FACULTAD DE CIENCIAS

ECONÓMICAS Y EMPRESARIALES

GRADO EN ADMINISTRACIÓN Y DIRECCIÓN DE EMPRESAS

Departamento de Administración de Empresas y Marketing

Curso Académico: 2017-2018

Modelo integral de Gestión de Riesgos empresariales y Compliance

Trabajo Fin de Grado presentado por Dña. Reyes Domínguez Pera en la convocatoria de Junio del curso 2017-2018, siendo tutor del mismo Prof. Doctor D. Fernando Criado García-Legaz.

Vº. Bº. del Tutor: Alumna:

D. Fernando Criado García-Legaz. Dña. Reyes Domínguez Pera

Sevilla, Mayo de 2018 reyesdpera7@hotmail.com

RESUMEN EJECUTIVO

El mundo en el que habitamos, está cambiado. Vivimos en un marco globalizado, con mercados altamente competitivos, dónde son continuos los casos de corrupción y las malas prácticas empresariales; además, el entorno se caracteriza por experimentar cambios continuos. Por ello, desde hace ya ciertos años, las compañías comienzan a preocuparse en gran medida por los riesgos a los que se encuentra sometido por el entorno (tanto a nivel interno como externo), y cómo serían capaces de afrontar los mismos. Así surge la cultura del riesgo, unida a la gestión de los riesgos empresariales.

De forma paralela a la gestión de riesgos, surgen los sistemas de cumplimiento normativo (sistemas de reciente creación). Nos apoyaremos en ellos a lo largo de nuestra investigación ya que los consideramos una pieza esencial a la hora de abordar riesgos (sobre todo para los riesgos de cumplimiento). El desarrollo de estos sistemas, consiste en preparar a la organización para la prevención y reacción frente a incumplimientos, partiendo de la identificación, el análisis y el conocimiento previo de sus riesgos, su relevancia y la tolerancia frente a los mismos. Su intención es conseguir una cultura ética y respetuosa con las leyes.

Para abordar nuestro trabajo, dispondremos por un lado de un marco teórico, abarcando en primer lugar temas de carácter introductorio, como son los Sistemas de Gestión de Calidad (incluyendo modelos de excelencia como el europeo), seguido por nuestro tema central de gestión de riesgos empresariales, unido a la vinculación con la normativa de Compliance. Posteriormente abordaremos el marco práctico, en el que propondremos un modelo teórico de gestión de riesgos (aplicable a cualquier tipo de empresa con independencia de la titularidad del capital o tamaño). Es decir, un modelo homogéneo a nivel general, que es susceptible de ser aplicado a cualquier empresa según su propia realidad empresarial. Seguidamente aportaremos las líneas maestras necesarias para llevar a cabo el modelo, unido al diseño y puesta en marcha de planes preventivos y propuestas de mejora sobre los riesgos detectados que dispongan de un alto grado de criticidad. Finalmente, presentaremos al Cuadro de Mando Integral como herramienta clave, para el control y supervisión de los riesgos, cuya aplicación requeriría el uso de indicadores clave de riesgos.

Estos modelos, apoyados por ciertos referentes como el modelo norteamericano COSO y algunas normativas, como la ISO 31000: 2018, de Gestión del Riesgo y la UNE 19601: 2017 de Sistemas de Gestión de Compliance, ayudarán a las compañías en la obtención de una verdadera cultura de prevención de riesgos y de cumplimiento.

TÉRMINOS CLAVES: Gestión de Riesgos Empresariales; Compliance; Normativas ISO; COSO; Sistemas de Gestión; Calidad y Excelencia; Modelo de riesgos empresariales.

ÍNDICE

ÍNDICE DE FIGURAS

CAPÍTULO 1
INTRODUCCIÓN, JUSTIFICACIÓN, OBJETIVOS Y METODOLOGÍA DEL TRABAJO

1.1 INTRODUCCIÓN Y JUSTIFICACIÓN DEL TEMA

El tema central de este Trabajo Fin de Grado es vincular la Gestión de la Calidad y los Sistemas de Cumplimiento Normativo o Compliance, con los riesgos organizacionales a los que se encuentran expuestas las compañías actualmente.

Creemos que nuestra investigación cobra sentido debido a una serie de acontecimientos, relacionados con los riesgos corporativos, que han venido sucediendo e incrementándose en los últimos años. La cultura del riesgo se está implantando en las compañías cada vez con más fuerza, debido en parte a la corrupción tan presente, las malas prácticas empresariales y los sistemas de gobiernos corporativos. Esto ha llevado a ciertos cambios en el Código Penal -mediante el surgimiento de la responsabilidad penal de la persona jurídica- (2015), en la Circular nº 1 de la Fiscalía del Estado (2016), la creación de nuevas normas ISO (2011 en adelante), una mayor transparencia, entre otros. Todo ello, ha dado lugar a nuevos enfoques directivos dónde las compañías optan por plantear el establecimiento de ciertos modelos de gestión de riesgos empresariales. En este sentido, los sistemas de cumplimiento normativo pueden ser la mejor opción para poder abordarlos.

Debido a lo novedoso, actual e innovador que nos resulta este tema, creemos que era necesario entrar en la investigación del mismo; el cuál puede llegar a servir de guía a todo aquel que sienta la necesidad de indagar y de poseer cierto conocimiento sobre la materia.

Por todo lo comentado, consideramos la materia en general y nuestra investigación en particular, todo un reto futuro para aquellas compañías que pretendan obtener un éxito duradero y sostenible. De hecho, son ya muchas las empresas que están otorgándole al tema gran trascendencia y creemos firmemente que esta se incremente en los años próximos.

Lo anterior mencionado, unido a nuestro propio interés y la curiosidad sobre la temática, no ha llevado a decidir adentrarnos en contenidos científicos más allá de lo estudiado a lo largo de la carrera, llegándolo a tomar como reto a nivel personal (un tanto ambicioso), con expectativas de formación y aprendizaje durante toda la investigación.

1.2 OBJETIVOS

Los objetivos establecidos a la hora de confeccionar nuestro trabajo de investigación se podrían clasificar en dos categorías. Por un lado encontramos los objetivos teóricos y por otro lado los objetivos empíricos.
Se concretarían de la siguiente manera:

1.2.1 Objetivos teóricos

- Identificar la bibliografía científica y los referentes o estándares más actuales en el ámbito de la excelencia, la gestión del riesgo y el cumplimiento.
- Revisar y seleccionar la bibliográfica identificada que nos posibilite conocer el estado de la cuestión a través de los autores y entidades más reputados en la materia.
- Conocer las directrices y requerimientos del modelo EFQM de Excelencia 2013, la UNE-EN ISO 31000 de Marzo de 2018 (hemos tenido que modificar la versión a lo largo de nuestra investigación, por la nueva entrada en vigor y la sustitución de la ya obsoleta norma de 2010), así como el estándar norteamericano COSO de 2013 y la normativa de Sistemas de Gestión de Compliance, UNE 19601 de 2017.
- Satisfacer retos personales cumpliendo con un proyecto ambicioso e innovador (en las corrientes científicas), cuyo conocimiento en la materia puede ser de gran utilidad a nivel laboral con vistas a un futuro próximo.

1.2.2 Objetivos prácticos

- Aportar un esquema de modelo referido a los tres ámbitos esenciales de análisis (riesgos, estrategia y cumplimiento).
- Establecer los vínculos de relación entre las diferentes variables propuestas en el modelo teórico de referencia diseñado.
- Sugerir las líneas maestras para la puesta en marcha del modelo propuesto, unido al diseño y la ejecución de planes preventivos, amén de actuaciones y propuestas de mejora para los riesgos identificados.
- Intención de realizar un cuadro de mandos simplificado a nivel general, como herramienta de gestión para abordar el control y la supervisión de los riesgos oportunos.

1.3 METODOLOGÍA

Con la finalidad de dar respuesta a los objetivos fijados en el presente Trabajo Fin de Grado, hemos hecho uso de una combinatoria metodológica que se concretan y clasifican en:

- Identificación, revisión y obtención de fuentes científicas de la bibliografía vigente.
- Extracción de las principales aportaciones de los autores y de los modelos de referencia utilizados.
- Integración de los elementos teóricos clave y las propuestas de estándares y normas internacionales vigentes a fecha.
- Diseño de un modelo teórico de gestión del riesgo aplicable a una pequeña y mediana empresa, unido a las líneas maestras para su aplicación.
- Introducción a la propuesta de un cuadro de mandos simplificado como herramienta de gestión integral de los riesgos empresariales.

Para ello, nos hemos apoyado en ciertas normativas como son las ISO 31000 de Gestión de Riesgos organizacionales, las ISO 19600 de Sistemas de Gestión de Compliance, la legislación básica vigente y sobretodo en el modelo norteamericano COSO, el cuál usamos como máximo referente a la hora de clasificar los riesgos organizacionales.

En definitiva, hemos combinado la revisión teórica junto a su posterior análisis práctico correspondiente.

CAPÍTULO 2

BASES TEÓRICAS-CIENTÍFICAS

2.1 PREÁMBULO

Para abordar nuestro marco teórico, tendremos que tratar ciertos temas. Por un lado, encontraremos el foco de nuestra investigación, que es la materia de gestión de riesgos en las organizaciones, unido a la vinculación existente con el tema tan actual de cumplimiento normativo o compliance. Pero previo a ello, deberemos de exponer cierta información en la que hablaremos de la calidad y los sistemas de gestión normalizados por un lado y, por otro, de la calidad vinculada con los modelos de excelencia (en concreto trataremos el modelo europeo EFQM de excelencia).

A lo largo de todo el marco teórico, hemos usado ciertos referentes. Entre ellos, le otorgamos gran valor al modelo norteamericano COSO (reconocido a nivel mundial como guía de buenas prácticas empresariales) y una serie de normativas ISO como la 31000 de Gestión del Riesgo o la ISO 19600 de Sistemas de Gestión de Compliance.

2.2 CALIDAD Y SISTEMAS DE GESTIÓN NORMALIZADOS

2.2.1 Introducción

La definición más reciente sobre el término calidad esta propuesta en la norma UNE-EN ISO 9000[1] (2015: 9) y se expresa en los términos siguientes: “Una organización orientada a la calidad promueve una cultura que da como resultado comportamientos, actitudes, actividades y procesos para proporcionar valor mediante el cumplimiento de las necesidades y expectativas de los clientes y otras partes interesadas. La calidad de los productos y servicios de una organización está determinada por la capacidad para satisfacer a los clientes, y por el impacto previsto y el no previsto sobre las partes interesadas pertinentes”.

La Gestión de la Calidad es entendida como una manera de hacer las cosas, un método de gestión y no un objetivo en sí mismo. Es el conjunto de decisiones estratégicas y tácticas que

[1] En adelante UNE 9000.

se toman en la empresa con el objetivo concreto de mejorar los productos, servicios, procesos y la gestión empresarial a nivel general (Criado y Calvo de Mora, 2004: 203-204).

Debemos mencionar que el gran cambio que sucede a nivel evolutivo es pasar del enfoque de control o correctivo al enfoque de gestión o preventivo. Es aquí donde se empiezan a preocupar las empresas por obtener certificados de calidad basados en las normas de la Organización Internacional de Normalización (en lo sucesivo ISO) y en la obtención de sellos de excelencia basados en modelos de excelencia como el europeo (conocido como European Foundation for Quality Management Model (en los sucesivo EFQM). Desde entonces hasta la actualidad, la demostración de la calidad se ha convertido en un tema de preocupación en el ámbito empresarial. Por ello, la Unión Europea (UE) y los países miembros vienen actualizando y poniendo en vigor normativas legales, institucionales y procedimientos encaminados a demostrar esta calidad.

Entre el enfoque correctivo y el preventivo, tiene lugar el referido al control de los procesos (en la actualidad es denominado como gestión de procesos o reingeniería de procesos), mediante el cual las compañías pretendían asegurarse que los procesos estaban bajo control reduciéndose así la variabilidad de sus resultados. Es de vital interés señalar la importancia que tienen hoy día la gestión de los procesos, lo que implica que la dirección de las organizaciones disponga de una visión por procesos.

Vinculado con los Sistemas de Gestión de Calidad (SGC), debemos hacer mención de las normas ISO 9000. Éstas son un conjunto de normas y directrices internacionales que se van revisando y actualizando sus diferentes versiones; así hoy, la familia de normas de la serie 9000 son: UNE-EN ISO 9000: 2015. Sistemas de Gestión de la Calidad. Fundamentos y vocabulario; la UNE-EN ISO 9001: 2015. Sistema de Gestión de la Calidad. Requisitos y; la UNE-EN ISO 9004: 2009. Gestión para el éxito sostenido de una organización.

Centrándonos en la norma ISO 9001: 2015 que es la única norma certificable e incluye requisitos, podemos decir que introduce un cambio en la estructura de contenidos (requisitos). Se les exige a los responsables, una estructura de "alto nivel", donde los tiempos y recursos que se invierten en su gestión, se reduzcan notablemente. Esta nueva estructura atiende a: alcance, referencias normativas, términos y definiciones, contexto de la organización[2], liderazgo, planificación, procesos soporte, procesos de operación y, en último

[2] Entre los nuevos requisitos se encuentra el análisis del contexto que se trata de la necesidad de tener en cuenta y analizar el entorno socio-económico de la empresa y los vínculos existentes con los stakeholders. Este análisis facilitará la detección de necesidades y problemas que puedan generar un impacto al planificar la Gestión de la Calidad.

lugar, el análisis, la medición y la mejora. Con esta nueva estructura, algunos requisitos se han modificado o eliminado (ISO Tools, 2015).

A tenor del objeto y el alcance de nuestro trabajo de investigación debemos destacar el pensamiento basado en los riesgos por ser esencial para el logro eficaz del SGC (nos centraremos a posteriori en él por su relevancia). Este concepto ya ha estado implícito en ediciones previas, mediante la planificación, revisión y mejora. Según esta norma, la compañía necesita entender su contexto, planificar e implementar posteriormente acciones para poder abordar riesgos y oportunidades. Así se alcanzarán mejores resultados, se previenen efectos negativos y se logra la mejora (UNE-EN ISO 9001:2015).

2.2.2 Cambios relevantes en las Normas ISO 9000 e ISO 14001 de 2015

A modo de inciso y por la mención previa de los nuevos requisitos y del pensamiento basado en riesgos, creemos que es conveniente resaltar esos contenidos ya que posteriormente realizaremos una clasificación en el apartado de riesgos al tratar los distintos tipos de riesgos organizacionales existentes. Por ello, destacamos los siguientes cambios más relevantes de las versiones vigentes de 2015, de la serie ISO 9000 y la norma ISO 14001[3]:

1. El análisis permanente del contexto: La organización debe determinar las cuestiones externas e internas que son pertinentes para su propósito y la dirección estratégica, así como aquellas que afecten a su capacidad para lograr los resultados previstos de su SGC (o su sistema de gestión ambiental si hacemos referencia la ISO 14001). La organización debe realizar el seguimiento y revisión de la información sobre estas cuestiones (UNE-EN ISO 9001 -2015: 14-; UNE-EN ISO 14001 -2015: 17-). Así, se deben identificar y gestionar los riesgos estratégicos, de transparencia y de cumplimiento.
2. Análisis de los riesgos vinculados a los procesos: la organización de identificar y gestionar los riesgos operacionales, es decir, se pueden gestionar los riesgos que pueden afectar a los procesos así como a los resultados globales del SGC (UNE-EN ISO 9001, 2015).

Desde las últimas décadas, los modelos de gestión de la calidad pueden desglosarse en dos grandes grupos: sistemas que siguen normas o estándares (como la UNE-EN ISO 9001: 2015) y, los sistemas de gestión que se apoyan en Modelos de Excelencia (como el modelo europeo

[3] La Norma Internacional UNE-EN ISO 14001:2015 sobre Sistema de Gestión ambiental tiene como propósito proporcionar a las empresas un marco de referencia que proteja el medio ambiente y responda a las condiciones ambientales estando en equilibrio con las necesidades socioeconómicas (UNE-EN ISO 14001, 2015).

EFQM de 2013). Por ello, éste será el núcleo central del próximo apartado, en el que abordaremos resumidamente el modelo.

2.3 CALIDAD Y SISTEMAS DE GESTIÓN BASADOS EN LA EXCELENCIA

2.3.1 La excelencia y la importancia de satisfacer a todos los stakeholders

La excelencia es una cualidad de aquello que es extraordinariamente bueno y excede de las normas ordinarias. Según Aristóteles (384 a.C - 322 a.C), decía que "somos lo que hacemos día a día. Por eso la excelencia no es entendida como un acto, sino como un hábito".

Según Criado y Calvo de Mora (2004), una organización excelente es un modelo de referencia para la gestión. La excelencia es un concepto más genérico e integrador que el referido a la calidad. Se basa en obtener los estándares más altos de rendimiento de la organización alcanzando la eficacia y la eficiencia tanto interna como externa.

Originalmente, como indica Reeves y Bednar (1994: 437), la excelencia puede parecer un término subjetivo y abstracto, planteándose problemas de cómo evaluar la excelencia, quién determina los estándares de qué es excelente y qué no. Pero finalmente, quién juzga la calidad es el cliente (enfoque al cliente). Por ello, pensamos que obviando su subjetividad, la concepción de calidad como excelencia es el concepto más completo. Desde esta perspectiva, hablamos de la Gestión Total de Calidad (GCT) o Total Quality Management (TQM), definiéndola como un enfoque de gestión integral de las empresas, el cual incluye factores sociales, estratégicos y técnicos. Se orienta al logro de resultados excelentes en relación a todos sus grupos de interés (Criado, 2016).

Los modelos de excelencia propuestos por los grandes maestros o surgidos en el ámbito internacional se basan en la filosofía de la mejora continua o Kaizen[4], la innovación y la formación continuada.

Destacan varios modelos basados en Premios a la Excelencia, los cuales aconsejan qué deben hacer las organizaciones para ser consideradas líderes en el ámbito de la GCT y lograr resultados excelentes. Los más difundidos son el modelo propuesto por Deming en Japón (1951), el modelo Malcon Baldrige de los EEUU (1987) y el modelo europeo EFQM (1991), en el que nos centramos (Yusof y Aspinwall, 2000: 285-289).

[4] La filosofía Kaizen trata de acciones concretas, simples y diarias que implica a todos los trabajadores de la compañía, tratando de ser cada vez mejores. Para la profesora Goy Yamamoto, Kaizen representa una actitud y un compromiso del trabajador con su trabajo, sus compañeros, clientes y empresa. Implica mantener la disciplina y las rutinas de chequeos para no fallar, detectar errores fácilmente y tomar decisiones adecuadas rápidamente (Oliver, 2017).

2.3.2 Modelo EFQM

Si reunimos a un grupo de personas en una habitación y les preguntamos qué es la Excelencia, recibiremos muchas respuestas pero todas ellas deberían tener algo en común: La excelencia es hacerlo lo mejor posible…Cada día, nos recuerdan la importancia de esforzarse para la excelencia, ya sea en la vida personal como laboral. Si fomentamos una cultura de Excelencia dentro de las organizaciones, estaremos abriendo el camino al éxito (EFQM Leading Excellence, capturado 2018)[5]. Como hemos mencionado, las organizaciones excelentes logran y mantienen niveles sobresalientes de rendimiento que satisfacen o exceden las necesidades y expectativas de todos sus grupos de interés.

En Europa, el Premio de Excelencia fue fundado en 1991 por la European Foundation for Quality Management (EFQM)[6] si bien nace como institución privada en 1989 cuando presenta la misión. La última versión vigente del prestigioso modelo es del año 2013.

El modelo se fundamenta en ciertos principios (EFQM Model, 2013): Crear un futuro sostenible, añadir valor para los clientes, aprovechar la creatividad y la innovación mediante la mejora continua y la innovación sistemática, liderar con visión, inspiración e integridad, alcanzar el éxito mediante el talento de las personas y, mantener resultados sobresalientes.

Algunos rasgos distintivos del modelo vigente de 2013 son (EFQM)[7]: Está formado por un marco completo, operativo y útil como guía para la efectiva implantación de TQM en cualquier tipo de organización (organismos privados, públicos y mixtos) al estar formado por principios generales. Por otro lado, es vital en este entorno de cambio que el éxito puede depender de las alianzas establecidas. Por ello, se desarrollan alianzas duraderas basadas en la confianza mutua, respeto y transparencia generando valor en la compañía y mejorando la competitividad. También destacar que desde su fundación, EFQM se compromete con la investigación y actualización del modelo. Así asegura ser dinámico y en la línea de pensamiento de gestión actual. Por ello, desde la primera versión de 1991, han ido sucediéndose varias revisiones y adaptaciones.

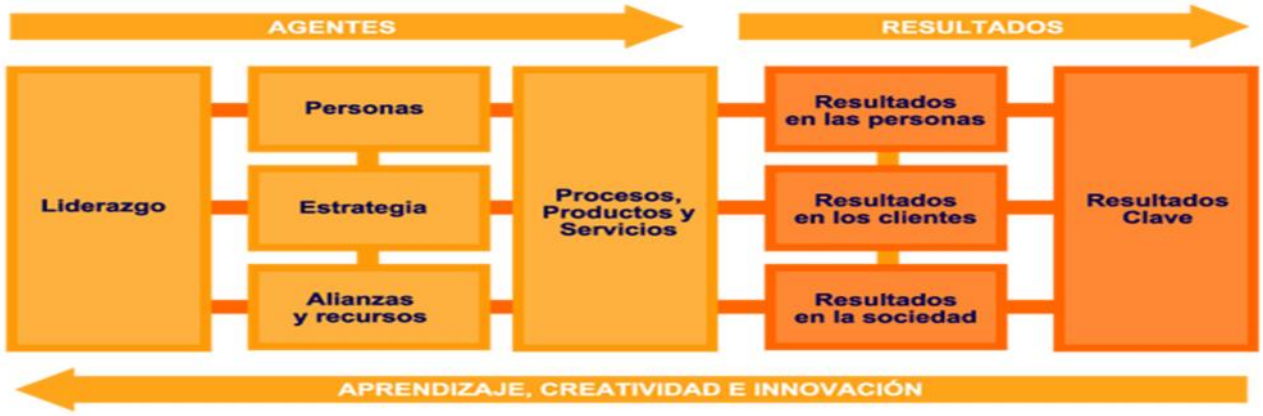
Para la correcta implantación del TQM y la medición de los resultados que está obteniendo la compañía, el modelo propone 9 criterios que sirven de guía. Destacamos que son criterios y no requisitos lo que usamos. Estos elementos nos indicarán el grado de progresión que sigue

[5] Capturado: Efqm.org; fecha: 26/02/2018
[6] Capturado: Efqm.org; fecha: 26/02/2018
[7] Capturado: Efqm.org; fecha: 26/02/2018

la empresa para llegar a la gestión excelente. Dichos nueve criterios se clasifican en 2 categorías (factores claves de implantación o agentes facilitadores y resultados). Es decir, tiene una estructura similar a la de los modelos de excelencia comentados, a nivel general.

Los criterios agentes son cinco: liderazgo, personas, estrategia y política, alianzas y recursos y, procesos productos y servicios. Los criterios de resultados por su parte son cuatro: en las personas, en los clientes, en la sociedad y en los resultados clave. Todos los criterios tienen subcriterios y su peso varía en función de la importancia relativa de cada uno. Sin embargo, los dos grandes bloques (agentes y resultados) si se puntúan de igual forma con 500 puntos cada uno (Criado y Vázquez, 1999).

La representación gráfica del modelo es la siguiente:



Fuente: EFQM (2013)[8]

Figura 1: Modelo EFQM de Excelencia 2013

La flechas representadas, en concreto la de la parte inferior, es la gran impulsora de la excelencia. Debido a su dirección, muestra el carácter dinámico del modelo, señalando que el aprendizaje, la innovación y la creatividad, impulsan los efectos que los agentes generan sobre los resultados, destacando la mejora continua del sistema.

El modelo utiliza como herramienta de autoevaluación, la lógica REDER, constituida por 4 elementos (resultados, enfoques, despliegue, evaluación y revisión), que determinan qué deben hacer las organizaciones en la autoevaluación. La principal utilidad de la lógica se sitúa en poder usarse tanto por miembros de la organización, al realizar la autoevaluación con EFQM y, también, por evaluadores externos (ajenos a la empresa y expertos independientes) en el desarrollo de los procesos de evaluación externa.

Queremos destacar que nuestra investigación se fundamenta en tres pilares, sirviéndonos los mismos para obtener a posteriori nuestro modelo teórico de gestión integral de riesgos. Estos

[8] Capturado: Efqm.org; fecha: 28/02/2018

tres bloques son estrategia, riesgos y cumplimiento. Por ello, en el siguiente apartado, abordamos uno de ellos, la gestión de riesgos empresariales. Resaltar asimismo cómo el modelo EFQM se sustenta en el pilar referido a la estrategia empresarial; pues bien, este modelo junto a las cinco fuerzas de Porter, nos sirven de fundamento o base para el bloque estratégico. Simplemente resaltar que mediante el modelo de las 5 fuerzas competitivas de Porter (1979) y publicado en la revista Harvard Business Review (2008), se pueden maximizar los recursos y superar a la competencia. Según su autor, Michael Eugene Porter, si no se cuenta con un plan que esté perfectamente elaborado, no se puede sobrevivir en el mundo de los negocios.

2.4 GESTIÓN DE RIESGOS

2.4.1 Introducción, concepto de riesgo y términos asociados

Vivimos en un mundo cambiante y en un marco globalizado, con mercados altamente competitivos y entornos sometidos a cambios continuos. Los consumidores se encuentran interconectados, son más sofisticados, impulsados en parte, por la mayor disponibilidad de información. La presión de las compañías para triunfar, junto a la presión para tener éxito basado en los principios de sostenibilidad, son enormes (COSO[9], 2013: 1).

La sostenibilidad es entendida como responsabilidad de todos y se define desarrollo sostenible como aquel desarrollo que satisface las necesidades del presente sin comprometer la capacidad de las generaciones futuras para cumplir sus propias necesidades (Informe Brundtland, 1987: 43). Usamos sostenibilidad como sinónimo de RSC, abarcando aspectos tanto sociales, ambientales como económicos. Según COSO (2013), para proporcionar valor a través de la sostenibilidad, las organizaciones deben ser capaces de reconocer, gestionar y responder tanto a las oportunidades como a los riesgos. Por eso, la sostenibilidad se ha convertido en una prioridad a nivel estratégico sirviendo de vehículo para lograr una ventaja competitiva y crecimiento a través del posicionamiento de productos, servicios y marcas que atraen a las partes interesadas de la organización; ya que, los clientes lo esperan, los empleados lo demandan y los accionistas confían en gozar de la sostenibilidad.

[9] Committee of Sponsoring Organizations of the Treadway Commission.

Las organizaciones pueden llegar a experimentar ciertas circunstancias desfavorables, que si suceden, producen consecuencias negativas sobre los activos de la empresa provocando su indisponibilidad, pérdida de valor o un funcionamiento inadecuado.

De aquí, surge la cultura de riesgo en las organizaciones, que se refiere a "Las normas de comportamiento para los individuos y grupos de interés que determinan la capacidad colectiva de identificar y entender los riesgos actuales y futuros, así como discutir y actuar de forma abierta sobre los mismos" (AMIS[10], 2015:4).

Antes de continuar, queremos resaltar que en los próximos párrafos vamos a mencionar ciertos vocablos afines al riesgo, los cuales nos resultan imposibles de explicar todos ellos en nuestro proyecto, debido a la amplitud permitida. Por ello, hemos decidido crear el anexo II de conceptos vinculados o asociados al riesgo (Pág. 52) para profundizar en ellos.

La norma UNE-ISO 31000 (2018:7) define riesgo como "Efecto de la incertidumbre sobre los objetivos". Los objetivos pueden ser de naturaleza diversa y se trataría de un término asociado a sucesos potenciales y futuras consecuencias. De la definición, se extrae que riesgo e incertidumbre son términos relacionados pero no homónimos. En este sentido, la ya obsoleta norma de 2010 definía la incertidumbre como "El estado, incluso parcial, de deficiencia de información relativa a la comprensión o al conocimiento del suceso, sus consecuencias o de su probabilidad" (UNE-ISO 31000, 2010: 8). Ya el insigne economista Knight (1921) decía que la asunción de riesgos es consustancial al desempeño de la labor de empresario. También sostenía la diferencia existente entre riesgo e incertidumbre, siendo el riesgo la aleatoriedad medible (conocida su probabilidad), mientras la incertidumbre es aleatoriedad no medible (probabilidad desconocida).

Por otro lado, hay autores como Métayer e Hirsch (2007) que proponen no confundir los términos peligro y amenaza pues mientras una amenaza se podría transformar en una oportunidad, el peligro en ningún caso.

Podemos calificar los riesgos de manera cuantitativa y cualitativa, asignándoles importancias relativas y priorizando los esfuerzos de forma no arbitraria. También existen ciertos riesgos ocultos o no identificados y riesgos no controlados. Otro tipo de riesgos son los inherentes[11]. Éstos surgen de la exposición que tenga la actividad en particular y la probabilidad que un choque negativo afecte a la empresa. El riesgo inherente, al ser intrínseco, no puede ser

[10] Asociación Mexicana de Instituciones de Seguros.
[11] Es el riesgo intrínseco de cada actividad, sin tener en cuenta los controles que de éste hagan en la propia organización.

eliminado, es decir, podrá minimizarse su probabilidad y reducir el impacto, pero la propia actividad llevará consigo la posibilidad de su ocurrencia (Thomson Reuters, 2017: 42).

Todas las actividades de una organización implican riesgos. Es decir, el nivel de riesgo al que se somete una organización nunca será cero. Si el riesgo existe por inherente, el riesgo residual (entendido como aquel remanente después del tratamiento del propio riesgo)[12] nunca podrá erradicarse entero.

Según el Instituto Nacional de Ciberseguridad (Julio de 2015), en adelante INCIBE, el nivel de riesgo es una estimación de aquello que puede ocurrir y se valora de manera cuantitativa. El riesgo se valora en término de coste derivado del valor de los activos afectados considerando también los daños producidos en el propio activo. En ocasiones, es bueno realizar además un análisis cualitativo del riesgo.

El hecho de trabajar con variables económicas hace que se pueda establecer de manera sencilla el ya mencionado umbral de riesgo o apetito del riesgo. Este concepto es el máximo nivel de riesgo que se atreve o está dispuesta a soportar la dirección de la organización a la par que se esfuerza para que crezca el valor añadido ofrecido a sus stakeholders. Para mantener el nivel de riesgo por debajo de este umbral, las organizaciones soportan un determinado coste, conocido como coste de protección (INCIBE, 2015:6-7).

Debido al entorno cambiante comentado, los logros que se obtienen hoy no son una garantía para el futuro próximo. Por ello, los esfuerzos empleados para maximizar los beneficios y contar con garantías de éxito, deben ser aplicados de manera metódica, estructurada, sin criterios arbitrarios y siguiendo la mejora continua. Así, "el valor se maximiza cuando se establece una estrategia y objetivos que consiguen un equilibrio óptimo entre las metas de crecimiento y rentabilidad y los riesgos asociados a los mismos" (Abella, 2006: 24).

Del término umbral ya explicado, surge la gestión del riesgo cuyo objetivo es mantener el riesgo por debajo del umbral fijado previamente. Para COSO (2004), esta gestión se define como aquel proceso efectuado por el Consejo de Administración de una organización, su dirección y el resto de personal, aplicable a la definición de estrategias en toda la organización. Está diseñado para identificar eventos potenciales que puedan perjudicar a la compañía, gestionar sus riesgos dentro del riesgo aceptado y proporcionar una seguridad razonable sobre el logro de los objetivos.

[12] ISO Gestión del Riesgo GUÍA 73, 2009, definición 3.8.1.6. Esta norma se corresponde con la española UNE-ISO GUÍA 73: 2010 IN).

En cuanto a los tipos de riesgos, en nuestra búsqueda hemos encontrado bastante diversidad, debiendo aclarar como en la revisión bibliográfica realizada no hemos podido dar con una clasificación o tipología de riesgos consensuada en el ámbito científico (referido a los riesgos estratégicos y operativos); todo lo contrario en relación a los de cumplimiento, con los que sí parece haber consenso prácticamente unánime.

Así, encontramos tipologías de riesgos estratégicos que atienden a criterios de la naturaleza del riesgo (de mercado, crédito, liquidez, operativo, o legal), otras a su temporalidad (inminente, a corto plazo…), según percepción y asunción, en virtud de su impacto y temporalidad, según su origen (interno y externo) o entre otros, quienes los clasifican en financieros, estratégicos y de negocio.

En este sentido y debido a lo comentado, nos quedamos con COSO (2013) como referente mundial de mayor reputación y seguimiento entre grandes empresas e instituciones diversas para establecer nuestra clasificación de riesgos. Previo a la clasificación, vamos a dedicar unos párrafos a introducir esta organización norteamericana dedicada a la creación de guías y marcos de trabajo de buenas prácticas en el ámbito de gestión de cumplimiento, orientada a los riesgos organizacionales y siendo aplicable a todo tipo de organizaciones.

2.4.2 Metodología COSO: Antecedentes, tipos de riesgo y componentes

Originalmente formado en 1985, el Committee of Sponsoring Organizations of the Treadway Commission se crea como consecuencia de las malas prácticas empresariales en los años anteriores de crisis. Actualmente, el objetivo de COSO es proporcionar un liderazgo pensado en tres temas interrelacionados: gestión de riesgos empresariales (ERM), control interno y disuasión del fraude. Fue un proyecto conjunto de cinco organizaciones del sector privado que abordan los riesgos de la compañía mediante una metodología integradora creando valor en la misma (COSO, 2013: 12). Estas asociaciones norteamericanas son el Instituto de Auditores Internos (IIA), la Asociación Americana de Contabilidad (AAA), el Instituto Americano de Contadores Públicos Certificados (AICPA), Financial Executives International (FEI) e, Instituto de Contadores de Gestión (IMA).

En 1992, se publica el primer modelo de COSO con el fin de ayudar a las organizaciones a evaluar y mejorar sus sistemas de control interno. Dicho referente definía al control interno como un proceso que se genera por la dirección y trabajadores de una compañía. Está diseñado para proporcionar un grado de seguridad adecuado en la consecución de los

objetivos. Dicho estándar abarca tan sólo cinco componentes que se verán aumentados en la siguiente versión de COSO de 2004.

Esta última versión, COSO o ERM (Enterprise Risk Management) de 2004, extiende el concepto de control interno vigente en la anterior versión a la gestión de cumplimientos orientada al riesgo, implicando a la totalidad de la compañía. COSO 2004 está orientado a lograr los objetivos de las empresas así como asegurarse una información eficaz cumpliendo con las leyes y normas, evitando daños en la reputación de la compañía y creándoles valor.

La última versión apareció en 2013 (COSO ERM 2013), se trata de una metodología capaz de abordar la gestión de riesgos en las empresas desde un enfoque integrador, tratándose de una gran oportunidad para crear valor para sus stakeholders (ISO Tools, 2015).

No debemos olvidar tratar su carácter genérico, ya que se puede aplicar a todo tipo de organizaciones. Permite a la compañía establecer la relación de riesgos clave en toda la empresa, y cómo puede identificar, abordar y supervisar estas incertidumbres (COSO, 2013).

Para conseguir su misión, las organizaciones necesitan desarrollar estrategias y objetivos interrelacionados en toda la empresa. El modelo de COSO (2013), clasifica estas estrategias y objetivos en cuatro tipos de riesgos diferentes los cuales tomaremos como referentes: estratégicos, operacionales, de informes o transparencia y de cumplimiento. Estas categorías proporcionan una dimensión organizacional que crea un fuerte contexto para el riesgo considerado. En ellas, tendremos en cuenta el concepto de sostenibilidad que hemos ido tratando al considerar que su incorporación ofrece una oportunidad para aumentar la efectividad de las prácticas de gestión de riesgos y mejorar el rendimiento empresarial. A continuación definimos cada uno de ellos, dejando su explicación para posteriori.

- Estratégicos: Se generan al más alto nivel de la compañía y están conectados con la misión y visión de la misma (Abella, 2006: 22).
- Operacionales o de proceso: Son aquellos relacionados de manera directa con la eficacia y eficiencia de las operaciones de la entidad, sin olvidar los objetivos relativos al desempeño y la rentabilidad (Abella, 2006).
- Riesgos de transparencia, relativos a la información suministrada a terceros: Según COSO (2013), frente a la creciente presión para ser transparente, cada vez más organizaciones eligen informar sobre sostenibilidad, entendida como sinónimo de RSC. Los riesgos de información se concentran en todos aquellos que tienen que ver con la transparencia de la empresa frente a sus grupos de interés.
- De cumplimiento: Incluye riesgos relacionados con el cumplimiento por parte de la organización, de todos los requisitos reglamentarios, legales y normativas aplicables, las

que trataremos en el siguiente epígrafe sobre Compliance. Haciendo referencia a la norma ISO 19600 sobre SG de Compliance (2014), la organización debe identificar y evaluar sus riesgos de compliance, relacionando sus obligaciones de cumplimiento con sus actividades, productos, servicios y aspectos relevantes de sus operaciones.

También es importante resaltar una última dimensión adicional y a menudo puede ser un factor clave cuando surgen problemas de sostenibilidad, y es la reputación. Aunque generalmente se aborda en la categoría estratégica, COSO, en su informe Demystifying sustainability risk (2013: 3) cree que es importante resaltarla aún más, ya que lo contempla como un resultado y como una consideración clave relativa a otros riesgos, como son los de operación. Hacemos hincapié a como cada vez de manera más frecuente, mediante las opiniones expresadas por los usuarios en redes sociales, se puede posicionar la reputación o marca de una organización sobre su desempeño sostenible.
Antes de continuar con la gestión de riesgos, vamos a vincular los cuatro tipos de riesgos que menciona COSO (2013), con sus ocho elementos integrantes.

La metodología COSO II (2004) y COSO III (2013), pasan de los cinco componentes de COSO I, a ocho elementos interrelacionados a tener en cuenta para la gestión de riesgos efectiva. En ellos, incluimos la sostenibilidad ya que según COSO (mayo 2013), la sostenibilidad puede y debe integrarse entre estos. Vamos a mencionar estos componentes, algunos ya tratados, y comentaremos a posteriori ciertos rasgos de ellos en el marco práctico. Estos componentes son el ambiente interno, el establecimiento de objetivos, la identificación de acontecimientos o eventos, la evaluación del riesgo, la respuesta al mismo, actividades de control, la información y comunicación y, en último lugar, la supervisión.

COSO 2004 y COSO 2013 interrelacionan entre si cada uno de los ocho elementos mencionados, alineándolos con los cuatro tipos de riesgos y vinculándolos con todos los niveles de la organización, destacando como novedad la representación del nivel estratégico. Su representación gráfica sería el siguiente cubo:

Fuente: Traducido de COSO (2013: 2).

Figura 2: El cubo de COSO

Además de la metodología norteamericana comentada, existen a día de hoy otras guías de buenas prácticas basadas en riesgos. Centrándonos en las generalistas, destacamos la normativa ISO 31000: 2018 (recientemente actualizada), entendida como norma global, no certificable que aporta directrices en materia de gestión de riesgos. Esta norma, anula y sustituye a la UNE-ISO 31000: 2010 como ya indicamos.

2.4.3 Norma UNE-ISO 31000: 2018 de Gestión de Riesgos

Como bien indica la nueva norma de 2018, la gestión del riesgo es iterativa y asiste a las organizaciones a establecer su estrategia, lograr sus objetivos y tomar decisiones informadas. El enfoque genérico de esta norma proporciona principios y directrices para gestionar cualquier forma de riesgo de manera sistemática, transparente y fiable, dentro de cualquier alcance y contexto. De esta manera, puede utilizarse por cualquier empresa privada, pública o social, grupo, individuo o asociación sin ser específica de una industria o sector. Pero, sin olvidar la importancia del contexto específico de cada empresa, con unos objetivos, entorno y partes interesadas concretas.

Mientras todas las organizaciones gestionan riesgos a diferentes niveles, esta norma internacional establece una serie de principios que deben de cumplirse en todas las compañías para la gestión eficaz del riesgo. ISO 31000 (2009), recomendaba que se desarrollase, implementase y mejorase de manera continuada un marco de trabajo, cuyo objetivo fuese integrar el proceso de gestión del riesgo en los procesos de gobierno, de estrategia y planificación, de gestión y de elaboración de informes, así como en las políticas los valores y

en la cultura de toda la organización. Debemos aclarar que la nueva norma vigente desde marzo de 2018 incide en el marco de referencia, cuya función es asistir a la organización en integrar la gestión de riesgos en todas sus actividades y funciones significativas. Su tarea implica diseñar, implementar, valorar y mejorar la gestión del riesgo a lo largo de toda la organización (UNE-ISO 31000, 2018: 10).

Según ISO 31000: 2018 se deben cumplir ciertos principios para que la gestión de riesgos sea eficiente, cree y proteja el valor, siendo estos los siguientes: ser una parte integral de todas las actividades de la compañía, ser estructurada y exhaustiva, contribuyendo así a resultados coherentes y comparables; debe adaptarse al contexto interno y externo de la organización incluyendo la integración de factores humanos y culturales, la mejora continua mediante el aprendizaje y experiencia; requiere de una participación apropiada y oportuna de las partes interesadas, siendo dinámica ya que los riesgos pueden aparecer, cambiar o desaparecer; por último, la organización debe disponer de la mejor información posible tanto histórica como actualizada, así como de las expectativas futuras.

Como bien indica la UNE-ISO 31000: 2018, la gestión de riesgos es parte de la gobernanza, y el liderazgo es fundamental en la manera en que se gestiona la organización en todos sus niveles. Esto contribuye a la mejora de los sistemas de gestión. Haciendo referencia al Instituto Nacional de Ciberseguridad (INC, 2015: 10), observamos como hace especial hincapié en que la dirección de la compañía debe estar totalmente comprometida e integrada en los procesos de la empresa y debe disponer de una rigurosa planificación estratégica, un marco de trabajo (ahora conocido como marco de referencia). Éste, debía ser revisado periódicamente y adaptarse a los cambios que suceden en su entorno tomando las decisiones oportunas para obtener la mejora continua.

Por otro lado, debemos hacer mención a que se debe hacer un seguimiento y revisión de riesgos de manera continuada (en todas las etapas del proceso), para asegurarse y mejorar la calidad y eficacia del diseño, la implementación y resultados del proceso.

Por último y, en la medida que nos servirá para la parte empírica de nuestro trabajo, existen ciertas herramientas para gestionar riesgos como la matriz de riesgo, la cual permite clasificar y visualizar los riesgos generales mediante la definición de categorías de consecuencias y de su probabilidad de ocurrencia (ISO gestión del riesgo guía 73: 2009). La finalidad básica de esta será permitir observar de forma clara y sencilla las áreas o ámbitos afectados por cada uno de los riesgos detectados y analizados. También existe como herramienta el mapa de riesgo, donde se posicionarán los riesgos detectados en función de

su mayor probabilidad y gravedad de su impacto en la organización. Mediante este mapa se permite el conocimiento sistemático y actualizable de los riesgos a los que se expone la organización en base, normalmente, a los criterios de existencia de factores de riesgos y gravedad del riesgo (Thomson Reuters, 2017: 41-42). Como hemos adelantado, profundizaremos sobre el mapa en nuestra parte práctica del trabajo.

Concluyendo con este apartado, creemos conveniente mencionar que para hacer frente a los riesgos organizacionales (ya que ignorarlos no es una opción), los sistemas de cumplimiento normativo son sin dudarlo la forma más ordenada y metódica para el control de riesgos a los que debe hacer frente cualquier organización.

2.5 COMPLIANCE

2.5.1 Conceptos, historia del compliance, evolución y legislación básica

Como se ha dicho, la forma más adecuada de control de riesgos y, en especial los asociados al cumplimento, son los sistemas de gestión de cumplimiento. El desarrollo de sistemas de cumplimiento orientados al riesgo consiste en preparar a la organización para la prevención y reacción frente a incumplimientos, partiendo del análisis y conocimiento de cuáles son sus riesgos, su relevancia y la tolerancia de la organización frente a éstos (Benítez, 2017:37).

Las organizaciones cuya meta es tener éxito a largo plazo necesitan mantener una cultura de integridad y de cumplimiento, considerando las necesidades y expectativas de las partes interesadas. Por tanto, integridad y compliance son clave y una oportunidad para una organización exitosa y sostenible (UNE-ISO 19600: 2014).

Podemos definir compliance como el resultado de que una organización cumpla con sus obligaciones, convirtiéndose en sostenible, introduciéndola en la cultura de la organización y en el comportamiento y actitud del personal que trabaja en la compañía (UNE-ISO 19600: 2014); o, como lo define Bocanegra (2016) entendido como el desarrollo e implementación de un programa para el riesgo de cumplimiento y así conseguir sostenibilidad empresarial, proteger la imagen y la reputación. Aclarar que cuando hablamos de organización no nos referimos solo a empresas sino a persona o grupo de personas que tienen sus funciones propias con responsabilidad, autoridad y relaciones para el logro de objetivos.

Maza, antiguo fiscal general del Estado (2016-2017), comenzó el II Congreso Internacional de Compliance (2017), dónde citaba como el tema de compliance se está volviendo cada vez más relevante en nuestra sociedad. Comentaba que: "Los acontecimientos tanto pasados como recientes, hacen que comprobemos la complejidad enorme que tiene el mundo delictivo. La complejidad de los delitos cometidos en el seno de las organizaciones. Tanto complejidad desde el punto de la comisión de los hechos, por la gravedad de los efectos que produce, como sobre todo para la dificultad para la investigación y complejidad para reprimir esas conductas, evitarlas o castigarlas con la finalidad preventiva que siempre debe regir en el Derecho Penal". El salto de la corrupción al derecho Penal es cuando la OCDE y las Naciones Unidas se dan cuenta que la mejor herramienta para combatir la corrupción es tener mecanismos de control interno en las empresas. Y de no tenerlos, o no aplicarlos correctamente, se derive entonces una responsabilidad penal.

"Un SG de compliance eficaz y que abarque a toda la organización permite que la misma demuestre su compromiso de cumplir con la normativa, incluyendo requisitos legales, cogidos de la industria y los estándares de la organización; así como los estándares de buen gobierno corporativo, las mejores prácticas, la ética y las expectativas de la comunidad en general" (UNE-ISO 19600, 2015: 5).

Hacer especial hincapié en que este sistema de gestión, como bien indica el Dossier de Compliance y la norma UNE 19601 (2017: 4): "No es un objetivo en sí mismo, sino un instrumento para conseguir o afianzar una cultura ética y de respeto a la Ley. Por eso, casi más importante que un acertado diseño del sistema, es comprobar que realmente funciona y genera la cultura pretendida".

Los países anglosajones, cuentan con una larga y asentada cultura en materia de compliance, en especial EEUU, dónde son muchas las empresas que disponen ya de avanzados programas de cumplimiento normativo. De hecho, la Señora Villegas comenta en el II Congreso de Compliance Internacional (2017), que deberíamos importar los modelos de EEUU y de Gran Bretaña, al comentar que debemos de mirar al exterior, a aquellos países que tienen mayor poder en este ámbito ya que sus influencias pueden ser variadas.

Centrándonos en el ámbito nacional, en los últimos años, España ha evolucionado muy rápido en la madurez con respecto a Compliance o cumplimiento normativo. Ha pasado de estar restringido para pequeños grupos de expertos a integrarse en el vocabulario común de los empresarios, llegando a ser asunto clave en la agenda de determinados Consejos de Administración. De hecho, y tal y como sostiene Casanovas (2017: 4): "Muchas empresas

están actualmente migrando sus estructuras básicas de compliance a modelos de mayor valor añadido, que cubran las expectativas de los operadores internacionales".

A modo de información de carácter general, hacer mención a cómo el sistema de compliance no es obligatorio por ley a día de hoy, pero si se comete un delito puede que se deriven responsabilidades penales por no tenerlo.

Al hablar de cumplimiento normativo, tenemos que hacer mención a la legislación básica o normativa actual aplicable a todas las empresas, y éstas son:

1) Código penal (CP): El mayor impulso de la función de compliance, junto con la mayor preocupación de las empresas y la Administración por incorporar buenas prácticas de compliance penal, ha sido debido por las reformas operadas en las Leyes Orgánicas 5/2010 y sobre todo la de 1/2015 del CP, modificando la Ley Orgánica 10/1995. "Éstas supusieron un cambio histórico en el ordenamiento jurídico español, al establecer por primera vez, la responsabilidad penal, directa y autónoma de las personas jurídicas. Las empresas pueden ahora ser responsables penalmente de los delitos cometidos en su nombre y en su beneficio (tanto directo como indirecto), por sus representantes legales o administradores, o por delitos cometidos por sus empleados, cuando hayan podido realizar los hechos por haberse incumplido, por parte de los representantes o administradores, los deberes de vigilancia y control de su actividad atendidas las concretas circunstancias del caso" (ICA[13], 2018: 13).

Haciendo referencia a su artículo 31 bis (Apdo.2-3: 27088-27089), al referirse a los criterios que deberán cumplir para generar la exención de la responsabilidad penal de la persona jurídica, precisándose en el apartado quinto del mismo artículo, establece: "El órgano de administración ha adoptado y ejecutado con eficacia , antes de la comisión del delito, modelos de organización y gestión que incluyen las medidas de vigilancia y control idóneas para prevenir delitos de la misma naturaleza o para reducir de forma significativa el riesgo de su comisión; la supervisión del funcionamiento y del cumplimiento del modelo de prevención implantado". Es decir, el Código Penal asigna al Órgano de Administración la responsabilidad de la adopción y ejecución de los SG de cumplimiento penal, llegando a suceder en las jurisdicciones que a la hora de determinar la sanción por no cumplir la ley, los tribunales han tenido en cuenta su compromiso existente de cumplimiento.

En definitiva, desde la reforma del CP surge la necesaria implantación en las empresas de programas de organización y gestión para la prevención de delitos que pueden atenuar e incluso eximir la responsabilidad penal de las personas jurídicas. Por ello, destacamos el

[13] Instituto de Consejeros-Administradores.

comentario que se efectúa en el II Congreso Internacional de Compliance (2017), dónde se alude que más que eludir una responsabilidad penal de la persona jurídica, lo que se pretende conseguir es que la empresa tenga una cultura de cumplimiento y que exista un efecto preventivo en la misma.

2) Ley de Sociedades de Capital, tras la reforma operada por la Ley 31/ 2014 de 3 de Diciembre para la mejora del gobierno corporativo (en adelante, LSC): Necesidad de regular en mayor medida el gobierno corporativo con normas de carácter vinculante, al identificar como causas de la pasada crisis financiera la deficiente composición de los órganos de dirección y administración, la asunción imprudente de riesgos, unidas a la falta de transparencia, estructuras complejas del gobierno corporativo e indeterminación de responsabilidades dentro de las empresas (ICA, 2018).

3) Circular 1/2016 de la Fiscalía General del Estado sobre la Responsabilidad Penal de las personas jurídicas conforme a la reforma del CP 2015: Imparte instrucciones a fiscales para valorar la eficacia de los planes de compliance en empresas como eximentes o atenuantes de su responsabilidad penal. Se configura como un valioso documento para interpretar el alcance de la nueva normativa (ICA, 2018).

4) Norma ISO 19600 (Diciembre 2014) sobre Compliance Management Systems: Es el estándar internacional que incorpora las mejores prácticas internacionales sobre SG de compliance. Esta norma se corresponde con la norma española UNE-ISO 19600 de 2015.

5) Norma UNE 19601 sobre Sistemas de Gestión de Compliance Penal: Es sin dudarlo la principal novedad española en materia de compliance, tanto por actualidad como por importancia. Surge en mayo 2017 (publicada por AENOR[14] y el BOE[15]), mediante la que toma forma el primer estándar oficial nacional que favorece la homogeneidad entre SG para la prevención de delitos en las empresas. Es la primera norma española que incluye requisitos para implantar, mantener y mejorar un sistema de Compliance que permite reducir el riesgo penal y prevenir delitos en las compañías (Thomson Reuters, 2017). Es aplicable a todo tipo de organizaciones con independencia de su tamaño, naturaleza o actividad, ámbito público o privado, con o sin ánimo de lucro. Profundizaremos en ella a posteriori por su transcendencia.

6) Norma ISO 37001: 2016 sobre Anti-Bribery Management Systems: Se trata de un estándar internacional sobre requerimientos y mejores prácticas internacionales referente a sistemas de gestión anti soborno y anticorrupción la cual se está adoptando con rapidez. Es

[14] Asociación Española de Normalización.

[15] Boletín Oficial del Estado

una norma clave en la lucha contra el soborno para cualquier tipo de compañía. Su principal finalidad es ayudar a las organizaciones a promover una cultura ética evitando el deterioro de imagen y desconfianza de consumidores generada por las malas prácticas (Thomson Reuters, 2017). Esta norma formula requisitos y no directrices y, cómo resultado, las empresas pueden certificarse con esta ISO. Los certificados de sistema de gestión son una de las diferencias con la norma 19600 ya que esta última no los proporciona.

7) Ley de Transparencia y la fundación Forética: La Ley 19/2013 de transparencia, acceso a la información pública y buen gobierno, es una ley pensada para el sector público. Las sociedades privadas aparecen excluidas de su ámbito subjetivo de aplicación (BOE núm. 295 de 2013). Sin embargo, la frontera entre público y privado está cada vez más difuminada y de hecho, la incidencia de la ley de transparencia en el sector privado alcanza ya ciertos aspectos (a pesar que haya otros que no aparecen recogidos expresamente en la ley), y otros que aparecen pero que deberían modificarse (Ágora, 2016).

La ley de transparencia de España es una norma que tiene como objetivo reforzar el derecho de los ciudadanos a acceder a la información sobre actividades públicas. Pero nosotros queremos centrarnos en el ámbito de las compañías privadas, ya que según Ágora (2016), existe una relación inversamente proporcional entre transparencia por un lado y opacidad, y corrupción por otro. El concepto de transparencia, a pesar de surgir primero en las Administraciones Públicas, a día de hoy se les exige, entre otras a las empresas cotizadas. De hecho, la transparencia empresarial es desde los últimos años, de especial interés con vista a los clientes, accionistas, socios, etc. De hecho, este concepto en las empresas, se ve reflejado en la RSC de la compañía. Se dice que la transparencia genera confianza entre aquellos que tienen relación con la entidad (BBVA Empresas, 2015).

Debido a su vinculación con la materia, nos gustaría hacer referencia a la asociación Forética. Se trata de una asociación de empresas y profesionales de la responsabilidad social empresarial y sostenibilidad, líder en España y Latinoamérica, que tiene como misión fomentar la integración de los aspectos sociales, ambientales y de buen gobierno en la estrategia y gestión de empresas y organizaciones. Formada por más de 200 socios, entre ellos el 40% de empresas que cotizan en el Ibex 35, filiales de multinacionales, pequeñas y medianas empresas (PYMES), ONG de referencias y socios personales. Forética, es propietaria de la Norma SGE 21 (primer SG de la responsabilidad social que permite voluntariamente alcanzar una certificación).

El carácter internacional de Forética le permite estar a la vanguardia de las tendencias en RSC y ponerlas a disposición de empresas y organizaciones con soluciones y servicios que

maximizan la contribución positiva al entorno. Por ello, centenares de organizaciones se están certificando con la Norma en España y Latinoamérica (Web oficial de Forética)[16]. Además tiene iniciativa en tema de la corrupción, tomando medidas que evitan el abuso del poder con vistas a obtener ganancias personales.

Acabada la mención de las normas de carácter general, mencionar que existen otras normas relevantes como el Reglamento (UE) 2016/679, de 27 de Abril que trata de la nueva figura del delegado de protección de datos personales o data protection officer, entendida como una figura independiente.

Finalmente, en materia legislativa hay que hacer mención al ámbito internacional, ya que se han promulgado en las últimas décadas multitud de normas y tratados, algunos de ellos con gran importancia. Vamos a enumerar determinados: Foreign Corrupt Practices Art (1977) (USA), Sarbanes-Oxley Act (2002) (USA), aprobadas tras ciertos escándalos de corrupción en empresas cotizadas americanas. Mencionamos también la conocida Ley antisoborno UK Bribery Act (2010), la cual se tiene en la actualidad como referente en la lucha de la corrupción debido a su carácter extraterritorial en la aplicación penal (ICA, 2018). De todas formas, queremos aclarar cómo no hemos podido abordar en profundidad todas estas normativas, debido a la extensión permitida en nuestra investigación docente.

2.5.2 Aspectos clave de la Norma UNE 19601:2017

Sus antecedentes surgen cuando AENOR creó en Abril de 2013 el Subcomité sobre SG del Cumplimiento y SG de Anticorrupción. Sus miembros tuvieron la ocasión de acceder a documentos y participar en debates de los proyectos de normalización internacional sobre gestión de Compliance (ISO 19600) y antisoborno (ISO 37001), llegando a conocer las mejores prácticas que se estaban debatiendo y plasmando en ellos. En Enero de 2015 se aprueba la creación del grupo ad-hoc en el seno del subcomité para normalizar sobre sistemas de gestión de compliance penal, de modo que los conocimientos y experiencia adquiridos en las dinámicas de normalización internacional revirtieran en la creación del primer estándar nacional sobre prevención penal de 2017 (Thomson Reuters, 2017).

Como ya anunciamos, se fundamenta en la norma internacional IS0 19600:2014, basada en una serie de principios como son el buen gobierno, proporcionalidad, transparencia y

[16] Capturado: Forética.org; fecha: 18/03/2018

sostenibilidad. Por ello, la UNE 19601, al surgir de procesos de normalización internacional sobre Compliance, se convierte automáticamente en un referente en su materia, ya que además de cumplir con el CP español, se completa con los estándares internacionales.

Siguiendo la filosofía de la ISO 19600, facilitamos el aprendizaje de la norma española, su comprensión y aplicación dentro y fuera de nuestras fronteras. A nuestras empresas les resulta más cómodo explicar su modelo al público extraterritorial si se alinean con estructuras conocidas internacionalmente y fácilmente comparables con las de otros países que gozan de normas modernas en la materia. Por ello, las organizaciones que usan estándares oficiales disfrutan de la ventaja competitiva que les otorga su reconocimiento en el mercado (al igual que sucedió en su día con la famosa serie de normas ISO 9000 de SGC).

Es de interés señalar que:

- "Disponer de un Sistema de Gestión de Compliance acorde con la norma UNE 19601 no garantiza que no se hayan producido delitos o que no vayan a producirse. Sin embargo, su correcta ejecución disminuye la probabilidad de que suceda y constituye una evidencia más de gestión responsable" (Thomson Reuters, 2017:4).
- A diferencia de la norma ISO 19600, según Thomson Reuters (2017), la norma española 19601 de 2017 se certifica. El certificado durará tres años, pero auditándose anualmente su cumplimiento.
- La normativa española establece un canal de denuncias donde la confidencialidad y el anonimato del denunciante de hechos que impliquen un riesgo penal, deben quedar garantizados, prohibiendo cualquier represalia contra el que utilice estos canales (Thomson Reuters, 2017).
- La eficacia de un sistema de compliance sólo se puede medir si seguimos un sistema de norma continua (II Congreso Internacional de Compliance, 2017).

Por otro lado, destacar que las organizaciones que quieran implantar un SG de cumplimiento, deben de poseer ciertos requisitos, siendo algunos de ellos un desarrollo de las condiciones que exige el CP[17]. No obstante, existen muchos otros que exceden lo exigido y tienen su origen en las buenas prácticas internacionales. Destacamos algunos como:

- La identificación de actividades en cuyo ámbito se puedan cometer delitos que deben ser prevenidos, poniendo en conocimiento las conductas potencialmente delictivas.
- El establecimiento de protocolos que concreten el proceso formativo de voluntad de la persona jurídica, adopción de decisiones y su posterior ejecución.

[17] Ley Orgánica 1/201 reforma CP, 2015.

- Disponer de modelos de gestión de los recursos financieros adecuados impidiendo así la comisión de los delitos que deben ser prevenidos, así como contar con la partida presupuestaria para conseguir los objetivos del modelo.
- La obligación de informar de posibles riesgos e incumplimientos al organismo encargado de vigilar el funcionamiento del modelo de prevención.
- La disposición de un sistema disciplinario que sancione correctamente el incumplimiento de las medidas establecidas y adopte acciones correctivas.

2.5.3 El Consejo de Administración y la figura del Compliance Officer

La iniciativa del órgano de administración al desarrollar este tipo de programas de prevención de delitos es clave, pues es el mismo órgano el que ostenta el poder de gestión y en el desempeño de sus funciones, el administrador tiene el deber de exigir y el derecho de recabar de la sociedad, la información adecuada y necesaria que le sirva para el cumplimiento de sus obligaciones (Ley 31/2014, modificación de LSC. Art.225:99802).

El Consejo de Administración debe designar la figura de compliance officer (oficial de cumplimiento), entendida como una figura con autonomía respecto a la Administración, para así poder desarrollar su función en el seno de la empresa. Pero destacar que a la vez, ambas deben estar coordinadas, porque como expresa Adán Nieto en el II Congreso Internacional de Compliance (2017), el compliance officer es una figura auxiliar y no ejecutiva.
El compliance officer puede ser específico de un área de la compañía o afecto a un sector (por ejemplo: responsable en materia de blanqueo de capitales, medioambiente, etc.), o por el contrario ser genérico y estar regulado por la norma ISO 19600.

"Esta figura debe tener cuidado de ejecutar diligentemente el modelo de Compliance que tenga asignado, asumiendo la responsabilidad por no hacerlo, como le sucedería a cualquier otro profesional en el contexto de sus obligaciones" (Casanovas, 2017: 4). Al ser una figura clave para el mantenimiento y mejora de la cultura de integridad, sus actividades deben ser respaldadas visiblemente desde la empresa y también desde las Administraciones Públicas, incluida la oficina judicial. Por ello, es esencial la creación de una fuerte relación de confianza entre las áreas de la organización y el compliance officer (Luceño y Herrera, 2017).

CAPÍTULO 3

PROPUESTA DE MODELO TEÓRICO DE GESTIÓN DEL RIESGO

3.1 PREÁMBULO

Una vez analizada y estudiada en profundidad la parte teórica de nuestro Trabajo Fin de Grado, nos centramos en la parte práctica de nuestra investigación. Partiendo de los fundamentos teóricos, previamente explicados con sus diversas fuentes, vamos a obtener nuestra propuesta. Para ello, nos basamos en tres pilares fundamentales que hemos ido tratando tanto explícita como implícitamente a lo largo del presente trabajo. Ellos son los riesgos empresariales, la estrategia y el cumplimiento normativo o compliance. Mediante estas tres bases, sus relaciones existentes, y tomando como referente la UNE 19601:2017, el modelo norteamericano COSO, las normativas y legislaciones correspondientes, llegaremos a la propuesta final de un modelo teórico de gestión integral de riesgos.

El modelo es aplicable a cualquier tipo de empresa (sector, tamaño, capacidad, titularidad del capital, etc.), debido al carácter generalista que ofrece el mismo. No obstante, nosotros nos centraremos en las pequeñas y medianas empresas (PYMES) por ser las que predominan en el territorio español. Creemos que el carácter general del modelo, es lo más adecuado ya que así sirve de base a todas las compañías; pero sin olvidarnos de la existencia del contexto y características específicas de cada organización. Así, cada empresa deberá matizar sus aspectos concretos debido a la diversidad existente en el tejido empresarial actual.

El modelo lo representaremos esquemáticamente para conseguir un efecto visual y así resultar más cómodo a la hora de explicar y de ser entendido por aquellos interesados en la materia.

Una vez mostrada nuestra propuesta y habiendo proporcionado diferentes ejemplos de riesgos que deberán ser conocidos, nos centraremos en abordar las líneas maestras para la puesta en marcha de dicho modelo (comenzando con el establecimiento de la política, pasando por las diferentes fases, hasta llegar al diseño y puesta en marcha de planes preventivos y el seguimiento y la revisión del modelo).

Una vez llegado a este punto, introduciremos en nuestra propuesta, la idea de utilizar el Cuadro de Mando Integral (CMI) como herramienta clave de gestión para optimizar la medición, el seguimiento, el control y la supervisión. Dicho cuadro de mandos establece indicadores claves de riesgo para PYMES (esto no quiere decir que se tengan que descartar otras herramientas

posibles). Señalar que nos hubiese sido de gran interés poder realizar la propuesta del CMI, basada en Norton y Kaplan (1990), mediante la filosofía de clasificaciones de indicadores del mismo, pero ajustada a la gestión de riesgos propuesta por COSO (por ser nuestro referente). Debido a nuestra limitación de espacio permitida en el trabajo, nos ceñiremos a introducir esta herramienta y a establecer una pequeña variación terminológica (adaptada a la gestión de riesgos tratada) y que sería la que utilizaríamos para su ejecución.

3.2 RASGOS CARACTERÍSTICOS DEL MODELO PROPUESTO

El modelo teórico planteado para gestionar los riesgos empresariales, se caracteriza por agilizar y mejorar el funcionamiento de la compañía reduciendo la incertidumbre. Dicha reducción se obtiene a través de la introducción de la gestión de riesgos organizacionales dentro la estrategia organizativa, de aquellos procesos que resultan esenciales para la compañía y de las relaciones de valor añadido con los grupos de interés.

Durante toda nuestra investigación, hemos hablado de la importancia del papel fundamental que deben de ejercer los gerentes de las organizaciones. Pues bien, gracias a esta herramienta, se podría llegar a fortalecer el gobierno corporativo, además de facilitar a los directivos el control, enfocado hacia la creación y protección del valor a lo stakeholders.

Mediante la gestión de riesgos se pretende mantener el riesgo por debajo del umbral fijado con anterioridad, gestionándolos dentro de un nivel aceptado. Con el modelo integral de gestión de riesgos propuesto por otro lado, pretendemos facilitar la revisión de la estrategia empresarial; así mismo, se utilizan mecanismos de revisión y adaptación de la empresa.

El modelo que proponemos no es sólo compatible con los sistemas normalizados tipo ISO 9001 ó 14001, sino también con los modelos de excelencia (el EFQM 2013 vigente) y permite aprovechar numerosas sinergias de los mismos.

Nuestro modelo no distingue a priori entre empresas o personas jurídicas de carácter público o privado, pudiendo ser utilizado en cualquiera de ellas independientemente de la titularidad del capital de la empresa.

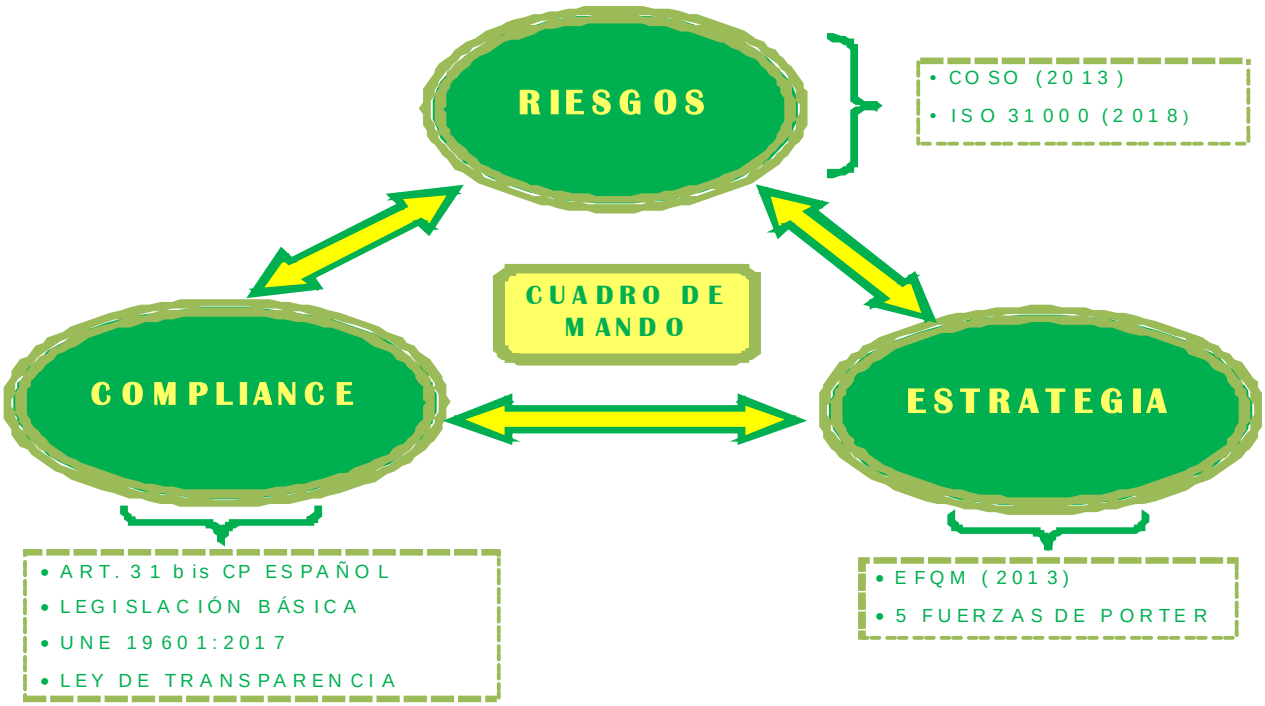
Podría reducir de costes al aplicar un mejor cumplimiento de requisitos legales y otros y, una característica final muy relevante es la referida al ámbito jurídico-penal. Nuestra propuesta contempla la introducción de indicadores referidos a las circunstancias y procesos vinculados a los delitos incluidos en dicho artículo.

Gracias a estos mecanismos de prevención, anticipación, cumplimiento normativo, actuación correcta, entre otros, se puede llegar a evitar impactos jurídicos tanto para la compañía como a nivel personal de los directivos, administradores y empleados de la compañía. Es decir, la posesión de dichos modelos podría ser una causa atenuante e incluso eximente en algunos casos, de directivos y empresas incursas en procesos penales. A pesar de esta reducción o exención de responsabilidad penal, queremos resaltar que mucho más importante nos resulta el hecho de conseguir implantar una cultura de cumplimiento previa en la que se centren los esfuerzos en las actuaciones preventivas.

En aquellos casos en los el delito no se haya podido prevenir, se hace mención en el II Congreso Internacional de Compliance (2017), que la fiscalía general valora la conducta de la persona jurídica después del delito. Se responde a una cultura verdaderamente de cumplimiento cuando "La empresa se compromete y colabora activamente con la investigación, cuando se compromete a revisar el programa en aquellos aspectos en los que puede haber fallado, cuando aplica medidas disciplinarias sobre aquellas personas físicas que hayan cometido el delito, cuando intentan reparar inmediatamente el daño, cuando realizan una investigación interna que ponen a disposición del órgano judicial" (Luzón, 2017). Estas conductas resultan muy relevantes para la fiscalía y es aquí cuando se puede permitir la reducción e incluso la exención de la pena.

Una vez comentadas las características esenciales del modelo a nivel general, procedemos a representarlo de manera gráfica y esquemática, en un intento de que así resulte más cómoda la comprensión de sus aspectos prácticos para el uso empresarial.

Seguidamente y previo a extendernos con las líneas maestras para la puesta en marcha del modelo presente (a continuación representado), y su posterior diseño y ejecución de planes preventivos en función de la evaluación de los riesgos detectados, procedemos a comentar ciertos tipos de riesgos, respetando la clasificación establecida por COSO y la cuál tomamos como referente en nuestro marco teórico.



Fuente: Elaboración propia

Figura 3: Modelo propuesto de gestión integral de riesgos

3.3 ALGUNOS TIPOS DE RIESGOS QUE DEBEN SER CONOCIDOS

Cuando definimos riesgo, mencionamos al célebre economista Knight (1921) que decía que la asunción de riesgos es inherente al desempeñar el papel de empresario. La gestión del riesgo es un tema que preocupa en el ámbito directivo como indicamos. De hecho, datos de un pasado cercano dicen que en 2004, “Más del 85% de las empresas pensaba tener en funcionamiento un sistema de gestión integral de riesgos en menos de 3 años. Es decir, en 2007” (Price Water House Coopers, 2004:38).

Como se observa en nuestro esquema teórico, para abordar el tema de riesgos, hemos usado dos bloques claves. Por un lado la prestigiosa norma de gestión de riesgos, conocida como ISO 31000:2018 de Gestión del Riesgo. La usamos por su enfoque genérico ya que gestionar cualquier forma de riesgo de manera sistemática, transparente y fiable, dentro de cualquier alcance y contexto (sin olvidarnos del contexto específico de cada empresa, sus objetivos, entorno y partes interesadas concretas) y por su idea de que la gestión de riesgos es parte de la gobernanza y, que el liderazgo es fundamental en la gestión. Por otro lado, le

damos especial hincapié al modelo norteamericano, marcado también por su carácter genérico que hace que sea aplicable a toda compañía. Como indicamos en el apartado teórico de riesgos empresariales, a la hora de clasificar los riesgos nos encontramos con bastante diversidad y nos resultó difícil establecer una clasificación clara. Finalmente pactamos que COSO (2013) sería el mejor referente a la hora de establecer la tipología.

No obstante, por problemas de extensión, en el anexo III incluiremos la clasificación de riesgos sugerida por COSO (2013).

Finalmente señalar que la norma UNE-EN 31010 (2011), de técnicas de apreciación al riesgo, contiene numerosas técnicas, así como una metodología a seguir para identificar y evaluar los diversos tipos de riesgos existentes. Señalamos algunas que nos han resultado interesantes como la Técnica Delphi (marcada por la opinión de expertos, pero no aporta datos cuantitativos), el Análisis de fiabilidad Humana (HRA) (que puede servir para ver la influencia o posibles riesgos de los errores cometidos por los humanos; además es cuantificable), el Análisis del árbol de fallos, el Análisis de causa y consecuencia (ambas cuantificables), entre otras. No podemos profundizar más sobre ellas debido a la extensión permitida en el trabajo. Puede consultar los anexos A y B de la norma para más información.

3.4 LÍNEAS MAESTRAS PARA LA PUESTA EN MARCHA DEL MODELO

En este apartado vamos a abarcar todas las partes o fases que debería de poseer el modelo, desde la definición de la política del mismo, pasando por el diseño de la estructura, el diagnostico de riesgos (por un lado del contexto y por otro de los procesos), evaluación, creación del mapa de riesgos, identificación de riesgos prioritarios (mediante la ayuda del mapa obtenido),el diseño y puesta en marcha de planes preventivos, unido al control, y en último lugar la supervisión y revisión del modelo. Procedemos a todo ello:

3.4.1 Definición de la política (objetivos)

Para definir la política de nuestro modelo nos hemos basado en la política de la norma UNE-EN ISO 9001 (2015), la UNE-ISO 19600: 2015, en la 31000: 2018 sobre gestión de riesgos y dentro del modelo EFQM, en su agente facilitador denominado como política.

Una vez consultado con los trabajadores de la compañía, el órgano de gobierno (individual o colectivo) y la alta dirección deberían de establecer una política que: se adecue al propósito y contexto de la organización, incluya el compromiso de cumplir los requisitos que sean aplicables, proporcione un marco de referencia para establecer los objetivos e incluya a la mejora continua como uno de los aspectos clave.

Podemos hacer mención a ciertos temas vinculados con la política, como son:

- Compromiso firme, decidido y sin fisuras de la alta dirección (Benítez, 2017).
- La política debería determinar cuáles son las partes interesadas y así diseñar la misma en función de las necesidades y expectativas presentes y futuras de todos sus grupos de interés o stakeholders; creando valor para todos ellos.
- Por otro lado de debe de determinar el alcance del modelo y las obligaciones (que dentro del área de cumplimiento normativo, pueden ser tanto de origen interno (Soft Law), como externo (Hard Law o Soft Law)[18]).
- Aconsejamos a las empresas en sus comienzos con el modelo que establezcan la base de los objetivos organizacionales para las consideraciones de riesgo y actividades de gestión, debiendo alinearse con la estrategia de la empresa. Los mismos deben establecerse antes de la identificación de posibles acontecimientos que dificulten su consecución.
- El compromiso de tener los recursos disponibles necesarios, para así poder facilitar la obligación de rendir cuentas.
- Se debe disponer de programas de formación para asegurarse que todos los empleados están formados en la materia. Así se permite que los empleados comuniquen riesgos que previamente no hubieran identificado, sirviendo como una fuente de mejora continua.
- Por otro lado, la política se tendría que comunicar de una forma apropiada. Lo ideal sería que estuviese disponible como información documentada y escrita en un lenguaje sencillo para que todos los empleados la comprendiesen sin ningún tipo de problemas.

En definitiva, la integración de este modelo de gestión de riesgos, debería ser en la compañía un proceso dinámico e iterativo; debiéndose de adecuar a las necesidades y la cultura organizacional. Debería ser una parte más, y no estar separada del propósito, el compromiso, el liderazgo y la gobernanza empresarial. En definitiva, debería establecerse de acuerdo con los valores, objetivos, estrategia y operaciones de la compañía.

[18] Requeriment o Hard Law son aquellos requerimientos con las partes interesadas. Commitments o Soft Law son directrices, estándares, recomendaciones, guías, prácticas y buenos usos que reflejan el estado de la cuestión en un área de actividad. En materia de compliance, el Soft Law acostumbra a ser mucho más rico y detallado que el Hard Law y resulta imprescindible para el diseño y desarrollo de los SG de Cumplimiento (Bonati, F. Capturado en bonatipenal.com; fecha: 25/04/2018).

3.4.2 Diseño de la estructura

Este apartado debería abordar todo lo relativo a la estructura organizativa vinculada con la materia. Es decir, se tratarían temas como el Consejo de Administración y la figura de compliance officer, todo ello ya explicado en nuestro apartado teórico de compliance, en el subapartado de "Responsabilidad del Consejo de Administración y la figura del compliance officer".[19] Por ello, no vamos a extendernos más. Simplemente recalcar como ya dijimos, que en el caso de las PYMES, empresas en las que nosotros nos centramos, no tiene sentido hablar de Consejo de Administración, por la posible carencia del mismo. Pero sí sería requisito necesario, poseer al menos la figura de compliance officer (personal que puede ser tanto interno como externo a la compañía).

3.4.3 Diagnóstico de riesgos

Ya en las normas ISO de SGC, hablábamos de la necesidad y el beneficio que aporta el poder abordar riesgos y oportunidades que estén asociados con los objetivos y el contexto de la empresa; debido a que un pensamiento basado en los riesgos y oportunidades, es esencial para poder lograr la correcta implantación de tales sistemas. De hecho, tratamos la necesidad del análisis permanente de contexto, identificando así los riesgos estratégicos, de transparencia o de información y de cumplimiento. Por otro lado, abordábamos el análisis de los riesgos vinculados a los procesos, identificando los riesgos operacionales. Pues son estos dos términos (contexto y procesos), los que debería de tratar la empresa a la hora de realizar el diagnóstico de riesgos. Profundizamos en ellos:

1) Por un lado, el contexto: El contexto de la empresa como bien conocemos, se divide en dos categorías (macroentorno y microentorno). Ambas están formadas por factores externos gran parte de los cuales no son controlables por la compañía. Lo ideal sería poder preverlos. El macro incluye aspectos como el ambiente político, tendencias económicas, evolución tecnológica, cambios socioculturales entre otros. El micro por su parte, contiene aquellas fuerzas que se encuentran cercanas a la organización y que por tanto, influyen más directamente a la hora de satisfacer a sus clientes. Aborda desde la propia empresa, los clientes, proveedores, los sustitutos, las amenazas de los entrantes potenciales y los competidores.

[19] Consultar apartado 2.5.3, página 28 para obtener información sobre la materia.

Para que la compañía pueda tratar el macro y el micro, debería realizar un análisis DAFO donde se gestionasen las debilidades, amenazas, fortalezas y oportunidades. Al estar tratando un modelo para la gestión de riesgos, sería prestar una mayor atención a las debilidades propias de la empresa y las amenazas del exterior; pero eso no quiere decir que deban olvidarse del análisis de las fortalezas y oportunidades, ya que también podrían ser el origen de riesgos asociados a la compañía.

Para el análisis del macro y el micro, proponemos el empleo de dos herramientas muy conocidas. Por un lado, para el macro, el análisis PESTEL (trata todo lo político, económico, social, tecnológico y legal). Nos gustaría resaltar que al estar abordando la materia de compliance en nuestro modelo teórico, estimamos oportuno que en las empresas, se hiciese especial hincapié en el ámbito legal. Por otro lado, para tratar el micro, aconsejamos la utilización de las 5 fuerzas de Porter[20] ya explicadas en el marco teórico, en el apartado de la excelencia y EFQM[21].

Comentario aparte, queremos resaltar una serie de aspectos concretos del contexto, basadas en la metodología norteamericana COSO (2013):

- Dentro del microentorno, en la propia organización, se abordará el estudio, en sentido amplio, de las necesidades de la organización, definiendo previamente a la empresa, tratando aspectos como: La estructura societaria, el volumen (en el caso de las PYMES sería hasta 50 millones de euros), el sector de actividad, la estructura interna de la misma y el ámbito de actuación, ya que si abarca el campo de la internacionalización debería considerar entonces, legislaciones extranjeras en materia de cumplimento (sobre todo norteamericanas por su avance poseído en la materia).

  También se analiza la situación de partida en materia de riesgos y cumplimiento, es decir, su madurez organizativa al respecto.
- Ambiente interno: Dentro del estudio del microentorno, en concreto dentro de la propia empresa, se deberían de tratar los valores y la filosofía de la misma, reflejando el tono de la organización y cómo considera y gestiona el riesgo. Se debería establecer el escenario para lo que se define el apetito o grado de aversión al riesgo.

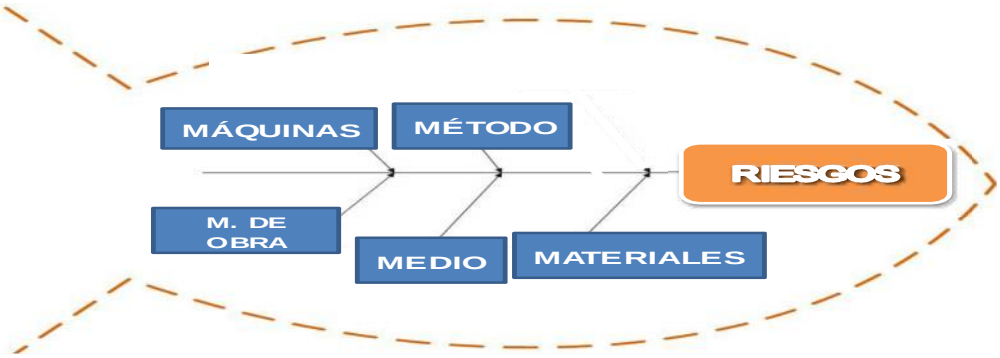
  El ambiente interno forma la base sobre la que se posicionan el resto de elementos e influye de manera significativa en los demás objetivos y estrategias. Es decir, es una

[20] Estas fuerzas abarcan: La posibilidad de amenaza ante nuevos competidores, el poder de negociación de los proveedores, tener capacidad para negociar con los compradores asiduos y de personas que lo van consumir una sola vez, amenaza de ingresos por productos secundarios y la rivalidad entre los competidores.

[21] Consultar apartado 2.3,2 página 12

oportunidad para alinear y conducir proactivamente a la organización (COSO 2013:7). Debe ser la actualización de la visión de liderazgo y las aspiraciones estratégicas.

2) Por otro lado, los procesos: Aquí se abordaría los riesgos operacionales o de proceso. Creemos que la organización podría usar para ello, la herramienta de las 5M de Ishikawa (1943) o también conocido como diagrama causa-efecto o diagrama de la espina de pescado. Esta herramienta se basa en cinco bloques fundamentales y en base a los mismos girarán las posibles causas del problema (en nuestro caso, serían causas de la existencia de riesgos). Estos pilares son: la maquinaria que interviene en el proceso, el método aplicado, la mano de obra, el medio ambiente y los materiales. Se trataría de una representación gráfica visual similar a la original, pero con la particularidad de situar el riesgo a tratar (dentro de los riesgos de proceso) en la "cabeza del pescado" y en la espina central se representarían las causas de los mismos.



Fuente: Elaboración propia

Figura 4: Las 5M de Ishikawa adaptada a los riesgos de proceso

Existen otras herramientas perfectamente aplicables por la empresa al ser complementarias con la anterior, es decir, no excluyentes con las 5M. Ellas son el Análisis Modal de Fallos y Efectos (AMFE), y el 6 Sigma. Nos gustaría poder profundizar en las mismas pero debido a la extensión permitida en nuestro trabajo, nos ceñimos a nombrarlas exclusivamente.

Finalmente, tras el diagnóstico realizado, se debería de abordar la medición de la incertidumbre; ya que un importante resultado del análisis, se enjuicia la incertidumbre del entorno. Para ello, nos servimos del prestigioso autor Mintzberg, H. (1984), que señala que para conocer el nivel de incertidumbre del entorno se debe analizar variables como:

- Estabilidad: cantidad, profundidad, rapidez e impredecibilidad de los cambios.
- Complejidad: número de factores y cambios en los mismos, grado de comprensibilidad o requerimiento de conocimientos o técnicas complejas o simples.
- Diversidad: cantidad de variables que afectan y grado de similitud en las mismas.
- Hostilidad: derivada de la competencia y del incremento de amenazas.

Para enjuiciar el grado de incertidumbre, la empresa podría construir una tabla que recogiese la estimación de las variables mencionadas. Para su elaboración la organización debería de apoyarse en los resultados obtenidos tras el análisis del contexto y los procesos.

VARIABLE	SITUACIÓN	TENDENCIA	VALORACIÓN
Estabilidad	-	-	-
Complejidad	-	-	-
Diversidad	-	-	-
Hostilidad	-	-	-
GRADO DE INCERTIDUMBRE			—

Fuente: Elaboración propia

Figura 5: Medición de la incertidumbre

Mediante su representación, podemos observar que hemos usado tres variables: situación, tendencia y valoración. La situación se evaluaría en una escala de: nula, muy baja, baja, alta, muy alta. También podría cuantificarse asignando valores como: 0, 1, 2, 3, 4 y 5. La tendencia podría ser o creciente, decreciente o estable y por último la valoración por tanto podría ir desde muy negativa hasta muy positiva.
El grado de incertidumbre obtenido, es una valoración general en función de las estimaciones realizadas, y así se podría hablar de diferentes grados de incertidumbre con una escala parecida a la anterior. Así por ejemplo, si la mayoría de variables tuviesen una valoración muy negativa se enjuiciaría el grado de incertidumbre como muy elevado.

Una vez realizado todo lo anterior, la empresa procedería a la identificación de acontecimientos o eventos. Es decir, la compañía tendría que reconocer todo evento que pueda tener impacto (ya sea positivo o negativo, externo o interno) sobre el cumplimiento de los objetivos. A la hora de identificar los riesgos, se debería de abordar tanto amenazas y debilidades como fortalezas y oportunidades (como ya indicamos en el DAFO). Identificados y clasificados los posibles riesgos, el órgano responsable de la empresa, debería entonces obtener la "Matriz de Riesgos" dónde se codificarían y describirían los riesgos generales inicialmente detectados y analizados[22].

[22] Para más información sobre la matriz, puede consultar el apartado teórico 2.4 de Gestión de Riesgos; pág. 21

Antes de continuar con las siguientes fases, queremos alegar un concepto muy vinculado al tema de gestión de riesgos, como es el término aversión al riesgo por parte de los directivos de las compañías. Debemos volver a mencionar a Knight (1921), por ser el padre de todo esto, mediante su teoría del empresario-riesgo. Él indicaba que el gerente puede tomar tres posturas frente al riesgo: indiferencia, preferencia al mismo y por último la aversión. Nosotros nos centramos en este último ya que en nuestra investigación partimos de la premisa que ignorar los riesgos empresariales no es una opción.

Debemos de señalar que en este aspecto, es muy decisiva la actitud que toman los directivos frente al mismo. Como es evidente, cada directivo tendrá un perfil distinto, con características propias, rasgos personales, una cultura organizativa distinta, ciertos gustos y preferencias, etc. y es por ello que existen diferentes posturas a la hora de abordar los riesgos. Podemos ir desde el directivo más conservador (tendente a maximizar su aversión al riesgo), hasta aquellos más atrevidos o arriesgados (tendencia a asumir mayores riesgos).

3.4.4 Evaluación de riesgos

A continuación vendría la etapa de evaluación de riesgos. Las organizaciones deberían de identificar y analizar en este momento, los riesgos fundamentales para la consecución de los objetivos. Se llevarán a cabo técnicas tanto cuantitativas como cualitativas. Primero se centrará en el riesgo inherente y posteriormente en el riesgo residual (Abella, 2006).

El órgano responsable de la empresa, en colaboración con otros directivos o responsables que consideren oportunos, son quienes habrán de proceder a la evaluación y análisis de cada uno de los riesgos identificados, valorando en cada caso la probabilidad de que el riesgo se produzca y la gravedad que tendría su ocurrencia para la empresa.

El análisis y la evaluación de riesgos variarán según los criterios utilizados en el sistema de gestión de riesgos. Siempre se debe partir de dos variables. Por un lado, la probabilidad[23] o nivel de posibilidades de materialización del riesgo y por otro, el impacto, gravedad o consecuencias de su materialización. Destacamos de nuevo el carácter subjetivo con que nos encontramos a la hora de determinar la cuantificación de la probabilidad y gravedad; ya que como hemos dicho, esto dependerá del perfil de cada directivo. Así por ejemplo, si tenemos cierto riesgo idéntico para dos directivos, aquel con menor aversión al riesgo, le dará una gravedad menor al asunto; mientras el conservador le dará una mayor importancia.

[23] Puede consultar más información sobre la misma en el Anexo II sobre términos vinculados al riesgo, página 52

El resultado del análisis y evaluación, es el mapa de riesgo que abordamos a continuación.

3.4.5 Obtención del mapa de riesgos

En esta figura, se irán posicionando los riesgos detectados en función de su probabilidad y gravedad en la compañía[24]. El mapa lo representaríamos gráficamente mediante los niveles de impacto y de sus probabilidades. Cada riesgo tomará un valor, surgido de multiplicar su nivel de probabilidad por el impacto otorgado al mismo (Thomson Reuters, 2017). Denominamos gravedad como sinónimo de impacto.

Los criterios o criticidad, para determinar el nivel de probabilidad y de gravedad, variarán en función del tipo de riesgo tratado. Así, si le otorgamos a la matriz cinco niveles por vector; el valor o importancia del riesgo podría ir desde 1 (el nivel de la probabilidad y de gravedad tendrían que ser 1), hasta 25 (el valor de cada uno de ellos sería 5). En definitiva, el producto de ambos factores, daría como resultado un valor de riesgos comprendido entre 1 y 25. Su representación gráfica sería:

		Gravedad				
		1	2	3	4	5
Probabilidad	1	1	2	3	4	5
	2	2	4	6	8	10
	3	3	6	9	12	15
	4	4	8	12	16	20
	5	5	10	15	20	25

Fuente: Elaboración propia

Figura 6: Representación del mapa de riesgos

Riesgo Insignificante / Asumible[25]
Riesgo Bajo / Aceptable con controles
Riesgo Medio / Indeseable
Riesgo Alto / Intolerable

A modo de ejemplo, si ciertos riesgos nos resultasen muy graves y tuviesen mucha probabilidad de ocurrir, evidentemente nos tendríamos que centrar en ellos.

[24] Puede consultar más información teórica, en el apartado teórico 2.4 de Gestión de Riesgos; página 21

[25] Para conocer las actuaciones a tomar, en función del tipo de riesgo, consulte el Anexo IV; pág. 54

Continuando con nuestro modelo, hemos considerado relevante la existencia de una herramienta o principio muy antiguo, como es el Principio de Pareto con la regla 80/20[26] (según la cual, aproximadamente el 80% de los efectos de una situación se determina por el 20% de las causas más importantes) y su conocida frase de "Pocos vitales, muchos triviales", es decir que hay muchos problemas sin importancia frente a unos pocos muy importantes. Nosotros hemos versionado estas ideas, basándonos en que existe una minoría de riesgos, que consideramos vitales, frente al resto de riesgos, de carácter mayoritario y que serían los triviales. En definitiva, el 20% de nuestros riesgos más importantes o significativos, son los que generarían el 80 % de las causas.

3.4.6 Identificación de riesgos prioritarios

Creemos que es posible encontrarnos frecuentemente con la regla 80-20 en las empresas a la hora de gestionar los riesgos. Si estuviésemos en lo cierto, quizás este principio, pueda servirnos como herramienta para establecer los riesgos de carácter prioritario. Amén de basarnos en Pareto para identificar este tipo de riesgos, nos basaríamos en los resultados obtenidos en el mapa previo, de la siguiente forma: Si observamos el resultado del gráfico, los valores que estuviesen por encima de cierta cuantía (previamente establecida), serían los que consideraríamos como riesgos más importantes. Señalar que la cuantía se vería influenciada de nuevo por el carácter subjetivo que abarcan las decisiones directivas a la hora de clasificar riesgos, es decir, por el concepto de aversión al riesgo argumentado.

Una vez llevado a cabo la detección, análisis y evaluación de riesgos, no debemos olvidar introducir la información y comunicación. Según Thomson Reuters (2017), se debe aglutinar y completar toda la documentación generada y obtenida. Contar con documentos que informan sobre la metodología seguida, resulta esencial para la organización. La información tiene que estar disponible para todos los niveles de la empresa. Este tema es crítico para gestionar riesgos y oportunidades. La elección de no informar, puede aumentar los riesgos de reputación o limitar oportunidades ya que las empresas que no publican esta información pueden parecer menos transparentes que sus competidores que si lo hacen. Los stakeholders esperan que las organizaciones no solo compartan sus éxitos, sino también sus fracasos y aquellas áreas de mejora (COSO, 2013).

[26] Para más información sobre Pareto, consultar Criado y Calvo de Mora (2004); Tema 4.

3.4.7 Diseño y puesta en marcha de planes preventivos para riesgos prioritarios

Una vez identificados los riesgos prioritarios, se debería pasar al diseño e implementación de las medidas necesarias para mitigar los riesgos, establecer una serie de indicadores y planes preventivos. Es decir, ahora es el momento de realizar las actividades de control. Lo que se pretende, llegado a este momento y analizando los datos obtenidos, sería realizar un plan de contingencias, es decir, con los resultados obtenidos, qué debemos hacer y cómo debemos tratar cada riesgo.

Como ya se adelantó, según el grado de aversión al riesgo que posea cada gerente o equipo directivo, llevará a tomar diferentes respuestas frente a los riesgos. Para su correcta gestión, las empresas deberían analizar el riesgo y posteriormente, ejecutar su tratamiento. Cuando posean la respuesta al riesgo más correcta para la situación en cuestión, se efectuará la reevaluación del riesgo residual. Las opciones para abordarlos las evalúa la dirección en función de cuatro categorías no excluyentes (UNE-EN ISO 9001:2015; 17-18):

- Evitar riesgos sin proseguir con la actividad riesgosa.
- Eliminar la fuente de riesgo. Reducir o mitigarlo estableciendo medidas para que el riesgo se sitúe por debajo del umbral.
- Compartirlo con terceros mediante su contratación para gestionarlo o mantener riesgos mediante decisiones informadas.
- Aceptarlo, asumiendo el riesgo conocido para perseguir una oportunidad.

Para dar respuesta a los riesgos, en primer lugar habría que identificar las actuaciones o controles relacionados con cada riesgo, ya existentes en la actualidad. Esto lo realizaría el órgano responsable de la empresa, en colaboración de otros directivos o responsables oportunos. En base a la prioridad de cada riesgo y a los controles o actuaciones existentes, se establecerían actuaciones adicionales. El personal involucrado debería comprender las disposiciones y realizar un seguimiento sobre el avance según lo planificado. Estas medidas podrán ser procedimientos, políticas y controles que asegurasen la adecuada ejecución de acciones contra riesgos (COSO, 2013).

Según Thomson Reuters (2017), se debe huir de medidas estandarizadas o “prefabricadas”, es decir, que estén listas teóricamente para adaptarse a cualquier organización. Con ello no queremos decir que se tuviesen que descartarse todas las medidas de control ya existentes,

(hay veces que podrían ser útiles y nos llevaría a reducir costes como de diseño); pero previamente, habría que asegurarse que se adaptasen a las necesidades de la empresa.

A la hora de diseñar los planes preventivos y basándonos en la norma de Gestión del Riego (UNE-ISO 31000: 2018), se debería: fundamentar la selección de las opciones propuestas, incluyendo los beneficios que se esperarían de los mismos; las acciones propuestas, los plazos que tuviesen previstos para su realización y finalización, informes y seguimientos requeridos, entre otros. En adición, estos planes deberían de integrase en los planes a nivel general de gestión de la organización. Una vez diseñados los planes preventivos y con los objetivos claramente definidos, lo que procedería, sería estimar aquellos recursos necesarios para poder llevarlo a cabo. Dentro de estos recursos, queremos hacer especial mención a la estructura organizativa o grupos de personas que se encargarían de su realización.

Para la correcta implementación de los controles diseñados para la mitigación de riesgos, se establecería un calendario de implementación en consonancia con los objetivos establecidos y la evaluación efectuada de riesgos detectados.

3.4.8 Seguimiento, revisión y supervisión (mediante el CMI)

Finalmente, tiene lugar la fase de supervisión por parte del órgano responsable en la compañía (junto con los directivos o responsables que considerase oportunos), para asegurarse que la organización estaría logrando sus objetivos y consiguiendo una mejora continua, dentro del umbral de riesgo y manteniendo la satisfacción de los interesados. Realizarían una revisión anual de riesgos en sus diversas categorías, identificando/revisando, evaluando, analizando y realizando propuestas de actuaciones y seguimiento. Igualmente, la gestión de riesgos debería ser objeto de tratamiento como mínimo, en la revisión anual realizada por la alta dirección y/o consejo de administración. Pero honestamente, se debería supervisar de manera continuada lo que sucediese en la práctica para realizar posteriores correcciones y así evaluar puntos débiles y áreas de mejora. Según el artículo de COSO, "Demystifying sustainability risk[27]" las empresas se deberían hacer preguntas del estilo a: ¿Son actividades o procesos alineados con la estrategia corporativa?, ¿Están siendo ejecutados de tal manera para permitirle a la empresa alcanzar mejor sus objetivos estratégicos?, ¿Las actividades agregan valor en términos de riesgo, conciencia y comprensión?, ¿Son lo

[27] Año 2013;página 9

suficientemente ágiles para responder a cambios en el ambiente de riesgo a medida que surgen problemas?", etc.

Al final, la efectividad de los enfoques de supervisión radica en la integridad, puntualidad y transparencia de resultados, así como lo que se hace con los resultados para administrar iniciativas de sostenibilidad y mitigar riesgos.

Finalmente, queremos dejar constancia que para el control y el seguimiento de todo el modelo, optaríamos por realizarlo mediante un Cuadro de Mando simplificado, basándonos en sus inventores (David P. Norton y Robert S. Kaplan, 1990), pero con la peculiaridad de pequeños cambios terminológicos. El cuadro de mando, entendido como herramienta de gestión, surge por la necesidad de relacionar de forma definitiva la estrategia y su ejecución empleando indicadores y objetivos en torno a cuatro perspectivas (financiera, de relación con los clientes, procesos internos y formación o aprendizaje y crecimiento)
Hemos decidido usar esta herramienta ya que según Kaplan y Norton (2002), los directivos como pilotos que son de la compañía, necesitan un instrumento que mida su entorno junto al rendimiento, para conducir el viaje hacia la excelencia futura. Y es que, como bien indicamos al finalizar el marco teórico, una de las herramientas para realizar un seguimiento de cómo de bien lo están haciendo las empresas es usando el CMI o Balanced Scorecards.

Según COSO (2013), usando indicadores clave de riesgo, las organizaciones pueden planificar, medir y controlar su gestión del riesgo de sostenibilidad en cada nivel de la compañía. La gerencia comunicaría esta información utilizando tableros ejecutivos.

Por lo comentado, nos hubiese gustado realizar la estructura general del mismo, con indicadores de riesgos para las organizaciones en general, y las PYMES en particular; pero debido a la extensión ya abarcada en nuestro trabajo y por el límite permitido del mismo, nos ceñimos a mencionar simplemente las pequeñas variaciones que hubiésemos aplicado al mismo. A lo largo de nuestra propuesta, seguiríamos la filosofía de clasificaciones de indicadores del CMI, pero ajustada a la gestión de riesgos propuesta por COSO al ser nuestro referente. En la clasificación establecida por el CMI, existen cuatro perspectivas ya nombradas, pues en base a ellas, obtenemos la variación terminológica siguiente: La perspectiva financiera, nosotros la denominaríamos económico-financiera que incluyese (indicadores de solvencia, activos, inversiones, rentabilidad, entre otros), la de procesos se denominaría igual; la que ellos llaman clientes, nosotros ampliaríamos dicha perspectiva mediante la denominación de grupos de interés o stakeholders. Finalmente, la que se denomina formación o personas, tendría idéntica nomenclatura.

CAPÍTULO 4

CONCLUSIONES Y LIMITACIONES DEL TRABAJO

4.1 CONCLUSIONES

Puesto que la sociedad en la que vivimos, marcada desde hace años por acontecimientos relacionados con las malas prácticas organizacionales, la corrupción tan presente y la necesidad de tratar los riesgos empresariales, creemos que toda la materia abordada en nuestra investigación verá incrementada su relevancia en el futuro próximo. Todo ello, debido al papel tan importante que están empezando a ejercer en muchas compañías, los sistemas de cumplimiento (entendido como la mejor opción para hacer frente a los riesgos organizacionales, mediante la prevención y reacción frente a los incumplimientos que puedan llegar a suceder). Por ello, consideramos la materia todo un reto futuro para aquellas compañías que pretendan obtener un éxito duradero y sostenible.

En definitiva, el hecho de poseer en las compañías un modelo de gestión de riesgos (aplicable a cualquier tipo de empresa con independencia de la titularidad del capital), puede dar lugar a una serie de efectos de carácter positivo ya que el mismo, estimula y mejora el funcionamiento de la organización, llegando a reducir su incertidumbre mediante la introducción de la gestión de riesgos dentro de la propia estrategia empresarial, abordando los procesos claves, introduciendo normativas relacionadas con la materia de compliance y mediante la creación de valor con los stakeholders.

A través de la posesión de estos modelos, basados en mecanismos de anticipación, prevención, cumplimiento normativo, actuación correcta, el buen gobierno, la transparencia y la sostenibilidad, creemos que se puede: Fortalecer el gobierno corporativo, ofrecer una mejor reputación para la compañía, unido a una mayor credibilidad y confianza frente a terceros; amén de la posibilidad de evitar ciertos impactos jurídicos. Es decir, gozar de estos modelos puede dar lugar a que las empresas incursas en procesos penales, puedan atenuar e incluso eximir ciertas responsabilidades penales. Pero volvemos a hacer hincapié, en que lo que realmente buscamos con la posesión de dichos modelos es conseguir tener implantada en la

compañía una verdadera cultura de prevención de riesgos y de cumplimiento, todo ello previo a la existencia de delitos.

4.2 LIMITACIONES DEL TRABAJO DE INVESTIGACIÓN

Por otro lado, durante la composición de nuestro trabajo, nos hemos encontrado con una serie de limitaciones que nos gustaría señalar. Las sintetizamos de la siguiente manera:

- En primer lugar, nos hemos encontrado con una cuantía relevante de limitación del espacio permitido para redactar nuestra investigación. Debido al tiempo dedicado al presente documento, hemos podido investigar en ciertos aspectos de la materia en mayor profundidad, pero simplemente los hemos mencionado o sintetizado, ya que su explicación nos ha resultado imposible por no gozar del espacio necesario para ello. Entre ellos queremos destacar por su relevancia, la intención que teníamos de proyectar la propuesta de cuadro de mando a realizar de forma genérica para las compañías. Así, no hemos podido cumplir con este objetivo que indicamos al inicio del documento presente.
- Por otro lado, a la hora de abordar el marco práctico, nos vimos con la dificultad de no poder llevarlo a cabo en una empresa cercana. Por ello, decidimos crear un modelo genérico (lo cual pensamos que resulta coherente ya que así sirve de guía genérica para organizaciones con diferentes características). Por ello, nos quedaría pendiente en un futuro su aplicación real, ya que debemos de señalar que nos gustaría poder ponerlo en práctica.
- Finalmente, nos hemos basado en ciertos autores, maestros, normas o referentes, por considerarlos bajo nuestro juicio como los más apropiados. Pero existen otros no empleados que quizás resultan ser buenas fuentes de apoyo.

BIBLIOGRAFÍA

Abella, R. (2006): "COSO II y la gestión integral de riesgos del negocio". Estrategia Financiera, 225. Capturado en: http://pdfs.wke.es/6/6/7/3/pd0000016673.pdf; fecha: 14/02/2018.

Ágora. Inteligencia colectiva para la sostenibilidad. (nd): Capturado en https://www.agorarsc.org/ley-de-transparencia-sector-privado-y-rsc-1a-parte/; fecha: 05/03/2018

Aristóteles (384 a.C-322 a.C), Citado por Criado, F. (2016).

Asociación Mexicana de Instituciones de Seguros (AMIS). (2015, Abril 14): "Gestión de riesgo empresarial para efectos de solvencia".

BBVA Empresas. (2015, Abril 29): "Qué es la transparencia empresarial y cómo puede implantarse". Capturado en http://www.bbvacontuempresa.es/a/que-es-la-transparencia-empresarial-y-puede-implantarse; fecha 15/03/2018

Behar, H. (2007): It's not about the coffee: Leadership Principles from a Life at Starbucks.

Benítez, D. (2017): Dossier Compliance y Norma UNE 19601, Thomson Reuters.

Bocanegra, Y. (2016, Septiembre 6). Capturado en Linkedin Business Development Latin America and Caribbean; fecha: 05/03/2018

Bonati, F. (nd): Capturado en https://www.bonattipenal.com/legal-compliance-iii-diccionario-basico/; fecha: 25/04/2018.

Casanovas, A. (2017): "El estándar nacional de compliance penal". Dossier Compliance y Norma UNE 19601, Thomson Reuters, 4.

Club Gestión de Calidad (2000): Guías de evaluación del modelo europeo de excelencia para PYMES. Madrid.

COSO (2013, Mayo): Thought Leadership in ERM - Demystifying Sustainability Risk. Integrating the triple bottom line into an enterprise risk management program. Capturado en http://www.ey.com/Publication/vwLUAssets/Demystifying_sustainability_risk/$FILE/Demystifying-Sustainability-Risk.pdf; fecha: 13/02 2018.

Criado, F. (2016): Apuntes de la asignatura Gestión de la Calidad de la Universidad de Sevilla

Criado, F. y Calvo de Mora, A. (2004): Gestión de la Calidad: fundamentos, desarrollos y aplicaciones prácticas. Ed. @3d, SL. Sevilla.

Criado, F. y Vázquez, A. (1999): Manual de calidad en la gestión: aplicaciones al ámbito universitario. Secretariado de Publicaciones de la Universidad de Sevilla. Sevilla

Crosby, P. (1979): Quality is Free: The art of Making Quality Certain. McGraw-Hill. New York

Deming, E.W. (1989): Calidad, productividad y competitividad. La salida de la crisis. Díaz de Santos. Madrid.

EFQM Leading Excellence (nd): EFQM model. Capturado en http://webcache.googleusercontent.com/search?q=cache:http://www.efqm.org/&gws_rd=cr&dcr=0&ei=uvqPWsSDIoztUvX5vYgI; fecha: 26/02/2018.

II Congreso Internacional de Compliance. (2017, Mayo 11-12). Madrid.

Imai, M. (1988): El Kaizen. La clave de la ventaja competitiva japonesa. CECSA. México

INCIBE. (2016, Julio 6): "Gestión de riesgos. Una guía de aproximación para el empresario". Capturado en: https://www.incibe.es/protege-tu-empresa/guias/gestion-riesgos-guia-empresario; fecha: 03/03/2018.

Instituto de Consejeros-Administradores (ICA). (2018, Febrero): El compliance y el Consejo de Administración: Guía Práctica, Febrero, 13-17. Madrid.

Ishikawa, K. (1943): Traducción del japonés al inglés por David J. Traducción Margarita Cárdenas (1997). ¿Qué es el control total de calidad? La modalidad japonesa.

ISO GUÍA 73 (2009): Gestión del Riesgo. Vocabulario. ISO. Definición 3.8.1.6. Cuba

Juran, J. M. (1951): Quality control handbook. McGraw-Hill. New York

Kaplan, R. y Norton, D. (1990): Cuadro de Mando Integral. The Balanced Scorecard, version 2002, 2ª edición, ed. Gestión 2000

Knight, F. (1921): Risk, Uncertainty and Profit. Houghton Mifflin. New York.

Ley 19/2013, de 9 de Diciembre, de Transparencia, acceso a la información pública y buen gobierno. (BOE núm.295 de 2013). Capturado en: https://www.boe.es/boe/dias/2013/12/10/pdfs/BOE-A-2013-12887.pdf

Ley 31/2014, de 3 de Diciembre, por la que se modifica la Ley de Sociedades de Capital para la mejora del gobierno corporativo. (Art. 225 LSC. Sec. I. Pág. 99802)

Ley Orgánica 1/2015, de 30 de Marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de Noviembre, del Código Penal de 2015, ARTICULO 31 BIS: Sec. I. Pág. 27088 (BOE núm. 77, de 31 de marzo de 2015)

Luceño, J.L. y Herrera, R. (2017): "El Compliance como responsabilidad del Consejo de Administración". Dossier Compliance y Norma UNE 19601, Thomson Reuters, 18-19.

Maza, J.M. (2017, Mayo 11-12). II Congreso Internacional de Compliance. Madrid.

Métayer, Y. e Hirsch, L. (2007): Primeros pasos en la gestión de riesgos. AENOR Ediciones. Madrid.

Matesanz, V. (29 Octubre 2017): "Las 10 claves de Richard Branson para tener éxito". Capturado en Forbes.es http://forbes.es/listas/5658/las-10-claves-de-richard-branson-para-tener-exito/10/; fecha: 26/02/2018

Mintzberg, H. (1984): La estructuración de las organizaciones. Ariel. Barcelona.

Nieto, A. (2017, Mayo 11-12). II Congreso Internacional de Compliance. Madrid.

Oliver, R. (2017, Junio 7, 19:12): "Trabajar al estilo japonés". El País. Capturado en https://elpais.com/economia/2017/06/07/actualidad/1496855106_996045.html; fecha: 20/02/2018. Menciona a Goy Yamamoto, A.

Parasurman, A., Zeithaml, V. A, y Berry, L.L. (1994): Reassessment of Expectations as a Comparison Standard in Measuring Service Quality: implications for further research. Journal of Marketing, Vol. 58.

Price Water House Coopers. (2004): 7th Annual Global CEO Survey, "Managing Risk: An Assessment of CEO Preparedness", 38. Capturado en http://www.top-consultant.com/deutschland/editorial/ceosurvey.pdf; fecha: 05/03/ 2018

Qualired. (2015, Diciembre 3, 08:17): "Los 7 principios de gestión de la calidad según ISO 9001: 2015", capturado en http://www.qualired.com/despachos1.asp?cod_des=62662; fecha: 10/02/2018.

Reeves, C.A. y Bednar, D.A. (1994): Defining Quality: alternatives and implications. Academy of Management Review, Vol. 19, nº3.

Rios, J. (2007 Octubre 30): "Filosofía del cuadro de mando integral". Capturado en http://www.empresarials.ub.edu/ec/pdfs/15462-ESP-Folosofia%20del%20Cuadro%20de%20Mando%20Integral%20_definitiu_.pdf; fecha: 01/05/ 2018.

Serra, R. (nd): "ISO 31000:2009. Herramienta para evaluar la gestión de riesgos". Capturado en https://www.isaca.org/chapters8/Montevideo/cigras/Documents/cigras2011-cserra-presentacion1%20modo%20de%20compatibilidad.pdf Uruguay; fecha: 03/03/2018.

Software ISO. (2015, Enero 12): "ISO 9001:2015, COSO como metodología de gestión de riesgo". Capturado en https://www.isotools.org/2015/01/12/iso-90012015-coso-como-metodologia-gestion-riesgo; fecha: 26/02/2018

Thomson Reuters. (2017, Abril): Dossier Compliance y Norma UNE 19601.

UNE-EN ISO 9000 (2015): Sistemas de gestión de la calidad. Fundamentos y vocabulario. AENOR, Madrid.

UNE-EN ISO 9001 (2015): Sistemas de gestión de la calidad. Requisitos. AENOR, Madrid

UNE-EN ISO 14001 (2015): Sistemas de gestión ambiental. Requisitos con orientación para su uso. AENOR, Madrid.

UNE-ISO 31000 (2010): Gestión de riesgos. Principios y directrices. AENOR, Madrid

UNE-ISO 31000 (2018): Gestión del riesgo. Directrices. AENOR, Madrid

UNE-EN 31010 (2011): Gestión del riesgo. Técnicas de apreciación al riesgo. AENOR, Madrid

UNE-ISO 19600 (2015): Sistemas de gestión de compliance. Directrices. AENOR, Madrid

UNE 19601 (2017): Sistemas de gestión de compliance penal. Requisitos con orientación para su uso. UNE, Madrid
Villegas, M. (2017, Mayo 11-12). II Congreso Internacional de Compliance. Madrid.

Wikiquote, la colección libre de citas y frases célebres. (2014, Abril 9): Frase célebre de Alfred de Musset. Capturado en https://es.wikiquote.org/w/index.php?title=Alfred_de_Musset&oldid=280131; fecha: 27/03/2018

World Commission on Environment and Development (WCED) (1987): Our Common Future. Oxford: Oxford University Press, p. 43

Yusof, S.M y Aspinwall, E. (2000): Total Quality Management implementation frameworks: Comparison and review. Total Quality Management, Vol.11, nº3. Pp. 285-289.

5 Fuerzas de Porter. (Nd): Capturado en http://www.5fuerzasdeporter.com/; fecha 12/05/2018.

ANEXOS

ANEXO I: ACRÓNIMOS

AENOR: Asociación Española de Normalización
AMIS: Asociación Mexicana de Instituciones de Seguros
BOE: Boletín Oficial del Estado
CMI: Cuadro de Mando Integral
CNMV: Comisión Nacional del Mercado de Valores
COSO: Committee of Sponsoring Organizations of the Treadway Commission
CP: Código Penal
EFQM: European Foundation for Quality Management
EN: European Norm
ERM: Entrerprise Risk Management
GCT: Gestión de Calidad Total
ICA: Instituto de Consejeros-Administradores
INCIBE: Instituto Nacional de Ciberseguridad
ISO: International for Standart Organization
LSC: Ley de Sociedades de Capital
PYMES: Pequeñas y Medianas Empresas
RSC: Responsabilidad Social Corporativa
SG: Sistema de Gestión
SGC: Sistema de Gestión de Calidad
TQM: Total Quality Management
UE: Unión Europea
UNE: Una Norma Española
US: Universidad de Sevilla

ANEXO II: CONCEPTOS VINCULADOS O ASOCIADOS AL RIESGO

CONCEPTO	DEFINICIÓN Y ASPECTOS RELEVANTES	FUENTE
Efecto	Desviación respecto a lo previsto. Puede ser positivo, negativo o ambos y puede abordar, crear o resultar en oportunidades y amenazas.	UNE-ISO 31000 (2018:7)
Incertidumbre	La incertidumbre junto con los objetivos, dan lugar al riesgo. Se origina en ambiente interno y externo en el que opera la compañía. Esta puede ser incertidumbre que: • Es una consecuencia de factores sociológicos, culturales y psicológicos asociados con el comportamiento humano. • Se produce por procesos naturales caracterizados por variabilidad inherente como por ejemplo el clima. • Surge de información incompleta o inexacta • Cambia en el tiempo debido por ejemplo a las tendencias, nueva información, etc. • Se produce por la percepción de incertidumbre que puede variar entre partes de la organización y sus partes involucradas	UNE-ISO TR 31004 (2015:13)
Probabilidad	Posibilidad de que algo suceda. Aclarando que en la gestión de riesgos, se utiliza para indicar la posibilidad de que algo suceda, esté definida, medida o determinada objetiva o subjetivamente, cuantitativa o cualitativamente y descrita utilizando términos generales o matemáticos	UNE-ISO 31000 (2018:8)
Riesgo de compliance	Efecto de la incertidumbre en los objetivos de compliance. Este riesgo se puede caracterizar por la probabilidad de que ocurran y las consecuencias de los incumplimientos de compliance respecto a las obligaciones de compliance de una organización.	UNE-ISO 19600 (Abril 2015)
Fuente de riesgo	Elemento que por sí solo en con la combinación de otros, tiene el potencial de generar riesgos	UNE-ISO 31000 (2018)
Evento	Ocurrencia o cambio de un conjunto particular de circunstancias. Puede ser también algo previsto que no llega a ocurrir, o algo que no se ha previsto y ocurre.	UNE-ISO 31000 (2018)
Consecuencia	Resultado de un evento que afecta a los objetivos. Puede ser cierta o incierta, tener efectos directos o indirectos, positivos o negativos sobre los objetivos. Puede expresarse de manera cuantitativa y cualitativa.	UNE-ISO 31000 (2018)
Control	Medida que mantiene y/o modifica un riesgo. Aclarar que los controles no siempre pueden producir el efecto de modificación previsto o asumido	UNE-ISO 31000 (2018:8)

ANEXO III: TIPOLOGÍA DE RIESGOS SEGÚN COSO (2013)

- Los riesgos estratégicos: Las PYMES al tratar estos riesgos, deben de abordar cualquier riesgo que afecte a la estrategia o al posicionamiento de la empresa en una industria. Las organizaciones deberán considerar una serie de problemas de sostenibilidad, muchos de los cuales pueden tener un gran impacto estratégico.

  Estos riesgos abarcan una clasificación bastante amplia, como son: Los derivados de inversiones estratégicas, acuerdos con socios o partners, relaciones con los stakeholders, cambios cuantitativos y/o cualitativos en la demanda del consumidor debido a la rapidez de cambio en sus deseos y a la rapidez de cambio de la tecnología, por la inflexibilidad organizativa, vínculos a proceso estratégicos del negocio, reputacionales, de RSC, gestión del capital intelectual, posición de comercialización, entre otros.

  A modo de ejemplo, podemos poner el caso de los consumidores que se preocupan cada vez más por el impacto social o el medio ambiente de los productos o servicios que consumen. Esto puede proporcionar por un lado, nuevas oportunidades para las empresas mediante el desarrollo, como podría ser, de nuevas líneas de productos verdes, mejorando los productos existentes para darles una ventaja competitiva, o mudarse a nuevos mercados. Sin embargo, estas oportunidades también conllevan por otro lado algún tipo de riesgo estratégico (COSO, 2013:3).
- Los riesgos operacionales o de proceso: Nos referimos a aquellos que se relacionan directamente con la eficacia y la eficiencia de los procesos u operaciones de la compañía, pero sin olvidarnos de los objetivos relativos al desempeño y rentabilidad, como comentamos en la teoría.[28]

  El contexto para operaciones comerciales ha cambiado significativamente en los últimos años y seguirá variando. Dentro del riesgo operacional los factores de sostenibilidad (RSC), a menudo tienen un impacto gigante en la reputación de las empresas y en sus resultados comerciales. Las empresas en general y las PYMES en especial, no deben minimizarlo o pasarlo por alto, porque entonces se producirán factores de riesgo e impactos potenciales de suma importancia.

  Los riesgos de procesos se contemplan también en COSO desde una perspectiva amplia incluyendo todo tipo de riesgos vinculados con los procesos clave y de apoyo del negocio como: riesgos derivados de las relaciones con los agentes, riesgos del clima o el medioambiente (incrementados en los últimos años), materiales, de maquinaria, vinculados con los recursos. También abarca las actividades que conforman la cadena de

[28] Abella (2006)

valor, los asociados con programas de proveedores sostenibles de la industria donde opera la empresa, tecnológicos, entre otros.

A modo de ejemplo, a causa del terremoto de Fukushima, Toyota perdió una producción de aproximadamente 370000 vehículos y por un tiempo dejó de ser el fabricante de automóviles número uno del mundo.[29]

- Riesgos de información o transparencia: Debido a la mayor y continua presión para ser transparente, el número de compañías que eligen informar sobre sostenibilidad, está aumentando notablemente en los últimos años. Los informes de RSC ayudan a los lectores a entender cómo de bien lo están haciendo las organizaciones.

  Estos riesgos, como bien indicamos anteriormente, son los que tienen que ver con la transparencia de la organización frente a sus grupos de interés. Abarca desde su credibilidad, los contenidos difundidos, la periodicidad, las metodologías y los indicadores utilizados para su medición, la accesibilidad a la información, entre otros.

  Tratan datos e información vinculada con los derechos humanos, de información sobre emisiones y consumo de energía, políticas corporativas, composición de la junta, entre otros.

  Todos estos datos, también están disponibles para inversores a través de servicios de información comercial tales como Bloomberg y Thomson Reuters; y para individuos inversores a través de sitios web como Fidelity.com. La información sobre estos sitios proviene principalmente de datos públicos disponibles revelados voluntariamente por las organizaciones, lo que aumenta la importancia de una divulgación transparente creíble. De manera anecdótica, promulgar que una serie de bolsas de valores como NASDAQ, Brasil y Singapur, han anunciado que apoyan a las empresas que figuran en sus intercambios para publicar informes anuales de sostenibilidad (COSO, 2013).

- Los riesgos de cumplimiento: Cuando hablamos de estos riesgos, las PYMES deben de abordar aquellos que se relacionen con la compañía y su cumplimiento, los requisitos reglamentarios, legales y aquellas normativas aplicables que tratamos previamente al hablar de la legislación básica en materia de compliance. En definitiva y volviendo a COSO (2013), incluye aquellos relacionados con las normas y acuerdos a los que estuviese sometida legalmente la empresa por su titularidad, actividad, tamaño, ámbito geográfico de las operaciones o cualquier otra circunstancia.

  Las principales áreas resultantes de riesgo directo o indirecto de las medidas reguladoras son variadas y pueden incluir desde riesgos relativos a los derechos humanos, los

[29] COSO (2013)

vinculados a la seguridad y salud laboral, pasado por los referidos al impacto ambiental, acuerdos y contratos con los clientes, proveedores o partners, etc., hasta llegar a las normas de anti soborno. Integrados dentro de los riesgos de cumplimiento, existen también los financieros y son cuatro: liquidez, solvencia, tipo de interés y cambio.

"Muchas empresas se enfrentan a regulaciones nuevas y en expansión de riesgos de cumplimiento resultantes de un número creciente de programas internacionales, nacionales y regionales. Estas iniciativas no solo abren nuevos riesgos de cumplimiento regulatorio para organizaciones, sino también reputacionales." Ejemplo: Un nuevo conjunto de normas de código de construcción en las zonas costeras como respuesta a aumento del nivel del mar. En áreas como Florida, ya están degradando los cimientos de edificios y reduciendo su esperanza de vida de manera anticipada (COSO, 2013:5).

ANEXO IV: ACTUACIONES A TOMAR CON CADA RIESGO EN FUNCIÓN DE SU IMPORTANCIA

Podemos establecer una clasificación en función de cuatro categorías: Alto, medio, bajo e insignificante. Los explicamos a continuación:

A) Riesgo ALTO: Se considera intolerable. El riesgo requiere de una acción inmediata, el coste no debe ser una limitación y el no hacer nada no es una opción aceptable. Este tipo de riesgo representa una situación de emergencia y deberán establecerse controles temporales inmediatos. La mitigación debe hacerse por medio de controles de ingeniería y/o por factores humanos hasta reducirlos a un tipo C o preferentemente de tipo D en un periodo de tiempo aproximado inferior a 90 días.

B) Riesgo MEDIO: Se considera indeseable. Este tipo de riesgo debería ser reducido y existe margen para investigar y analizar con más detalle. No obstante la acción correctiva debería darse en los primeros 90 días. Si la situación se demora más tiempo deberían de establecerse controles temporales inmediatos para reducir el mismo.

C) Riesgo BAJO: Se considera aceptable con controles. El riesgo es poco significativo, pero en función de si los controles actuales se consideran suficientes pueden o no requerirse actuaciones adicionales (dependerá de las decisiones del Director General), de forma que la mitigación debería enfocarse en la disciplina operativa y en la confiabilidad de los sistemas.

D) Riesgo INSIGNIFICANTE: Se considera asumible. Este riesgo no requiere acciones adicionales a los controles ya actuales. Puede programarse su atención y reducción conjuntamente con otras mejoras operativas.