en su totalidad, aunque nada impide que esa tolerancia se aplique por ejemplo a una unidad de negocio.

El nivel de riesgo está directamente relacionado con la estrategia trazada donde el rendimiento deseado de una estrategia debe estar alineado con el nivel de riesgo que la organización esté dispuesta a asumir. El nivel de riesgo al que se somete una organización puede venir determinado por criterios puramente subjetivos o bien puede venir determinado por una autoridad. Como ejemplo podríamos poner a las Aseguradoras y el nivel de riesgo Financiero que están dispuestas a asumir para poder cumplir con los Criterios de Solvencia II. Las Aseguradoras tendrán que diseñar una estrategia o plan de negocio muy estricto que les permita crear valor para sus accionistas y a su vez les permita cumplir con la Autoridad Europea. Desde un punto de vista subjetivo, aunque los objetivos y la estrategia puedan determinar un nivel de riesgo, este tendrá que ser acorde con los procesos y la estructura de la organización ya que su análisis requiere dotar de infraestructura a la organización.

Como veremos a continuación una incorrecta estrategia a la hora de determinar el nivel de riesgo puede tener consecuencias muy graves. Pensemos en la crisis financiera de septiembre de 2008. La crisis de las hipotecas subprime provocó el cierre de Lehman Brothers uno de los Bancos de inversión más relevantes y longevos de los Estados Unidos. Fundado en 1850, su quiebra ha sido considerada la mayor de la historia de Estados Unidos, así como la mayor quiebra de un banco de inversión desde la caída del banco de inversión Drexel Burnham Lambert dieciocho años antes. Entre los muchos factores que provocaron la caída de este gigante de la banca de inversión uno de ellos fue el excesivo apalancamiento en las inversiones del banco. La superación del nivel de riesgo objetivo, así como una estrategia insostenible en el medio plazo y la no aplicación de un proceso de gerencia de riesgos adecuada no solo no le permitieron cumplir con los objetivos del banco, sino que provocaron su quiebra.

El nivel de riesgo se puede medir tanto de forma cualitativa, a través de la categorización (Muy alto, alto, medio, bajo) o bien pueden tomar en consideración criterios cuantitativos para intentar equilibrar la balanza entre el riesgo asumible y los objetivos pretendidos.

La mejor manera de visualizar el nivel de riesgo es a través de una matriz. En la siguiente matriz de riesgo se toma en consideración distintos condicionantes como la probabilidad y la consecuencia permitiendo visualizar el riesgo asociado a cada una de las combinaciones entre consecuencia y probabilidad.

Aunque se pueden hacer tantas clasificaciones de la probabilidad como se quiera un ejemplo sería el siguiente: muy alta, alta, moderada y baja.

Tabla para la determinación del Nivel de Riesgo

Probabilidad	Consecuencia				
	Baja	Menor	Moderada	mayor	severa
Muy probable	bajo	medio	alto	muy Alto	muy alto
Probable	bajo	medio	alto	alto	muy alto
Posible	bajo	medio	medio	alto	alto
Improbable	bajo	bajo	medio	medio	alto
Raro	bajo	bajo	bajo	medio	medio

Tabla 6.

Para poder interpretar la matriz de riesgo hay que atender a la descripción de cada nivel de riesgo que marcará las pautas de actuación dentro de la organización. Imaginemos una planta nuclear:

Nivel de riesgo muy Alto: nivel alto de riesgo que resulta intolerable y que requiere ser controlado de forma inmediata. El acceso y exposición al riesgo debe restringirse hasta que el nivel de riesgo disminuya hasta un nivel de riesgo aceptable.

Nivel de riesgo alto: nivel de riesgo inaceptable que deberá ser controlado inmediatamente. Las medidas de control incluirán la sustitución y aislamiento del riesgo. Estos controles para reducir el riesgo, deberán ser realizados durante las primeras veinticuatro horas desde que se considere el nivel de riesgo alto.

Nivel de riesgo medio: nivel de riesgo inaceptable. Se tomarán medidas para controlar el riesgo hasta un nivel bajo o inexistente durante los siguientes 14 días.

Nivel de riesgo bajo: nivel de riesgo aceptable. No se requieren llevar a cabo medidas de control específicas. No obstante, se podrán llevar a cabo medidas que sean sencillas y poco costosas para mantener este nivel de riesgo o reducirlo a inexistente.

Atendiendo a la clasificación que acabamos de leer podemos afirmar que el nivel de riesgo determina la asignación de recursos dentro de la organización. Evidentemente un nivel de riesgo muy alto, o alto requieren asignar una gran cantidad de recursos para en primer lugar estabilizar y controlar el nivel de riesgo. El objetivo principal de controlar el riesgo es eliminarlo lo antes posible. Cuando no es posible el riesgo debe ser minimizado lo máximo posible utilizando aquellas medidas de control que resulten lo más prácticas posibles para minimizar el riesgo.

Incluso aun cuando el nivel de riesgo sea bajo la organización llevará a cabo medidas de prevención que permitan seguir manteniendo el nivel de riesgo bajo.

La gerencia de una organización se encargará de establecer una estrategia que sea compatible con el nivel de riesgo aceptado y determinará las tareas que sus unidades de negocio tendrán que llevar a cabo para poder monitorear los Riesgos de una forma eficaz.

3.7. Términos relativos a la evaluación del riesgo.[67]

3.7.1. Evaluación del riesgo.

3.7.1.1. Actitud ante el riesgo.

3.7.1.2. Apetito por el riesgo.

3.7.1.3. Tolerancia al riesgo.

3.7.1.4. Aversión al riesgo.

3.7.1.5. Agregación de riesgos.

3.7.1.6. Aceptación del riesgo.

3.7.1. Evaluación del riesgo.

La Guía 73:2009 define evaluación del riesgo como "**el proceso de comparación de los resultados del análisis del riesgo (3.6.1) con los criterios de riesgo (3.3.1.3) para determinar si el riesgo (1.1) y/o su magnitud son aceptables o tolerables**".[68]

La evaluación del riesgo constituye la fase previa inherente a cualquier proceso de decisión. Implica conocer el nivel de riesgo y mediante su comparación con el criterio de riesgo, que está basado en la significatividad de éste para la organización, llegar a establecer una conclusión sólida y fundamentada sobre la aceptabilidad o no del citado riesgo.

Conviene hacer hincapié en este último aspecto, pues efectivamente no existen criterios de aceptabilidad absolutos; de la misma manera que no existe posibilidad de evitar totalmente el riesgo y, por tanto, puede ocurrir, y de hecho ocurre, que lo inaceptable para una organización no lo sea para otra y viceversa. En base a esta comparación, se puede considerar la necesidad de tratamiento.

La evaluación del riesgo sienta las bases para el tratamiento del riesgo siendo su objetivo definir prioridades que dependen de factores como la tolerancia al riesgo, la actitud frente al riesgo, las percepciones de los individuos, los requisitos legales, reglamentarios y de otros tipos, de los recursos disponibles, de la supresión, modificación o permanencia de los controles existentes, de la actividad, del contexto interno

---

67 Los comentarios a los siguientes términos han sido desarrollados por: **D. Ángel Escorial** 3.7.1. Evaluación del riesgo y siguientes relativos a la evaluación del riesgo: 3.7.1.1. Actitud ante el riesgo; 3.7.1.2. Apetito por el riesgo; 3.7.1.3. Tolerancia al riesgo; 3.7.1.4 Aversión al riesgo; 3.7.1.5 Agregación de riesgos y 3.7.1.6. Aceptación del riesgo.

68 A propósito del término evaluación del riesgo, la UNE-ISO Guía 73:2009 contiene la siguiente "NOTA: La evaluación del riesgo ayuda a la toma de decisiones sobre el tratamiento del riesgo (3.8.1).

y externo del riesgo, de consideraciones éticas, financieras y otras y de la necesidad o no de llevar a cabo un análisis de riesgos más detallado.

Existen numerosas metodologías para desarrollar la evaluación del riesgo tanto entre las consideradas en la UNE-ISO 31010:2009 como otras y la organización puede optar por una de ellas, aplicar una combinación de varias o crear la suya propia.

Así, todo proceso de evaluación del riesgo comporta, al menos, el desarrollo de las siguientes tareas:

- Consideración del nivel de riesgo.
- Consideración del criterio de aceptabilidad.
- Comparación del nivel con el criterio.
- Establecimiento de conclusiones de aceptabilidad.
- Recomendaciones de mejora.
- Priorización de opciones de tratamiento.
- Necesidad o no de análisis posteriores.

La no aceptación de riesgos con consecuencias negativas se produce cuando el nivel del riesgo de la amenaza es superior al criterio de ese riesgo mientras que en el caso de los riesgos con consecuencias positivas es lo contrario al resultar inferior a las expectativas del criterio de aceptabilidad.

Podemos manejar como ejemplo de evaluación del riesgo el control de la velocidad de la conducción en autopista. El nivel del riesgo sería la velocidad elegida por el conductor que se contrastaría con el criterio de riesgo dimanante de los límites de velocidad establecidos legalmente en España entre 60 y 120km/h para este tipo de vía. De la comparación de la velocidad real (nivel de riesgo) con los criterios legales surgiría la aceptación de la velocidad si estuviese en el rango legal o el tratamiento para aumentarla o reducirla en caso de estar fuera de este rango.

3.7.1.1. Actitud ante el riesgo.

La Guía 73:2009 define actitud frente al riesgo como el "**enfoque de la organización para apreciar un riesgo (1.1) y eventualmente buscarlo, retenerlo, tomarlo o rechazarlo**".

De la combinación de las definiciones actitud y riesgo se puede considerar la 'actitud ante el riesgo' como el estado de ánimo elegido en cuanto a las incertidumbres que pudieran tener un efecto positivo o negativo en los objetivos o, dicho de otra manera, es la respuesta elegida a la percepción de incertidumbre significativa.

Se suelen distinguir dos actitudes frente al riesgo:

- aversión hacia el riesgo (incómodo con el riesgo y lo rechaza)
- tolerancia al riesgo (busca retener y tomar riesgo para conseguir los objetivos)

La organización o el individuo no pueden concebir una estrategia de operaciones razonablemente sensata sin pensar cuidadosamente sobre su enfoque del riesgo.

Asimismo, la asimilación de la actitud que se asumirá frente al riesgo ante las actuaciones que se realicen, es determinante para efectuar el análisis del mismo, debido a que permite manejar un parámetro con el cual se confrontaran los resultados obtenidos, determinando de esta forma la viabilidad del proyecto para la organización.

En el caso del ejemplo de la velocidad en las autopistas españolas la actitud ante este riesgo vendrá definida por el estado de ánimo del conductor para conducir buscando, reteniendo, tomando o rechazando el riesgo en función de los límites de velocidad, la experiencia, confianza y habilidad del conductor, condiciones de la vía, climatología, etc.

3.7.1.2. Apetito por el riesgo.

La Guía 73:2009 define apetito por el riesgo como "**cantidad y tipo de riesgo (1.1) que una organización está preparada para buscar o retener**".

Se trata de uno de los 53 términos definidos en la Guía 73:2009 pero que no se utiliza en la norma ISO 31000:2009.

"Cantidad y tipo de riesgo" se refieren a establecer una cantidad determinada como umbral y proceder a la calificación y cuantificación de esta cantidad. Los componentes usuales del riesgo son la probabilidad y la consecuencia de un suceso, que se combinan para producir una medida del riesgo que es el nivel del riesgo. El tipo de riesgo es importante por dos razones, primero porque define unidades de medida para la agregación y en segundo lugar para permitir la desagregación en grupos homogéneos para el tratamiento.

"Que una organización esté preparada" se refiere a la libertad de elección, reflejada en la capacidad de la organización para mantener el riesgo con consecuencias negativas sin colapsar. La limitación a un nivel de confort frente al riesgo se logra indirectamente en la Guía 73:2009 con el concepto de tolerancia al riesgo. Aunque no se pone un límite en el apetito de riesgo, se coloca en la organización para permitir la flexibilidad y el tratamiento a través de diferentes tipos de riesgo: "disposición a soportar riesgo" implica resistencia para sostener sus consecuencias negativas.

"Buscar o retener" define dos actitudes distintas. Buscar el riesgo hace referencia a algo que no tenemos y retener el riesgo se refiere a mantener algo que tenemos. La intención real es determinada por la actitud ante el riesgo; un término que se define en ISO 31000 y se usa en la definición de aversión al riesgo. Esta norma ISO 31000, en cambio, no maneja explícitamente el apetito del riesgo, sino que lo trata indirectamente en relación con los conceptos de "creación de valor" y "actitud ante el riesgo".

También usa el concepto "criterio de riesgo" como el término de referencia frente al cual se evalúa la importancia de un riesgo.

De acuerdo con el modelo para la práctica de control interno de COSO, actualizado en mayo de 2013, se define el concepto de apetito de riesgo como el riesgo que se está dispuesto a aceptar en la búsqueda de la misión/visión de la entidad o individuo. Es así, un hito más en la fijación de la estrategia y los objetivos.

El "Marco Integrado de Gestión de Riesgos" de COSO define el apetito de riesgo como la cantidad de riesgo, desde un punto de vista amplio, que una organización está dispuesta o desea aceptar en la persecución de valor.

La norma British Standard 31100 sobre "Gestión de Riesgo" se refiere al apetito como la cantidad y tipo de riesgo que una organización está preparada para afrontar, aceptar o tolerar.

En definitiva, el concepto de apetito de riesgo hace referencia a perseguir el riesgo, o dicho de otro modo, a la cantidad agregada de riesgo que la organización activamente quiere o está dispuesta a asumir para crear valor y mantenerlo (primer principio de la gestión del riesgo en la norma ISO 31000). Dada su relevancia y las implicaciones a nivel estratégico que conlleva, debe ser un concepto establecido por el máximo órgano responsable de la organización. Cada organización persigue varios objetivos al mismo tiempo para agregar valor a sus grupos de interés y debería entender el apetito de riesgo como el riesgo que desea buscar o retener, siempre que esté bajo control, para lograr sus objetivos.

Continuando con el ejemplo de la velocidad en las autopistas españolas el apetito de riesgo vendrá definido por la velocidad que el conductor está preparado para buscar y retener mediante el sistema de control automático de la velocidad del que hoy en día muchos coches disponen. Señalemos que el criterio de riesgo sería distinto en función del país donde se conduzca estando por ejemplo la velocidad ilimitada en las autopistas de Alemania (salvo donde se limite de forma expresa) tal y como estuvo en España hasta 1974. En el caso de la conducción en gran parte de los trazados de las autopistas alemanas, el apetito de riesgo vendrá condicionado por las condiciones de la vía, el tráfico, la climatología y las condiciones del conductor y no por un límite máximo legal. Sin embargo, en las autopistas españolas, como en el de la mayoría de las naciones, el apetito por el riesgo del conductor está claramente influido por el requisito legal que limita la velocidad con imposición de sanciones administrativas e incluso penales en caso de incumplimiento.

3.7.1.3. Tolerancia al riesgo.

La Guía 73:2009 define la tolerancia al riesgo como la "**disponibilidad de una organización o de las partes interesadas (3.2.1.1) para soportar el riesgo (1.1) después del tratamiento del riesgo (apartado 3.8.1) con objeto de conseguir sus objetivos**".[69]

---

69 A propósito del término tolerancia al riesgo, la UNE-ISO Guía 73:2009 contiene la siguiente "NOTA: La tolerancia al riesgo puede estar influenciada por requisitos legales o reglamentarios".

El concepto de tolerancia al riesgo implica un nivel aceptable de variación en los resultados o actuaciones de la organización relativas a la consecución o logro de sus objetivos. Dicho de otro modo, la tolerancia es la cantidad máxima de riesgo que una organización o individuo están dispuestos a aceptar para lograr sus objetivos. Se refiere a lo que una organización se puede permitir gestionar. Riesgos que, en caso de aparecer, la compañía tiene que ser capaz de soportar.

También se puede definir como la desviación respecto al nivel de riesgo en el que la organización se siente cómoda. Sirve de alerta para evitar llegar al nivel que establece su capacidad.

La tolerancia debe servir como indicador que informe a la organización si puntualmente está asumiendo un nivel de riesgo por encima del deseado pudiendo así reconducir la situación. Además, debe servir como alerta para evitar llegar a niveles que superen la capacidad de la organización, exponiéndola a riesgos que no podría soportar en caso de materializarse.

En sentido financiero la tolerancia al riesgo puede definirse como el grado de variabilidad en el retorno de la inversión que una entidad o un individuo está dispuesto a soportar. La tolerancia al riesgo es una componente importante en la inversión, ya que se debe tener una comprensión realista de su capacidad y de las posibles oscilaciones en el valor de la inversión.

En el ejemplo de las víctimas de tráfico, los 'air-bag' que se accionan automáticamente tras colisión para proteger a los ocupantes del vehículo se desarrollaron en 1974. Se probó que este tratamiento reducía el riesgo de lesiones en los ocupantes de los vehículos por lo que se incrementaron estas medidas efectivas e incluso fueron requeridas por la ley debido a la disminución de la tolerancia de la opinión social a los daños derivados del resultado de una colisión. En 1991, los 'air-bag' se hicieron obligatorios en España. El tratamiento del riesgo de víctimas de tráfico mediante 'air-bag' redujo la probabilidad de sufrir un daño grave en personas en una colisión, pero no redujo sin embargo la probabilidad de ocurrencia de la colisión que ha precisado de otros tratamientos como los controles de proximidad o de mantenimiento de carril.

La tolerancia al riesgo está vinculada con las capacidades, percepciones e intenciones de personas que pueden influenciar la consecución de los objetivos de la organización y con los factores humanos y culturales de la organización que influencian cómo se perciben los riesgos y cómo se implementarán los tratamientos del riesgo. Una cultura de la organización se ve a menudo influenciada por "un fuerte compromiso de la Dirección", cómo enfocan y resuelven problemas los líderes de la organización, deciden sobre qué riesgos perseguir o evitar y establecen la actitud de la organización ante el riesgo. Un ejemplo es una organización que lleva un nuevo negocio agresivo que opera con alto nivel de incertidumbre. Para tener éxito, tales organizaciones necesitan ser muy explícitas acerca de su apetito y tolerancia al riesgo para comunicar estos aspectos a los tomadores de decisiones. En este contexto, el apetito de riesgo se sitúa a nivel estratégico (cuánto riesgo quiere o desea la organización) mientras que la tolerancia se articula en las decisiones tácticas (cuánto riesgo soporta la organización tras el tratamiento de tal forma que pueda alcanzar sus objetivos).

En el caso del ejemplo de la velocidad en las autopistas españolas la tolerancia al riesgo sería la velocidad máxima que el conductor está dispuesto a aceptar para lograr su objetivo de viaje y en el que establecería el límite automático de control de velocidad.

3.7.1.4. Aversión al riesgo.

La Guía 73:2009 define la aversión al riesgo como "**actitud de rechazar el riesgo (1.1)**".

Se trata de otro de los 53 términos definidos en la Guía 73:2009 que no se utiliza en la norma ISO 31000:2009.

La "aversión al riesgo" es un término que se conceptualiza como "la actitud hacia el riesgo en la que se exige un rendimiento más alto por aceptar un riesgo mayor" lo que nos permite entender que, al aceptar inversiones más peligrosas para nuestros intereses, se espera un rendimiento que justifique el riesgo adicional que lleva implícito.

Existen distintos grados de aversión que establecen el perfil respecto del riesgo de la organización (conservador, estándar o arriesgado). En general, una persona con una alta aversión al riesgo (correspondiente a un perfil conservador), suele escoger opciones con menores beneficios esperados, pero con más estabilidad. Por otro lado, un individuo con baja aversión al riesgo (perfil arriesgado), suele elegir oportunidades que le puedan dar mayores beneficios a cambio de poder sufrir pérdidas eventuales.

Por último, en el caso del ejemplo de la velocidad en las autopistas españolas la aversión al riesgo vendrá definida por el perfil respecto del riesgo de velocidad del conductor.

3.7.1.5. Agregación de riesgos.

La Guía 73:2009 define la agregación de riesgos como la "**combinación de un número de riesgos en un solo riesgo (1.1) para desarrollar una comprensión más completa del riesgo general**".

Se trata de uno de los 53 términos definidos en la Guía 73:2009 pero que no se utiliza en la norma ISO 31000:2009.

Una agregación de riesgos apropiada es fundamental para la adecuada gestión de los riesgos en toda la organización. Su objetivo principal es proporcionar una buena información del riesgo cara a la gestión correspondiente para una toma de decisiones informada.

La agregación de riesgos se puede hacer mediante diferentes métodos y cada uno tener un propósito distinto para el individuo o dentro de la organización.

La agregación de riesgos se puede realizar a diferentes niveles agregación de riesgos de un departamento, de una actividad, de una organización entera, etc. Un ejemplo

habitual de agregación de riesgos es el mapa de riesgos de FERMA (ver 3.3.1. establecimiento del contexto) que agrega los riesgos en cuatro grandes grupos: estratégicos, financieros, operacionales y del azar.

Desde el punto de vista cuantitativo, se pueden agregar riesgos y considerar un promedio o bien asignar pesos en función de criterios propios de la organización o del mercado.

3.7.1.6. Aceptación del riesgo.

La Guía 73:2009 define aceptación del riesgo como "**decisión informada a favor de tomar un riesgo (1.1) particular**".[70]

Se trata de uno de los 53 términos definidos en la Guía 73:2009 pero que no se utiliza en la norma ISO 31000:2009.

La aceptación del riesgo es una opción de tratamiento utilizado fundamentalmente en el campo de los negocios o de la inversión. Se produce cuando se acepta el coste de administrar un determinado tipo de riesgo, porque el riesgo no es suficiente para justificar el coste adicional que se necesita para evitar ese riesgo.

El riesgo nunca es totalmente eliminable, por lo que es necesario definir una estrategia de aceptación del riesgo estableciendo criterios de aceptación y especificar niveles de riesgo aceptable.

Una vez aceptados los riesgos residuales se consideran como riesgos conocidos por la gestión de la organización. El nivel y magnitud de los riesgos aceptados constituyen uno de los parámetros principales del proceso de gestión de riesgos.

Un ejemplo de aceptación de un riesgo cotidiano con consecuencias negativas es la conducción de un automóvil que incluye la aceptación del riesgo de tener o causar lesiones, incluso la muerte en caso de colisión o atropello.

Para riesgos con consecuencias positivas, la aceptación se enfoca como la búsqueda de una oportunidad que tendría un efecto positivo en el logro de los objetivos. Una decisión es aceptada cuando la magnitud del potencial impacto positivo sobre los objetivos es suficiente para motivar la búsqueda del riesgo.

Un ejemplo de este enfoque positivo es el caso del negocio de una tienda de venta al por menor rentable. Se abriría una tienda dónde la información sugiere que haya suficiente información positiva de existencia de mercado de venta al por menor que optimice este riesgo y minimice la incertidumbre. El empresario abriría una tienda para buscar el riesgo relacionado con el mercado y la demanda de sus productos.

---

70 A propósito del término Aceptación del riesgo, la UNE-ISO Guía 73:2009 contiene las siguientes notas: "NOTA 1: La aceptación del riesgo puede tener lugar sin que exista tratamiento del riesgo (3.8.1) o durante el proceso de tratamiento del riesgo. NOTA 2: Los riesgos aceptados son objeto de seguimiento (3.8.2.1) y de revisión (3.8.2.2)."

3.8. Términos relativos al tratamiento del riesgo.

3.8.1 Tratamiento del riesgo. [71]

3.8.1.1 Control.

3.8.1.2 Evitación del riesgo.

3.8.1.3 Reparto del riesgo.

3.8.1.4 Financiación del riesgo.

3.8.1.5 Retención del riesgo.

3.8.1.6 Riesgo residual.

3.8.1.7 Resiliencia.

3.8.1. Tratamiento del riesgo.

La Guía 73:2009 define el tratamiento del riesgo como el proceso destinado a modificar el riesgo.

La gerencia de riesgos en un entorno global se está perfilando como una estrategia financiera y empresarial que proporciona una importante ventaja competitiva a las empresas que disponen de ella.

El diseño de un proceso de implementación de la gestión de los riesgos en las empresas, no pretende establecer procedimientos de aplicación mecánica para su desarrollo, sino servir como guía o marco general para el desarrollo de un diseño propio de implementación de la gestión de los riesgos. Cada proceso deberá ser objeto de estudio particular analizándose en cada caso la necesidad de adaptación de los cuestionarios, documentos, listados, análisis …

Una vez que hemos identificado los riesgos de la empresa, tanto internos como externos, se debe proceder a desarrollar programas, planes y procedimientos que ayuden a dar información, comunicación, prevención y tratamiento de los riesgos, contando con:

- Administración de contratistas y proveedores.

- Comunicación a los visitantes, a la comunidad y a las autoridades.

---

71 Los comentarios sobre términos siguientes han sido desarrollados por **Dña. Isabel Casares San José-Martí:** 3.8.1Tratamiento del riesgo; 3.8.1.1Control; 3.8.1.2 Evitación del riesgo; 3.8.1.3 Reparto del riesgo; 3.8.1.4 Financiación del riesgo; 3.8.1.5; Retención del riesgo 3.8.1.6; Riesgo residual y 3.8.1.7 Resiliencia.

- Programas de gestión de riesgos.

- Subprograma de medicina preventiva y del trabajo.

- Subprograma de higiene industrial.

- Subprograma de seguridad industrial.

- Planes de emergencia, crisis y continuidad del negocio.

- Subprograma de gestión ambiental.

Todos los procedimientos de la empresa deben estar justificados mediante la determinación de indicadores (cobertura y eficacia), resultados de los indicadores, análisis de tendencias, replanteamiento de las actividades del programa e implementación de los mismos.

Una vez analizados y cuantificados los riesgos, así como el impacto que tienen en su plan de negocio, se debe analizar cuál es el nivel de oportunidad en caso de asumir el riesgo, en función del nivel de riesgo y oportunidad y, en caso, de que se decida asumir el riesgo, se deberá emprender un proceso de tratamiento de riesgos consistente en seleccionar y aplicar las medidas más adecuadas, con el fin de poder modificar el riesgo, para evitar de este modo los daños intrínsecos al factor de riesgo, o bien aprovechar las ventajas que pueda reportarnos.

Cualquier sistema de tratamiento de riesgos debe garantizar como mínimo:

- Un funcionamiento efectivo y eficiente de la organización.
- Controles internos y externos efectivos.
- Conformidad con las leyes y reglamentos vigentes.

El Control Interno es un proceso llevado a cabo por el Consejo de Administración, el Comité de Administración de Riesgos, la Unidad de Riesgos y el resto del personal de la organización, diseñado para proporcionar una garantía razonable sobre el logro de objetivos relacionados con operaciones, reporte y cumplimiento.

Dentro del proceso de la implementación de la gestión de riesgos en las empresas, es fundamental establecer un manual de administración de riesgos que recoja exactamente los requerimientos concretos exigidos (informes, listados, normas, procesos, …), lo que exigiría a la Entidad un esfuerzo en la implementación y un coste continuado en el mantenimiento, así como el establecimiento de una norma abierta que contuviese principios generales sobre lo que es el control interno y la medición de los riesgos, dejando a la propia entidad la capacidad de desarrollo interno según sus propias estrategias, con la ventaja de poder utilizar parte de la estructura actual, pero con la desventaja de no tener medidos de manera clara e inequívoca los requerimientos mínimos de control exigidos.

- La unidad de riesgos debería estar formada por una o más personas no implicadas en las funciones operativas y comerciales de la entidad.

- La unidad de riesgos se responsabilizará de supervisar el cumplimiento de las normas y revisará permanente los procedimientos y sistemas relativos al control interno de la empresa y al seguimiento y gestión de riesgos, con el fin de evaluar el cumplimiento de todas las medidas y límites establecidos y verificar su validez, proponiendo las modificaciones que considere necesarias, denunciando las ineficiencias observadas e informando puntualmente al Consejo de Administración o Directorio de la Entidad.

Uno de los resultados obligatorios de la implementación de sistemas de evaluación y gestión de riesgos es la determinación de políticas de asunción de riesgos, las cuales deben contemplar límites a la exposición de los riesgos, que deben ir asociados con la definición constante en su estrategia, para cada área de la entidad. Estas políticas deben ser adoptadas por el Consejo de Administración o Directorio de la entidad y la gerencia, y constar por escrito y ser incorporadas en los manuales de administración de riesgos.

Los límites operativos que establecerán las entidades consistirán en autorizaciones previas al proceso para la asunción de todos los riesgos de la entidad, así como:

- Procedimientos a seguir en caso de superación o incumplimiento de los límites establecidos.

- Cuando se haya previsto realizar operaciones que excedan los límites establecidos, dichas operaciones deberán estar documentadas y contar con la autorización previa del Consejo de Administración o del gerente de riesgos, a quien se le ha delegado dicha competencia.

- Implementar los sistemas de control necesarios para evitar que los excesos sobre los límites establecidos se repitan de manera sistemática o injustificada.

- La Unidad de Control de riesgos deberá asegurarse de que las operaciones se hacen teniendo en cuenta la mejor situación para el cliente y que hayan sido informados de los riesgos reales o potenciales que asumen, con el detalle necesario para que puedan formarse una opinión fundada, y que se ha recabado su autorización expresa antes de realizar por su cuenta cualquiera de las operaciones anteriores.

Sin embargo, la realización de ciertas funciones o tareas que incorporen mayor riesgo operativo pueden ser realizadas desde la organización, siempre y cuando quede asegurada la segregación entre dichas funciones, o bien pueden asignarse ciertas tareas de personal externo perteneciente a otras entidades del grupo o terceras empresas especializadas en administración y consultoría. Si se opta por esta última solución, el Consejo de Administración debe asegurarse de la profesionalidad, capacidad y experiencia de los terceros, y hacer extensivos a los servicios subcontratados los procedimientos y controles establecidos en la organización o, en su caso, desarrollados con carácter específico.

La empresa debe asegurarse de que los recursos humanos sean suficientes y adecuados para:

- La consecución de una eficiente y eficaz gestión del negocio y de los riesgos asumidos.
- El control de las operaciones realizadas y su registro.
- Los contrastes sobre los criterios de valoración del patrimonio de la entidad.
- La adecuada gestión.

Para asegurar la formación técnica y profesionalidad de su personal las entidades deben establecer planes de formación y evaluación continuada, sobre todo:

- Para los que realizan funciones comerciales.
- Para los que gestionan y miden riesgos.
- Para los que desarrollan actividades cuya complejidad y constante evolución requiere una permanente actualización.

Todo ello, con una definición clara de los requisitos mínimos de formación y experiencia exigibles a empleados y directivos para el desempeño de las tareas y responsabilidades encomendadas.

En resumen, se complementará con los soportes informáticos y los medios materiales necesarios para llevar a cabo las tareas de administración, gestión de reclamaciones, control y registro contable de las operaciones que se realicen, con garantías suficientes de seguridad y capacidad.

Asimismo, deberá mantenerse un sistema de archivo que contenga la documentación soporte de todas las operaciones contabilizadas y de clientes, proveedores y reclamantes, que permita la localización de documentos en un periodo de tiempo razonable.

Por otro lado, las entidades deben conocer adecuadamente y a tiempo los riesgos que están asumiendo, para poder evaluar su capacidad de absorber las pérdidas que eventualmente pueda ocasionarles su actividad. Esto supondrá que los sistemas de información para la gestión estarán orientados hacia la evaluación de riesgos y la toma de decisiones, en concordancia con los planes y objetivos fijados por el Consejo de Administración y debiendo implementar los controles necesarios para asegurar la autenticidad y veracidad de la información que es manejada por el Consejo de Administración y por los distintos niveles jerárquicos.

Los sistemas de generación de información contable y de gestión de riesgos deberán proporcionar una visión precisa y completa de la situación financiera y patrimonial de las entidades sujetas y contar con la documentación soporte necesario para el correcto proceso administrativo de las operaciones.

Deberá establecerse un sistema eficaz y eficiente de comunicaciones internas y externas que asegure que la información relevante para la gestión y el control de riesgos llegan a todos los responsables, así como los procedimientos a seguir antes de operar en nuevos productos o servicios.

Las entidades deben tener la capacidad de realizar periódicamente una medición y seguimiento de todos sus riesgos potenciales, siendo capaces de efectuar valoraciones a precio de mercado y poder realizar los oportunos contrastes sobre las hipótesis financieras y económicas que, en su caso, determinarán una modificación de los procedimientos de valoración de los compromisos de la entidad.

El manual de Administración de Riesgos tendrá que ser descriptivo y exigir el análisis de los principales riesgos, a través del estudio del grado de exposición específico de la entidad a los mismos, y mediante un control sistemático de los límites que se marquen como tolerables, los cuales podrían estar en relación con el resto de factores aplicados a la solvencia de la entidad. Para ello:

- Se deberá contar con algún sistema de medición y control de riesgos financieros en base a duraciones, sensibilidades o modelos estadísticos internos de valoración de pérdidas potenciales.

- Periódicamente deberán realizarse simulaciones de escenarios específicos de crisis y plan de continuidad de negocio para analizar los eventuales efectos que pudieran derivarse sobre la solvencia y cobertura de los compromisos de las entidades.

- Se deberán realizar revisiones de riesgos de forma sistemática, por personal distinto al que identificó los riesgos, contrastándose con información de fuentes externas a la entidad.

- Deberá quedar evidencia documental de la realización de conciliaciones. Un responsable distinto a quien efectuó la conciliación verificará el cumplimiento periódico de dicho procedimiento, evaluando las partidas conciliatorias y las diferencias registradas y emitiendo un informe sobre las incidencias más significativas.

- La periodicidad en la realización de las revisiones será fijada por la unidad de control en función de las necesidades de las entidades sujetas y la importancia de los riesgos.

- La realización de las revisiones y controles deberá ser previa a la remisión de los resultados al organismo de control, debiendo comunicarse de inmediato las incidencias más importantes derivadas de dichos riesgos.

- Establecer criterios objetivos para el registro de las participaciones significativas y sus incidencias y hacer revisiones periódicas para asegurarse de su correcta contabilización y valoración.

• Seguimiento de las participaciones y la estructura de la entidad y verificar la información suministrada sobre la variación en los porcentajes de participación.

• Tomar las medidas adecuadas para disponer de una información pormenorizada de los riesgos correspondientes a los canales de distribución, sucursales, reclamantes y otros terceros.

• Procedimientos adecuados para implementar los procedimientos y controles adecuados para evitar que se produzcan quebrantos derivados de riesgos legales, reputacionales y operacionales o la realización de actividades fraudulentas en sus relaciones con los clientes, proveedores, sucursales y cualquier tercero.

• Desarrollar e implementar procedimientos formales de autorización, control y seguimiento de límites de operaciones y otros saldos deudores, otros canales de distribución, así como para la clasificación de saldos como morosos, dudosos o fallidos, atendiendo a las estimaciones y cumplimiento del calendario de dotaciones que les sea de aplicación, contando con expedientes individualizados que contengan toda la documentación relativa a su entidad, contratos firmados y otras informaciones necesarias, además de otros datos sobre su capacidad financiera.

• Establecer procedimientos para la salvaguarda de estos expedientes, así como para su permanente actualización.

• Contrastar toda la información, periódicamente, para que esté de acuerdo con los criterios establecidos en la normativa aplicable a las entidades.

• De operar a través de sucursales se deberán dotar de los medios necesarios para el adecuado desarrollo de su actividad.

• Las sucursales u oficinas deberán estar integradas en los procedimientos de control interno establecidos. En particular, los procedimientos deberán asegurar la revisión y control permanente de los riesgos

En el contenido del informe anual deben constar los principales resultados del sistema de evaluación y gestión de riesgos, riesgos identificados como relevantes, las mediciones realizadas y la estrategia establecida para administrarlos. El informe además incluirá el pronunciamiento del Comité de Administración integral de riesgos sobre el cumplimiento de los lineamientos definidos para la administración de los diferentes riesgos asumidos.

Mediante el informe, el Consejo de Administración de la Entidad dejará constancia del cumplimiento de lo dispuesto en materia de control interno, con las particularidades y precisiones que a continuación se detallan:

• Eficacia y eficiencia del sistema de control interno.

• Fiabilidad e integridad de la información.

• Análisis y gestión de riesgos.

• Cumplimiento normativo.

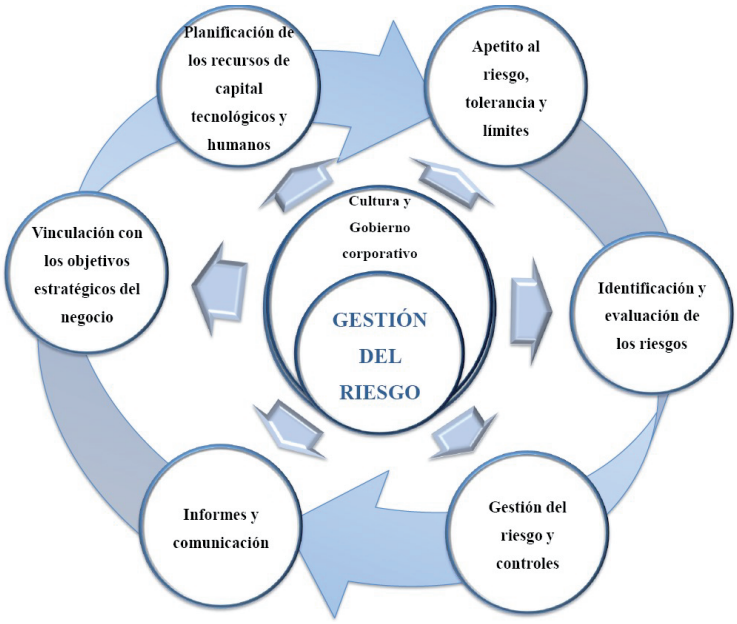

Gráfico 20.

El tratamiento de los riesgos implica, identificar las diferentes opciones para manejar los riesgos. Algunas de esas opciones son:

• No exposición (eliminación del riesgo). - Decisión consciente de no exponerse a un riesgo determinado (por ejemplo, las empresas pueden decidir eliminar ciertas líneas de negocio, productos, …)

• Prevención y control de pérdidas (reducir el riesgo). - Medidas para disminuir la probabilidad o gravedad de la pérdida (por ejemplo, una empresa puede disminuir o minimizar el riesgo de fraude mejorando la selección de su personal).

• Retención del riesgo (asunción del riesgo). - Consiste en absorber el riesgo y cubrir las pérdidas con los propios recursos.

• Transferencia (transferir el riesgo). - Consiste en trasladar el riesgo a otras entidades especializadas como a través del reaseguro o coaseguro. Las políticas y estrategias de la entidad aseguradora deben definir el nivel de riesgo considerado como aceptable; este nivel se manifiesta en límites de riesgo puestos en práctica a través de políticas, normas, procesos y procedimientos que establecen la responsabilidad y la autoridad para fijar esos límites, los cuales pueden ajustarse si cambian las condiciones o las tolerancias al riesgo por la entidad.

Tratamiento del riesgo: Aceptar y monitorear los riesgos de baja prioridad. Para otros riesgos, desarrollar e implementar un plan de administración específico que incluya consideraciones de fondeo.

El tratamiento del riesgo involucra las siguientes acciones: Identificar el rango de opciones para tratar los riesgos, evaluar las opciones, preparar planes para el tratamiento e implementarlos.

Tras la evaluación de los riesgos más relevantes de la organización, la dirección determina cómo responder a ellos. Las respuestas pueden ser las de evitar, reducir, compartir y aceptar el riesgo. Al considerar su respuesta, la dirección evalúa su efecto sobre la probabilidad e impacto del riesgo, así como los costes y beneficios, y selecciona aquella que sitúe el riesgo residual dentro de las tolerancias al riesgo establecidas. La dirección identifica cualquier oportunidad que pueda existir y asume una perspectiva del riesgo globalmente para la entidad o bien una perspectiva de la cartera de riesgos, determinando si el riesgo residual global concuerda con el riesgo aceptado por la entidad.

Ejemplos de respuestas al riesgo según tipos posibles

Evitar	**Compartir / Transferir**
• Prescindir de una unidad de negocio, línea de producto o segmento geográfico. • Decidir no emprender nuevas iniciativas/actividades que podrían dar lugar a riesgos.	• Adoptar seguros contra pérdidas inesperadas significativas. • Entrar en una sociedad de capital riesgo/sociedad compartida. • Establecer acuerdos con otras empresas. • Protegerse contra los riesgos utilizando instrumentos del mercado de capital a largo plazo. • Externalizar procesos de negocio. • Distribuir el riesgo mediante acuerdos contractuales con clientes, proveedores u
Reducir	**Aceptar**
• Diversificar las ofertas de productos. • Establecer límites operativos. • Establecer procesos de negocio eficaces. • Aumentar la implicación de la dirección en la toma de decisiones y el seguimiento. • Reequilibrar la cartera de activos para reducir el índice de riesgo con respecto a determinados tipos de pérdidas. • Reasignar el capital entre las unidades operativas.	• Provisionar las posibles pérdidas. • Confiar en las compensaciones naturales existentes dentro de una cartera. • Aceptar el riesgo si se adapta a las tolerancias al riesgo existentes.

Tabla 7.

3.8.1.1 Control.

La Guía 73:2009 define el control como la medida que modifica un riesgo.

Mediante la información obtenida en la evaluación de riesgos, es el proceso de toma de decisión para tratar y/o reducir los riesgos, para implantar las medidas correctoras, exigir su cumplimiento y la evaluación periódica de su eficacia.

El propósito del control de riesgo es analizar el funcionamiento, la efectividad y el cumplimiento de las medidas de protección, para determinar y ajustar sus deficiencias.

Las actividades del proceso, tienen que estar integradas en el plan operativo institucional, donde se definen los momentos de las intervenciones y los responsables de ejecución.

Medir el cumplimiento y la efectividad de las medidas de protección requiere que levantemos constantemente registros sobre la ejecución de las actividades, los eventos de ataques y sus respectivos resultados. Estos tenemos que analizados frecuentemente. Dependiendo de la gravedad, el incumplimiento y el sobrepasar de las normas y reglas, requieren sanciones institucionales para los funcionarios.

En el proceso continuo de la gestión del riesgo, las conclusiones que salen como resultado del control de riesgo, nos sirven como fuente de información, cuando se entra otra vez en el proceso del análisis de riesgo.

El control interno se define como un proceso efectuado por la dirección y el resto del personal de una entidad, diseñado con el objeto de proporcionar un grado de seguridad razonable en cuanto a la consecución de los objetivos dentro de las siguientes categorías:

- Eficacia y eficiencia de las operaciones.
- Confiabilidad de la información financiera.
- Cumplimiento de las leyes, reglamentos y normas (que sean aplicables).

Las actividades de control son: las políticas, procedimientos, técnicas, prácticas y mecanismos que permiten a la Dirección administrar (mitigar) los riesgos identificados durante el proceso de evaluación de riesgos y asegurar que se llevan a cabo los lineamientos establecidos por ella. Se ejecutan en todos los niveles de la unidad y en cada una de las etapas de la gestión, partiendo de la elaboración de un Mapa de Riesgos.

En la evaluación del Sistema de Control Interno no solo debe considerarse si fueron establecidas las actividades relevantes para los riesgos identificados, sino también si las mismas son aplicadas en la realidad y si los resultados obtenidos fueron los esperados.

Existe una amplia variedad de controles, sin embargo, vamos a centrarnos en aquellos controles que tienen impacto en los resultados de las entidades, enumerando los

controles más relevantes para prevenir, detectar y corregir incorrecciones de importancia en los estados financieros y los controles básicos para gestionar los riesgos de negocio más significativos para la Entidad.

Las actividades de control son las políticas y procedimientos establecidos por la dirección y otros miembros de la organización con autoridad para emitirlos, como respuesta a los riesgos que podrían afectar el logro de los objetivos. Los procedimientos son las acciones de las personas para implantar las políticas, directamente o a través de la aplicación de tecnología, y ayudar a asegurar que se llevan a cabo las respuestas de la dirección a los riesgos.

Las actividades de control pueden ser clasificadas por la naturaleza de los objetivos de la entidad con la que están relacionadas: estrategia, operaciones, información y cumplimiento.

Debido a que cada entidad tiene su propio conjunto de objetivos y enfoques de implantación, existirán diferencias en las respuestas al riesgo y las actividades de control relacionadas.

Cada entidad está gestionada por personas diferentes que tienen criterios individuales diferentes en la aplicación de controles. Es más, los controles reflejan el entorno y sector en que opera una entidad, así como su dimensión y complejidad de organización, la naturaleza y alcance de sus actividades y sus antecedentes y cultura. Por esta razón las actividades de control no pueden generalizarse y deberán ser la respuesta a la medida de la necesidad de los objetivos y los riesgos de cada organización.

El componente actividades de control establece los siguientes factores:

1. Integración con las decisiones sobre riesgos
2. Principales actividades de control
3. Controles sobre los sistemas de información

1. Integración con las decisiones sobre riesgos

Después de haber seleccionado las respuestas al riesgo, la dirección establece actividades de control necesarias para disminuir los riesgos y alcanzar los objetivos en sus diferentes categorías.

Establecer una matriz que relacione los riesgos seleccionados con los controles establecidos por la organización, brindará una seguridad razonable de que los riesgos se mitigan y de que los objetivos se alcanzarán con razonable seguridad de que no existan errores o irregularidades. Será recomendable que esta matriz u otro documento relacionen los riesgos y los controles con los objetivos en sus diferentes jerarquías.

Para la autoevaluación por parte de la administración o la evaluación independiente de la calidad de los elementos de este componente, se deben considerar como mínimo los siguientes puntos:

Grado en que las actividades de control guardan relación con los objetivos y las decisiones adoptadas por la dirección sobre los riesgos.

Calidad de la información y comunicación sobre las decisiones adoptadas por la dirección sobre el estudio de los riesgos.

2. Principales actividades de control

Se han propuesto muchas descripciones diferentes de los tipos de actividades de control, incluyendo los controles de prevención, detección, manuales, informáticos y de dirección.

Estas actividades de control deben enmarcarse en políticas y procedimientos emitidos por la dirección y otros niveles de la organización encargados de ejecutarlos. La política establece lo que debe hacerse y los procedimientos la forma para llevarla a cabo.

Las actividades de control incluyen controles preventivos, para detener ciertas transacciones riesgosas antes de su ejecución, y, controles de detección, para identificar aquellas que tienen posibles errores o irregularidades.

Las actividades de control combinan controles informáticos y manuales, incluyendo aquellos automatizados que aseguran la captación correcta de la información, y procedimientos de autorización y aprobación de las decisiones de inversión por parte de las personas responsables.

A continuación, se presentan las siguientes actividades de control como una ilustración general, que no debe ser considerada exhaustiva:

- **Revisiones y supervisiones**: La alta dirección revisa el funcionamiento real en contraste con presupuestos, previsiones y datos de períodos previos y de competidores. También se supervisa la implantación de planes financieros o de otro tipo.

- **Gestión directa de funciones o actividades**: Los directivos que gestionan las funciones o actividades revisan los informes de rendimiento. Estos directores también se centran en temas de cumplimiento, revisando los informes que requieren los reguladores sobre nuevos depósitos que superen unos importes específicos.

- **Procesamiento de la información**: Se lleva a cabo una variedad de controles para verificar la exactitud, integridad y autorización de las transacciones. Se aceptará el pedido de un cliente, sólo después de verificar con un fichero de clientes y el límite de crédito autorizado.

• **Repetición**: Las acciones aplicadas durante el procesamiento de las operaciones se repiten por otra persona para validar los datos y los controles aplicados.

• **Validación**: Mediante la autorización, comparación y verificación de la pertinencia y la legalidad de la transacción.

• **Aseguramiento**: Mediante la aplicación de los controles establecidos para reducir los riesgos y los errores en la ejecución de las actividades.

• **Especialización funcional**: Se insertan en la estructura de la organización como la separación de funciones, la supervisión de los procesos, las evaluaciones ejecutadas por la auditoría interna y otras.

• **Controles físicos**: Los equipos, existencias, valores, efectivo y demás activos están físicamente asegurados, se someten periódicamente a recuentos y se contrastan con los importes de los registros de control.

• **Indicadores de rendimiento**: El contraste entre sí de diferentes conjuntos de datos operativos o financieros junto con el análisis de relaciones y las acciones de investigación y corrección, constituye una actividad de control.

• **Segregación de funciones**: Las funciones se dividen o segregan entre diferentes personas para reducir el riesgo de error o fraude.

Para la **autoevaluación por parte de la administración o la evaluación independiente de la calidad de los controles** de este componente, se deben considerar como mínimo los siguientes puntos:

• Apoyo de la alta dirección para el diseño y aplicación de los controles en función de los riesgos.

• Forma en que los controles se incorporan a los procesos.

• Relación de las actividades de control seleccionadas, con los objetivos y con los riesgos.

• Existencia de mecanismos para analizar las alternativas de controles a seleccionar.

• Grado de comprensión de los funcionarios involucrados en el diseño de los procesos para incorporar controles apropiados que guarden una relación adecuada de costos con beneficios.

• Calidad de los sistemas de información y comunicación.

3. Controles sobre los sistemas de información

Pueden usarse amplios grupos de actividades de control de los sistemas de información.

El primero lo forman los controles generales, que se aplican a muchos de esos sistemas y ayudan a asegurar que siguen funcionando continua y adecuadamente.

El segundo son los controles de aplicación, que incluyen fases informatizadas dentro del software para controlar el proceso.

Ambos tipos de controles, combinados con controles manuales de proceso cuando sea necesario, operan juntos para asegurar la integridad, exactitud y validez de la información.

Los **controles generales** incluyen controles sobre la gestión de la tecnología de información, su infraestructura, la gestión de seguridad y la adquisición, desarrollo y mantenimiento del software. Se presentan a continuación algunos ejemplos de controles comunes dentro de estas categorías.

√ Gestión de la tecnología de información: Un comité de trabajo proporciona supervisión, seguimiento e información de las actividades de tecnología informática y las iniciativas para su mejora.

√ Infraestructura de la tecnología de información: Los controles se aplican a la definición, adquisición, instalación, configuración integración y mantenimiento de los sistemas.

√ Gestión de la seguridad: Son controles de acceso lógico tales como contraseñas seguras de restricción de accesos a la red, bases de datos y aplicaciones.

√ Adquisición, desarrollo y mantenimiento del software: Los controles sobre la adquisición e implantación del software se incorporan a un proceso establecido para gestionar el cambio, incluyendo los requisitos de documentación, la comprobación de la aceptación del usuario, las pruebas de carga y las evaluaciones del riesgo de proyectos.

Los **controles de aplicación** se centran directamente en la integridad, exactitud, autorización y validez de la captación y procesamiento de datos. Ayudan a asegurar que los datos se captan o generan en el momento de necesitarlos, que las aplicaciones de soporte estén disponibles y que los errores de interfaz se detecten rápidamente.

Un objetivo importante de los controles de aplicación es prevenir que los errores se introduzcan en el sistema, así como detectarlos y corregirlos una vez introducidos en él. Se resumen algunos ejemplos de controles de aplicación:

√ Equilibrar las actividades de control: Detectar los errores en la captación de datos, mediante la conciliación entre los importes introducidos, manual o automáticamente, y un total de control.

√ Dígitos de control: Validan los datos mediante cálculos. La numeración de los repuestos de una empresa contiene un dígito de control que detecta y corrige pedidos inexactos a sus proveedores.

√ Listados predefinidos de datos: Proporcionan al usuario listas preestablecidas de datos aceptables.

√ Pruebas de razonabilidad de datos: Comparan los datos captados con una pauta existente o aprendida de razonabilidad.

√ Pruebas lógicas: Incluyen el uso de límites de rango o pruebas alfanuméricas o de valor.

Para la **autoevaluación por parte de la administración o la evaluación independiente de la calidad** de los elementos de este componente, se deben considerar como mínimo los siguientes puntos:

• Existencia de un plan estratégico de tecnologías de información que guarde relación con los objetivos institucionales y la gestión de los riesgos.

• Existencia y apoyo para el desarrollo de tecnología de información relacionada con los controles y la gestión de los riesgos.

• Apoyo de la dirección a la implantación de los planes estratégicos de tecnología de información.

• Idoneidad de la metodología para integrar las estrategias, las operaciones, los requerimientos de información y comunicación y el cumplimiento de las normas, con el desarrollo tecnológico de la institución.

• La calidad de la información y comunicación sobre los planes y los avances sobre tecnología de información.

Tal y como está definida la estructura organizativa de las entidades, se establece un mapa de riesgos global con la siguiente estructura para la eficacia y eficiencia de los controles:

• Actividad, conjunto de acciones realizadas con el fin de alcanzar los objetivos del proceso en el que intervienen.

• Objetivo perseguido por la actividad que debe ir en consonancia con los objetivos estratégicos establecidos por la Entidad.

• Riesgo, hace referencia a los hechos que pueden acaecer e impedir el correcto desarrollo de la actividad y por tanto el incumplimiento del objetivo establecido.

• Normativa, normas de carácter externo (legislación) o interno (manuales de procedimiento o directivas de actuación) que especifiquen las pautas a seguir en el desarrollo de la actividad.

• Control, entendiendo por tal el mecanismo establecido para mitigar o anular el impacto del riesgo que afecta al proceso.

• Periodicidad, carencia con la que debe realizarse el control.

• Responsable, persona encargada de realizar el control o supervisar su cumplimiento.

• Recomendaciones, evaluación de los controles establecidos.

El siguiente gráfico resume el mapa de riesgos por actividades de negocio que recoge la información de los ciclos de actividad por cada área o departamento:

Gráfico 21.

De esta forma, pueden analizarse los procedimientos de control encargados a cada área o departamento, la finalidad de los mismos y analizar a través de ellos los controles establecidos, para así, si los procedimientos están bien definidos, obtener los mapas de actividades sobre los que centrar los riesgos que amenazan el negocio. Esta aproximación debe ser posterior a la ejecución de un conjunto de comprobaciones que permitan analizar la exposición específica a los riesgos generales de una entidad.

3.8.1.2 Evitación del riesgo.

La Guía 73:2009 define la evitación del riesgo como la decisión argumentada de no implicarse en una actividad o de retirarse de ella, con el objeto de no estar expuesto a un riesgo particular.

Podemos decir que la evitación del riesgo es la acción y efecto de precaver o evitar que suceda una cosa. Evitar, etimológicamente significa apartar algún daño, peligro o molestia, impidiendo que suceda. Excusar, huir de incurrir en algo. Huir el trato de alguien, apartarse de su comunicación.

Las estrategias fundamentales de la evitación del riesgo, consisten en minimizar la probabilidad de que el riesgo se presente. Para ello existen 4 opciones principales para tratar de evitar que los riesgos pasen a ser una realidad negativa para nuestra empresa: transferencia, reducción, elusión y diversificación.

Una vez se han identificado y analizado los riesgos, debe tenerse en cuenta cuales pueden ofrecer una oportunidad de beneficio, y cuales suponen una amenaza, así como la probabilidad de manifestarse de cada uno de ellos.

Dependiendo por tanto del tipo de riesgo al que se enfrente, y de la situación y características en que se encuentre la empresa, debemos elegir la estrategia de evitación de riesgos más adecuada.

- Transferencia: representa el conjunto de procedimientos cuyo objetivo es eliminar el riesgo transfiriéndolo de un lugar a otro. Consiste, por ejemplo, en vender un activo dudoso, asegurar una actividad con importantes riesgos, contratar pólizas de seguros, etc.

- Reducción: busca, bien reducir la probabilidad de ocurrencia de un riesgo, bien reducir sus consecuencias, o bien lograr ambos objetivos a la vez. La probabilidad de ocurrencia de un riesgo puede reducirse a través de controles de gestión, arreglos organizacionales, y procedimientos encaminados a reducir la frecuencia o la oportunidad de que ocurra un error. Las consecuencias pueden reducirse asegurando o garantizando que todos los controles se encuentren en el lugar apropiado para minimizar cualquier consecuencia adversa.

- Elusión: existen dos opciones para intentar eludir un riesgo; una, no proceder con la actividad que incorporaría el riesgo; dos, escoger medios alternativos para la actividad, que logren el mismo resultado y no incorporen el riesgo detectado. El problema de eludir riesgos es que podemos perder oportunidades de negocio, y además, otros riesgos no identificados inicialmente, pueden volverse más significativos.

- Diversificación: consiste en intentar extender el riesgo de un área en concreto, a diferentes secciones, con el fin de impedir la pérdida de todo el negocio. Son ejemplos de diversificación orientarse a nuevos mercados y proveedores, diversificar la lista de productos y servicios, etc.

Tal como hemos visto, existen diferentes estrategias, que correctamente aplicadas, nos resultarán sumamente útiles en nuestra tarea de gestión y elusión de riesgos mediante acciones concretas, que nos permiten responder a determinados riesgos, que afecten a la actividad de nuestro negocio.

Las estrategias de minimización se aplican cuando los riesgos ya han producido sus efectos, y son, por tanto, una realidad. En este momento, lo único que cabe es tomar medidas correctoras con el fin de minimizar las consecuencias.

Estas situaciones producen retrasos en los proyectos, gabinetes de crisis, etc., por lo que no son aconsejables, y sólo deben ser utilizadas como medida de emergencia. La principal medida que se puede adoptar en estas situaciones, con el fin de paliar los efectos derivados de la realización del riesgo, son los Planes de Contingencia que definen los procedimientos y procesos alternativos que se han de acometer en una organización cuando un riesgo deja de serlo para convertirse en realidad, así como las personas implicadas en dichos procedimientos. Se asume, por tanto, que han fallado las estrategias de evitación y monitorización de los riesgos, y sus efectos ya son inevitables.

3.8.1.3 Reparto del riesgo.

La Guía 73:2009 define el reparto del riesgo como la forma de tratamiento del riesgo que implica una distribución acordada del riesgo con otras partes.

Analizando otras definiciones nos encontramos con:

1. Distribuir algo dividiéndolo en partes.
2. Distribuir por lugares distintos o entre personas diferentes.
3. Clasificar (ordenar).
4. Entregar a personas distintas lo que han encargado o deben recibir.
5. Señalar o atribuir partes a un todo.
6. Extender o distribuir uniformemente una materia sobre una superficie.
7. Cargar una contribución o gravamen por partes.
8. Dar a cada cosa su oportuna colocación o el destino conveniente.

Cuando se trata de invertir, el riesgo (la posibilidad de que una inversión disminuya su valor) es prácticamente inevitable. Mientras que la idea de cualquier tipo de riesgo nos puede resultar incómoda, el riesgo de inversión no es necesariamente algo malo. Pero tiene que saber a qué se enfrenta si quiere enfrentarlo en forma eficaz.

En la transferencia a seguros, la dispersión, distribución o el reparto del riesgo se utiliza para que el costo del seguro sea justo y equitativo tanto para el grupo de asegurados como para la Compañía Aseguradora, igualando los riesgos que componen su cartera, a través de las diferentes formas de compartir el riesgo:

DEDUCIBLE: Cantidad o porcentaje cuyo importe ha de superarse para que se pague una reclamación. Importe de toda pérdida que corren a cargo del Asegurado. Representa un ahorro en primas para el Asegurado.

COASEGURO: Participación de dos o más empresas de seguros en un mismo riesgo, en virtud de contratos directos realizados por cada una de ellas con el Asegurado. También se define como un porcentaje de la pérdida que quedará a cargo del Asegurado en cada siniestro.

FRANQUICIA: Porcentaje de la suma asegurada. Si la pérdida es mayor que ese porcentaje, la indemnización se hará integra.

REASEGURO: Es el contrato en virtud del cual una empresa de seguros toma a su cargo total o parcialmente un riesgo ya cubierto por otra o el remanente de daños que exceda de la cantidad asegurada por el Asegurador directo.

CONTRASEGURO: Es el convenio en virtud del cual una empresa de seguros se obliga a reintegrar al contratante las primas o cuotas satisfechas o cubiertas cuando se cumplan determinadas condiciones.

Evitar: Supone dejar de realizar la actividad que genere el riesgo. Por ejemplo, cuando una entidad transportista decide no continuar con su expansión geográfica y se centra en el desarrollo de su especialización de servicios.

Reducir: Tratamos de reducir el impacto o la probabilidad en caso de que el riesgo ocurra, o incluso de reducir ambos a un mismo tiempo. Esta es una de las más típicas decisiones empresariales cotidianas, como, por ejemplo, la prevención de riesgos; que los conductores realicen una revisión de sus vehículos antes de comenzar un viaje.

Compartir: La probabilidad o impacto del riesgo se traslada de titular, al menos en parte. Las técnicas más comunes de compartir riesgos son las de la utilización de pólizas de seguros, la realización de operaciones de cobertura, o incluso la exteriorización de la actividad objeto de riesgo. El riesgo de gestión fraudulenta de los gestos comerciales en el caso de falta de mercancía podría evitarse si el delegado de la agencia tuviese que trasladar a un tercero la ocurrencia del daño, y no pudiera aplicar descuentos a sus facturas si no es con el visto bueno del departamento de operaciones de la entidad de transportes.

Aceptar: Aceptar un riesgo es asumir que puede ocurrir, y saber que la entidad tiene recursos suficientes para hacer frente al mismo, y le resulta más ventajoso que aplicar cualquiera de las reglas anteriormente descritas.

3.8.1.4 Financiación del riesgo

La Guía 73:2009 define la financiación del riesgo como la forma de tratamiento del riesgo que implica la gestión de contingentes para la previsión de fondos, a fin de hacer frente o a modificar las consecuencias financieras que se pudiesen presentar.

La financiación del riesgo es la acción y efecto de financiar (aportar dinero para una empresa o proyecto, sufragar los gastos de una obra o actividad). La financiación con-

siste en aportar dinero y recursos para la adquisición de bienes o servicios. Es habitual que la financiación se canalice mediante créditos o préstamos (quien recibe el dinero, debe devolverlo en el futuro).

Otra clasificación de financiación puede realizarse tomando en cuenta la procedencia de los recursos. La financiación externa es aquella que procede de inversores que no pertenecen a la empresa (la financiación bancaria, la emisión de obligaciones, etc.), mientras que la financiación interna tiene su origen en fondos producidos por la propia empresa a través de su actividad (amortizaciones, reservas, etc.)

3.8.1.5 Retención del riesgo.

La Guía 73:2009 define la retención del riesgo como la aceptación de los beneficios potenciales de una ganancia o de las cargas por pérdida motivadas por un riesgo particular.

El objetivo principal del tratamiento de los riesgos sugiere un proceso de decisión abierto a las alternativas que se ofrecen a la empresa para reducir la peligrosidad y coste de los riesgos.

Dentro de este ámbito, la retención de riesgos se configura como el proceso de verificación y cuantificación de los riesgos y de las posibilidades de transferencia, que conlleve a la adopción de medidas de un menor coste económico para la empresa, generando, por tanto, una reducción paulatina y a largo plazo del coste de los riesgos de la empresa.

La magnitud de riesgo, sujeta a la restricción impuesta por la capacidad financiera de la empresa para asumir los riesgos retenidos, constituye el eje fundamental para llevar a cabo un proceso de retención plenamente planificado.

La retención de riesgos es el conjunto de actividades llevadas a cabo en la empresa, especialmente de tipo financiero, para compensar directamente las posibles pérdidas accidentales que puedan sobrevenir en la misma. Puede revestir diversas formas:

a) Retención pasiva o asunción de riesgos. A su vez puede ser de dos clases:

- √ Consciente o intencionada. Es la que obedece a un plan meditado de absorción de pérdidas aleatorias.

- √ Inconsciente o no planificada. Es la más frecuente y puede poner en peligro la estabilidad de la empresa. Ignorar la existencia de un riesgo no es un tratamiento del riesgo.

b) Retención activa o retención propiamente dicha, también llamada autoseguro. Implica un programa definido de la empresa para compensar pérdidas que son inciertas en magnitud y frecuencia en un año cualquiera, y que, si ocurrieran sin una previa planificación financiera, podrían causar serios problemas económicos e incluso la in-

solvencia. Realmente la asunción inconsciente no puede ser considerada como una estrategia en Gerencia de riesgos.

Por el contrario, el autoseguro e incluso la asunción planificada pueden plantearse:

A. Total. La empresa decide financiar o asumir directamente todas las pérdidas previsible.

B. Parcial. La empresa reparte y comparte el riesgo, normalmente con un Asegurador convencional (AUTOSEGURO PARCIAL) a través de mecanismos como:

- Coaseguro, voluntario o involuntario (regla proporcional).
- Franquicia, por siniestro o acumulada en varios siniestros hasta que la suma de éstos alcance un determinado límite.
- Límite de responsabilidad para el Asegurador (primer riesgo), propio de coberturas de Responsabilidad Civil General.

La tarificación retrospectiva *(BURNING COST)* y la utilización de Compañías aseguradoras cautivas son también, en cierta medida, formas especiales de retención parcial o total de riesgos. Retención de Riesgo y Seguro no son conceptos sustitutivos, sino complementarios.

El Gerente de Riesgos debe decidir cuánto y cómo retener, al tiempo que cuánto y cómo asegurar. La retención del riesgo está definida como un plan financiero diseñado para enfrentar las pérdidas fortuitas que puedan ocurrir dentro de una empresa. La retención del riesgo es un término general el cual incluye diferentes formas de auto-aseguramiento, así como la Asunción del riesgo. El método del auto-aseguramiento se puede distinguir del método de la simple asunción del riesgo en que el segundo, en contraste con el auto-aseguramiento, usualmente no envuelve un plan formal, una reserva especial para pérdidas o un fondo de pérdidas.

3.8.1.6 Riesgo residual.

La Guía 73:2009 define el riesgo residual como el riesgo remanente después del tratamiento del riesgo.

Podemos decir que es el riesgo que queda después de que se hayan tomado todas las medidas preventivas y detectivas.

Según la norma ISO 27001 es el riesgo remanente que existe después de que se hayan tomado las medidas de seguridad.

El nivel de riesgo al que está sometido una organización nunca puede erradicarse totalmente. Se trata de buscar un equilibrio entre el nivel de recursos y mecanismos que es preciso dedicar para minimizar estos riesgos y un cierto nivel de confianza que se puede considerar suficiente (nivel de riesgo aceptable).

El nivel de riesgo existente después de la implantación de salvaguardas se denomina riesgo residual, y es el que separa a la organización de la "Seguridad Total o Perfecta". Una cobertura completa desde el punto de vista económico la aportaría un plan de riesgos conjunto, que incluyera la gestión efectiva de los riesgos detectados mediante la implantación de las salvaguardas correspondientes complementado con una póliza de riesgo que cubriera el riesgo residual.

Por ejemplo, las compañías aseguradoras exigen para la contratación del seguro de riesgo electrónico la existencia de un plan de gestión de riesgos, como prueba del compromiso efectivo de los asegurados sobre la gestión de su seguridad y como base para el cálculo de la prima.

El nivel de riesgo residual, es el riesgo que la institución puede asumir después de aplicar medidas o salvaguardias de seguridad. El nivel de riesgo residual obtenido supera el riesgo potencial, por tanto, todo lo que éste por debajo de este nivel no se considera una amenaza importante para la empresa.

Es aquel riesgo que subsiste, después de haber implementado controles. Es importante advertir que el nivel de riesgo al que está sometido una compañía nunca puede erradicarse totalmente. Por ello, se debe buscar un equilibrio entre el nivel de recursos y mecanismos que es preciso dedicar para minimizar o mitigar estos riesgos y un cierto nivel de confianza que se puede considerar suficiente (nivel de riesgo aceptable). El riesgo residual puede verse como aquello que separa a la compañía de la seguridad absoluta.

El riesgo residual es aquél que permanece después de que la dirección desarrolle sus respuestas a los riesgos. El riesgo residual refleja el riesgo remanente una vez se han implantado de manera eficaz las acciones planificadas por la dirección para mitigar el riesgo inherente.

Estas acciones pueden incluir las estrategias de diversificación relativas a las concentraciones de clientes, productos u otras, las políticas y procedimientos que establezcan límites, autorizaciones y otros protocolos, el personal de supervisión para revisar medidas de rendimiento e implantar acciones al respecto o la automatización de criterios para estandarizar y acelerar la toma de decisiones recurrentes y la aprobación de transacciones. Además, pueden reducir la probabilidad de ocurrencia de un posible evento, su impacto o ambos conceptos a la vez.

El riesgo residual es aquél que permanece después de que la dirección desarrolle sus respuestas a los riesgos. Refleja el riesgo remanente una vez se han implantado de manera eficaz las acciones planificadas por la dirección para mitigar el riesgo inherente.

Estas acciones pueden incluir las estrategias de diversificación relativas a las concentraciones de clientes, productos u otras, las políticas y procedimientos que establezcan límites, autorizaciones y otros protocolos, el personal de supervisión para revisar medidas de rendimiento e implantar acciones al respecto o la automatización de criterios para estandarizar y acelerar la toma de decisiones recurrentes y la aproba-

ción de transacciones. Además, pueden reducir la probabilidad de ocurrencia de un posible evento, su impacto o ambos conceptos a la vez.

3.8.1.7 Resiliencia.

La Guía 73:2009 define la resiliencia como la capacidad de adaptación de una organización en un entorno complejo y cambiante.

La **resiliencia** es la capacidad que tiene una persona o un grupo de **recuperarse frente a la adversidad** para seguir proyectando el futuro. En ocasiones, las circunstancias difíciles o los traumas permiten desarrollar recursos que se encontraban latentes y que el individuo desconocía hasta el momento.

Resiliencia significa **volver a la normalidad,** es decir, la **capacidad de volver al estado natural, especialmente después de alguna situación crítica e inusual**. Es un término derivado del latín, del verbo, *resilio, resilire* que significa ´saltar hacia atrás, rebotar´.

La resiliencia, puede ser vista, como la capacidad o aptitud que posee algunos individuos para superarse de una adversidad. No obstante, no todos los individuos poseen esta característica ni se relaciona con la genética, muchas veces dicha habilidad el individuo la desconoce y la descubre cuando se encuentre en una situación dura que logra su fuerte actitud de superarse y seguir en frente.

Toda persona llamada resiliente es aquella que en un momento de su vida convirtió el dolor en una virtud, como: el sufrimiento de una enfermedad, la pérdida de un ser humano, pérdida de cualquier parte de su cuerpo, etc. En este sentido, se puede mencionar individuos famosos conocidos por su trayectoria y por su superación personal, es el caso del científico Stephen Hawking, la piloto de fórmula 1 María de Villota, actriz Adamari López, entre otros.

En consideración de lo anterior, **la resiliencia es sinónimo de** fortaleza, invulnerabilidad, resistencia, entre otros. La resiliencia tiene varios significados en el ámbito de la ecología, la psicología, la física y la gestión, como también en los sistemas tecnológicos, la Cultura Emprendedora, en Derecho y la sociología.

En sistemas tecnológicos, la resiliencia es la capacidad de un sistema de soportar y recuperarse ante desastres y perturbaciones.

En el ámbito de la gestión, la resiliencia es parte de los procesos de gestión de cambios. Las personas que trabajan en las organizaciones deben tener un gran equilibrio emocional, especialmente para hacer frente a los problemas del trabajo, cuando las situaciones no salen como esperaban y lo que se puede hacer para minimizar la situación.

Las organizaciones empresariales están utilizando el principio de la resiliencia para resolver las graves dificultades y problemas que están enfrentando en el mercado globalizado en el cual desarrollan sus actividades.

Las organizaciones desarrollan las actividades de control a través de políticas que establecen las líneas generales del control interno y procedimientos que llevan dichas políticas a la práctica con las siguientes características:

- **Establece políticas y procedimientos para respaldar la implementación de las instrucciones adoptadas por la dirección:** La dirección establece actividades de control que se incorporan en los procesos de negocio y en el día a día de las actividades de los empleados a través de políticas que establecen lo que se espera de ellos, así como procedimientos relevantes que especifican las actuaciones a realizar.

- **Establece responsabilidades sobre la ejecución de las políticas y procedimientos:** La dirección establece las responsabilidades oportunas sobre las actividades de control por parte de la dirección de la unidad de negocio o función en la que residan los riesgos correspondientes.

- **Se efectúa en el momento oportuno**: El personal responsable lleva a cabo las actividades de control en el momento oportuno según lo definido en las políticas en los procedimientos.

- **Adopta medidas correctivas**: Se define el personal responsable de investigar y actuar con respecto a los asuntos identificados como resultado de la ejecución de las actividades de control.

- **Se pone en práctica a través de personal competente:** El personal competente que dispone de las facultades apropiadas lleva a cabo las actividades de control con diligencia y con una continua atención

- **Revisa las políticas y procedimientos:** La dirección revisa periódicamente las actividades de control para determinar que siguen siendo relevantes y las actualiza cuando es necesario.

Las políticas reflejan la visión de la dirección sobre lo que debe hacerse para llevar a cabo el control. Dicha visión puede documentarse por escrito y plasmarse expresamente en otras comunicaciones o bien de manera implícita a través de las decisiones y medidas adoptadas por la dirección. Los procedimientos se componen de medidas que implementan una política.

Las actividades de control hacen referencia específicamente a aquellas políticas y procedimientos que contribuyen a la **mitigación de los riesgos** para la consecución de los objetivos en niveles aceptables.

Una **política**, podría exigir que se revisen las actividades llevadas a cabo por la empresa, sin embargo, el **procedimiento** es la revisión en sí, llevada a cabo en el momento oportuno y prestando atención a los factores establecidos en las políticas, tales como la naturaleza, el volumen de negocio, el patrimonio neto, ...

Las políticas y los procedimientos a menudo se comunican oralmente. Las políticas no escritas pueden ser eficaces cuando la política en sí es una práctica bien comprendida y establecida en el seno de la organización, así como en el caso de organizaciones de menor tamaño en las que los canales de comunicación implican un número limitado de niveles directivos y en las que existe una estrecha interacción y supervisión del personal. Sin embargo, a pesar de que constituyen una alternativa eficiente en costes para algunas organizaciones, **las políticas y procedimientos no escritos pueden ser más fáciles de evitar**, resultando muy costosas para la organización si existe una elevada rotación de personal y pudiendo reducir la responsabilidad por la rendición de cuentas al respecto. Cuando se sometan a la revisión de partes externas e independientes a la organización, las políticas y procedimientos deberán estar formalmente documentadas.

En cualquier caso, independientemente de si una política se documenta por escrito o no, deberá establecer claramente las responsabilidades derivadas de la misma, las cuales recaerán en último término en la dirección de la organización y de las unidades de negocio en las que residan los riesgos. Los procedimientos deberán dejar claras las responsabilidades que asumirá el personal que lleve a cabo la actividad de control. De igual manera, las políticas deberán ser puestas en práctica de manera **consciente y meditada**, al tiempo que los procedimientos relacionados deberán ser llevados a cabo en el momento oportuno, con diligencia y con coherencia por parte del personal competente.

Los **procedimientos** deberán incluir el plazo en el que una actividad de control y cualesquiera medidas correctivas de seguimiento deban ser llevadas a la práctica. Los procedimientos que se lleven a cabo en un momento que no sea el apropiado podrán reducir la utilidad de la actividad de control.

A la hora de llevar a cabo la actividad de control deberán investigarse y, en caso oportuno, adoptarse **medidas correctivas** con respecto a los asuntos identificados para su seguimiento.

Una actividad de control debidamente diseñada por lo general no podrá ser gestionada por miembros del personal que no cuenten con las **competencias y con facultades suficientes para desarrollar dicha actividad de control.** El nivel de competencias requeridas para llevar a cabo una actividad de control dependerá de factores tales como la complejidad de la actividad de control y la complejidad y el volumen de las transacciones correspondientes. De igual manera, un procedimiento no será de utilidad si se lleva a cabo de memoria, y sin prestar la atención adecuada y de forma continua a los riesgos a los que se dirija dicha política. De igual manera, puede que sea necesario que el personal cuente con facultades suficientes para llevar a cabo todos los aspectos del control, incluida la adopción de medidas correctivas.

La dirección deberá **reevaluar de manera periódica las políticas y los procedimientos,** así como las actividades de control relacionadas para garantizar que se mantiene su eficacia y relevancia, con independencia de su capacidad de respuesta ante los cambios significativos que se puedan producir en los riesgos o en los objetivos de la organización. Los cambios significativos que se puedan producir serán evaluados a través del proceso de evaluación de riesgos. Los cambios que se produzcan en el personal, en los procesos y en las tecnologías podrán reducir la eficacia de las

actividades de control y hacer que en algunos casos sean redundantes y por tanto innecesarias. Siempre que se produzca uno de estos cambios, la dirección deberá reevaluar la relevancia de los controles existentes y actualizarlos según sea necesario.

La **información y comunicación** respalda el funcionamiento de todos los componentes del control interno. En combinación con los otros componentes, información y comunicación respalda la consecución de los objetivos de la organización, incluidos objetivos relevantes para la información interna y externa. Los controles existentes dentro de información y comunicación soportan la capacidad de la organización para utilizar la información adecuada y para llevar a cabo sus responsabilidades de control interno.

Un sistema de información es un conjunto de actividades, que implica tanto a personas, procesos, datos y/o tecnologías, que permite a la organización además obtener, generar, utilizar y comunicar transacciones e información para mantener la adecuada responsabilidad por la rendición de cuentas, medir y revisar el desempeño de la organización o el avance en la consecución de los objetivos.

3.8.2. Términos relativos al seguimiento y la revisión. [72]

3.8.2.1 Seguimiento.

3.8.2.2 Revisión.

3.8.2.3 Informe del riesgo.

3.8.2.4 Registro de riesgos.

3.8.2.5 Perfil del riesgo.

3.8.2.6 Auditoría de la gestión del riesgo.

3.8.2. Términos relativos al seguimiento y la revisión.

3.8.2.1 Seguimiento.

- DLE: m. Acción y efecto de seguir o seguirse (RAE de la Lengua).

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

---

72 Los comentarios de los apartados siguientes fueron elaborados por **D. Javier Álvarez**: 3.8.2. Términos relativos al seguimiento y la revisión; 3.8.2.1 Seguimiento.; 3.8.2.2 Revisión; 3.8.2.3 Informe del riesgo; 3.8.2.4 Registro de riesgos; 3.8.2.5 Perfil del riesgo y 3.8.2.6 Auditoría de la gestión del riesgo.

- Nota: El seguimiento se puede aplicar a un marco de trabajo de gestión del riesgo, a un proceso de gestión del riesgo, a un riesgo o al control.

a) Análisis a la Norma:

La Norma es confusa en su diferenciación entre Seguimiento y otros términos que van a ser utilizados con posterioridad de manera explícita, tal como revisión:

- En tanto seguimiento se define como "observación crítica", deja de ser una actitud pasiva a otra de aportación de criterio y opinión sobre la observación.

- Mientras tanto, define revisión como "idoneidad, adecuación", lo cual supone una actitud de aportación de criterio, lo que redunda en la definición anterior.

Es por ello que la aplicación de la Norma en estos conceptos queda a la discrecionalidad de diferencias asumidas entre uno y otro epígrafe. En cualquiera de los casos, ambas definiciones son substantivos derivados de verbos de acción, por lo que presuponen actividad sobre un objeto en el cual ejercer las mismas. Según expresa la propia norma, este objeto de seguimiento es un marco de trabajo, o un proceso, aplicados ambos a un riesgo específico.

Grandes diferencias pueden extraerse de uno u otro caso de Seguimiento:

- Por definición formal, marco se entiende (DLE) como conjunto de circunstancias o ámbito. En este mismo texto, también se define Marco como cerco o armadura que rodea algo. En cualquiera de los casos, parece clara una referencia al entorno exterior a algo. Es por tanto la norma una inducción a presentar riesgos como sistema abierto, que interactúa con su entorno, el cual le provee o al que suministra algo.

    - Admitiendo que riesgos es, efectivamente, un sistema abierto, son pocos los tipos de eventos, bajo cualquier taxonomía, que proceden del exterior. En concreto, sólo pueden identificarse como tales, riesgos catastróficos, reputacionales y estratégicos, cada uno de ellos de naturaleza bien distinta y de seguimiento bastante dispar.

    - Como quiera que la norma está ideada para facilitar su puesta en práctica, se supone que por marco entiende todo agente exterior que pueda influir o condicionar el desarrollo de la actividad.

        - Dado que catastróficos son denominados los riesgos sobre los que se desconocen, or el estado actual de la ciencia, sus componentes vectoriales (frecuencia/impacto/velocidad de propagación), se entiende que quedan excluidos de la norma.

        - Por el contrario, reputacionales y estratégicos son riesgos que involucran agentes y consideraciones de contexto, que influencian el diseño y

ejecución de la actividad, y cuyas componentes vectoriales son conocidas, en parte. Sin embargo, la posibilidad de Seguimiento de cada uno de ellos es bastante distinta:

·Reputacional es un riesgo de percepción (cualitativo y analógico), por lo que su seguimiento sólo puede efectuarse bajo métodos de toma de opinión y tendencia. Es de señalar que, por el contrario de prácticas del mercado muy enraizadas, reputación es riesgo en tanto afecte a colectivos que resultan de interés para nosotros, y que carecen de experiencia cierta sobre nuestras prestaciones.

·Estratégico es un riesgo determinista (cuantitativo, discreto de fracaso en objetivos propuestos), afectado por una serie de supuestos, por lo que su seguimiento ha de hacerse conforme simulaciones sobre ellos. Estratégicos son riesgos que se desenvuelven en la duda de lo posible, siendo por ello que exigen un tratamiento según Escenarios posibilistas. También la práctica del mercado ha degenerado y vulgarizado la utilización de este término y método de trabajo.

o Como quiera que la deducción etimológica de marco ayuda poco a tomar iniciativas, se entiende que la norma, en su petición de Seguimiento, interpretando su ambigüedad, se refiere al conjunto de prácticas de trabajo en gestión de riesgos. Para ello es necesario diferenciar la presencia de gestión, de la mera ejecución:

▪ Conforme a la Doctrina del *"Management"* mejor aceptada (P. Drucker), gestión se identifica allí donde una actividad cuenta con las funciones de planificación, organización y control para la misma. Entiende que estas funciones se conciben y un pitido rarísimo en acúfenos este aplica como sistema cíclico, con retroalimentación de cada uno de ellos en el siguiente y consecuencia del antecedente. Este mismo ciclo identifica liderazgo como cuarta función y central a la Gestión.

▪ Al contrario del pensamiento intuitivo, resulta bastante complejo encontrar estas tres funciones desarrolladas, según conveniencia, en las distintas entidades públicas o privadas. Mucho más difícil es encontrarlas en armonía de coherencia respecto a sus fines.

▪ Dado que planificación de riesgos es reflejo directo de las actividades de cada entidad y su criticidad respecto a vulnerabilidades, es evidente que toda organización ha de tener la propia. En consecuencia, la norma poco ayuda respecto a esta función, salvo apelar a su necesidad, sin mejor detalle.

▪ Dado que organización es consecuencia directa de la planificación que quiera llevarse a cabo, es imposible predeterminar aquélla sin haber estipulado esta última. En consecuencia, la norma poco ayuda respecto a esta función, salvo, de nuevo, apelar a su necesidad genérica.

- Es por tanto en indicadores (control) donde la norma apela como objeto del seguimiento, dado que ellos son necesarios en tanto se quiera adoptar cualquier gobierno sobre el devenir de los riesgos.

  - Gobierno es el acto continuado de repartir y ejercer autoridad, reflejado en la toma de decisiones, respecto a los riesgos tratados.

- También por definición formal, proceso es todo conjunto de actividades sucesivas. Dado que la mayor utilización del término obedece a Teoría de Sistemas, es en la misma donde se añade, para concebir un proceso, la necesidad de ser actividades repetidas y donde se produce alguna transformación de los elementos de entrada para obtener los de salida. Aunque ha habido muchas definiciones sobre calidad en procesos a lo largo del tiempo, todas ellas coinciden en que los atributos esenciales para la misma son eficacia y eficiencia.

  - Eficacia está referida a que el Proceso cumpla con las expectativas de su usuario o destinatario final. Estas expectativas siempre incluyen, en forma explícita o implícita, Tiempo de Respuesta.

  - Eficiencia está referida a los costes involucrados en activar y resolver el Proceso en toda su dimensión. Aunque éste es un atributo ignorado por el usuario (mientras no haya de costearlo), es de suma importancia para el ejecutante.

- Se deduce por ello que es eficacia el elemento diferenciador primario donde aplicar seguimiento, para posteriormente revisar la Eficiencia del mismo. Muchos son los Procesos que aparecen en cualquier marco de gestión de riesgos, siendo los más relevantes los de su ciclo lógico: Identificación, evaluación y tratamiento. Cualquiera que sean éstos y aquéllos, al final su acierto se mide por la fiabilidad de Indicadores de Riesgo que propicien su mitigación:

  - Los Indicadores recogen toda la labor desarrollada en todo el ciclo lógico y dictaminan sobre el resultado del mismo.

  - En tanto los procesos provean y actualicen Indicadores de Riesgo adecuados a la actividad desarrollada, son Eficaces respecto a la misma y a sus usuarios.

  - Los Indicadores, al igual que los procesos a los que se refieren, forman una arquitectura propia, que puede expresarse con la granularidad requerida a discreción.

- Recopilando lo anterior referido a procesos, se asume que, en su referencia, la norma sólo puede estar orientada a Indicadores, ya que ellos recogen la calificación de aquéllos.

Sin necesidad de revisar más el significado definitorio de la norma y por sentido utilitarista, este documento asume que el objeto paciente del seguimiento son los

indicadores de riesgo, como síntesis de la aplicación de cualquier marco y procesos. Como es fácil deducir, distintos Indicadores involucran distintos modos de seguimiento, tanto por la variabilidad de su expresión, como por la expresión y fiabilidad de su contenido y alcance. Esto es especialmente sensible en sistemas abiertos de riesgos, debido al comportamiento del entorno y la complejidad de su deducción.

Dada la dificultad etimológica de diferenciar algunos epígrafes presentados en la norma, el acto de seguimiento se ha estructurado en 2 componentes: establecimiento de indicadores y actores del seguimiento a ellos.

b) Criterios en la clasificación de riesgos:

Una parte esencial en el análisis de riesgos es determinar su naturaleza, origen o tipo de impacto para los principales de ellos. Sea cual sea la metodología de gestión de riesgos aplicada, la fase más crítica es adoptar algún método que asegure la identificación de todos los relevantes, dado que no hay mayor riesgo que aquél ignorado. Cuando una clasificación obedece a algún criterio útil, las posibilidades de eficiencia aumentan:

- En la fase de evaluación, en tanto permita identificar los elementos comunes de muchos de ellos, o acumulación de efectos y vulnerabilidades.

- En la fase de tratamiento, donde el tipo de clasificación aplicada puede ayudar a introducir efectos multiplicativos en las contramedidas.

De manera genérica, pueden encontrarse distintos enfoques de clasificar los riesgos relativos a cualquier entidad, tanto ésta sea de carácter público, como privado. Aunque no hay una manera universal de clasificación de riesgos, el enfoque más común que se encuentra en los textos es la definida para el sector financiero, dada la tradición de trabajos que sobre el mismo se han desarrollado. Como es de suponer, este enfoque tiene muchos inconvenientes para cualquier entorno ajeno a este sector. ISO 31.000 elude pronunciarse sobre algún criterio de clasificación, dejando el mismo a discreción de cada organización, en la consideración del tipo de riesgos que afronta.

La manera de clasificar resulta importante, porque de ella se deducen, o se interrumpen, las eficiencias y facilidades que pueden obtenerse en la gestión de riesgos global y, por ende, puede afectar al modo de supervisión y arquitectura de autoridad que se establece para la misma. Es habitual encontrar tres tipos de clasificaciones, por orden de frecuencia en el mercado:

- Por sus impactos: Es el método tradicional implantado por aseguradoras (según daños en activos distintos asegurables), lo que ha llevado a distintas agrupaciones de riesgos según han avanzado en su registro histórico y conocimiento. Carece de visión sistémica integrada, por lo que sólo puede tratar impactos individuales, perdiendo así eficiencia.

• Por eventos ocurridos: Es el método aplicado por el regulador para el sector financiero, por motivos utilitaristas al mismo, lo que ha arrastrado su uso en otros entornos, a pesar de lo específico de la casuística de origen. Carece de visión sistémica integrada, por lo que sólo puede tratar eventos individualizados. Incluso rechaza la consideración de alguna tipología de riesgos por considerarla ajena en sus fines (¿).

• Por sus causas: Es el método fundamentado en el entendimiento de la entidad como un "todo", por lo que presenta los riesgos según cadena de valor integrada de actividades. Facilita la identificación exhaustiva y en entendimiento de las dependencias mutuas.

Con independencia de la perspectiva anterior, la razón primera de cualquier clasificación de riesgos debería obedecer a las capacidades que tenga la organización para gestionar contramedidas de manera eficiente. Pero este principio ha de ser compatible con el aseguramiento en la identificación suficiente, sin el cual el resto de ventajas quedan viciadas.

Cuando una entidad falla al clarificar cómo ordenar los riesgos (taxonomía) según lo que se quiere alcanzar con su gestión, la asignación de responsabilidades en su tratamiento llega a ser muy deficiente, las prioridades mal ordenadas, los recursos mal asignados, y los indicadores poco alineados para la toma de decisiones consecuentes. La incertidumbre en que se desarrolla la actividad económica y social, así como los eventos inesperados que asaltan la vida cotidiana de entidades y personas, tienen su génesis en los defectos de clasificación de riesgos asumidos.

c) Indicadores de actividad (KPIs):

Por la falta de uniformidad en el criterio de clasificación, pueden encontrarse distintos Indicadores de riesgos correspondientes a lógicas distintas de agrupación, o relacionados de manera distinta en la agregación que, finalmente, identifica el apetito como sumatorio de los riesgos incurridos en cada momento, deducibles desde Indicadores previstos al caso.

Sea cual sea la lógica de clasificación de riesgos aplicada, lo importante es tener la mejor aproximación a una Identificación lo más amplia posible para todo lo que pueda ser relevante, así como la inter-relación de aparición que se pueda producir entre ellos.

De esta sencilla premisa última se deduce que los indicadores, para ser completos, habrán de corresponder a los distintos dominios de acción que, por naturaleza, cualquier entidad tiene o depende de ellos. Y es debido a esta naturaleza distinta de dominios, y su causalidad diferente, donde los objetivos de riesgo, y sus indicadores, pueden estructurarse y corresponder a la Cadena de Valor en los grados de detalle que, en cada momento, se considere necesario. En otros términos, los riesgos son un sistema reflejo de otro primario de actividades para la generación de valor, observa-

bles por sus propias magnitudes (KPIs), y los indicadores de riesgo (KRIs) han de ser fieles a este reflejo.

Tal como se ha enumerado, otras versiones de indicadores son comunes, según el sentido de taxonomía que se aplique a riesgos, pero se pierde entonces el sentido sistémico de los mismos, por lo que aparecen problemas de desorden, inseguridad sobre su exhaustividad y, en definitiva, problemas de control sobre riesgos no identificados.

Por la fuerza de mercado y efecto sistémico del sector financiero, y la relevancia que ha adoptado el regulador por defectos de otras prácticas, hoy la presentación de indicadores de riesgos que se admiten como formales presentan serios problemas de integridad, identificándose de forma parcelada, con escasa o nula conexión deductiva.

Desde cualquier perspectiva, los Indicadores de riesgo son los relativos a las desviaciones que presenten los objetivos de cualquier naturaleza perseguidos, por lo que es totalmente factible presentar aquéllos como porcentajes de deterioro respecto a éstos (%), a los que se conoce habitualmente como KPIs (*Key Performance Indicators*). Con ello, los porcentajes de desviación de las métricas operacionales pueden tomarse, en muchos casos, como Indicadores de riesgo factibles y exactos.

De esta manera se manifiesta la exacta relación biunívoca de arquitecturas entre objetivos operacionales (KPIs), ligados a la consecución de valor, y riesgos relativos a ellos (KRIs). También puede expresarse este aserto en el modo de que es imposible dominar riesgos cuando se ignora la arquitectura operacional de la que proceden. En otros términos, todo análisis de riesgos comienza por el entendimiento de contenidos y propósitos operacionales.

Cualquiera que revise los actuales inventarios formalizados de tipos de riesgos, basados en prácticas de exhaustividad dudosa, deduce fácilmente cómo muchas áreas operacionales han quedado huérfanas de consideración, por lo que muchos de aquéllos continúan ignorados. En este caso, el propio modelo de trabajo es un riesgo en sí mismo, aunque ignorado dentro de la dinámica finalista adoptada.

d) Key Risk Indicators (KRIs):

Si partimos de la conceptualización de que riesgo es toda incertidumbre (desviación cuantificada, favorable o negativa) respecto al propósito alcanzable de una acción (ISO-G73), resulta obvio que indicadores de riesgo son todos aquéllos que señalan desviaciones sobre objetivos explicitados de alguna acción. En definitiva, allí donde hay objetivos, y toda acción humana los tiene, hay riesgos e indicadores (implícitos o explícitos) respecto a ellos. Dado que la acción de cualquier entidad siempre está orientada a la maximización del valor (utilidad en casos individuales), la práctica de gestión de riesgos consiste en la sostenibilidad de esta maximización.

Aunque definiciones anteriores pudieran calificarse de evidentes y ajenas a toda aportación, la clasificación de riesgos y, por ende, la determinación de indicadores para ellos, da fe de las diferencias de concepción con que estos axiomas se tratan.

Si se sigue ISO G-73, riesgo puede ser descrito por un evento, un cambio en circunstancias, o una consecuencia. Bajo esta definición finalista de riesgo se enmarcan multitud de definiciones puntuales o sectoriales que pueden encontrarse en el mercado, donde el mismo concepto se presenta con énfasis en beneficios parciales, tales como evitar volatilidad, proteger contra disrupciones de actividad, u optimizar el retorno de una inversión.

Si bien la definición anterior de desviación sobre KPIs es acorde a prácticas suficientes en el seguimiento de riesgos para muchas entidades, siempre aporta una visión sobre hechos ya ocurridos o en tránsito, que reduce los tiempos de reacción. Es por ello que, en otros casos, se prefiere complementar esta visión KPIs de métricas ya alcanzadas o previsionales, con otras que informen con antelación de mayor alcance del valor posible que ellas tomarán. Como se denota en la descripción, se trata de identificar una situación cuando aún adopta un perfil de posible, antes de pasar a probable. Aunque la ciencia estadística utilice ambos términos con total indiferencia, la propia semántica explica sus diferencias de contenido y causalidad.

Por lo tanto, se busca así trabajar con Indicadores que identifiquen causas (*drivers*) de los valores finales que KPIs llegarán a registrar, anticipando con ello las posibles acciones de corrección que puedan efectuarse para reconducir éstos. Es así como aparecen los KRIs (*Key Risk Indicators*) como señales anticipadas de consecución o desvío de los objetivos operacionales. Como resulta definido, KPI tiene una dependencia cierta (directa o derivada) de KRI y, según sea la fuerza de esta dependencia (desde inducción, hasta implicación), KRI pronostica el sentido de evolución y alcance del KPI dependiente.

- Algunos autores definen KRIs como magnitudes de riesgo cuando sobrepasan el margen de variación permitido a ellos en el marco diseñado de actuación y los objetivos que se esperan del mismo. Ello sólo es una visión extrema de la definición anterior utilizada, dado que también son útiles como alertas intermedias anunciadoras de los resultados últimos más posibles primero, y luego probables.

- Otros estándares existentes en el mercado sólo incorporan el concepto KRI en el caso de supuestos estratégicos, lo cual asume que las prácticas operacionales se consideran como sistema cerrado de resultado fijo, carente de riesgo originado en el contexto (¿).

- Aunque KRIs adoptan la forma de variables (continuas o discretas) que toman distintos valores en el tiempo, donde lo importante es la tendencia, en ocasiones son entendidos como eventos. De hecho, la inquietud ante distintos eventos (trigger), por su repercusión futura, es una manifestación de KRI implícito y que tomará valores distintos, o con distinta frecuencia, a partir de entonces.

- En la práctica profesionalizada, KRI se estructura en distintos estadios de secuencia de hechos. Cuanto más cercano se identifique con el "hecho raíz-R",

más valioso resulta KRI, dado que otorga un mayor tiempo de identificación, preparación y reacción ante el evento emergente.

- De todo lo enunciado, es fácil deducir que la práctica KRIs es un impulso de adelantarse en el tiempo de reacción ante la variabilidad de KPIs. Además de este objetivo, la práctica KRIs también contiene otras aportaciones, si se saben registrar y ordenar con inteligencia, tales como análisis de tendencias y visión prospectiva de eventos, antes de que los mismos maduren y produzcan sus efectos. Esta prospección puede utilizarse para evitar daño, pero también para conseguir beneficio de ella al entender nuevas oportunidades en el nuevo entorno generado.

  Los indicadores de riesgo son específicos para cada entidad en cada período lógico de competitividad, dado que obedecerán a objetivos de sensibilidad, externa e interna, distintos en cada fase de desarrollo. La selección de KRIs, en cada etapa de competitividad, se convierte en el factor crítico de elección, dado que orientará la acción global de la entidad a favor de alcanzar sus objetivos. En general, cuanto más volátil sea el entorno, mayor complejidad (y relevancia) tienen los KRIs cuando son acertados. Lo contrario es igualmente cierto.

  KRIs se pueden diseñar y tratar de forma independiente o agregada, según la dependencia con KPIs quede mejor manifestada y ayude mejor a la toma de decisiones correctoras a tiempo.

e) Frecuencia de elaboración y seguimiento:

Más allá del diseño de contenido, KRI se cualifica por la oportunidad en la información de alerta que proporciona (tiempo de aviso).

Son múltiples los escritos y documentos formales que pueden encontrarse con el argumento de periodicidad de actualización y presentación de KRIs conforme a la relevancia de sus destinatarios en la organización.

- Según este enfoque, la frecuencia fija de KRIs abarca desde información en el momento de ocurrencia para mandos intermedios, hasta periodicidad de ella estructurada, de semanas o meses, cuando se escala en la organización.

- En realidad, esta determinación carece de sentido y, dada su aceptación en algunos estándares de mercado, demuestra la escasa tradición existente en el uso de KRIs como elementos para la toma de decisiones con urgencia suficiente. Es esta urgencia (por velocidad de propagación), y la severidad del riesgo, la que define destinatario y frecuencia de actualización en KRIs.

La frecuencia de actualización y contraste de KRIs ha de venir definida por la velocidad de cambio de cada uno de ellos, o su agregado, comparada con la urgencia para introducir medidas que compensen el efecto sobre KPIs que la magnitud del KRI anuncia.

- Por lo tanto, gestión de riesgos, consiste en un contraste y corrección continuos de velocidades entre Indicador de deterioro potencial y contra-efectos de las medidas paliativas para ello. Tan rápidas como sean las contramedidas, en activación y efecto, tan desactualizados pueden ser los KRIs. Y lo contrario también es cierto.

- Es la misión pues de la autoridad de cualquier entidad disminuir los tiempos de ejecución de medidas paliativas, de forma que puedan producir efectos suficientes que contrarresten al anunciado por KRI.

- En tanto la variación del KRI sea relevante para cuestionar el tipo o efectividad de las contramedidas ideadas para su efecto, es necesario conocer su magnitud. Mientras tanto, es innecesario activar alertas.

- La distribución de alertas para esta variabilidad del KRI dependerá de la magnitud de la misma y de la necesidad de autorizar contramedidas oportunas. Dado que las contramedidas involucran incurrir en costes de recursos, existirán distintos grados de ellas y distintas autoridades para autorizar su activación.

- Estas contramedidas han de formar parte de un conjunto de acciones previstas por anticipado (fase de planificación-respuesta a incidentes (IR)) en el establecimiento de objetivos e identificación de KRIs relacionados, junto con acciones deducibles.

- Por desgracia, la inestabilidad permanente del resultado operacional y, por ende, de su valor final en multitud de entidades, demuestra que IR es, en el mejor de los casos, una práctica administrativa si efectos correctivos.

En definitiva, el seguimiento a aplicar a KRI viene condicionado por la lógica expresada en el párrafo anterior relativa a variaciones del mismo respecto a impacto final en KPI, siendo por ello que puede presentar intensidad muy dispar según cada momento de actividad y fiabilidad en sus objetivos. En otros términos, las contramedidas determinan los KRIs a implantar.

f) Tolerancia:

Se define tolerancia como el margen de variación de KRIs admisible sin que los KPIs relacionados pierdan su objetivo de magnitud buscada. En definitiva, tolerancia son las variaciones admisibles de KRIs por su escasa afección a KPIs.

En general, su uso más común procede de las finanzas privadas, donde cada inversor es calificado como conservador, medio o arriesgado en su tolerancia a la variabilidad del valor de sus activos adquiridos.

La relación entre KRIs y tolerancia depende del contenido y significado de aquéllos:

- En general, existe relación indirecta entre KRIs y tolerancia, dado que son medidas de magnitudes distintas, pero relacionadas:

- Cuando KRIs está expresado en magnitudes relativas de desviación (%) sobre KPIs, tolerancia es el límite máximo superior admisible de su agregado.

- Cuando KRIs está expresado en magnitudes absolutas, su agregación es imposible, por lo que para relacionarlo con tolerancia habría que reconocer a ésta como función múltiple de los valores máximos de cada valor individual. Esta función se supone muy compleja y carece de significado y utilización.

• Es por ello que tolerancia siempre es una expresión de máximos, expresión de un conjunto de riesgos y contramedidas ideadas. El cambio de cualquiera de estas últimas, situación siempre esperable con las contramedidas por mejora permanente en la gestión, cambia la magnitud de tolerancia.

- Mayor tolerancia significa mayor capacidad de reacción ante eventos ideados o ciertos. Lo contrario también se cumple.

La tolerancia suele reclamarse cuando una entidad se enfrenta a situaciones límite de comportamiento de su contexto o de sus operaciones. Por ejemplo, la deficiente gestión de riesgos descubierta en tiempos recientes para algunos sectores muy sensibles a tolerancia, tal como es el sector financiero, ha venido a recomendar al regulador expresar y exigir la misma en forma de montante de capital. Esta definición de tolerancia tiene algún inconveniente en su aceptación directa:

• Capital es magnitud "stock", mientras que riesgos a los que responde es magnitud "flujo". Ello produce un comparativo temporal distorsionada, cuando menos.

- Rebasar o adecuarse a la tolerancia depende de la política de trabajo establecida y del control en las prácticas que se sigan sobre ella.

- Es indiferente el capital que en un momento se defina como tolerancia si las prácticas deterioran el mismo de manera continua y rápida.

• Tolerancia es resultado directo del tipo de contramedidas que preparadas para responder a riesgos en ciertos estadios de materialización. Fijar tolerancia en una magnitud fija supone que las contramedidas permanecen estáticas en el tiempo, lo que contradice la existencia de gestión continua de mejora sobre ellas.

• Tolerancia límite se equipara con capital, lo que produce una inmovilización de recursos y penaliza el rendimiento, dado que, raras veces, el límite se admite como escenario perdurable de trabajo.

En definitiva, la maximización del valor exige una gestión continuada de la función de multi-variables del riesgo, representada por los distintos registros de KRIs. Esta función, y su gestión, son distintas para cada entidad en cada período competitivo, dado que corresponde a mejor inteligencia sobre un riesgo dado, o mejor articulación de contramedidas, por cualquier motivo.

- Resulta simplista reducir esta diversidad y complejidad de situaciones (función de riesgos maximizada) con exigencias genéricas de capital.

- Cuando esta receta-exigencia de capital tiene repercusión, es muestra del escaso desarrollo y hábito existente en las especificaciones de gestión de riesgos.

Entre estas exigencias de máximos y mínimos de gestión, cada entidad se apalanca en su tolerancia como modo de sostenibilidad del valor entregable a sus accionistas.

g) Apetito de riesgo:

El concepto de apetito identifica la posición de riesgo en un momento dado en una entidad. En tanto en cuanto éste coincida con el deseado, debido al diseño de operaciones y disponibilidad de contramedidas eficientes, apetito aprobado y ejecutado convergen.

- Apetito ha de ser diseñado, declarado y aprobado de forma preventiva y oficial.

- Apetito se ha convertido en una exigencia formal de declaración en muchas entidades cuando presentan su situación y perspectivas de ejecución a analistas e inversores.

    - Curiosamente, ISO 31000 ignora tratar apetito, a pesar de su mención en otros estándares y su exigencia en cotizaciones públicas formales.

- Reducir apetito siempre supone costes añadidos, de retorno dudoso, u oportunidad rechazada, por lo que puede ser castigado por inversores y observadores de una entidad.

- Ampliar apetito puede ser muestra de inteligencia sobre los riesgos identificados, pero también muestra de incapacidad de idear contramedidas eficientes. En tanto es una magnitud declarada, es de esperar que solo se pueda justificar en el primer caso, por lo que cualquier evento fuera del mismo supone clara responsabilidad de gestión.

- Todo apetito por encima del declarado y aprobado es difícil de justificar.

Todo lo enunciado sustenta que la mejor medida del desempeño estaría en ligar resultado neto y apetito incurrido. Ello debería revisarse como tendencia lograda para evitar aleatoriedad y obtener evidencia de sostenibilidad eficiente.

Como puede deducirse, cuando apetito alcanza las dimensiones de tolerancia, la entidad opera en una situación crítica de resultados admisibles respecto a pronosticados. Para algún tipo de función de riesgos tratados, esta coincidencia de dimensiones puede engendrar fallos de continuidad.

h) Indicadores sumatorio:

Tanto tolerancia, como sumatorio máximo admisible de desviación de KPIs (o conjunto de máximos de KRIs), junto a apetito perteneciente a aquélla, por facilidad de trabajar con perspectiva de agregados, terminan siendo los elementos centrales de seguimiento en gestión de riesgos:

- Se elaboran informes, de periodicidad conforme conveniencia, sobre el estado de los mismos y comparación temporal.
    - Cuando menos una vez al año, corresponde al máximo órgano de gestión de cualquier entidad, la aprobación o cuestionamiento y ajuste de la magnitud de apetito y tolerancia admisibles y de trabajo futuro.
- Otros órganos de la organización, individuales o colectivos, actúan de responsables de mayor frecuencia en el seguimiento de indicadores que conforman apetito y riesgos concretos, así como de adoptar o aprobar las contramedidas preparadas para su mitigación o corrección. Es común utilizar las figuras de comités para estas prácticas de seguimiento.
    - Se ha proliferado en la idea de nominar comités ajenos al ejercicio de operaciones, por motivos de criterio independiente.
        - En realidad, sólo los involucrados en las operaciones conocen los defectos corrientes, subsanaciones y costes posibles de éstas, por lo que el comité queda a expensas de la opinión de aquéllos.
        - La existencia del comité es una salida simple ante un problema complejo, como es el de la gestión de riesgos distribuida.
        - La coincidencia de comités con eventos, tal como escándalos recientes, hará revisar los conceptos y prácticas efectivas de riesgos aplicados.
    - El supuesto de que los involucrados en operaciones evitan identificar riesgos en las mismas, indica la escasa tradición en debatir y analizar tolerancia y apetito.
- Normalmente, cada entidad establece un escalado de notificación y reacción, conforme las desviaciones (sobre KRIs/KPIs) toman valores preocupantes:
    - Se trabaja con un protocolo (actuación normalizada) según grados de desviación incurridos. Estos distintos grados, que representan riesgos ciertos, reciben distintas apelaciones o distinciones (colores) para mejor identificación, según organizaciones.
    - Se trabaja con un conjunto de contramedidas a adoptar (normalizadas-Incident Response-IR) según grados de desviación incurridos.

- El objetivo es actuar sobre riesgos antes de que los mismos se materialicen.

- Estas medidas están sometidas a condicionantes de velocidad comparada, antes enumerado (propagación vs cauterización).

- Cualquier contramedida tiene un coste (personas/procesos/equipos), por lo que su activación ha de ser comparada con el valor de KPI en juego.

i) Fuentes de información de KRIs:

Uno de los elementos más críticos para enraizar la gestión de riesgos en cualquier entidad es la credibilidad de KRIs tratados. Credibilidad que procede del entendimiento y claridad en la repercusión que ellos tienen sobre KPIs, así como de la forma de obtención de aquéllos. Es por tanto la transparencia de afección y obtención atributo imprescindible para conseguir la relevancia de atención, movilización y acción que se persigue con KRIs. Cualquier confusión en este entendimiento puede tener efectos trágicos, ya sea por sobre-actuación, retardo fatal, o inacción.

En muchas ocasiones, la situación que puede afectar a KPIs no puede venir definida por un único indicador KRI, sino por un colectivo de ellos. En otros casos, es preferencia de los observadores trabajar con un colectivo de Indicadores como elementos de contraste de una situación venidera. Cualquiera que sea la preferencia, la incertidumbre sigue abarcando multitud de espacios de la actividad humana, tanto individual como colectiva, por lo que la búsqueda de Indicadores de relación directa con eventos siempre es una tarea ambicionada.

- Tal es esta ambición, que la búsqueda de fuentes fiables de datos e interpretación ha venido en aumento en los últimos años desde todo tipo de Instituciones, tanto públicas, como privadas. Así han proliferado los pronósticos de opinión sobre situaciones venideras como método de ganar relevancia de marca.

- Al mismo tiempo, también han proliferado las revisiones posteriores del nivel de acierto de cada entidad pronosticadora, siendo sus conclusiones muy negativas, tal como los hechos demuestran.

    - El caso más relevante y cotidiano de desacierto es la inversión en Bolsa.

    - Otros hechos sorprendentes denuncian los defectos de las previsiones al uso.

En la era de la avalancha de datos *(Big Data)* la evolución de eventos está demostrando que no es la cantidad de registros donde se esconden los pronósticos, sino en la inteligencia de identificar aquéllos realmente definitorios de situaciones subyacentes *(Smart Data)*. Seguirá por tanto siendo necesario sustentarse en la opinión de expertos, hasta desarrollar la capacidad propia equivalente, la deducción de situaciones

futuras y su relación con KRIs entendibles. Es en la calidad y fiabilidad de estas fuentes donde gran parte de la incertidumbre que hoy atosiga al mundo, empresarial y ciudadano, podrá encontrar resolución hacia tratamiento de KRIs, para aquéllos que lo sepan gestionar como ventaja competitiva por conocimiento privilegiado.

Si bien esto puede parecer muy excusable en lo relativo al entorno exterior y sus afecciones, poco lo es en el interior, como prueba de multitud de riesgos que hoy no son analizables por falta de datos de eventos sobre ellos. Finalmente, la interconexión entre ambos espacios de riesgos queda desenfocada por falta de atención suficiente a las dependencias.

Mientras tanto, algunas entidades otorgan la potestad de actuación en riesgos a algunos de sus miembros, esperando que ellos mismos aprendan cuáles son los KRIs adecuados, en un proceso de prueba y error. Los defectos de objetividad, además de precisión, de estas situaciones han llevado a la necesidad de aplicar una opinión colectiva en el seguimiento de riesgos. Es así como se genera el proceso de revisión de riesgos.

j) La selección de los niveles de alarma y seguimiento:

Ser proactivo y previsor ante situaciones de riesgo es factible cuando los indicadores referidos a ellas están claramente delineados. Es por ello que KRIs han de tener un conjunto de características que fortalezcan su utilidad para los fines que fueron pensados. Es por ello que su sentido de anunciador de eventos, con suficiencia de reacción, ha de quedar claramente contrastado y consensuado. Una vez que los indicadores han sido determinados, la organización encargada de su seguimiento ha de establecer y validar los distintos niveles de alerta y reacción que semejante indicador puede adoptar. El esclarecimiento de estos niveles, junto a su grado de continencia, fuerza un análisis de equilibrio con las definiciones marco de apetito y tolerancia, el cual requiere de aprobación definitiva por el órgano competente.

Mientras KRIs ayuda a las organizaciones a combatir las adversidades haciendo previsibles sus resultados comprometidos, también hay distintas variantes por las cuales los Indicadores fallan en su cometido. Entre ellas, las más comunes son las siguientes:

- Dificultad en identificar KRI para cada riesgo analizado.
- Focalización insuficiente en las causas del riesgo y señales sobre el estado de ellas.
- Dificultad en el seguimiento de la gama de KRIs adoptados.
- Desligazón entre KPIs y KRIs.
- Desligazón entre grados de KRIs y contramedidas de reparación.

k) Quién ejecuta el seguimiento:

Supuesta una definición de apetito y tolerancia por parte de los órganos de gestión superiores, conforme a los intereses de cada entidad en cada período de evolución (algunas lo ligan al ciclo económico), se entiende por seguimiento la función de custodia o vigilancia del cumplimiento de ambos compromisos-límite.

- Se antepone que ambos conceptos han sido suficientemente explicados a los distintos involucrados en su seguimiento y que hay consenso y claridad en su método de obtención.

La acción de seguimiento merece ser asignada a aquel colectivo que, por razones de experiencia, mejor sensibilidad y criterio puede aportar al reconocimiento de niveles y tendencias que presentan tanto las magnitudes agregadas de apetito y tolerancia, como sus componentes intermedios.

- Parece obvio que nadie habrá de mejor sensibilidad y entendimiento de evolución previsible que los profesionales ligados con el desarrollo de la actividad cuyo riesgo se está observando.

- El tratamiento del riesgo viene a afianzar la consecución de los objetivos de la actividad desempeñada.

- Sin embargo, aparecen conflictos de objetividad en posiciones tan involucradas con las actividades y sus riesgos, dado que pueden forzar situaciones en defensa de criterios propios, por ocultación de inestabilidad.

    - Este supuesto indica una concepción del riesgo basada en apreciaciones, en lugar de indicadores intermedios indiscutibles.

- Esta búsqueda de la objetividad ha aconsejado desarrollar el seguimiento de riesgos en figuras paralelas a los propios ejecutores, tomando este paralelismo distintas formas.

    - Aunque esta evolución pertenece al supuesto de defecto de indicadores intermedios, es la de mayor aceptación en casi todos los casos.

    - El paralelismo de mayor uso ha sido el establecimiento de comités supervisores del riesgo incurrido, lo que redunda en suponer la necesidad de cruzar criterios personales. Esta figura de comité incorpora distintos inconvenientes:

        - Ralentiza los tiempos de respuesta, por la necesidad de presencia colectiva y acuerdo múltiple.

        - Diluye la responsabilidad individual al ocultarlo en una amalgama de protagonistas.

        - Con el tiempo, se han mostrado muy ajenos a la experiencia y sensibilidad, así como a la supervisión efectiva, que la materia tratada requería.

- Los inconvenientes naturales de actuar según comités han aconsejado una participación de los mismos según excepciones, donde sólo las situaciones de riesgo que rebasan estándares acordados son sometidas al conocimiento de órganos de gobierno superiores.

Sea la figura de seguimiento individual o colectiva, resulta bastante esperable que las situaciones de riesgo involucren la actuación de distintos protagonistas, por lo que la inclinación común es representar la participación de los mismos según un esquema RACI.

- RACI identifica para cada situación los protagonistas que deben tomar acción sobre ella, así como los que han de ser consultados e informados.

- RACI se convierte en un proceso de asignación de responsabilidades de distinto grado, conforme la distinta capacidad de acción de diversos miembros de una organización.

- RACI se convierte en el sistema de comunicación estructurado según urgencias distintas a atender.

- Conforme la suficiencia de tiempos de respuesta obtenidos, RACI se convierte en un testigo sobre la idoneidad del reparto de KRIs.

En la actualidad es discutido y discutible que se requieran figuras profesionales especiales para la gestión de riesgos en cualquier organización, supeditando la existencia de ellas al estadio de desarrollo y madurez en esta práctica que pueda encontrarse en la entidad.

3.8.2.2 Revisión.

- DEL: Del latín “revisio”. f. Acción de revisar.

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

    - Nota: La revisión se puede aplicar a un marco de trabajo de la gestión del riesgo, a un proceso de gestión del riesgo, a un riesgo o a su control.

a) Análisis a la norma:

En el uso del castellano común, revisión se convierte en una diferenciación etimológica sucinta respecto a términos anteriores utilizados en la misma norma, tal como seguimiento, por lo que su diferenciación resulta discrecional conforme a la oportunidad y hábitos de uso. Para la comprobación de semejante confusión, sólo hay que acudir a cualquier diccionario de sinónimos.

En todos (o mayoría de) los escritos profesionales que pueden encontrarse respecto a revisión en riesgos, la dispersión de contenidos es muy amplia, dándose la mayor frecuencia de aparición el referido al proceso de tratamiento de riesgos y sus distintas fases, aunque el mismo no forma "per se" un modelo de actuación.

- La propia definición de ERM (Enterprise Risk Management) exige para su existencia la presencia de proceso, principios y marco.

- No puede decirse que exista marco hasta que el proceso quede complementado por indicadores (o asignación de métricas).

- No puede admitirse que exista marco hasta que la estructura organizacional, para hacerse cargo de su custodia y corrección cuando necesario (gobierno), haya sido estipulada y sus actuaciones protocolizadas (escalado).

Dada esta confusión conceptual, lo mejor es acudir a la norma y revisar todo lo que su definición induce.

b) De la idoneidad y adecuación.

Monitorización y revisión deberían ser funciones planificadas como parte de cualquier proceso o modelo de gestión de riesgos. Los resultados de tales funciones deberían ser registrados y comunicados, tanto interna como externamente, según sean los distintos órganos de acción directa y responsabilidad de decisiones que se hayan establecido referidos a riesgos. Estos registros han de formar parte de la inquietud por la mejora constante, o la transformación, de la práctica de riesgos adoptada.

Como resulta entendible, Revisión tiene una doble existencia temporal: i) Por una parte, como re-estudio de adecuación del modelo de tratamiento de riesgos adoptado respecto a criterios actualizados que puedan producirse sobre el mismo, y ii) Por otra parte, como la acción de comparar los eventos ocurridos respecto a las expectativas establecidas en el modelo para ellos. En otros términos y siguiendo la definición primitiva, revisión es el registro y análisis de las desviaciones potenciales o reales, sobre los objetivos operacionales de actividad buscados.

Tomando de la norma las exigencias de idoneidad y adecuación, es obvio que un modelo como el enunciado puede sufrir defectos para cumplimentar éstas, por varios motivos:

1. Identificación insuficiente, errónea o ineficiente de los riesgos en curso, o deficiencia en conceptualización de ellos.

    - Este defecto comienza en el tipo de clasificación (taxonomía) aplicada a los riesgos, según se expone en apartados anteriores. Acudir a taxonomías de riesgos contra-intuitivas exige una utilización de epígrafes memorizados, con carencia de ligazón, integridad y continuidad causal entre ellos.

- En algunos casos, por motivos de simpleza, riesgos de una naturaleza están calificados de otra (Basilea-Crédito) para facilitar aplicación de criterios existentes o suavizar sus efectos (Operacionales). Cualquier revisión de la génesis de las regulaciones principales confirmará estos hechos.

- En otros casos (seguros), riesgos que se van identificando se agrupan bajo calificativos genéricos, tales como "Otros", prueba de orfandad con criterios previos del análisis, o insuficiencia definitoria de éste.

o La taxonomía utilizada se convierte en un riesgo en sí misma (riesgo de modelo), dado que es común olvidar o ignorar riesgos intermedios a cada uno de los grupos formados. De hecho, es habitual que el contenido de riesgos correspondientes a cada epígrafe utilizado cambie con el tiempo, lo que da idea de la inseguridad en su identificación. Esto es muy repetido en entidades aseguradoras.

o Con un modelo basado en el recordatorio de epígrafes autistas de tipo de riesgo, se pierde la perspectiva de la concatenación entre ellos, por lo que se ignoran los "efectos cadena". También se pierde la perspectiva de integración de riesgos para asimilar tratamientos.

o Existen algunas publicaciones donde, entidades de renombre, presentan un inventario de lo que ellas consideran "cobertura total" en riesgos. La comparación con una descripción somera de "riesgos por naturaleza de actividades rutinarias", demuestra que tal cobertura deja mucho que desear. La realidad de eventos es muestra redundante de estas carencias.

2. Evaluación ajena a sus verdaderas dimensiones de frecuencia, impacto y velocidad de propagación.

o A pesar del común uso del concepto de probabilidad en la evaluación de riesgos, el cálculo de la misma resulta cargado de subjetividad. Probabilidad es una percepción, de escaso rigor y, por ello, individualizada a cada opinante. Su agregación resulta imposible, por lo que es difícil contestar a la pregunta de riesgo total de una institución. Esta frustración debería impulsar el cambio de un método ampliamente divulgado.

o La propia definición básica de probabilidad, entendida como la relación entre casos ciertos y posibles, carece de aplicabilidad en riesgos al desconocerse ambos componentes.

- Igualmente, cuando la probabilidad se admite como muy alta, se confunde con dejación de funciones, dado que algo debería anteponerse para evitarla, incluyendo renunciar al riesgo.

o Es así que la evaluación sólo toma sentido cuando se refiere a frecuencia de un hecho. Para ello se requiere que existan registros histó-

ricos sobre la aparición del evento, situación difícil para algunos casos de ellos, hasta ahora ignorados o achacados al azar. Ello hace que el método predictivo por experiencia se vuelva obligado.

- Velocidad de propagación apenas cuenta con alguna referencia en todos los escritos sobre riesgos, a pesar de ser el factor determinante en el diseño de contramedidas.

- Cuando la gerencia de riesgos carece de registros para evaluar riesgos en curso o previstos, en sus 3 dimensiones definitorias, requiere adoptar proyecciones según criterio, lo cual necesita cercanía y conocimiento de los factores que influencian el evento.

- Esta situación de riesgos sin registros previos, condiciona una organización de supervisión y autorización para los mismos distinta a otra cualquiera basada en métricas objetivas.

- Es el conocimiento de riesgos, en cuanto a sus manifestaciones en origen, el elemento diferenciador de competitividad. Entidades de gran habilidad en identificar riesgos, serán las que mejor provecho saquen de especular o adelantarse a los mismos.

- Es este dominio de Indicadores y su fiabilidad el que dictamina el tipo de organización para custodiarlos. Por lo tanto, resulta rechazable admitir organizaciones-tipo para tratar riesgos, dado que depende del grado de inteligencia y dominio sobre los afrontados.

- En definitiva, la capacidad estratégica de cualquier entidad viene condicionada por su habilidad para identificar y gestionar riesgos.

3. Diseño de contramedidas insuficientes o deficitarias en su carácter de coste-beneficio.

- Cuando los riesgos quedan lejos de las actividades a las que afecta, es probable que las contramedidas sean escogidas de forma contradictoria con aquéllas.

- Las contramedidas son decisiones puntuales de activar un proceso que afectará a otros procesos operativos en uso y sus compromisos de prestaciones finales. Esta interacción de procesos necesita de una visión de equilibrio para impactar lo menos posible en el servicio comprometido. Sólo las personas que están cerca de los procesos comunes pueden entender dónde está el equilibrio buscado para no deteriorar el servicio al usuario final.

- Esta situación resulta aún más delicada en tanto las contramedidas tienen, además del carácter de efecto contra-riesgo, otro carácter de velocidad para resultar efectiva en el tiempo. Es así que el punto de equilibrio se muestra más complejo de identificar.

- Las contramedidas tienen un coste, por lo que el tipo de riesgos a asumir, en validación de sus contramedidas, depende del beneficio resultante de su aceptación.

- Todas estas circunstancias hacen que la organización aplicable a la gestión de riesgos ha de ser específica a cada entidad, en consideración de sus capacidades de contramedidas.

4. Indicadores deficientes, en concepto, detalle, o registro de velocidad, para alertar la presencia y evolución de riesgos.

- El atributo mayor para los Indicadores es que sirvan para la toma de decisiones oportunas. En tanto el tiempo y alcance de las decisiones son correctos, los Indicadores cuentan con un buen diseño. Lo contrario también es cierto.

- Aunque distintas ofertas de tecnología se presentan como contendoras de Indicadores fiables y últimos, el criterio humano resulta imprescindible para estos propósitos.

- Contar con Indicadores adecuados y orientados a las amenazas emergentes sobre los propósitos de las actividades resulta un factor diferencial en un entorno donde multitud de entidades desaparecen por incapacidad de reaccionar a tiempo.

- Estos Indicadores nunca son fijos, sino que en detalle o alcance varían con el tiempo, según las contramedidas se orientan en mayor eficiencia cada día.

5. Distribución de responsabilidad de supervisión de indicadores desequilibrada con los tiempos de respuesta buscados, las capacidades de cada asignado o autoridad funcional de alerta. Es lo que en terminología sajona se denomina "*ownership*", concepto menos aceptado en las referencias en lengua española al tener un significado de propiedad absoluta, rígida e intransferible, contraria al concepto de colaboración.

- El tipo de contramedidas a activar induce el tipo de asignación de supervisión a adoptar.

- Los eventos a contemplar y las contramedidas a activar necesitan estar codificados y determinadas en flujos preconcebidos. La organización operante en cada caso requiere estar entrenada en su participación y cometido, de forma que la actuación resulte inercial y fácil para los tiempos de respuesta buscados.

- Es por ello que la capacidad de responder a distintos riesgos, una vez que han sido identificados, lo que determina y limita el tipo de estrategias a adoptar en una entidad si quiere que la misma tenga alguna capacidad de predicción en operaciones.

Ni la norma, ni el Diccionario de la Academia incluyen en el concepto de revisión acciones consecuentes con su resultado, pero la lógica elemental implica que tales acciones han de formar parte imbricada en dicho concepto como respuesta a situaciones desviadas de sus propósitos. Se sobrentiende que es lo que la norma califica como "idoneidad".

- Como resulta obvio, revisar exige primero una selección de indicadores y determinación de sus correctos valores de comportamiento.

- Del mismo modo, revisar incluye contrastar que el nivel de tolerancia establecido para las distintas desviaciones de las variables críticas queda dentro del margen admisible respecto a los objetivos perseguidos.

- Sin ambas predefiniciones, la acción de revisar se convierte en un acto de opinión, sin referencias acordadas.

- Por lo tanto, lo que se revisa es el comportamiento de la actividad dentro de un rango de Indicadores anteriormente definido como admisible.

c) Los efectos de la revisión:

Establecidas las anteriores distinciones, revisión resulta esencial para monitorizar la exposición al riesgo, acordar el tratamiento de los excesos e identificar las oportunidades emergentes. Cuando un proceso de revisión se sistematiza, la organización puede beneficiarse en distintas facilidades inerciales de trabajo, tal como las siguientes:

- Mejora el proceso de toma de decisiones.

- Orienta, conduce y facilita la ejecución de la estrategia.

- Introduce visibilidad operacional en agregados claros.

- Impulsa la eficiencia en la auditoría Interna.

Los beneficios del proceso de revisión son suficientemente atractivos como para introducir el cuestionamiento de su logro. Este logro es mayor allí donde Revisión se aplica de una forma estructurada y disciplinada en sus componentes y protagonistas.

Por tradición e intereses corporativistas, un esquema de Gobierno basado en "tres líneas de defensa" se ha concebido como solución obligada de revisión-alarma-contención en riesgos.

- En realidad, nada hay que afiance el número de líneas idóneo, ni tampoco quiénes han de ser sus protagonistas. Esto último es aún más evidente en una tendencia regulatoria de involucrar con responsabilidades claras a los miembros del consejo de cualquier entidad.

- El esquema de las tres líneas es una inclinación, repetida en gestión de riesgos, de dictar el órgano antes que la función a desempeñar. Ello no sólo es contrario al sentido común, sino que también contradice cualquier diseño arquitectónico lógico de gobierno.

- Los desarrollos de gobierno de riesgos más actuales mantienen la figura de tres líneas como metafórica, usando la misma para destacar tres capacidades distintivas. Estas capacidades siempre están sustentadas en conocimientos específicos sobre los riesgos afrontados.

Revisión es un proceso formal, cuya estructura se solapa con la del modelo de tratamiento de riesgos creado. Así no sólo ejercita un examen solapado al seguimiento del mismo, sino que adecúa la dimensión y especificaciones de cada fase a las experiencias de suficiencia o escasez de indicadores, tiempos de reacción o capacidad de custodia oportuna (escalado). En caso contrario, se convierte en una formalidad burocrática.

Como ocurre en todo proceso, la criticidad de la aportación del mismo se afirma en cada una de sus etapas. Cuando los riesgos están mal deducidos en su identificación, el resto de etapas carecen de garantía suficiente. Una calificación de riesgos se entiende disciplinada cuando:

a. Procede de una taxonomía lógica, completa y causal en la clasificación de riesgos primaria, según el tipo de actividad empresarial analizada.

b. Se aplica una metodología común en el cálculo de las variables de ponderación del riesgo:

i. Frecuencia, impacto y velocidad de propagación son las variables de mayor aportación en esta metodología.

ii. Por el contrario de la práctica popular, posibilidad es apreciación subjetiva o indefinida de cálculo, por lo que su inclusión en el método de calificación adolece de rigor básico.

d) El modelo:

Un modelo es un método cuantitativo, sistema o aproximación que aplica teorías estadísticas, económicas, financieras o matemáticas y supuestos, para alcanzar estimaciones mediante el procesamiento de datos (Fed OCC SR11-7). Enunciado demasiado determinista para las posibilidades que lo cotidiano aporta. Es por ello que también se acepta que modelo es una representación simplificada de la realidad (SR11-7). Todos los modelos constan de algunos supuestos y aproximaciones en la enmarcación del problema a tratar. Conscientemente o no, vivimos y nos desarrollamos según modelos. Son los modelos los que nos fijan el entendimiento y aprendizaje de las experiencias simples y complejas de la vida. Los modelos son explícitos o implícitos,

pero condicionan nuestro comportamiento de manera constante, tanto en nuestras reacciones individuales, como colectivas y de empresa.

Es por ello que modelo de riesgos ha de partir, y tomar referencia, de la actividad que trata de evaluar. Y en la misma lógica, revisión depende del modelo de evaluación de riesgos aplicado, y debe seguir el método del mismo para ratificar o corregir sus consideraciones y resultados.

Sin lugar a dudas, puede afirmarse que las deficiencias en este paralelismo de modelos, y la complacencia con ellas de los responsables principales de multitud de organizaciones, han sido factores de gran influencia en las distintas crisis económicas y financieras periódicas y sus fallos de detección, a pesar de los recursos de Revisión constante involucrados:

- De un lado, los modelos de riesgo al uso, afectados por tácticas actuariales, hacen un excesivo énfasis en proyección de datos históricos, con relevancia aguda en los más actuales, suponiendo que estos mismos se repetirán en proyecciones futuras, con independencia del cambiante entorno. Ello ocasiona actitudes pro-cíclicas de escasa perspectiva.

- De otro lado, la gerencia de las organizaciones suele descansar en fórmulas apriorísticas ligadas al cumplimiento, tomando al mismo como tributo único o prioritario, aunque de escasa aportación en los objetivos finales y momento vital de la actividad.

- Finalmente, se abusa con facilidad de la traslación de riesgos al seguro, allí donde hay coberturas comerciales, con independencia de las alternativas de tratamiento y su repercusión en la obligada maximización del valor. La recuperación financiera del coste actualizado de un activo es una concepción limitada de su aportación al valor de su utilización.

El resultado de esta cultura de riesgos, entendida como iniciativa de gobierno escogida y predominante, es el rechazo del juicio y criterio individual de la experiencia implícita (no transformada en estadísticas), y debilitamiento de la responsabilidad individual y colectiva sobre aquéllos.

e) El concepto de madurez:

A pesar de la escasa tradición en evaluar entidades según su acomodo a los riesgos, distintas prácticas internacionales están enfatizando en que la información sobre los mismos forme parte de la comunicación formal que se presenta a distintos interesados. Dado que los riesgos es una afección de carácter individual, que depende de las ambiciones de cada entidad y sus capacidades de reacción frente a eventos, no existe, salvo desviación sobre objetivos, una medida estándar de común aceptación sobre la bondad en la sujeción de eventos.

Las discrepancias de concepción en riesgos proceden del retraso en la consideración de cualquier empresa como un conjunto de procesos de finalidad concreta. Es así que todo riesgo es un defecto en el funcionamiento de los mencionados procesos, y que se repara reforzando o rediseñando el mismo.

Es por ello que debido a que cualquier tratamiento de riesgos termina siendo un proceso, en su finalidad y modo de trabajo, son las calificaciones de proceso los métodos más habituales para evaluar las capacidades en la gestión de aquéllos:

- A cada riesgo identificado le corresponde una o varias contramedidas de mitigación.

- Las contramedidas son procesos, los cuales se componen de actividades repetibles que involucran a personas, tiempo y, en algunos casos, tecnología.

- Los procesos, cualquiera que sea su composición, son evaluados según eficacia (incluye tiempo de reacción y respuesta) y eficiencia.

La fiabilidad de un proceso, en cuanto a su comportamiento y resultados repetidos, es lo que se denomina estabilidad. Los grados de estabilidad de los procesos aplicados en una entidad definen la madurez de la misma.

- Es por tanto madurez la medida de mejor definición de la capacidad de tratamiento de riesgos de cualquier organización.

El concepto de madurez fue instaurado hace muchos años en el mundo empresarial por la Universidad de Carnegie-Mellon (US), siendo aplicado inicialmente a los procesos de desarrollo del software, con motivo de evaluar el rigor procedimental en la elaboración del mismo.

  - Desde entonces se ha convertido en un grado de evaluación ambicionado por muchas organizaciones para ratificar el rigor final de sus trabajos.

- Posteriormente, el modelo de madurez se aplica a multitud de contenidos, queriendo mostrar con ello la disciplina procedimental de trabajo aplicada para distintos fines.

- La práctica habitual es estructurar la madurez según 5 grados de perfección, según la garantía de reacción y el uso que de la misma se hace.

  - El estado de menor madurez es cuando existen reacciones aleatorias o individualistas, aunque las mismas sean correctas.

  - El estadio de mayor madurez es cuando la optimización del proceso repetitivo ha alcanzado su límite superior, por lo que debe dejarse al mismo en un estado de activación inercial (automatizada).

  - La práctica cotidiana en multitud de organizaciones demuestra que a mayor madurez, menor coste de atención, por lo que la eficiencia mejora con aquélla.

- Los estadios de madurez se consiguen por avance progresivo y secuencial, dado que demuestran grados mejorados de disciplina colectiva en el trabajo, lo cual nunca se improvisa.

Riesgos, como contenido fundamentado en procesos, es también un espacio tratable según grados de madurez, indicando con ello la estabilidad de las contramedidas aplicadas para cada caso.

En una descripción global, se pueden entender dos tipos de riesgos: Conocidos y desconocidos. Por lo tanto, los procesos aplicables de contramedidas estarán condicionados, en su atributo de eficacia, en dos condicionantes de tiempo: Tiempo de Descubrimiento y Tiempo de Resolución. A estas etapas temporales se suele añadir otra de Estudio Forense, donde se busca reducir los tiempos antes enunciados según mejor conocimiento de su casuística.

- Ambos condicionantes de tiempo han demostrado quedar muy lejos de las necesidades de garantizar la actividad sin sobresaltos.

- Esta deficiente situación demuestra que los procesos que constituyen las contramedidas son muy ineficaces para el fin por el que han sido adoptados.

- Esta realidad cotidiana de deficiencia en eficacia de procesos, es repetida por las noticias sobre eventos y desviaciones sobre objetivos con las que normalmente convivimos, demostrando un estadio genérico de madurez muy elemental (o incapaz), incluso en las entidades de mayor significación.

En definitiva, el método de la madurez es una aproximación sensata y útil en la valoración de la práctica de riesgos en cualquier entidad. A pesar de su larga tradición en el mercado para algunos contenidos, su aplicación en el espacio de riesgos es aún muy deficiente, por lo que debe incrementarse el esfuerzo sobre la misma.

Los órganos de supervisión de cualquier entidad deberían preocuparse y ser informados por el estadio de madurez para sus riesgos principales, tanto alcanzada como aspirada, de la organización de la que forman parte, entendiendo y cuestionando el avance que se quiere conseguir en el mismo. Por desgracia, esta información raramente aparece en los documentos periódicos que se publican para accionistas y otros colectivos interesados en una entidad.

- La madurez es una demostración de la capacidad de cualquier entidad en afrontar los riesgos que la afectan. Por la misma razón, es una definición de la predictibilidad de resultados que puede conseguir. Lo contrario, es el origen de la volatilidad, elemento común del desarrollo social y económico actual.

- Dado que los riesgos se renuevan con frecuencia, y que las contramedidas están sujetas a un esfuerzo continuo de eficiencia, madurez nunca es un evento, sino un proceso cíclico de aprendizaje y mejora permanente. Es en su responsabilidad sobre este proceso cíclico donde los órganos de gobierno identifican la información que resulta necesaria para desempeñar su actuación con solvencia profesional.

- Esta inquietud de solvencia es tan sensible, más allá de sus efectos legales y penales, que dichos órganos de gobierno suelen pedir ratificación de madurez propia a actores externos.

- Revisión por lo tanto ha de concentrarse en el avance sobre los grados de madurez que una entidad alcanza para sus riesgos de mayor impacto.

f) El órgano de revisión:

Aunque resulta común encontrar en muchos espacios de trabajo que se nomina, dota e institucionaliza, el órgano antes que su función, parece sensato entender ésta primero antes de aprobar aquél, aunque sólo sea para revisar el acoplamiento mínimo.

Una efectiva revisión es aquélla que ayuda al responsable último de una organización a verificar, de manera continua, que existe y se aplica un modelo o proceso para identificar, evaluar, priorizar y mitigar los riesgos más relevantes que afrontan. Este modelo o proceso siempre incluye una demarcación nítida, entre los distintos actuantes en el mismo, de responsabilidades y autoridad equivalente.

- Es responsabilidad de la propiedad de la entidad (Junta de Accionistas) definir, o al menos aceptar, los grados de apetito y tolerancia en que ha de actuar la misma.

- Es responsabilidad de la gestión definir los recursos con que el Modelo o proceso ha de contar, así como activar la atención constante al riesgo.

- Es responsabilidad del grupo de revisión comprobar la existencia y aplicación de método suficiente, dentro del marco de apetito y tolerancia, en el tratamiento de los riesgos incurridos. El método ha de incluir objetivos de riesgo y responsabilidades, así como métricas, contra-medidas y resultados esperados.

    - La responsabilidad de este grupo puede ser dividida en subgrupos más específicos, llegando incluso a la individualidad.

    - La adecuación entre las distintas asignaciones de personas o subgrupos y riesgos es parte del gobierno de la entidad que el propio grupo ha de, al menos, consensuar con la propiedad de la entidad.

- Todas las asignaciones anteriores, así como el método de trabajo aplicado y sus resultados, han de quedar formalmente documentados.

Cuando el grupo de revisión encuentra que el método de trabajo asignado carece de la capacidad de garantizar el tratamiento de riesgos, así debe comunicarlo a la Gerencia, con motivo de que sean paliadas las deficiencias de actuación detectadas. Diferentes organizaciones internacionales han desarrollado enfoques-marco que sirven de referencia primera para el desarrollo de método en revisión de riesgos:

- COSO, the Treasury Board of Canada Secretariat, o el Institute of International Finance son ejemplos de referencias útiles en la concepción global, aunque limitadas en sus coberturas de relaciones entre componentes.

- Para Sectores específicos también se han desarrollado algunas referencias útiles, tal como NAMIC (National Association of Mutual Insurance Companies) o Federal Reserve Board. Ambos casos han de ser tratados con cautela inteligente (sólo como ejemplo de alcance).

3.8.2.3 Informe del riesgo.

- DLE: Informe: m. Acción y efecto de informar. Descripción, oral o escrita de las características y circunstancias de un suceso o asunto.

- DLE: Riesgo: m. Contingencia o proximidad de un daño. Cada una de las contingencias que pueden ser objeto de un contrato de seguro.

- UNE-ISO: Forma de comunicación destinada a informar a determinadas partes interesadas, internas o externas, proporcionándoles información del estado actual del riesgo y de su gestión.

Aparece en el Diccionario de la Lengua Española una explicación del concepto de informe como una acción posible de ser ejercida de manera oral. Esta alternativa está desechada en el entendimiento formal del hecho de informar, dado que no deja posibilidad de trazado en la acción, salvo en el caso de grabación, lo cual presenta algunos problemas de fiabilidad legal en caso de conflicto.

Tampoco resulta acertada la definición que el Diccionario (DLE) hace del concepto riesgo, dado que lo circunscribe a aquéllos tratables por el seguro, lo cual limita mucho el espectro de casos considerados.

Dado que el Diccionario no ha incluido entre sus conceptos tratados la combinación de ambos términos anteriores, resulta de poca ayuda, o incluso confusa, la aportación deducible del mismo.

a) *Consideraciones a la norma:*

La norma introduce una matización en el hecho de producir informes que resulta aclaratoria para esta tarea: El destino de atención al mismo. Significa que la elaboración de Informes ha de hacerse en consonancia con el tipo de decisiones que han tomar sus destinatarios. Aunque evidente, este sentido en la elaboración de Informes pocas veces se nota considerado, abundando más el carácter estandarizado y genérico (contenidos comunes) de su cumplimentación. Es una muestra más del carácter de "clichés" con que la práctica de gestión del riesgo se está desenvolviendo.

A pesar de lo enumerado en anteriores párrafos, la orientación a la personalización hay que hacerla convivir con otros fines a los que los Informes han de servir. Entre ellos, de los más importantes son los requeridos por la comparación de registros a lo largo del tiempo para detectar y analizar tendencias, lo que obliga a cierta homogeneidad y continuidad en los campos y formatos tratados por los informes de riesgo.

Por todo este conjunto de considerandos, y guardando las exigencias primarias relativas a informe de riesgos y sus fines, tres perspectivas sobre el desarrollo del mismo merecen revisarse:

1. Su concepción individual.

2. Las exigencias del regulador para entidades cotizadas.

3. Contenido habitual del informe en entidades singulares.

A continuación, se expone el contenido para cada caso.

1. La concepción individual de informe de riesgos:

Conforme se ha expuesto en capítulos anteriores, riesgo es una magnitud vectorial (multidimensional) que, al menos, queda definido por tres características o dimensiones básicas: frecuencia, severidad y velocidad de maduración. Cualquier expresión de riesgo con alcance inferior a estas dimensiones es indeterminación sobre el mismo.

- Algunos autores evolucionados en el estudio de riesgos, incluyendo alguna referencia canónica, están tratando de forzar la inclusión de la dimensión "vulnerabilidad" en la consideración de cada uno de ellos. Pero resulta evidente que esta última dimensión obedece a las características del receptor de los efectos del riesgo (objeto), nunca a las particularidades del mismo (sujeto), y por ello no es generalizable.

Es pues función de los informes de riesgos elaborar y presentar a las distintas audiencias, y explicitar según estas tres dimensiones, tanto los eventos de mayor significado ya incurridos, como los que quedan en curso, así como las medidas tomadas para paliar o anularlos.

- La componente histórica de esta declaración tiene por motivo esclarecer el contexto de ocurrencias y capacidades de reacción.

- La componente de situación actual es una llamada a la toma, discusión o participación, de decisiones en marcha o preventivas.

El debate sobre los contenidos del informe de riesgos parece resuelto cuando los destinatarios forman parte activa del entramado operativo cotidiano de actividades, pues entonces su orientación ha de hacerse hacia la mejor eficiencia de involucración de aquéllos en las tareas de reconocimiento y reacciones a abordar frente a la incertidum-

bre de resultados en éstas. En este caso de audiencia, cuanta mayor precisión sobre la situación, mejor entendimiento y detalle en la respuesta buscada para la misma.

- La precisión del informe de riesgos viene definida por aquellas particularidades o detalles que ayudan a tomar decisiones a sus interesados.

Sin embargo, para audiencias ajenas a estos entornos de reacción frente a incertidumbre de actividades, tal como son accionistas y otros Públicos de observancia (*stakeholders*), se necesita encontrar un equilibrio entre la transparencia debida, concisión y relevancia para la opinión de aquéllos del mensaje a distribuir.

- Por el contrario de lo que mucha literatura profesional sugiere, prudencia en la información no coincide con ocultismo, sino con evitar alarmas artificiales.
    - En una reciente conferencia sobre Risk Reporting (ACCA), se encontró que 80% de los entrevistados entendía que cuando los informes de riesgos son voluminosos, buscan difuminar la criticidad de algún contenido.
    - Aun suponiendo exagerada la observación anterior, permanece la relativa a la usabilidad del documento.
- Más información no es equivalente a mejor información. El contenido a comunicar relativo a riesgos, tanto pasados como venideros, debe evitar presentar una maraña de anécdotas o generalidades que poco añaden al mensaje principal de acciones en marcha y esperanza de resultados, con calendario de sus efectos.
    - Para inversores poco sofisticados, cuantiosa información sobre riesgos es un indicativo de situaciones preocupantes, que es necesario entender.
    - Para inversores institucionales y analíticos, la percepción es contraria a la anterior.
- La información a presentar ha de ser suficiente para entender o cuestionar estas acciones en marcha respecto a los peligros a evitar, y proponer mejor orientación de las mismas, en caso de discrepancia.
- Debido a que la capacidad competitiva cada día se enraíza más en la habilidad para entender indicadores primarios de riesgos (drivers) singulares, la información ha de cuidarse de descubrir estas habilidades o su articulación, al menos en foros públicos.
- Sin embargo, otros métodos de identificación y acción sobre riesgos comunes pueden ser explicados en su tratamiento, dado que obedecen a prácticas de mitigación vulgares.
- Sin faltar a la verdad, los informes de riesgo en curso han de simular la recepción que pueden tener sus contenidos, especialmente para actores de la finan-

ciación, y anteponerse a las dudas que pudieran derivarse, mediante explicación convincente.

Con todo ello, resulta deducible que informe de riesgos (*Risk Reporting*) es una disciplina que está adoptando sus propios métodos en la época actual, manteniendo principios como los antepuestos, al tiempo que trata de aprender y responder a las exigencias de transparencia que eventos onerosos han agudizado. En caso contrario, el mismo informe, por sus efectos de confusión, es un riesgo a añadir sobre los que, supuestamente, informa.

Obviamente, hay un conflicto básico entre el tono positivista que toda Memoria anual quiere provocar y la naturaleza endógena de un informe de riesgos, que especula, con sentido pesimista, en la revisión de sus afirmaciones:

- Cualquier entidad evita dar la impresión de encontrarse sometida a mayores desavenencias que sus competidoras, o las deducibles de sus resultados inmediatos.

- La avalancha de regulación sobre riesgos ha orientado la atención al mero cumplimiento estático de ella, distrayendo otros análisis en riesgos más ligados a prácticas de trabajo, que es donde se producen las grandes perturbaciones sobre los objetivos buscados. Con ello, se propaga una cultura de "check-list" en lugar de reflexión y aprendizaje adaptable a amenazas y vulnerabilidades de cada caso.

Dado que riesgos es un componente reflejo del meta-sistema empresarial de funciones y, por ello, una práctica donde destacar, por aprovechamiento de tendencias sobre el resto de actuantes en un mercado, tomarlo como proceso a cumplimentar bajo el mínimo esfuerzo sólo produce carga burocrática, ignorando la diferenciación competitiva que puede aportar:

- Información de riesgos es una vía de desarrollo y depuración de la calidad gerencial. Es expresión de reconocimiento y dominio sobre la incertidumbre temporal.

- Información de riesgos es una vía de fuerza para adoptar prácticas sensatas en el tratamiento de activos críticos.

- A pesar de la fuerza de algunos interesados actores para condicionar la atención del mercado, cumplimiento no es un riesgo, sino una especificación de trabajo. Informar sobre cumplimiento debe ser tan inercial como expresar la arquitectura lógica de los modelos de trabajo según especificaciones de usuarios y clientes.

    - Con perfecto cumplimiento no se compite mejor, sino que se evitan multas, en el mejor de los casos. Un mercado sustentado en evitar multas es mejor abandonarlo.

- El único riesgo detrás del in-cumplimiento es cuánto tardará la autoridad en sancionarnos por el delito incurrido.

En definitiva, el valor aportado por la Gestión de Riesgos, tanto en su dimensión de daños como de oportunidades, está en demostrar su carácter preventivo y anticipado frente a eventos posibles. La muestra de sus efectos viene dada por situaciones de negocio que han sido aprovechadas por adelantamiento a sus efectos, o la estabilidad de rendimientos a pesar de las amenazas habidas.

Ello significa que riesgos forma parte de la diferenciación estratégica. Cuando los informes sobre riesgos toman la suficiente perspectiva, los mismos se incorporan a los diseños estratégicos de actuación, formando parte esencial de los casos a considerar y recursos a aplicar.

Es así que la información sobre riesgos ha de partir del entendimiento de la necesidad de grado (o límite) de movilización de la audiencia a la que se dirige, respecto al conjunto de acciones que puede ser necesario abordar. Para cumplir con este cometido, es recomendable establecer un escalado de detalle e información agregada, según sea el tipo de decisiones que el destinatario puede tomar y la reacción que se busca. Más allá de este detalle de escalado según alcance de la decisión a activar, la información de riesgos a elaborar ha de contar con los atributos de:

- Utilidad: Todo contenido en informe de riesgo ha de ser relevante. Información que resulte incapaz de estar orientada a la acción en las posibilidades de su receptor, bien sea por su carácter banal o por su tecnicismo, ha de ser suprimida en todo caso. Información clara y concisa es un requisito obligado para facilitar su contenido y comprensión.

- Oportunidad: Esta característica depende del tiempo de reacción de la organización. Es así que capacidades distintas suponen tiempos de reacción distintos, luego frecuencia de información también distinta. Ganar tiempo de reacción es el obligado ciclo de mejora permanente en la gestión de riesgos.

El resto de consideraciones son las debidas a la granularidad de la información a presentar, la cual viene determinada por el detalle de la variable que incentiva el riesgo. En tanto ese detalle de variable tenga visibilidad inmediata, más rápida y mejor reacción se puede esperar de su conocimiento.

Con todas estas consideraciones, hay un conjunto de contenidos que aparecen como imprescindibles en cualquier resolución de "*Reporting*" en riesgos:

- Identificación de riesgos críticos que una entidad afronta, preferible en texto llano y explícito.

- Explicación suficiente, aunque directa y concisa, del por qué la Dirección de la entidad considera determinados riesgos como críticos.

- Explicación suficiente sobre las contramedidas preparadas, o en acción, para mitigar los riesgos enumerados.

- Identificación (según las 3 dimensiones estructurales) de los riesgos emergentes.

- Explicación concisa de cómo la dirección identifica y evalúa riesgos en su actividad cotidiana.

2. La ciencia y regulación alrededor de informe de riesgos:

a) *La "ciencia" en reporting de riesgos:*

La gestión de riesgos y su "reporting" han sido elementos de atención intensa en años recientes. Si bien diferentes eventos han focalizado el estudio sobre los antecedentes y consecuentes de riesgos en la primera mitad de los 2000, la crisis financiera de 2008 ha puesto sus contenidos en la agenda prioritaria del regulador y de los inversores, preocupados por la inadvertencia de los eventos habidos.

La mayoría de guías y requerimientos para informes de riesgos han sido desarrollados a consecuencia de la última crisis financiera, pero ello ha tenido desigual aceptación dependiendo de los países involucrados:

- En US, la tradición se remonta hasta la década de los 70s, donde Security and Exchange Commission (SEC) ha solicitado, desde entonces para entidades cotizadas, una descripción detallada de los riesgos que afrontan.

- En Europa, la Directiva de Modernización de Cuentas (2003) indica que las entidades han de describir los riesgos que afrontan, tanto en su informe anual, como en resúmenes internos.

    - Alemania mantiene sus estándares especiales, más allá de la Directiva, sobre informe de riesgos (GAS 5).

    - En Reino Unido, el Código de Gobierno Corporativo (CGC) exige que, al menos una vez al año, se presente un informe sobre efectividad en la gestión de riesgos y sus procedimientos.

        - En 2013, *Financial Reporting Council* publicó un "papel de consulta" (FRC) donde propone una presentación integrada entre gestión de riesgos y control interno, e indicar las amenazas deducibles.

        - Si los cambios previstos en CGC siguen adelante, será exigible en el informe anual una explicación de evaluación de los principales riesgos y cómo los mismos son tratados en la entidad.

La crisis crediticia del 2008 terminó de concentrar el pensamiento del regulador en gestión de riesgos e Información sobre ella. Un conjunto de informes, desde *Financial Stability Forum* (2008), la Comisión Europea (2009), el Gobierno del Reino Unido (HM Treasury 2009), y otros en años inmediatos a la crisis, hicieron una llamada para mayor transparencia de riesgos en instituciones financieras.

La consecuencia fue un conjunto de nuevas guías, primero orientadas al Sector Financiero:

- IASB IFRS 7 sobre Transparencia en Instrumentos Financieros.
- Los requerimientos de acuerdos de Basilea III (Pilar 3 sobre adecuaciones de capital).
- Mejora de la Transparencia en Banca por la Financial Stability Board-2012.

En muchos casos, la preocupación por riesgos se ha plasmado en la creación de comités específicos a los mismos, para darles atención especializada. Pero como es sabido, el órgano no hace a la función, aunque cualquier versión de la misma acogerá. Es por ello que, a pesar de la proliferación de comités y nominaciones relativos a riesgos, tal como el regulador aconseja, la incertidumbre por incomprensión del entorno, resultados inesperados y problemas de solvencia siguen afluyendo con frecuencia preocupante.

La otra esperanza es que los trabajos ideados en Riesgos para el Sector Financiero terminen siendo adaptados y acomodados a otras industrias. Algunos Sectores están más expuestos que otros en cuanto a riesgos se refieren, pero, aunque los riesgos internos sean correctamente gestionados, ello no alivia su capacidad en "reporting":

- Todas las industrias desarrollan su actividad sometidas a condiciones de contexto que representan en sí riesgos, debido a su variabilidad. Estos riesgos son tratados como anecdotarios ajenos a los propósitos de rendimiento de la entidad informante y sus informes.
- Más allá del Sector Financiero, la industria extractiva destaca por sus riesgos afrontados e informes obligatorios.
- El sector farmacéutico tiene una larga tradición en elaboración y presentación de informes de riesgos.
- Aunque estas excepciones han tenido su origen en el daño potencial a terceras partes, en el futuro, el riesgo tendrá más contenido de previsibilidad de rendimientos, más allá de la revisión de reparaciones físicas.

b) *Las recomendaciones en España de CNMV:*

Aunque dictaminadas para Sociedades cotizadas, es fácil entender que las recomendaciones CNMV se convertirán en "mejores prácticas" para todo tipo de actor en el mercado local, incluido en Bolsa o no, ya que son referencias, aunque genéricas donde todo tipo de operativa puede enmarcarse, lógicas en la gobernanza de riesgos posibles.

En concreto, las menciones específicas a contenidos de riesgos se localizan en el obligado Informe de Gestión y, dentro del mismo, en los siguientes epígrafes (*ortografía original CNMV, salvo subrayado*):

- **Responsabilidad:** Los miembros de los órganos responsables de la elaboración de la información financiera de una sociedad garantizan que la información financiera incluida en las cuentas anuales ofrece la imagen fiel de la actividad y los resultados del periodo, mientras que el informe de gestión ha de contener una explicación fiel y suficiente de la evolución de la entidad, los factores que explican su rendimiento y los riesgos y oportunidades asociados con su actividad en el futuro.

  Por su parte, el comité de auditoría es el responsable de supervisar el proceso de elaboración y presentación de la información financiera regulada, entre la que se encuentra el informe de gestión. Por lo tanto, su misión respecto a este documento es similar a la que tiene en relación con los estados financieros. En particular, debe comprobar que contiene todas las menciones obligatorias y que además incluye la información suficiente para cumplir con su cometido.

- **Voluntariedad:** El marco de referencia no es vinculante. Por tanto, al respetar el principio de voluntariedad, se ofrecen una serie de comentarios y recomendaciones cuya aplicación se espera que contribuya a difundir una serie de buenas prácticas dirigidas a incrementar la comparabilidad entre entidades cotizadas y, en última instancia, a una mejor satisfacción de las necesidades de los usuarios de la información.

- **Pilar I. Objetivos del informe de gestión:** Además, el informe de gestión tiene como objetivo explicar los riesgos, incertidumbres y oportunidades a los que se enfrenta la entidad, que determinan su estado y rendimiento presentes y pueden ayudar a explicar su evolución futura.

  Por su parte, dentro de CNMV, el Comité Técnico OICV-IOSCO apunta en su informe que "una sociedad cotizada habrá de publicar, en términos muy generales, toda aquella información susceptible de influir en la decisión de inversión de un inversor". Este objetivo es muy genérico y podría resultar poco operativo en la práctica, porque conlleva la dificultad de seleccionar entre toda la información aquélla que es relevante. Por ello, se recomienda centrar el contenido del informe de manera que no se haya omitido ninguna información potencialmente importante para que los inversores, actuales o potenciales, formen su opinión sobre la entidad y fundamenten sus decisiones. Puesto que otros grupos de interés, además de los inversores, son también usuarios del informe de gestión, sus necesidades deberán también ser tenidas en cuenta a la hora de diseñar su forma y contenido.

  Este enunciado respecto al contenido, en principio tan amplio, se podría concretar en cuatro objetivos que deberán guiar la elaboración del informe de gestión por parte de la entidad cotizada. Dichos objetivos son los que siguen:

  1.2. Poner de manifiesto los riesgos, incertidumbres y oportunidades de la entidad. Puesto que la dirección y la gestión de cualquier entidad se realizan en un ambiente de riesgo e incertidumbre, el informe de gestión es el sitio apropiado para hacer constar los principales riesgos operativos

y financieros con que se enfrenta la entidad, para transmitir al usuario el grado relativo de seguridad con que se aborda la actividad desarrollada. De la misma forma, en el informe de gestión deben ponerse de manifiesto las oportunidades y ventajas que la entidad tiene y que puede aprovechar para obtener provecho en el futuro. El suministro de información prospectiva debe entenderse y asumirse en un contexto de riesgo o incertidumbre, y como tal debe ser revelada y explicada.

1.4. Presentar información relevante, fiable, comprensible, verificable, oportuna y útil para el usuario al que va dirigida. La información que se suministre deberá cumplir las características cualitativas de ser relevante y fiable. Además, debe redactarse de forma que sea comprensible por cualquiera que tenga conocimientos generales sobre la entidad y su actuación; contendrá información suficiente, oportuna y susceptible de contrastación si se trata de datos cuantitativos; y quedará justificada por la utilidad que suministre a los inversores, actuales y potenciales, así como al resto de los grupos interesados en la evolución de la entidad.

- **Pilar II. Contenido del informe de gestión:** Por lo tanto, cuando las medidas (por ejemplo el EBITDA, unidades producidas /persona, resultado recurrente) no estén definidas en la normativa contable, o cuando los indicadores puedan variar significativamente según quien los calcule (por ejemplo el ROCE, el capital regulatorio o la rentabilidad bursátil), se recomienda que la entidad: (1) explique por qué considera que es una magnitud relevante para que los inversores puedan comprender su situación financiera, resultado o flujos de caja; (2) describa su metodología de cálculo, las variables y datos que se han utilizado y su procedencia; y (3) concilie, si procede, dichas medidas con las magnitudes definidas en las normativa contable y que figuren en las cuentas anuales, o, de incluir factores o variables de naturaleza extracontable (unidades producidas/hombre, ventas por tienda, valor razonable por unidad de superficie…) que no sean o se hayan definido de manera distinta a otras similares de general aceptación, explique y concilie las diferencias con dichas medidas similares que sean de general aceptación. Adicionalmente, si la entidad decide cambiar la metodología o determinadas fuentes de obtención de datos, o discontinuar su publicación, deberá explicar las razones del cambio o discontinuación y adaptar los valores mostrados a efectos comparativos.

2.2.2. Cuestiones relativas al medioambiente y al personal (*afectados de riesgo*): Los usuarios de la información financiera valoran especialmente el conocimiento de determinados aspectos no financieros del desempeño de la entidad, entre los que destaca la dimensión social—con particular énfasis en el desarrollo del factor humano dentro de la empresa—y la gestión ambiental desarrollada. En ocasiones las entidades elaboran informes especiales y separados, confeccionados bajo la doble perspectiva descrita, con el fin de cubrir las necesidades de determinados usuarios. En esta guía no se van a tratar estos informes, que tienen su estandarización propia, sino la práctica que consiste en incluir dentro del informe de gestión indicadores y otra información elaborada para dar cuenta de los logros y dificultades de tipo social y ambiental.

Cuando la entidad incluya este tipo de información, deberá poner de manifiesto, al menos, los siguientes aspectos:

- Los objetivos, estrategia y planes de actuación en cada una de las áreas, haciendo referencia a los principales riesgos asumidos.

- Las actuaciones llevadas a cabo en el periodo, junto con los indicadores que contengan los resultados de la gestión realizada.

- La comparación con otros periodos o con los objetivos a alcanzar, explicando las mejoras logradas y las dificultades encontradas.

- Los planes y compromisos futuros, así como la probabilidad de que se lleven a cabo satisfactoriamente.

2.4. Principales riesgos e incertidumbres

La descripción de los principales riesgos e incertidumbres, ya sean de tipo operativo o financiero, a los que se enfrenta la entidad, debe formar parte del contenido del informe de gestión. Se deberá desvelar información relativa a, por un lado, la exposición de la entidad a los riesgos operativos, financieros, de precio, de crédito y de liquidez entre otros y, por otro, se hará mención, cuando sea preciso, a los objetivos y políticas de gestión de los riesgos a los que la entidad sea más sensible. Se recomienda tratar, al menos, los siguientes tipos de riesgos, cuando sean relevantes para la entidad:

2.4.1. Riesgos operativos.

A- Riesgo regulatorio

B- Otros riesgos de la explotación

2.4.2. Riesgos financieros.

A- Riesgo de mercado

A.1. Riesgo de tipo de interés

A.2. Riesgo de tipo de cambio

A.3. Riesgo de precio de los instrumentos financieros

A.4. Riesgo de precio de las materias primas

B- Riesgo de crédito.

C- Riesgo de liquidez (en la medida que no esté cubierto por lo tratado bajo el epígrafe 2.3 Liquidez y recursos de capital).

Al elaborar el informe de gestión, **se deberá desvelar aquella información referente a los riesgos más importantes** a los que está expuesta la entidad, en conjunción con las acciones previstas para mitigar los mismos. **La descripción de estos riesgos debería abarcar no sólo la exposición de la entidad a consecuencias negativas, sino también las oportunidades potenciales que puedan suponer.**

2.5. Circunstancias importantes ocurridas tras el cierre del ejercicio

Se recomienda que el informe de gestión recoja la información relativa a los acontecimientos ocurridos tras el cierre del ejercicio económico sobre el que se reporta. Éstos se definen como aquellos eventos, favorables o desfavorables, que tienen lugar entre la fecha de cierre del balance y la fecha en la que la publicación de los estados financieros es autorizada. Se pueden identificar dos tipos de eventos:

- Aquellos que proveen información de condiciones ya existentes en la fecha de cierre de balance. El efecto material de estos hechos sería el ajuste de magnitudes ya reflejadas en el balance (eventos que requieren un ajuste).

- Aquellos indicativos de condiciones que surgen tras la fecha de cierre del balance; que no modifican magnitudes consignadas en el balance, ya que dichos eventos no existían con anterioridad a la fecha de cierre del mismo (eventos que no requieren un ajuste).

La entidad debería centrarse en exponer únicamente aquellos eventos de carácter significativo, explicando las consecuencias que podrían tener en su evolución previsible, teniendo en cuenta la estrategia que se sigue para gestionar sus efectos, tanto si son favorables como si son desfavorables.

c) *Comentarios a la definición de CNMV:*

Resulta obvio que la doctrina elaborada por CNMV busca incluir la declaración de riesgos en la presentación formal y obligada del Informe de Gestión para entidades cotizadas. Los eventos de los que han sido víctimas muchas entidades cotizadas y el carácter de sorpresa que ellos han tenido sobre sus inversores, han puesto en duda la suficiencia de la información sobre riesgos estipulada. Algunas de las situaciones de ambigüedad informativa aún están pendientes de resolución judicial.

Es por tanto claro que un mejor desarrollo de especificaciones de información ha de ser exigido para evitar este elemento sorpresivo de evolución en entidades cotizadas. Cuáles son esas especificaciones forma parte del debate sobre panorámica de riesgos que se vienen enumerando desde capítulos anteriores.

Desde luego, la información requerida ha de ser relativa a las especificaciones de cada entidad, o suficientemente universal para la toma de decisiones sobre ella. En

la especificación que la propia CNMV presenta resulta evidente que sólo es aplicable, y de alguna utilidad, a entidades financieras que actúan bajo ciertas condiciones de mercado.

De nuevo, desde la taxonomía de una especie se define, o yerra, en su correcto entendimiento.

d) *Las prácticas de referencia:*

Más allá de las recomendaciones-doctrina de CNMV, resulta atractivo revisar qué utilización de la misma realizan entidades de presencia global las que, debido a su alta sensibilidad a la opinión de inversores, más diligencia aplican a la información sobre sus riesgos.

La característica común de todos los informes de riesgos de entidades singulares que pueden encontrarse en la actualidad es su falta de especificidad común. Significa que están diseñados con motivo de cumplir con el requisito de presentación, pero cuyo contenido siempre tiene un tono de diplomacia esperanzadora, cortesía de Relaciones Públicas, o autocomplacencia ratificadora.

Tanto analistas como inversores desearían encontrar en el informe de riesgos cuáles son las preocupaciones de los distintos directivos para cumplir con sus compromisos de medio y largo plazo, y cómo aquéllas son precavidas en el tiempo.

- Como cualquier acto de comunicación, el informe de riesgos ideal debería tener más imágenes que texto plano, explicándose en el mismo tanto los aciertos como las dudas de acciones pasadas y venideras.

- El informe de riesgos debería incluir cuál es el potencial de actuación de una entidad referido a los activos disponibles, para ser comparada con la utilización actual de los mismos. El sobre-dimensionamiento por infra-utilización es un riesgo de interés para cualquier destinatario de información, con motivo de poder evaluar los eventos ocurridos. El sentido contrario de la perspectiva también serviría para entender las necesidades añadidas a cubrir por inversiones.

En cierto sentido, se trataría de presentar una contabilidad previsional probabilística, con distintos grados de especulación según sean las reacciones de contramedidas que se pusieran en marcha.

- En 2012, ACCA (Association of Chartered Certified Accountants), al unísono con Long Finance and Chartered Institute for Securities & Investment, presentó una propuesta (Harris et al. 2012) sobre “Contabilidad Confidencial” relativa a incorporar la incertidumbre inherente en los guarismos presentados en los estados financieros.

- La recepción de la propuesta en instituciones de inversores fue tanto más positiva cuanta más criticidad había en el momento competitivo que la entidad abordaba.

Mientras esta concepción de transparencia toma raigambre en el mercado, el debate se cierne sobre el impulso a ella que ha de venir del regulador. Los esfuerzos por encontrar un estándar que pudiera cumplir con esta transparencia crítica están encontrando la oposición de los explotadores de información privilegiada. Sin embargo, según la inestabilidad continúa haciéndose preponderante en el desarrollo social y económico, la presentación de Estados Financieros Prospectivos de Riesgos se hará más necesaria. Es por ello que su puesta en escena dependerá de quién tenga la confianza suficiente en su propia de gestión como para ser transparente.

3.8.2.4 Registro de riesgos.

- DLE: Registro: Del latín regestum. m. Acción de registrar. Lugar donde se puede registrar o ver algo. Asiento que queda de lo que se registra. Cédula o albalá en que consta haberse registrado algo. Libro, a manera de índice, donde se apuntan noticias o datos.

- UNE-ISO: Registro de la información relativa a los riesgos identificados.

    - Nota: Algunas veces se utiliza el término “diario de riesgos” en vez de “registro de riesgos”.

a) Introducción:

Cada etapa en el proceso de gestión de riesgos merece ser registrada adecuadamente. Ello supone que tanto los supuestos de ocurrencia, como los métodos de identificación y evaluación aplicados, fuentes de datos, contrastes de fiabilidad y resultados, han de contar con un repositorio específico para cada caso, en la característica de que sean fáciles de cumplimentar, identificar su estado de contenidos y actualizar.

Es la acción de gobierno, que nace como respuesta a la concepción de los riesgos, la encargada de esta adecuación entre eventos, situaciones y registros. Varios son los criterios a aplicar, discrecionalmente, en el diseño y formato de los registros a adoptar, pero entre ellos, los de mayor importancia están referidos a:

- Las exigencias legales.

- Las especificaciones de procedimiento a cubrir.

- El coste de creación y mantenimiento de registros.

- La oportunidad de reutilización de registros.

b) La importancia de la formalización de registros:

Son múltiples las aportaciones que una formalización de registros incorpora en la gestión de riesgos. Entre ellas, las más importantes son:

- Dejar constancia de que el proceso global de gestión ha sido ejecutado.
- Facilitar la revisión del proceso y las decisiones incorporadas.
- Servir de base para el desarrollo del conocimiento compartido en la entidad.
- Hacer disponible el plan de mitigación de riesgos.
- Facilitar la trazabilidad de las decisiones y acciones tomadas.
- Impulsar la comunicación y socialización del plan de actuación sobre riesgos.

Tal como ha sido enunciado, el grado de detalle o extensión de cada contenido en estos registros está sometido a circunstancias concretas de cada entidad, por lo que no tienen sentido las generalizaciones. En cualquiera de los casos, la documentación relativa a cada etapa del proceso de gestión de riesgos debería contener:

- Los objetivos de la etapa.
- Las fuentes de información en que la etapa se ha basado.
- Los mayores supuestos aplicados en los análisis incluidos.
- La descripción de los distintos puestos y protagonistas involucrados (RACI).
- La decisión de acción que fue acordada.

La base de datos que registro de riesgos representa supone un cúmulo de aprendizaje posible sobre patrones de comportamiento de amenazas, vulnerabilidades y contramedidas. Ello permite que las habilidades de detección sean más factibles. Si estas deducciones pueden automatizarse, el universo de riesgos y acciones se simplifica o, al menos, se reduce.

c) El registro de riesgos:

Parece evidente que las exigencias de registros, si nos atenemos a la definición de ellos para riesgos, han carecido de atención suficiente en todo tipo de entidades. En caso contrario, el registro de eventos debería estar repleto del anecdotario de desviaciones que se producen respecto a los objetivos, bien sea por hechos inesperados, bien sea por fallos en el desarrollo de las tareas propias.

- De todos los registros a contemplar en la acción de gobierno, es el de riesgos el que actúa de referencia principal de todos los otros.

- Registro de riesgos es un documento o soporte formal que contiene todos los eventos posibles identificados, de manera acumulativa, en el ciclo de actividades de una entidad, que pueden impactar en los propósitos de ésta, globales o parciales.

Dos consideraciones pueden deducirse de esta definición anterior:

- Sólo son interesantes de contener en registro de riesgos aquellos eventos identificados que aún representen una amenaza para los propósitos de la entidad (riesgos actuales).

- Por motivos de análisis de eventos y comportamiento, o bien de facilidad y efecto de contramedidas, es recomendable mantener un registro histórico de riesgos, separado del anterior.

  - Por problemas de recogida de información, singulares entidades desarrollan un registro de simulaciones de eventos, dándoles una frecuencia acorde con la prudencia en la criticidad del activo a proteger.

En tanto en cuanto el registro esté codificado en el uso de sus términos más comunes, permitirá una cumplimentación rápida y repetida del mismo, lo que facilitará la percepción intuitiva de los contenidos y significados a tratar.

- Es por tanto el tipo de campo a considerar (dimensión) y su nivel de detalle (granularidad) lo que hace que el seguimiento del riesgo y su estudio se faciliten a través del registro.

- La dimensión y granularidad del registro deben servir no sólo por la distinta gradación de los riesgos en curso, sino también por el desarrollo de capacidades suficientes para hacerles frente. Esta última exigencia es la que condiciona las anteriores, por lo que se convierte en concepto diseñador del registro.

d) Por qué desarrollar y mantener registro de riesgos:

En multitud de ocasiones calificado como procedimiento burocrático y de escasa aportación práctica, hay varias razones estructurales en la gestión de riesgos que avalan la necesidad de contar con un registro formal para ellos. Entre ellas, las principales son:

- Proveer de un entendimiento común sobre los eventos potenciales considerados.

- Documentar las contramedidas ideadas según la identificación de eventos considerados, agrupando aquéllas por criterios de lógica simple.

- Formalizar una referencia permanente de trabajo en la función de notificación y "reporting" sobre riesgos, dándole homogeneidad temporal.

- Facilitar el uso de conceptos conocidos al referirse a campos del registro, mejorando la comunicación y entendimiento de la acción necesaria.

- Introducir un proceso sencillo de investigación y actualización de grados de riesgos y contramedidas, permitiendo un fácil seguimiento por los distintos actores involucrados.

- Identificar, de manera ordenada, el conjunto de atributos definitorios en cada uno de los riesgos en curso, tales como costes o responsables de ellos *("ownership")*.

- Ordenar la visión y atención a riesgos según algún criterio que se muestre útil.

Aunque la simple descripción del riesgo es muchas veces suficiente para su entendimiento y acción pertinente, hay circunstancias donde una detallada descripción resulta obligada por el tipo de contramedida que hay que activar en caso de aparición de aquél.

e) Unidades de medida a implantar en el registro de riesgos:

Por simplicidad de representación, ha sido común ubicar riesgos en un plano. Es por ello que lo habitual es la expresión simple de los mismos conforme a dos dimensiones. Aunque es claro que esta simpleza de representación presenta grandes problemas por ocultamiento de otras dimensiones cruciales, su aceptación se ha expandido conforme la preocupación por riesgos crecía.

También hay distintos criterios aplicables en la clasificación de riesgos, siendo común que cada autor seleccione alguno de ellos según sea el propósito de trabajo que le concierne. Desde luego, dado que gestión de riesgos involucra eventos posibles, la clasificación más elemental es aquélla que distingue entre sucesos conocidos y desconocidos. Algunos autores trabajan en riesgos maximizando el tipo de combinaciones que ambos conceptos pueden presentar.

- Para los eventos desconocidos, toda una gama de aproximaciones se recomienda para limitar la incertidumbre que ellos provocan.

- Entre los eventos conocidos, por Impacto es una clasificación que resulta muy común, por facilidades intuitivas y empíricas.

- La otra dimensión a utilizar en clasificación de eventos conocidos presenta mayores problemas:

    - Se busca una magnitud que sea objetiva y justificable en su determinación.

    - Se necesita una magnitud que permita trabajar con ella según operadores básicos, tal como la agregación o substracción.

- Frecuencia de evento consta de ambos atributos, por lo que resulta la magnitud escogida en las aproximaciones de análisis de riesgos más exigentes.

  - Incluso para eventos conocidos, frecuencia puede tener escasa historia como para ser representativa con su valor proyectado, por lo que hay que acudir a estimaciones calificadas por experiencia y predicción.

Es así que la otra magnitud más utilizada en la evaluación de riesgos es probabilidad. La fijación de esta magnitud resulta totalmente subjetiva, por lo que su determinación involucra una práctica de consenso y elaboración de considerandos claros y aceptables.

Con esta incertidumbre metodológica, los riesgos son clasificados según las Consecuencias que representan, lo cual suele concretarse en algún calificativo de gravedad variada. Esta expresión de gravedad puede obedecer a una naturaleza cuantitativa, semi-cuantitativa o cualitativa. Lo importante es diferenciar los riesgos y aplicar las medidas útiles para paliar sus efectos.

Desde luego, el calificativo correspondiente a cada riesgo formará parte de su identificación en el registro.

f) El contenido del registro:

Ni hay, ni debe haber, un formato obligado para contener el registro. Cada organización diseña el suyo con razón a cuál es su tradición y dominio en los casos de riesgos que ha de tratar y conforme a la premisa expuesta anteriormente (velocidad de identificación).

Sin embargo, sí parece obvio admitir que un conjunto de campos siempre va a presentarse, con independencia de los detalles secundarios que cada uno de ellos deba abarcar. Por lógica, estos campos siempre han de coincidir con:

- Listado y calificación de control del riesgo: Secuencia de codificación para revisar la aparición y orden de los riesgos tratados. Una descripción de sus causas e impactos predecibles. En concreto, sus campos serían:

  - Origen y originador: Identificación de la persona que propone el registro del riesgo, aunque este dato sea anónimo, salvo para el Administrador del registro. Fecha en que se produce la proposición.

  - Título del riesgo. Descripción breve y nemotécnica que sirve para localizar al riesgo dentro de cada grupo elaborado de trabajo, para actuar por criterios de homogeneidad.

  - Descripción del riesgo: Definición conceptual del por qué puede ser considerado como elemento de vigilancia en la actividad de una entidad.

- Categorización del riesgo:
    - Permite identificar al responsable natural de función de su custodia, así como quién puede ejercer un seguimiento normalizado.
    - Descripción literal de la naturaleza de riesgo.
        - Composición vectorial: Frecuencia, impacto, velocidad.
        - Exposición de la mitigación a desarrollar para el riesgo:
            - Acciones preventivas: Son aquéllas ideadas para reducir la frecuencia o reducir la severidad de su impacto.
            - Acciones de frenado: Son aquéllas planificadas que reduce la severidad inmediata cuando un evento ocurre.
            - Acciones de recuperación: Son aquéllas a tomar cuando un riesgo se ha materializado, y que permiten rehacer la actividad.
        - Los distintos responsables de las acciones anteriores (RACI) con detalle según exigencias de acción rápida.
            - Los recursos y reserva del presupuesto a involucrar en cada caso.
            - El calendario y la secuencia de tareas a poner en marcha.
        - "Status" de evolución en la implantación de controles y contramedidas. Detalles del mecanismo y frecuencia de revisión del "status".

Si bien estos campos anteriores son los más comunes de aparición en todos los registros existentes, presentan notables deficiencias debido a:

- Los riesgos incluidos obedecen a operaciones corrientes y apenas especulan situaciones de futuro, lo que indica una consideración estratégica apenas verbal.
- Casi nunca aparecen riesgos sobre supuestos del contorno exterior, tal como si las entidades vivieran en entornos aislados. Ello tiene una gran afección en cumplimiento.
- Casi todo el proceso aplicado al registro parece una revisión burocrática repetida y sin aportación sobre contenidos que todos conocen.
- Los debates que se incluyen están enfocados a mitigación, evitando revisar las actividades en marcha y su impacto en riesgos, lo que cuestionaría a muchas de aquéllas.

La conclusión es que hay muchos contenidos interesantes a incorporar en registro de riesgos, pero, como cualquier sistema, lo importante es tener visión de su eficacia y de

los problemas de actualización del mismo que habrán de ser abordados. Por lo tanto, más importante que contenidos, es la arquitectura sobre la que se construye registro de riesgos. La casuística de vulnerabilidades a cubrir, volatilidad de amenazas, inestabilidad de métricas y cambios operacionales determinan un equilibrio de eficacia y arquitectura muy complejo en ocasiones.

g) El Plan de acción:

Incluido o separado del registro de riesgos, el elemento más relevante es el plan de acción sobre el mismo.

- Lo importante es asegurarse que registro se convierte en la declaración de las métricas a alcanzar en la mitigación del riesgo, por lo que el mismo contiene un compendio de plan de acción para alcanzar las mismas, cuando éstas están en falta.

- Como todo plan de acción, éste contiene los responsables de participar en cada tarea diseñada en el mismo, así como la secuencia de ellas y su duración, a favor de las métricas buscadas.

- Cuanto mejor conocimiento del mencionado plan de acción, más fácil y adecuada puesta en marcha, por lo que la discusión entre sus involucrados para la elaboración del mismo resulta imprescindible.

El registro-plan de acción ha de ser exigible y auditable, por lo que alguna plasmación documentada ha de presentar. El conocimiento implícito resulta insuficiente en estos casos. El contraste de auditoría, sea externa o interna, sólo podrá verificar la existencia de componentes, alineamiento con otras funciones en marcha, y consenso suficiente, como el antedicho. Revisar la cobertura de casos límite también forma parte del contraste de auditoría. Es por ello que la práctica de Continuidad de Negocio y Recuperación ante Desastres, con otras denominaciones similares, han contado con la mejor tradición desde largo tiempo atrás.

3.8.2.5 Perfil del riesgo.

- DLE: Perfil: m. Postura en que no se deja ver sino una sola de las dos mitades laterales del cuerpo. Contorno de la figura de algo o alguien. Conjunto de rasgos peculiares que caracterizan a alguien o algo.

- UNE-ISO: Descripción de cualquier conjunto de riesgos.

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

a) Comentarios a la norma:

De nuevo, la norma resulta muy genérica y escasa como ayuda para enmarcar e instrumentalizar el concepto de perfil, por lo que un nuevo desarrollo se hace necesario para cada caso concreto.

b) Definición:

Se define perfil de riesgo como la representación, cuantitativa o cualitativa, en un momento del tiempo, de la exposición total de una entidad o persona a cierta gama de riesgos. Toda entidad, por el hecho de estar activa, encara un conjunto de riesgos. La primera iniciativa lógica para con ellos es realizar un inventario de su existencia y diferente significado de cada uno como impacto posible. Este es el contenido de perfil de riesgo.

c) Declaración del Perfil de Riesgo:

A pesar de su tradicional conceptualización y fácil entendimiento, Perfil de riesgo extrañamente aparece en presentaciones formales de entidades (*Estados Financieros y Memoria de Gestión*), con independencia de la naturaleza de éstas. Es por ello que la mejor recomendación para establecer uno propio es identificarse, de una manera simple, respecto a este requerido Perfil, según los mercados van entendiendo la relevancia de su significado y exigiendo su declaración. Esta revelación de Perfil ha de ejercitarse siguiendo 4 epígrafes complementarios, tales como sigue:

1. Inventario global: Relación y descripción de riesgos prioritarios por naturaleza, incluyendo el carácter actualizado de los mismos en forma ordenada, según materialidad, ya sea como Amenaza, o como Oportunidad. Esta relación exige cierta inteligencia en el modo de estructurar su presentación para hacer sencilla su comprensión y ayudar a la enumeración sin olvidos.

- Siendo coherentes con definiciones previas, los riesgos que se afrontan dependen de la variedad y complejidad de actividades que se acometan.

- Ligar actividades, en cuanto a dependencias entre sí, ayuda a dilucidar concatenación de riesgos.

1. Categorización: Expresión vectorial (factorizada en sus componentes-frecuencia/ impacto/velocidad) de los riesgos asumidos (incluidos en apetito), con expresión clara de su magnitud (cuanti-cualitativa), así como los grados de tolerancia admisibles para cada uno de ellos.

- En ocasiones, esta clasificación se hace por tipos de activos, escenarios de afección a los mismos y posibles amenazas, simples o combinadas, en esos escenarios.

- La lista de riesgos que una entidad afronta puede ser desbordante para cualquier tipo de gestión. Una manera de hacer esta lista manejable consiste en clasificarla en categorías que permitan acciones homogéneas sobre ellas.

2. Contramedidas diseñadas para los distintos riesgos de mayor relevancia, incluyendo la madurez definida de cada una de ellas. Capacidades requeridas para mejorar la madurez y tiempos estimados para ello.

3. Interdependencia de riesgos principales respecto a la cadena lógica en que pueden presentarse, y multiplicadores esperados en la aparición de los mismos.

- Aunque es común la familiaridad de los integrantes de muchas organizaciones con riesgos y su eventualidad, menos común resulta entender la dependencia entre ellos.

- En especial, esta falta de visión integrada se manifiesta en mayor escala en la relación entre riesgos estratégicos, de operaciones y de proyecto, principalmente cuando estos últimos vienen a substituir la presencia de aquellos primeros y segundos.

- Estas substituciones siempre añaden un Riesgo de Cambio en su aparición.

4. Vulnerabilidades, consecuencia de la descripción anterior, e impacto potencial de amenazas, con calendario referido a cada impacto posible, cuando se presenten de forma colectiva.

- Las amenazas siempre aprovechan vulnerabilidades. Una campaña de amenazas es un conjunto de escenarios que se presentan conjuntamente en afán de un objetivo común (APT-Advanced Persistent Threat). El Perfil de riesgo de una organización incluye esta información de APTs y sus contramedidas.

5. Respuesta a Incidentes (IR), entendido como el conjunto de protocolos y planes de actuación que hay que poner en marcha en el caso de ocurrencia de las amenazas anteriores de mejor visibilidad. Incluye situaciones de Crisis. En algunas organizaciones, un protocolo de este tipo se denomina Plan de Contingencias.

Perfil de riesgo puede ser definido para un Departamento específico, entidad o sub-entidad de una organización global, o para la totalidad de la misma, y, desde luego, admite el agregado en tanto el Perfil venga expresado en magnitudes sumables. Lo importante en Gestión de Riesgos es localizar el Perfil y sus custodios allí donde se toman, o pueden tomar, las decisiones que afectan al mismo.

La clave de descripción del Perfil no es tanto la posibilidad de identificar un conjunto de riesgos y acciones en marcha, sino hasta qué punto la presentación de riesgos formulada al inicio está estructurada en forma tal que se induzca en coherencia la toma de decisiones sobre ellos.

Muchas entidades trabajan en la actualidad definiendo el Perfil deseado, lo que significa alcanzar las capacidades que posibilitan desarrollarse y encarar un conjunto de riesgos conforme a escenarios hoy imposibles por defectos en aquéllas.

En el posicionamiento de Perfil, por dominio de las capacidades para hacerle frente, se ubica una de las posibilidades de diferenciación competitiva más impactante.

d) Consideraciones para establecer el Perfil de riesgo en cualquier entidad:

Más que un acto declarativo y voluntarista, Perfil de riesgo responde a un modelo de trabajo, entendido como ciclo permanente de ajuste por aprendizaje, que cada organización tiene vigente, en tanto está activa. Este proceso cíclico ha de contener, al menos, las siguientes etapas lógicas de consideración:

1. Identificar riesgos de forma exhaustiva: Significa introducir un marco suficiente para enumerar y determinar los distintos tipos de riesgo a los que una entidad está sometida. Sólo es posible llegar a esta exhaustividad bajo un epígrafe totalizador de la actividad, para asegurar cierta plenitud en la enumeración.

2. Entender las inter-relaciones de riesgos: Significa tener una traslación correcta de cualquier tipo de riesgo por naturaleza, en aquéllos otros que se generan a partir de los anteriores. Consiste en expresar los riesgos en tal forma que haga factible realizar sumatorios de presencia y efecto de cada riesgo individual apercibido. Esto obliga a trabajar con frecuencias y desechar el registro de probabilidades.

3. Localizar la inteligencia: Significa la capacidad, por área o unidad, de la organización para detectar y evaluar cada riesgo actuante. Habilidad que hay que multiplicar en cada uno de los puntos donde existen vulnerabilidades con posibilidad de acceso, o sensibles a riesgos provocados por la interacción con el exterior.

4. Clarificar las interfases entre las distintas áreas donde se han localizado riesgos: Significa que resulta común que varios riesgos se ubiquen en diferentes actores o distribución dispersa, lo que requiere aplicar una visión horizontal de procesos finalistas, desde inicio hasta cliente, para revisar su exposición.

5. Actuar conforme a expectativas: Significa que, además de las respuestas por relevancia de exposición, en ocasiones es necesario actuar sobre elementos no prioritarios por el hecho de alarma social que sobre ellos se produce, con independencia de su impacto potencial real.

Perfil de riesgo es pues una magnitud dinámica. Quiere decirse que cada entidad está ajustando continuamente su perfil a través de la mitigación o transferencia del incurrido, hasta que consigue alinear la organización con el deseado y comprometido. Este Perfil viene definido por la capacidad de reaccionar, si necesario, al mismo. Los

controles a desarrollar en indicadores de riesgo, tiene como fin revisar la estabilidad del Perfil comprometido.

e) Taxonomía de riesgos:

A pesar de toda la inestabilidad de resultados y comportamientos habida en los últimos años, los riesgos siguen padeciendo una alta discrecionalidad de clasificación de origen. La importancia de ello resulta evidente dado que, desde ella pueden estructurarse los sistemas de acción común a desarrollar sobre un conjunto de riesgos, logrando así una mejor eficiencia de acción y aprendizaje.

En términos generales, está admitido que los riesgos pueden clasificarse según 3 elementos de consideración: Sus causas, por eventos, o por sus impactos. Hasta ahora, las razones de escoger uno u otro criterio de clasificación han venido remitidas por los hábitos y facilidades de prorrogar prácticas de trabajo existentes:

- El sector bancario ha escogido para su clasificación de riesgos el criterio de Eventos.

- El sector asegurador siempre estructuró su actividad según impacto de Daños habidos.

Dada la profunda reestructuración a la que se ha visto abocado el Sector Bancario, la Regulación se ha multiplicado sobre la actividad del mismo, con lo que una específica definición de riesgos se ha acompañado al desarrollo de la legislación. Esta definición ha sido tomada como referencia esencial para muchos Sectores ajenos al tratado.

Siguiendo los métodos aplicados al Sector Bancario, el de seguros ha visto actualizarse su legislación en los últimos años, con adaptaciones a su marco de trabajo propio. Ello ha provocado que la clasificación final obedezca a la naturaleza anteriormente ideada para Banca, forzando los criterios aplicados a seguros.

- Tanto el sector bancario como el asegurador han recogido una legislación relativa a sus riesgos cuya finalidad es dotar de capital de actuación suficiente en caso de materialización conjunta de los mismos.

- Esta dotación de capital tiene así una finalidad de capacidad de respuesta ante eventos posibles, pero ajena a la maximización del valor al que la gestión de riesgos obedece.

Con todas estas iniciativas actuando sobre el mercado, lo común hoy es encontrar una clasificación de riesgos según los siguientes epígrafes:

- De mercado: Suele ser el grupo adoptado para agrupar a los riesgos genéricos de contexto que afectan a todo el conjunto de entidades actuantes en una industria concreta. Suele tener, por igual, un carácter de oportunidad. Todo tipo de supuesto genérico puede encontrarse en este epígrafe, por lo que obedecen

a naturaleza especulativa (what-if). Muchas entidades financieras han tenido, y tienen, parte de su negocio sometido a esta especulación, habiendo sido, y siendo, sus efectos catalogados bajo otro epígrafe distinto al de mercado (financieros). Ello ha contribuido a distorsionar una clasificación de riesgos basada en criterios claros por tipo de negocio, en lugar de contenido afectado.

- Operativos vs Financieros: Suelen tratarse de forma independiente, a pesar de obedecer estos últimos a las mismas exigencias de rigor de actuación que los primeros cuando carecen de la faceta especulativa enunciada anteriormente.

    - Sólo en caso donde finanzas es un negocio por sí mismo, con especulación cotidiana, tiene sentido la separación de tratamiento de ambos.

    - A pesar de su abundamiento de publicaciones, Finanzas de soporte obedece a los mismos criterios de predictibilidad, madurez y error que cualquier otro riesgo operacional.

    - Solo en el caso de Finanzas especulativas tiene cabida y sentido aplicar prácticas más ligadas a supuestos de ocurrencia, tal como ocurre en riesgos Estratégicos, los cuales, siempre se trasladan a operacionales para facilitar su gestión.

- Continuos vs Eventuales: Es una clasificación aclaratoria por sí misma, relacionada con el período de amenaza en que puede materializarse.

- Catastróficos vs Discretos: Suele ser una clasificación complementaria y eventual respecto a las anteriores para referirse a aquellos riesgos donde su desconocimiento de origen o evolución hace que las contramedidas sean ineficaces o inexistentes, siendo sus efectos dejados al azar.

Con independencia de los criterios seguidos para algunos casos específicos, cada entidad debe adoptar su propia aproximación y categorización de riesgos, en tanto cumpla con 2 condiciones esenciales:

- Asegurar que la Identificación de riesgos es completa, incluyendo su efecto agregado.

- Multiplicar la eficiencia de diseño y aplicación de contra-medidas.

f) Construcción del perfil de riesgo:

A pesar de la claridad de las consideraciones para su establecimiento, la construcción del perfil de riesgo puede encontrarse con dificultades de análisis o síntesis de sus distintos razonamientos. Es por ello que, ante las dificultades, se aplican 2 etapas secuenciales en la identificación del Perfil de riesgo:

- Primeramente, una perspectiva cualitativa, con motivo de poder limitar conceptualmente los valores que puede tomar cada componente del vector riesgo estudiado.

- Posteriormente, una redefinición cuantitativa hasta donde sea posible y tenga sentido, introduciendo tanto valores absolutos como escalas de referencia, donde posicionar cada uno de los riesgos o el agregado de los mismos.

La validez de un perfil así definido depende de la homogeneidad y equilibrio entre los distintos criterios aplicados, con independencia de la precisión con que puedan obtenerse magnitudes en los cálculos. Con motivo de revisar la validez de estas aproximaciones a Perfil, suele añadirse un contraste de sensibilidad, por el cual se revisan las variaciones de los resultados ante cambios marginales en los componentes de cálculo aplicados.

Lo lógico en las entidades evolucionadas es que comiencen su entendimiento de riesgos con este análisis cualitativo y, con su práctica y aprendizaje, lo cuantifiquen cada día con mejor precisión (aproximaciones sucesivas de ajuste).

Entre los métodos cualitativos más frecuentes se pueden identificar los siguientes:

- Análisis de Datos, Internos y Externos, existentes: Ante la falta de visión de riesgos en multitud de entidades, la comercialización de datos de ocurrencia relativos a ellos se ha convertido en un negocio floreciente. Presenta el inconveniente del ajuste de datos al contexto analizado, por lo que lo habitual es someterlos a ajuste de expertos mediante proyección de hechos pasados registrados.

- Entrevistas y debates colectivos: Dependiendo cómo sea la cultura de compartición en la organización analizada, el contraste de opiniones puede generar una inmejorable cualificación de riesgos. Desde luego, para riesgos dependientes, la opinión colectiva debe preponderar, dado que requieren de una opinión multi-localizada en sus consecuencias.

- Investigaciones: Suele ser el método más conveniente cuando los componentes de una opinión se encuentran dispersos. Se pueden estratificar por niveles de responsabilidad o experiencia en la materia, consiguiendo con ello una multi-dimensión en las respuestas. La calidad de lo obtenido depende mucho la claridad e inteligencia de las cuestiones al ser planteadas.

- Benchmarking: Es un análisis basado en la comparación con otros. Cuando es una iniciativa compartida y comprometida es cuando sus resultados mejores son. Cuando es un contraste puntual aparecen muchos problemas de homogeneidad en la información de contexto.

- Análisis de Escenarios: Técnica nacida de la planificación estratégica, es común verla aplicada a situaciones donde hay que limitar la incertidumbre. Está basada en supuestos de ocurrencia, los cuales hay que ligar a la evolución de algunas variables. Dada la complejidad que puede alcanzar este tipo de análisis

cuando se introducen multi-variables, lo más común es establecer condiciones de “ceteris paribus”.

d) Riesgos concatenados:

Riesgos es una dimensión cuya magnitud total no tiene por qué coincidir con la suma de las partes. Así ocurre cuando la aparición de un riesgo es debida a antecedentes deslocalizados del mismo. Es por ello que en el análisis de cualquier Cartera de riesgos hay que incluir las interacciones que se presentan entre los mismos. Es por ello la necesidad de considerar riesgos como un flujo horizontal en las organizaciones, tal como lo son los procesos de acumulación de valor para el cliente final.

Diversas plantillas y gráficas suelen utilizarse para reseñar esta concatenación entre riesgos. Entre ellas, las más utilizadas son las siguientes:

- Mapa de interdependencia en la Cadena de Valor: Consiste en la descripción de funciones con sus riesgos en el proceso de secuencia de actividades (filas) y contrastarla con sus efectos en otras actividades que se presentan en forma cruzada en un gráfico (columnas).

- Árboles Lógicos: Consiste en graficar un conjunto de factores inductores de riesgo y enlazarlos con las consecuencias que cada uno produce, de manera agrupada o individualizada.

El resultado de estas observaciones se concreta en el establecimiento de espectros de severidad: Se pueden definir distintas bandas de impacto, basadas en sensibilidad del capital o repercusiones históricas, las cuales son evaluadas según 3 estadios: Peor caso, más probable y optimista. Esto puede trasladarse a expresiones más formales para deducir algo menos subjetivo, cuantificándolo en cuanto a bajo/medio/alto riesgo.

- A partir de estas disquisiciones gráficas, buenas para la comunicación colectiva, se establecen prioridades de actuación en riesgos.

- Factores de la propia entidad, tal como vulnerabilidad o impedimento de contramedidas, pueden ponerse en contraste con las definiciones de riesgo anteriormente elaboradas para rectificar la prioridad de actuación en riesgos.

- Dado que ambas gráficas de factores corresponden a causas distintas y enfoques de distinto origen, merecen ser tratadas por separado.

- El tipo de mapas cruzados que sobre riesgos se elaboran son muy dependientes de la tradición de la entidad en utilizar perspectivas específicas.

El nivel de granularidad que se aplica a las definiciones de riesgo ha de ser tal que permita la identificación conveniente de la presencia y comportamiento del mismo para su mitigación a tiempo. Teniendo en cuenta que las entidades ajustan sus riesgos

conforme son las aspiraciones de maximización del valor, cualquier unidad de la misma, o su totalidad, puede presentar distintos perfiles de riesgo a lo largo del tiempo, siendo su comparación una perspectiva esencial sobre su gestión. El concepto esencial a defender en esta práctica es entender dónde y por qué se presentan diferencias respecto a otros competidores equivalentes.

3.8.2.6 Auditoría de la gestión del riesgo.

- DLE: Auditoría:

- UNE-ISO: Proceso sistemático, independiente y documentado destinado a obtener evidencias y evaluarlas objetivamente, a fin de determinar el grado de adecuación y de eficacia del marco de trabajo de la gestión del riesgo, o de una parte seleccionada de éste.

i) Introducción:

El término de auditoría es uno de los de mayor uso y abuso en el lenguaje cotidiano de la actividad empresarial, de cualquier naturaleza. Su universal utilización procede, en España, de la década de los setenta del siglo pasado, y, desde entonces, resulta fácil encontrar el término en publicaciones, generalistas u oficiales, con distinto contenido y propósito. En general, auditoría se suele relacionar con actividades de policía o contraste amenazante de cumplimiento en alguna referencia legal, por lo que su carácter potencial de agregador de valor queda desconocido, o anulado casi siempre.

En muchas ocasiones, más allá de donde existe un estándar indiscutible de referencia, este contraste carece de base admisible o consensuada, por lo que el ejercicio de auditoría y, aún peor, sus conclusiones, apenas rebasan la relevancia de ser una opinión discrecional, evaluable según receptor.

ii) Comentarios a la norma:

De manera global, puede decirse que la definición que introduce la norma es más un deseo que una realidad. Y como tal, introduce calificativos que, siempre, son elementos de opinión a falta de escala, por lo que su grado de severidad hay que tomarlo con precaución relativista:

- Sistemático: Puede referirse a que el conjunto de actividades que componen la auditoría forma un sistema en sí mismo. Ello significa que cada uno de sus componentes es interdependiente, por lo que no pueden ser tratados y considerados en aislamiento. También puede referirse a que la ejecución de la auditoría ha de realizarse de una forma sistemática, en cuanto a su cadencia.

- Referido a la primera alternativa, aunque redundante con la denominación de proceso, siempre queda dependiente de la metodología aplicada y el verdadero enfoque de sistema para la misma.

- Referido a la segunda alternativa de significado, la cadencia de ejercitar auditoría depende del tipo de problemas a resolver y la frecuencia de aparición de éstos. Si bien algunos tipos de auditoría se practican con temporalidad anual, este plazo puede ser demasiado amplio cuando quiere reforzarse una práctica sensible, por lo que mayor intensidad de contraste se hace recomendable.

  - En definitiva, la auditoría ha de adaptarse a la temporalidad (velocidad) de comportamiento de los riesgos, lo que demuestra los defectos de sistemas tradicionales carentes de esta consideración.

• Independiente: Cuando la norma cualifica como tal al proceso de auditoría, significa que ha de ser ajeno a los ejecutores habituales de la línea de producción u operaciones que es observada para calificar. Ello indica que auditoría se concibe como actividad de ejecutantes calificando la actuación de otros, lo cual siempre produce enfrentamiento de criterios, salvo que las referencias queden muy establecidas de antemano. Es por ello que las auditorías referidas a buenas prácticas resultan siempre conflictivas en conclusiones.

• Documentado: Como cualquier práctica profesional, la auditoría requiere soporte de actividades, tanto previo, como durante y de ejecución del ejercicio. Si bien el soporte para cada una de estas etapas resulta importante, por distintos motivos, la recopilación de evidencias es la más crucial de todas, dado que sobre ellas pueden presentarse todas las disputas de conclusiones. El dilema es la dimensión (grado) de eficiencia que se pone a la Documentación a elaborar, tanto por su cumplimentación, como por su fácil acceso e interrelacionado.

iii) El concepto de auditoría:

Tal como se deduce de algunos párrafos anteriores, el problema de la ejecución de auditoría es que hay que referirla a algún estándar o referencia acordada, y los mismos no siempre están disponibles o son declarados con precisión suficiente.

Si bien este es el caso para dominios de auditoría muy tradicionales, tal como es la aplicación de la contabilidad en la elaboración de los Estados Financieros de cualquier tipo de organización, para otros dominios resulta complejo sustentar una opinión, salvo evidencias groseras.

A pesar de esta disputa sobre referencias admisibles, la práctica de la auditoría avanza en variedad de contenidos. En ello juega un importante papel la necesidad de transparencia y contraste en las actuaciones de carácter profesional, tanto por motivos reputacionales, como de reducir la separación de criterio entre propiedad de una entidad y ejecución de sus actividades.

iv) Naturaleza de la auditoría:

Ante la avalancha de distintos contenidos de auditoría, es difícil presentar una clasificación de la misma que obedezca a alguna perspectiva razonable. Sin embargo, la redundancia en el mercado ha impuesto algunas denominaciones que van haciéndose identificables en cualquier entorno. Es así que, a menor complejidad, hay una primera clasificación inequívoca de auditoría:

- Externa: Aquélla realizada por profesionales ajenos a la organización revisada. El único dominio donde se ha posicionado esta práctica es en el mencionado de contabilidad, donde se produce una concentración de actuantes carente de toda lógica, dada la normalización de su aplicación.
    - Las restricciones de análisis y lenguaje a la que se ve sometida la auditoría externa de estados contables ha hecho que su alcance de significado haya tenido que revisarse con el tiempo, presentándose constantes disputas sobre su suficiencia de opinión.
    - Otros dominios funcionales intentados con el mismo propósito de opinión externa han resultado anecdóticos por falta de estándares de referencia.
        - Calidad ha tenido un desarrollo intenso en la búsqueda de estándares, pero su conclusión se ha limitado a capítulos en consideración, sin mayor especificación útil.
- Interna: Aquélla realizada por profesionales propios de la organización analizada, pero de involucración distinta a las actividades a revisar. Lo habitual es que auditoría interna se ejerza en revisión del seguimiento de políticas y niveles de admisión, tratamiento de eventos y excepciones, dictados por la superioridad de una organización.
    - Por lo tanto, la existencia de auditoría interna se ha orientado con el paso del tiempo a la revisión de existencia y ejecución del control interno.
    - Tal como antedicho, para el ejercicio de la misma no existen estándares de referencia, salvo el relacionado con el buen criterio, propio o de colectivos preocupados por normalizar la actividad referida a cada dominio posible e industria tratada.

v) Auditoría de riesgos:

Incluyendo todas las reservas que en párrafos anteriores se expresan, riesgos es uno de los dominios donde la práctica de auditoría se presenta útil como método de contraste ajeno a las prácticas de sus protagonistas. Sus considerandos específicos imponen un colectivo de precauciones para hacer útil, universal y eficiente su ejercicio. Entre ellos, los siguientes:

a) Condicionantes:

Si bien el concepto de riesgo ha adquirido aceptación universal a consecuencia de los eventos y crisis de expectativas económicas que se han mostrado incontroladas en los últimos años, el tratamiento de aquéllos cuenta con mucha dispersión debido a las variantes que existen sobre un componente elemental de su práctica: Método de identificación que garantice la exhaustividad.

Efectivamente, más allá de un problema de denominaciones, las diferencias de tratamiento proceden de discrepancias en el origen y naturaleza de los riesgos, incluyendo consideraciones de interfases y concatenación inercial entre procedencias distintas en origen, pero contagiosas en curso o destino. Ello hace que cualquier agrupación de riesgos, para acometer programas comunes de mitigación, presente grandes diferencias de aproximación y ejecución de salvaguardas. Mientras continúen las discrepancias en estas definiciones y se siga abusando de los modelos heredados de argumentos específicos (BIII) para algunas industrias, se carecerá de estándares viables y consensuados para el desarrollo de auditoría de contraste sobre ellos.

En el origen de este problema, como era previsible, encontramos que auditoría requiere de un estándar aceptado contra el cual comparar una práctica analizada. La existencia de estándares en el universo de riesgos es discutible, dado que los distintos modelos presentados han obedecido a problemas específicos a resolver en aquel momento (sistema financiero regulado y deficitario), o a enfatizar la necesidad de actuación intensiva de sus promotores (mercado de certificaciones y revisiones externas). Esto ha generado insolidaridad con los modelos habidos de otros colectivos que han rechazado estas argucias de pensamiento condicionado.

Con independencia de estas disparidades en la concepción de riesgos, resulta fácil admitir también dos naturalezas de auditoría en ellos, externa e interna.

- Externa, representada en requisitos de transparencia y alcance de informes referidos a riesgos: apetito y tolerancia.

- Interna, respecto a procedimientos de trabajo aplicados, desde identificación a tratamiento del riesgo, tanto en lo que concierne a su práctica, como al contenido de la misma, con énfasis en el control interno en uso y su suficiencia.

Adicionalmente, el término de auditoría recogió, en tiempos pasados, tanta aceptación que se generalizó, en la prensa especialista y usuarios poco evolucionados, el concepto de “tres líneas de defensa” respecto al riesgo. Sus argumentos principales son:

1. El dictamen de límites de riesgo en la superioridad de la entidad (Consejo y/o Dirección General). A veces, esta responsabilidad de primera definición queda otorgada (en confusión con lo anterior) a los distintos responsables de los procesos a evaluar.

2. La supervisión cotidiana de la evolución y riesgos de la actividad por los responsables directos de su contraste y alerta.

3. La periódica revisión, por parte de la auditoría, respecto a fiabilidad y seguimiento de lo anterior.

Las "tres líneas de defensa" sin duda han aportado un esquema de trabajo entendible en la potencial identificación y tratamiento del riesgo para entornos poco maduros en su práctica. Sin embargo, otros inconvenientes vinieron a obscurecer su admisión como método preventivo suficiente:

- La necesidad de actualización constante en la percepción del riesgo a tratar desde la primera línea de definición.

- La necesidad de comunicación suficiente en contenido y velocidad respecto a la ejecución y actualización de los distintos dictámenes elaborados.

    - A riesgos distintos les corresponden prevenciones, métodos y organizaciones distintos.

    - La multiplicidad y complejidad de riesgos a tratar genera departamentos especialistas aislados y prácticas autistas, de transparencia escasa.

    - Cuando aparece un riesgo estimable, el factor de velocidad para su mitigación se ha visto degenerado por falta de fluidez en el trabajo colectivo.

En la actualidad, la retórica de las tres líneas de defensa ha perdido todo su pasado esplendor ante otros enfoques más estructurados. Tal como queda enunciado en otros apartados, hoy en día se difunden esquemas de gobierno para riesgos que, manteniendo la metáfora de las tres líneas, desarrollan su contenido con otros argumentos más intensivos en capacidades, con menor preocupación de posiciones.

b) Riesgo de cumplimiento:

En el intermedio, dada la incertidumbre en que se desenvuelve la gestión de riesgos, como muestra el conjunto de eventos sistémicos y crisis redundantes, se ha visto la necesidad de enfatizar en el contraste de las prácticas de trabajo, bajo algún referente. A falta de mejor criterio, ha sido el referente del cumplimiento en que ha tomado el protagonismo de ocupación en auditoría de riesgos, con énfasis en todo lo relacionado con responsabilidades individuales.

El problema es que este referente resulta demasiado escaso para la misión que gestión de riesgos tiene, y las expectativas que sobre la misma, con buena lógica, proliferan en el mercado de cualquier latitud:

- Cumplimiento es un conjunto de especificaciones legales que hay que incluir en los métodos de trabajo.

- Su probabilidad de aparición es 100%, por lo que no cabe ninguna especulación sobre la misma. Es un evento fijo e incurrido.

- En concreto, siguiendo la casuística del sector financiero, la regulación sobre ella está referida a disponibilidad y trazabilidad de datos.

- Por lo tanto, su defecto o irregular contemplación, no es un riesgo, sino un delito a la espera de ser descubierto.

• Cumplimiento no es factor de competitividad. La mayor y mejor práctica de cumplimiento total no introduce diferenciaciones identificables por los clientes. La mejor aportación de cumplimiento es evitar sanciones.

- Si hay algún mercado donde cumplimiento es factor de diferenciación, ese mercado está corrompido en sus prácticas comunes y es mejor evitarlo.

• Mientras tanto, sobreabundan los cursos y seminarios dedicados a la materia, bajo el epígrafe de riesgos, lo que demuestra, en el mejor de los casos, la dispersión conceptual sobre éstos.

En consecuencia, aquellas entidades cuya práctica de auditoría toma como referencia central y única cumplimiento, dejan patente que la autoridad de la organización adolece del control suficiente sobre los procesos de trabajo aplicados en la misma, dado que ellos son los que deberían incluir con anterioridad las consideraciones que el regulador haya establecido como obligatorias, por lo que no tiene sentido su conceptualización como riesgo.

c) El control interno:

c1) Fundamentos:

Esta inestabilidad de propósito y referencia lógica respecto a la auditoría operativa ha hecho aparecer otras actividades paralelas o complementarias a la misma. Entre ellas, la más asentada es la de control interno, que siempre ha sido una actividad pareja y/o confusa respecto a la de implantación y seguimiento de métricas por gobierno básico.

• Aunque resulte supuesto, merece la pena repetir que, cuando se carece de métricas, se carece de gestión, por lo que aquéllas son consideradas imprescindibles en cualquier actividad que quiera superar el estadio de mera ejecución descontrolada.

• Control interno, y la designación de sus protagonistas, es parte de cualquier concepción de gobierno, en cuanto a métricas aplicadas a actividades concretas y sus desviaciones, con la lógica observancia de incompatibilidades de intereses en su custodia.

- Por razones históricas, control interno siempre fue concebido como una práctica de revisión de prácticas en consonancia con las políticas de casos de uso que una entidad ha definido como autorizadas.

- Dada la tradición de modelos de negocio basados en la explotación de activos, el control interno ha hecho énfasis en revisar las prácticas en la enajenación, utilización o compromisos sobre ellos, además del contraste de flujos financieros.

- Control interno es una actividad de atención continuada.

• El Control Interno practicado es punto esencial de revisión de la auditoría externa, dado que, en caso de correcta cumplimentación, reduce en gran medida su área de trabajo y examen.

- Para dar continuidad y mayor intensidad a la frecuencia de trabajo realizada por la auditoría externa, muchas entidades acuden a la auditoría interna con motivo que realicen con mayor continuidad la eficacia del control interno.

  ▪ En multitud de ocasiones se incluye en el alcance de la auditoría interna cuestiones relativas al desempeño de la función y la eficiencia en distintos departamentos de una entidad.

  ▪ Dados los requisitos de experiencia funcional que una opinión como la enunciada exige, este alcance suele evitarse al ser controvertido, salvo evidencias muy groseras.

• El control interno actúa por lo tanto sobre políticas, prácticas y procesos formalizados, revisando su cumplimiento e informando de las anomalías sobre el mismo. Allí donde se carece de las anteriores definiciones, allí donde control interno sólo puede informar de esta carencia.

Cuando una entidad cuenta con las prácticas mencionadas, auditoría se convierte en un análisis de estado para un momento concreto, mientras que control interno se convierte en una observación de tendencias conforme a prácticas aprobadas.

Con independencia de este acoplamiento de actividades, es cada vez más frecuente que auditoría interna (o externa en su defecto) oriente su dedicación a contrastar el uso y aplicación del control interno en toda práctica donde aparezcan o se transiten flujos financieros, siendo menos común en otros tipos de actividades.

• Durante la última década, según los dictámenes del regulador sobre prácticas a considerar han ido madurando en su concepción, sus requerimientos han sido incorporados a los nuevos sistemas y métodos de trabajo cotidianos. Ello ha provocado que auditoría, lógicamente, se haya vaciado de contenido respecto a aquellos dictámenes en cuanto aquéllos han sedimentado.

• En esta tendencia, la orientación de auditoría al control interno siempre provoca, por naturaleza de sus fines y medios, un sinfín de nuevos micro-procesos a

incorporar a los métodos cotidianos, recopilados en otro sinfín de manuales de procesos, imposibles de actualizar.

- La atención a estas circunstancias ha sido llamada de micro-gestión cotidiana, de escasa repercusión en las percepciones finales del cliente, salvo retardo de resolución de servicios.

- Algunos autores denominan a este espacio de trabajo de "riesgos operativos", diferenciados de los operacionales, negando que deban ser objetivo de doctrina alguna, dado que se subsanan por mejor diligencia de sus propios ejecutores. Incluso, se rechaza el término de "riesgo" para ellos, en favor de defectos de trabajo.

De toda la enumeración anterior, algunas deducciones pueden obtenerse de forma inercial:

- El control interno es un proceso, es decir, un medio para alcanzar un fin y no un fin en sí mismo.

  - Como tal proceso, se hace referencia a una cadena de acciones extendida a todas las actividades, inherentes a la gestión e integrados a los procesos básicos de la misma: planificación, organización y supervisión (COSO).

  - Tales acciones se hallan incorporadas (no añadidas) a la infraestructura operativa de la entidad para influir en el cumplimiento de sus objetivos y apoyar sus iniciativas de calidad en sus métodos y productos de trabajo.

- Lo ejecutan personas que actúan en todos los niveles como práctica incorporada a sus tareas cotidianas. No se trata solamente de cumplimentar manuales de organización funcional y procedimientos de trabajo adjuntos.

c2) Otras Definiciones:

Según la Comisión de normas de control interno de la Organización Internacional de Entidades Fiscalizadoras Superiores (INTOSAI), control interno puede ser definido como el plan de organización y el conjunto de planes, métodos, procedimientos y otras medidas de una institución, tendentes a ofrecer una garantía razonable de que se cumplan los siguientes objetivos principales:

- Promover operaciones metódicas, económicas, eficientes y eficaces, así como productos y servicios acordes a la calidad esperada.

- Preservar al patrimonio de pérdidas por despilfarro, abuso, mala gestión, errores, fraudes o irregularidades.

- Respetar las leyes y reglamentaciones, como también las directivas, y estimular al mismo tiempo la adhesión de los integrantes de la organización a las políticas y objetivos de la misma.

- Obtener datos financieros y de gestión completos y confiables, y presentarlos a través de informes oportunos.

Para la dirección de una entidad resulta primordial lograr los mejores resultados con economía de esfuerzos y recursos, es decir, al menor costo posible. Para ello debe controlar que sus decisiones se cumplan adecuadamente, en el sentido que las acciones ejecutadas se correspondan con aquéllas, dentro de un esquema básico que permita la iniciativa y contemple las circunstancias vigentes en cada momento.

Por consiguiente, siguiendo los lineamientos de INTOSAI, incumbe a la autoridad superior de una entidad la responsabilidad por el establecimiento de una estructura de control interno idónea y eficiente, así como su revisión y actualización periódica.

c2) Componentes del control interno:

El marco integrado de control que plantea el informe COSO consta de cinco componentes relacionados, derivados del estilo de la dirección, e integrados al proceso de gestión. Es un concepto y contenido proveniente de los antiguos modelos de revisión contable, que algunos estándares interesados en su práctica se han empeñado en mantener:

c21) Ambiente de control

c22) Evaluación de riesgos

c23) Actividades de control

c24) Información y comunicación

c25) Supervisión

A continuación se detalla el contenido de cada uno de ellos.

c21) Ambiente de control

Ambiente de control (desafortunada terminología histórica) se define como el conjunto de circunstancias que enmarcan el accionar de una entidad desde la perspectiva de la revisión interna de su práctica conforme a casos admitidos como formales, y que son determinantes del grado en que los principios de éste imperan sobre las conductas y los procedimientos de la organización.

Ambiente de control refleja la conducta vigente en una entidad respecto del comportamiento de sus actores, la responsabilidad con que encaran sus actividades, y la importancia que le asignan al control interno. Sirve de base de los otros componentes,

ya que es dentro del ambiente reinante donde se evalúan los riesgos y se definen las actividades de control tendentes a neutralizarlos. Simultáneamente, se capta la información relevante y se realizan las comunicaciones pertinentes, dentro de un proceso supervisado y adaptado a las circunstancias.

Ambiente de control es consecuencia de la actitud asumida por la Dirección, la Gerencia, y, por carácter reflejo, los demás actores de una organización con relación a la importancia del control interno y su incidencia sobre sus actividades y resultados.

Ambiente de control revisa el tono de rigor de trabajo en la organización y deduce la disciplina a través de la influencia que ejercen sus defectos sobre el comportamiento de los distintos actores en su conjunto. También constituye la estructura para el desarrollo de acciones de fortalecimiento del control, y de allí su trascendencia, pues como conjunción de medios, operadores y reglas previamente definidas, traduce la influencia colectiva de varios factores en el establecimiento, fortalecimiento o debilitamiento de políticas y procedimientos efectivos en una organización.

Los principales factores definitorios del ambiente de control son:

- La filosofía y estilo de trabajo en la Dirección y Gerencia, en cuanto a su grado de formalización, actuando como modelo de comportamiento (Rol Model).

- La estructura, el plan organizacional, los reglamentos y los manuales de procedimientos utilizados:

    - Las formas de asignación de responsabilidades y de desarrollo de carreras.

    - El grado de documentación de políticas y decisiones, y de formulación de programas que contengan metas, objetivos e indicadores de rendimiento.

    - En las organizaciones que lo justifiquen, la existencia de Consejos de Administración y comités de auditoría con suficiente grado de independencia y calificación profesional.

- La declaración de integridad, valores éticos, competencia profesional y compromiso de todos los componentes de la organización, así como su adhesión a políticas y objetivos establecidos.

Todos estos factores conjuntados constituyen la denominada “cultura empresarial en riesgos”, eufemismo bajo el cual se esconde una actitud de liderazgo en las prácticas de alerta sobre el mismo y la definición de carreras acordes con la prudente, pero inteligente, actitud hacia el mismo.

El ambiente de control será tan bueno como lo sean los factores que lo determinan. El mayor o menor grado de desarrollo y excelencia de éstos sustentará la fortaleza o debilidad del rigor en el trabajo que generan y, consecuentemente, el tono de la cultura de cumplimiento en la organización.

c22) Evaluación de riesgos:

El control interno ha sido pensado para limitar los riesgos que afectan a las actividades de las entidades. Su ejecución se realiza a través de la investigación y análisis de los riesgos relevantes y el punto hasta el cual los indicadores vigentes los identifica y evalúa respecto a las contra-medidas disponibles. Para ello debe adquirirse un conocimiento de las capacidades prácticas de la entidad, de manera que sea factible inventariar los puntos débiles, relacionándolos con los riesgos, tanto desde el enfoque de la organización y sus límites, como de la actividad desarrollada en ella.

La definición primaria de riesgos procede del establecimiento de objetivos. Si bien éstos no son un componente del control interno, constituyen la referencia básica sobre la que actuará el mismo.

Los objetivos (relacionados con operaciones, información financiera y cumplimiento), pueden ser explícitos o implícitos, generales o particulares. Estableciendo objetivos globales y por actividad, una entidad puede identificar los factores críticos de éxito y determinar los criterios para medir el rendimiento. Este rendimiento forma parte de los indicadores principales (KPIs), elementos de atención preferente del control interno. Las exigencias de velocidad de reacción suficiente pueden aconsejar disponer de otros indicadores premonitorios (KRIs) sobre los cuales enfocar la atención de control interno.

Es así como los objetivos de control interno son parte integrante de los genéricos y específicos de la entidad, por lo que han de ser determinísticos, así como adecuados, completos y razonables.

Una vez identificados los riesgos, su evaluación incluirá:

- Una estimación de su importancia / trascendencia.
- Una evaluación de la frecuencia de aparición o cualquier medida de intensidad.
- Una definición del modo en que habrán de gestionarse sus contramedidas.

Dado que las condiciones en que las entidades se desenvuelven suelen sufrir variaciones, se necesitan mecanismos para detectar y encarar el tratamiento de los riesgos asociados con el cambio. Aunque el proceso de evaluación es similar al de los otros riesgos, la gestión del cambio merece efectuarse independientemente, dada su gran importancia y las posibilidades de que el mismo pase inadvertido para quienes están inmersos en las rutinas de los procesos.

Existen circunstancias que pueden merecer una atención especial en función del impacto potencial que plantean:

- Cambios en el entorno.
- Redefinición de la política institucional.

- Reorganizaciones o reestructuraciones internas.
- Ingreso de empleados nuevos, o rotación de los existentes.
- Nuevos sistemas, procedimientos y tecnologías.
- Aceleración del crecimiento.
- Nuevos productos, actividades o funciones.

Los mecanismos para prever, identificar y administrar los cambios deben estar orientados hacia el futuro, de manera que permitan anticipar los más significativos a través de sistemas de alarma complementados con planes para un tratamiento adecuado de las variaciones. Es de nuevo en estas circunstancias donde las métricas, encuadradas como control interno u otra práctica, alcanzan todo su sentido.

c23) Actividades de control:

Es una definición tradicional de la práctica de pre-auditoría de estados financieros, que cuenta con sus problemas de adaptación a los nuevos modelos de atención a riesgos. En este sentido, la actividad puede estar referida a dos áreas de trabajo:

- De un lado, la existencia y método de cumplimentación de los indicadores, ya sean de rendimiento (KPI) como de riesgo precedente (KRI).
- De otro lado, la existencia de contramedidas correspondientes a la aparición de riesgo y su actualización, respecto a las variantes que éste pueda sufrir.

Por lo tanto, se entiende por actividad de control la revisión de la fiabilidad y oportunidad de los procedimientos que alimentan cualquiera de ambos elementos de gestión de riesgos, ya sea indicadores, ya sea contramedidas. Tal como dice la doctrina estandarizada, ambos actúan como reaseguro para el cumplimiento de objetivos, dado que tienen como misión la prevención y neutralización de los riesgos.

Estas actividades de control se ejecutan en todos los niveles de la organización, según participación en los elementos anteriores, lo cual toma como base el mapa de riesgos elaborado, en la mejor definición vectorial de los mismos.

Aunque las prácticas tradicionales reducen las observaciones de las actividades de control a áreas de conveniencia para ciertas prácticas, es necesario ampliar la corta enumeración que de ellas se hace, ampliando las mismas de la siguiente forma:

- Las operaciones y la conversión en las mismas de estrategia y reputación.
- La fiabilidad de la información financiera y de toma de decisiones.
- El cumplimiento de leyes y reglamentos y su concepción como especificación de trabajo rutinario.

En muchos casos, las actividades de control pensadas para un objetivo de los enumerados suelen ayudar también a otros de ellos: las mejoras operacionales pueden contribuir a las debilidades relacionadas con la fiabilidad de la información, y éstas con el cumplimiento normativo, y así sucesivamente.

A su vez, para cada uno de los objetivos enunciados existen diversos tipos de control:

- Preventivo / correctivos
- Manuales / automatizados o informáticos
- Gerenciales o directivos

En todos los niveles de la organización existen responsabilidades de control, y es preciso que los actores participantes conozcan cuáles son las que les competen, debiéndose por ello indicar las involucraciones.

c24) Información y comunicación:

Tal como se ha venido promulgando desde bastantes años atrás, aquello que no es medido, no puede ser gestionado ni mejorado. Aunque parezca chocante, la práctica profesional está llena de actividades sin algún correlato de medidas. Es por ello que el defecto principal, también en gestión de riesgos, es su gobierno.

Tal como ha quedado enunciado en otros capítulos, la práctica de riesgos se caracteriza por estar sometida a dos tipos de Indicadores que sustentan sus procesos de información: Los relacionados con los objetivos de la actividad donde se observa el riesgo (KPIs) y los indicadores adelantados de desviación para los mismos (KRIs). Sobre la custodia de los mismos es como se han de establecer los circuitos de información.

La generación y distribución de información es un proceso. Como tal está sometido a los condicionantes de calidad del mismo:

- Eficacia, en cuanto a contenido, frecuencia y precisión.
- Oportunidad, en cuanto al momento en que genera la información.
- Eficiencia, en cuanto a los costes involucrados en generar la información.

Aunque puede tener algunos efectos de movilización repartir la información de manera indiscriminada, las exigencias de acción oportuna piden discriminar y seleccionar los destinatarios de la información según el contenido de la misma.

Es el contenido de la información lo que dictamina el destinatario de la misma. Destinatario que viene catalogada por su capacidad de acción para actuar sobre las actividades sustento de la información y corregir la misma en su próximo registro.

Es esta capacidad de actuación sobre la información, en forma de Indicadores, lo que ha sido identificado por responsabilidades de cuyo desempeño se informa. Es el contraste entre responsabilidades sobre riesgos e indicadores de evolución de los mismos, así como la factibilidad de actuar o informar sobre ellos, el objetivo de control interno en su revisión de información y comunicación.

Las versiones simples sobre esta revisión se cumplimentan con ligazones individuales entre información y responsabilidad. La realidad demuestra que esta combinación es más compleja y que la información se reparte entre distintos destinatarios, ya que hay distintos grados de actuación involucrada. Es así como se determina un colectivo de destinatarios (RACI) en lugar de asignaciones únicas. Este es el tipo de organización que riesgos necesita y control interno revisa en su flujo y utilización.

Si bien la idoneidad de la información, principalmente en KRIs, es un tema de debate, aprendizaje y mejora permanente, la antelación de los mismos respecto al evento del que informan es aún un atributo más difícil de ajustar. Mientras tanto, toda información operacional, financiera o de cualquier otro tipo, puede resultar desfasada o inoportuna respecto a los fines perseguidos.

De dónde se deduce o alimenta la información a procesar resulta cada vez más controvertido, dado que la necesidad de contar con información suficientemente adelantada a los eventos ha dispersado las fuentes de suministro de datos, introduciendo con ello mayores debates de fiabilidad y garantía para la misma. Este nuevo escenario de información es igualmente objeto de análisis en control interno.

En ocasiones, son los propios sistemas de información los que incorporan niveles de alerta sobre Indicadores que permiten identificar situaciones habidas o emergentes. El tratamiento que se dé en cada caso a las alarmas forma parte del esquema de información rutinaria frente al de reacción inmediata.

Información, en fondo y forma, frecuencia, precisión, oportunidad y protagonistas RACI forman el entramado de información y comunicación que control interno debe contrastar.

c25) Supervisión:

Como es obvio deducir, las tareas de control interno pueden ser contrastadas por los profesionales al frente de cada actividad a revisar, dado que sólo consiste en revisar el comportamiento de la misma. Pero como quiera que ello puede acarrear conflicto de intereses por ocultación de situaciones enfrentadas, es elección de la Dirección asignar el desarrollo de la misma a una organización independiente de la analizada.

Dado que una organización ha de estar en mejora permanente, es común encontrarse de continuo en multitud de proyectos en desarrollo. Estos proyectos, como cualquier actividad, representan un riesgo en cuanto a su ejecución y aportación, y es misión de control interno opinar sobre los mismos. Estos proyectos, en su mayoría, deberían

estar destinados a mejorar la exposición de riesgos, por lo que su análisis de adecuación representa un elemento crucial del control interno.

Por lo tanto, dos tipos de actividades se pueden distinguir en la realización de control interno (COSO):

- Actividades Continuas, que son aquéllas incorporadas a las actividades normales y recurrentes que, ejecutándose en tiempo real y arraigadas a la gestión, generan respuestas dinámicas a las circunstancias sobrevinientes.

- Evaluaciones puntuales, que corresponden las siguientes consideraciones:

a) Su alcance y frecuencia están determinados por la naturaleza e importancia de los cambios y riesgos que éstos conllevan, la competencia y experiencia de quienes aplican los controles, y los resultados de la supervisión continuada.

b) Son ejecutados por los propios responsables de las áreas de gestión (autoevaluación), la auditoría interna (incluidas en el planeamiento o solicitadas especialmente por la dirección), y los auditores externos.

c) Constituyen en sí todo un proceso dentro del cual, aunque los enfoques y técnicas varíen, priman una disciplina apropiada y principios insoslayables.

  - La tarea del evaluador es averiguar el funcionamiento real del sistema: Que los controles existan y estén formalizados, que se apliquen cotidianamente como una rutina incorporada a los hábitos, y que resulten aptos para los fines perseguidos.

d) Responden a una determinada metodología, con técnicas y herramientas para medir la eficacia directamente o a través de la comparación con otros sistemas de control probados.

e) El nivel de documentación de los controles varía según la dimensión y complejidad de la entidad.

  - Existen controles informales que, aunque no estén documentados, se aplican correctamente y son eficaces, si bien un nivel adecuado de documentación suele aumentar la eficiencia de la evaluación, y resulta más útil al favorecer la comprensión del sistema por parte de los empleados. La naturaleza y el nivel de la documentación requieren mayor rigor cuando se necesite demostrar la fortaleza del sistema ante terceros.

f) Debe confeccionarse un plan de acción que contemple:

  - El alcance de la evaluación
  - Las actividades de supervisión continuadas existentes.
  - La tarea de los auditores internos y externos.

- Áreas o asuntos de mayor riesgo.
- Programa de evaluaciones.
- Evaluadores, metodología y herramientas de control.
- Presentación de conclusiones y documentación de soporte
- Seguimiento para que se adopten las correcciones pertinentes.

Las deficiencias o debilidades del sistema de control interno detectadas a través de los diferentes procedimientos de supervisión deben ser comunicadas a efectos de que se adopten las medidas de ajuste correspondientes.

Según el impacto de las deficiencias, los destinatarios de la información pueden ser tanto las personas responsables de la función o actividad implicada como las autoridades superiores.

g) Tendencias de la auditoría de riesgos:

En este estrangulamiento creciente del campo de actuación de la auditoría respecto a las distintas actividades empresariales y los riesgos en que incurren, está cuestionando el motivo de su existencia, a pesar de la palpable incertidumbre en que el devenir económico y social se desenvuelve.

Es así que, más allá de los actos rutinarios de contraste sobre la existencia y uso del control Iinterno, auditoría de riesgos está encontrando una llamada, cada vez más fuerte e inductiva, en planificación estratégica.

- Dada la preocupación sobre el valor de las entidades y la irregular evolución del mismo, han proliferado múltiples estudios en los últimos tiempos sobre sus condicionantes. Su conclusión redundante es que menos de 1/3 de variabilidad en pérdidas del valor depende de aportaciones, o denuncias, provenientes de auditoría, tanto externa, como interna.

- Sin embargo, cerca del 70% de las causas identificables detrás de una pérdida de valor fueron localizadas en supuestos e iniciativas estratégicas, espacio que, habitualmente, queda fuera del alcance de auditoría de cualquier tipo, salvo petición explícita de parte.

Por lo tanto, es en la práctica de la estrategia donde se producen las consideraciones de valor y riesgo de mayor alcance, por lo que es en ella donde la auditoría ha de realizar su trabajo de contraste y opinión.

La paradoja de esta nueva demanda de auditoría es que está referida a riesgos estratégicos, cuando la actividad que les da origen, tal como planificación estratégica, por lo regular está tratada de manera informal, o desde luego, carece de referencias estandarizadas sobre las que compararse. Es por ello que la práctica de auditoría que-

da enmarcada en revisar la suficiencia de métodos aplicados, evitando pronunciarse sobre sus contenidos.

h) Auditoría de riesgos estratégicos:

Existen multitud de aproximaciones a la práctica estratégica, algunas de mayor o menor aplicabilidad a cada entorno de mercado y actores a adoptar aquélla. En general, la práctica estratégica siempre consiste en construir una diferenciación frente a competidores, que sea sostenible en el tiempo.

- Por razones obvias, encontrar una diferenciación es una iniciativa compleja, que difícilmente puede ser sometida a críticas "a priori". Cuando algún tiempo ha pasado desde el lanzamiento de la iniciativa, resulta fácil entender si la diferenciación fue acertada, al revisar sus efectos.

- Lo que sí es opinable es el proceso de deducción de la diferencia, en cuanto al conjunto de actividades puestas en marcha y la participación, junto al consenso, que sobre ellas se ha obtenido.

- Por lo tanto, la auditoría factible está más relacionada con el alcance del procedimiento aplicado y participación colectiva involucrada, por lo que toma el carácter de control interno respecto al procedimiento seguido para obtener la diferenciación.

    - Esta función debe de partir de la existencia de una metodología explícita de planificación estratégica y riesgos ligados a ella.

    - La metodología asume circunstancias externas e internas, debiendo ambas contar con soporte documentado del acuerdo.

Para poder desarrollar esta tarea de forma inteligente, el auditor ha de contar con una visión integral de cómo la estrategia se engarza en otras actividades empresariales y cómo los riesgos de éstas pertenecen también a este conjunto integrado.

    - Resulta difícil encontrar una representación gráfica del conjunto de actividades desarrolladas por una entidad y la interrelación entre ellas. Por igual motivo, es difícil encontrar algún grafismo que presente la integración entre riesgos, a pesar del abuso del término en los discursos.

- A lo largo del tiempo han aparecido distintos marcos-estándar para paliar esta falta de integridad en la perspectiva, tanto de funciones primarias, como de riesgos. COSO-Framework es uno de estos intentos, pero apenas consigue algo más allá que acomodar un dibujo sin claridad de interdependencias en sus componentes.

Tal es así que la labor de auditoría sobre riesgos estratégicos está referida a un con-

junto de elementos en la planificación y ejecución de esta función, cuyos interrogantes principales son:

- Existencia de un proceso formal y suficiente de alcance. Grado de cumplimiento con el mismo. La oportunidad de comparar este proceso con otros de entidades reconocidas aporta pistas de defectos ignorados.

- Participación, en contenido y tiempo, de actores afectados por las decisiones en el proceso.

- Documentación de soporte para los objetivos y supuestos de sustento. Validación de los supuestos y consideraciones de volatilidad. Contramedidas preparadas.

- Instancias de aprobación existentes en el proceso y capacidad de veto o sugerencia de alternativas entre sus distintos actores.

- Claridad de métricas y relación de las mismas con plazos concretos de ejecución. Puntos de revisión de abandono o continuidad.

- Comunicación de los objetivos estratégicos y asimilación de los distintos involucrados en la relevancia de su participación.

Riesgos estratégicos son toda circunstancia que presente defectos en estos considerandos, dado que ello induce cumplir los objetivos propuestos. En otros términos, se audita la eficacia y colaboración en el proceso de identificación, evaluación y disposición de contramedidas para los eventos que afectan a la consecución de los objetivos estratégicos. Grado de madurez en el proceso.

f) Desde la orientación a riesgos a la creación de valor:

Con motivo de permanecer relevante más allá de la función de aseguramiento, auditoría interna necesita evolucionar su labor hacia generación de valor en lugar de detección de riesgos. Así conseguirá ser entendido como un colaborador en lugar de un coste necesario en la ejecución del negocio.

Con su desarrollado conocimiento de los procesos, políticas y procedimientos, auditoría interna tiene en su dominio un importante contenido para desempeñar una función de amplia generación de valor en la entidad a la que pertenece.

Para alcanzar una aportación significativa en su desempeño respecto a riesgos estratégicos, auditoría interna ha de alcanzar:

- Definir claramente la función en cuanto a auditar el proceso y no el plan en sí mismo.

- Entender el proceso de planificación estratégica.

- Profundo conocimiento del negocio, la industria y los factores de competitividad.
- Ligar conocimiento de riesgos y controles al desarrollo estratégico.
- Desarrollar un conjunto de preguntas conforme los estados de análisis.

Auditoría interna puede enfocar su actividad en la calidad de la información y las actividades de comunicación que sustentan la estrategia de la organización:

- Identificar los defectos entre las habilidades exigidas por la estrategia y las disponibles.

Cualquier iniciativa estratégica suele desarrollarse según un conjunto de fases que determinan el ciclo de vida de la misma, donde auditoría interna puede enfocar su actividad según el siguiente proceso de contenidos:

- Incepción: Existencia y adecuación entre los riesgos y el gobierno aplicado al proyecto.
  - Existencia de la documentación de sustento
  - Existe un contraste entre riesgos y mitigaciones
  - Existencia de un esquema de plan de ejecución
- Planificación, en cuanto a los supuestos en los que se sustenta
- Ejecución, en cuanto al control existente respecto a las especificaciones.
- Aceptación de los distintos integrantes del proyecto.
- Revisión de los resultados y su continuidad.

Como resultado, auditoría interna sustenta su trabajo y conclusiones en la documentación recopilada sobre el planeamiento y ejercicio estratégico, de la cual, los aspectos sobre los que enfatizar han de ser los siguientes:

- Detalle del mecanismo y frecuencia de revisión de los riesgos y el proceso en su totalidad.
- Las conclusiones de la auditoría y los procedimientos de monitorización.
- Detalle de cómo las anteriores recomendaciones han sido seguidas e implantadas.

ÍNDICE DE GRÁFICOS

ÍNDICE DE TABLAS


agers
Asociación Española
de Gerencia de
Riesgos y Seguros

www.agers.es