LA CERTIFICACIÓN Y LA GESTIÓN DE RIESGOS

MARTA VILLANUEVA FERNÁNDEZ

Directora General de la Asociación Española para la Calidad (AEC)

Para cualquier organización es necesario hoy en día gestionar de forma adecuada la incertidumbre que presentan sus actividades convirtiendo ese hecho en una ventaja competitiva mediante la identificación, evaluación y gestión de los riesgos a los que debe hacer frente.

De esta forma, la implantación y desarrollo de sistemas integrados de gestión de sistemas integradosde gestión de riesgos (*Enterprise Risk Management*, ERM), se ha convertido en un aspecto esencial de las organizaciones, siendo un componente transversal para la ges tión de otros factores relevantes como la calidad, la inteligencia estratégica y el cambio organizativo. El gestor debe ahora tener la capacidad de anticipar los eventos desfavorables (riesgos) y obtener el aprovechamiento de aquellos eventos favorables (oportunidades) para su negocio.

La Real Academia Española de la Lengua define riesgo como la contingencia o proximidad de un daño. Etimológicamente la palabra riesgo proviene de una palabra latina (*riscio*) y ésta a su vez del árabe (*rizq*) haciendo alusión a lo que depara la Providencia. Sin embargo, a la hora de definir riesgo en su sentido más amplio, ISO (International Organization for Standardization), lo define como: «Combinación de la probabilidad de ocurrencia y el impacto de un evento determinado, considerando que las consecuencias posibles del evento puedan ser tanto positivas como negativas».

Para clasificar los riesgos, el criterio para hacerlo puede basarse en múltiples aspectos en función de su origen y causas, de su impacto tanto económico como en otro tipo de magnitudes, o bien de la naturaleza del mismo:

Riesgos de impacto tipo 1. Producen un daño de manera muy rápida, ocasionando pérdidas inmediatas y potencialmente significativas.

Riesgos de impacto tipo 2. Producen daños de manera más lenta, originándose una pérdida gradual y creciente.

Riesgos de impacto tipo 3. Son aquellos en los que los daños se manifiestan de una manera espaciada y continua, al igual que los anteriores, aunque en este caso la pérdida sea creciente y potencialmente significativa.

Riesgos de impacto tipo 4. Producen pérdidas significativas de una manera inmediata y la probabilidad de recuperación es remota.

Cierto es que el concepto de riesgo ha evolucionado a lo largo de la historia. El desarrollo de instrumentos financieros y actuariales hizo evolucionar de forma significativa su concepción: desde el siglo XVII se

utilizaban las opciones en ciertos productos como el grano o el ganado (un ejemplo es la crisis de los tulipanes en los Países Bajos). En ese mismo siglo se comenzó a desarrollar formalmente la industria mercantil de los seguros (tradicionalmente vinculada a la gestión de riesgos) relacionada de forma muy estrecha con los viajes comerciales a ultramar.

Sin embargo será en el siglo XX cuando verdaderamente llegue el desarrollo de la gestión de riesgos. Concretamente, en 1963 aparece el trabajo de Robert I. Mehrs y Bob Hedges titulado «*Risk Management and the Business Enterprise*», que les valió a sus autores la consideración de padrinos de la gestión de riesgos desde un ámbito puramente empresarial.

Del mismo modo, supuso un hito relevante la aparición en 1974 del «Círculo de la Gestión de Riesgos», que definía la importancia de las actividades en un sistema de gestión de riesgos: evaluación, transferencia y financiación, control y comunicación.

Pero no sería hasta los años 80 cuando comenzasen los esfuerzos por la creación de estándares públicos y mejores prácticas para la gestión de riesgos. Fruto de esa labor, cristalizarían aportaciones significativas como la emisión del marco de control interno COSO en 1987 por la Treadway Commission en los Estados Unidos, la Cadbury Commission (y las subsiguientes comisiones Hempel y Turnbull) en el Reino Unido (1992), los estándares australiano y neocelandés de Gestión de Riesgos, que fueron los primeros a nivel mundial (1995).

De forma paralela a esta situación, se ha ido profesionalizando la gestión de riesgos, siendo cada vez más común la figura del Responsable de Gestión de Riesgos (*Chief Risk Officer* o *CRO* en sus siglas inglesas) en las organizaciones, y surgen las primeras asociaciones profesionales para este tipo de perfiles, destacando las siguientes: Risk & Insurance Management Society (Sociedad de Riesgos y Aseguramiento) (1975), seguida de sus equivalentes en Europa, Latinoamérica, África y Asia, la Society for Risk Analysis Sociedad para el Análisis de Riesgos) (1980), London's Institute of Risk Management (Instituto Londinense de Gestión de Riesgos) (1986), la Global ssociation of Risk Professionals (Asociación Global de rofesionales de Riesgos) (1996), y la Professional Risk Managers International Association (Asociación Internacional de Riesgos) (2002).

No todas las organizaciones presentan esa capacidad de convertir riesgos en oportunidades y aprovechar las mismas de una manera óptima para generar ventajas competitivas y optimizar la creación de valor. Esta capacidad se denomina «resiliencia», haciendo referencia así a la facilidad de adaptación y respuesta de una organización a los riesgos a los que se expone. Crear organizaciones resilientes es un paso más en la evolución de la gestión de riesgos y lleva implícito un cambio de actitud que consiste en repensar todas las posibles amenazas y riesgos en términos de fortalecimiento de las ventajas competitivas.

La resiliencia dentro de la organización requiere de ciertas condiciones previas con el fin de garantizar su óptimo aprovechamiento. Estas condiciones irían desde el dinamismo para acortar los tiempos de respuesta frente a los riesgos identificados a la flexibilidad y adaptabilidad, pasando por el mantenimiento de canales de comunicación abiertos a todos los grupos de interés de la organización o la creatividad necesaria para identificar oportunidades y posibles ventajas para el replanteamiento de las posibles respuestas.

Precisamente, la importancia de esta capacidad de creación de oportunidades y ventajas competitivas está provocando un cambio de paradigma, pasando de la gestión de riesgos en sentido estricto (*Risk Management* tradicional) a la gestión de oportunidades (*Opportunity Management*). En una primera etapa la gestión de riesgos se centró en la identificación de los riesgos fortuitos, vinculados con perjuicios de eventos asegurables (por ejemplo catástrofes naturales) basándose en la experiencia previa pasada, así como en la determinación del coste de dicho aseguramiento y la transferencia de riesgos a terceros (mercado asegurador).

Posteriormente se centró en la predicción de las posibles pérdidas derivadas de los eventos de riesgo, principalmente los riesgos asegurables señalados anteriormente así como los riesgos financieros, aplicando una base estadística y matemática para evaluar dichas pérdidas, complementando así la información disponible de registros históricos. Esta fase coincidiría con las turbulencias financieras vividas en los mercados internacionales a finales de los años 70 y primeros 80, con el fin del patrón oro, las crisis del petróleo, las subidas de tipos de interés y la significativa volatilidad del mercado de divisas.

En las siguientes etapas la gestión de riesgos sería abordada de una manera más integral, comenzando a identificarse riesgos desde un punto de vista holístico, ampliando el foco a los riesgos operacionales y estratégicos, y apareciendo los primeros mapas de riesgos que servían para contextualizar los riesgos identificados tanto a nivel organizativo como cuantitativo, sin olvidar el cálculo del impacto económico de esos posibles eventos desfavorables.

Posteriormente, y como evolución natural, se comenzó a ver a las organizaciones como responsables de riesgos de muy diverso tipo, muchas veces interrelacionados entre sí, comenzando a hablarse entonces de los sistemas integrales de gestión de riesgos que consideran las correlaciones existentes entre los diferentes eventos.

Esa interrelación y la heterogeneidad de riesgos afrontados han hecho que se hayan instaurado sistemas globales de gestión de riesgos que abarcan e interconectan de una manera integrada todas las áreas de las organizaciones, son los *Enterprise Risk Management Systems* (ERM).

La evolución de estos enfoques y técnicas de gestión de riesgos obedece a las siguientes circunstan-

cias que se han dado en las propias organizaciones y en su entorno de negocio:

• Aumento de la complejidad de los riesgos afrontados

Las organizaciones de hoy en día afrontan diferentes procesos como la globalización económica, la estandarización de las necesidades, la multiculturalidad, la fragmentación y diversidad de los mercados, las recesiones financieras y económicas, el avance tecnológico… Las actividades se convierten por tanto en procesos que quedan influidos y determinados por una multiplicidad de factores y riesgos altamente heterogéneos.

• Necesidad de una gestión integral

Aunque es necesario que exista cierta especialización en la gestión de riesgos, es igualmente importante tratarlos desde un punto de vista más global, sabiendo que hay múltiples factores que interconectan y correlacionan las causas e impactos de los riesgos y que es importante mantener una visión y gestión global sobre los mismos.

• Presión regulatoria

Las empresas, como organizaciones sociales, están sujetas a presiones regulatorias para garantizar la transparencia en su gestión y la información de eventos y riesgos relevantes a los grupos de interés que se relacionan con ellas.

Las normas y estándares que han estimulado este desarrollo son muy variados: existen diversos códigos de buen gobierno en cada país (Informe Cadbury para Reino Unido, Informe Dey en Canadá, el **Código de Buen Gobierno** en el caso de España), así como regulaciones sectoriales como es el caso de Basilea I y II para instituciones financieras o Solvencia II para aseguradoras.

NECESIDAD DE LA GESTIÓN DE RIESGOS. FACTORES INTERNOS Y EXTERNOS

Entre los factores puramente internos, destaca en primer lugar la generalización entre las organizaciones del objetivo de reducción de costes y el aumento de la eficiencia. Un proceso de gestión de riesgos eficaz supone que se minimicen los costes. Por otro lado, los procesos estratégicos de expansión y la diversificación hacia nuevos mercados o áreas de actividad condicionan a las organizaciones a que tomen decisiones internas y operen en nuevos sectores y actividades para las que necesitan disponer de información adecuada para tomar decisiones.

Inicialmente la gestión de riesgos se ha venido efectuando por los departamentos organizativos de manera independiente, lo que se ha llamado estructura de silo o cubos de riesgos (*silo structure* o *risk buckets*). Esto significa que se desestimaban como no relevantes las interrelaciones que se producen entre los riesgos, los efectos de éstos y las diferentes unidades de una organización.

Se podría dar el caso de que las acciones tomadas en una parte de la organización para reducir un determinado riesgo, provocasen que otra parte de la organización asumiese mayor riesgo, lo cual no es muy lógico.

Los sistemas que integran la información de riesgos de las diferentes partes de la organización y posibilitan su gestión única coordinada en base a un perfil único de riesgos de la organización (aunque la gestión específica de cada riesgo se realice por diversos gestores) se han mostrado como una herramienta eficaz para terminar con ese paradigma de gestión fragmentada de los riesgos y con los problemas que ello genera.

En cuanto a los factores externos, las organizaciones desarrollan sus actividades en entornos cada día más globales, más complejos, dinámicos y competitivos. Por otro lado, existe una tendencia creciente por parte de los reguladores de exigir a las organizaciones una transparencia cada vez mayor en la gestión de riesgos y mayor volumen de información que se proporciona a los mercados, de manera que se garantice que todos los grupos de interés consiguen la información necesaria para sus decisiones.

Las organizaciones internamente perciben que los sistemas de gestión de riesgos aportan beneficios significativos en la gestión de operaciones (eficiencia y menores costes en la transferencia de riesgos, información más completa en las decisiones, gestión proactiva de principales eventos, etc.) pero también el mercado percibe como mejor práctica este paradigma de gestión y penaliza a aquellos agentes que no tienen implantados ni reconocidos estos sistemas integrales de gestión de riesgos.

ACTIVIDADES DEL PROCESO DE LA GESTIÓN DE RIESGOS

La gestión de riesgos es un proceso no lineal, compuesto de una serie de actividades que se realizan de manera continua. Éstas se agrupan en cuatro etapas (gráfico 1 en página siguiente):

1 Identificación de eventos

2 Evaluación de eventos

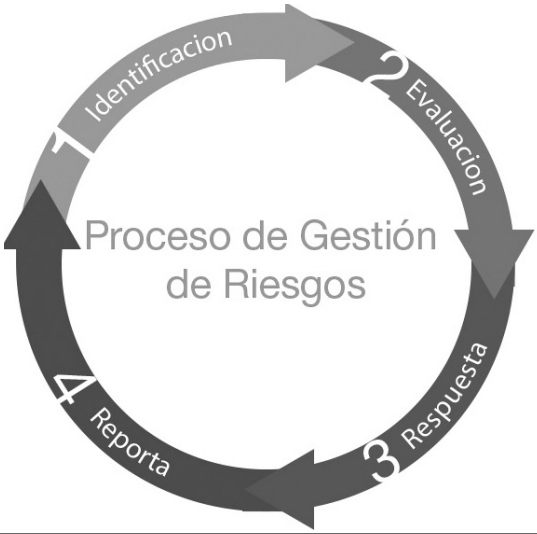
3 Respuesta al riesgo

4 Reporte y Comunicación

Identificación de eventos

La identificación de los riesgos es la primera fase y, en ella, se tipifican los riesgos que afronta la organi-

GRÁFICO 1
PROCESO DE LA GESTIÓN DE RIESGOS



FUENTE: Elaboración propia.

zación y que configura su perfil de riesgo. Pero no podemos olvidarnos de que los riesgos que identificamos siempre deben referirse siempre a los objetivos marcados en nuestra organización.

La identificación de riesgos no debe ser tan amplia como para que se identifique cualquier posible evento que afecte a la organización, sino que un riesgo es tal en la medida en que impida la consecución de los objetivos marcados. En definitiva, si no identificamos los riesgos sin atender a los objetivos, tampoco es posible su posterior priorización.

Una identificación completa de un riesgo debe considerar tanto sus causas como los posibles efectos adversos que se puedan derivar de la materialización del riesgo.

Hay que tener especial precaución en evitar identificaciones parciales de riesgos, siendo problemas comunes el identificar únicamente los efectos o no determinar las causas del riesgo.

Los riesgos, por tanto, deben identificarse a un nivel en el que se pueden indicar las causas y los efectos y que, por tanto, permite la articulación de medidas para su tratamiento y control.

Existen diversas técnicas para la identificación de riesgos, como por ejemplo la configuración de equipos multidisciplinares específicos o la realización de autoevaluaciones de riesgos (*risk self-assessment* o RSA).

Evaluación de eventos

La evaluación de eventos consiste en la estimación de los atributos determinantes del riesgo, que, como mínimo, deberá abarcar, la evaluación del impacto del riesgo y la probabilidad de ocurrencia. Evaluar eventos muy heterogéneos puede significar que para ciertos riesgos su cuantificación sea relativamente rápida, como por ejemplo los riesgos financieros, aunque para otros puede significar que sea difícil la estimación de cantidades concretas (por ejemplo, los riesgos reputacionales, con un componente muy significativo de subjetividad en su análisis y evaluación). En cualquier caso, resulta de utilidad tener un modelo específico para la evaluación de los impactos, de manera que sea un enfoque sistemático que garantice homogeneidad, transparencia y una documentación mínima adecuada de dicha evaluación.

Para algunos riesgos que sean verdaderamente difíciles de evaluar es cómodo utilizar escalas cualitativas con las que estimar el impacto y probabilidad. Las escalas más simples suelen contar con tres categorías para el impacto, que pueden ser alto, medio o bajo; y otras tres para la probabilidad, que pueden ser remota, posible o probable.

Por otro lado, si queremos ajustar más la evaluación, se puede trabajar con escalas de cinco intervalos, tales como: Insignificante, menor, moderado, alto o catastrófico, para el impacto. Y, remota, improbable, posible, probable o cierta, para la probabilidad (cuadro 1, en la página siguiente).

En la evaluación del impacto es importante distinguir entre el impacto inherente (el que representa el evento en sí) y el impacto residual (aquél impacto resultante, una vez que se han aplicado las actividades de control que desarrolla la organización).

Respuesta al riesgo

Una vez que el riesgo es evaluado, se tiene que comparar con el nivel de riesgo tolerable para la organi-

CUADRO 1
ESCALA PARA LA EVALUACIÓN DEL RIESGO

Según el impacto	Según la probabilidad
Insignificante	Remota
Menor	Improbable
Moderado	Posible
Alto	Probable
Catastrófico	Cierta

FUENTE: Elaboracion propia.

zación. Este riesgo tolerable es lo que se conoce como apetito al riesgo, es decir, cuánto riesgo está dispuesto a asumir una organización en sus actividades.

Existen varias respuestas posibles para los riesgos:

Reducir o Mitigar. Significa que la organización va a continuar con la actividad que genera el riesgo aunque tiene implantados controles que intentan reducir el riesgo residual afrontado, tanto si reducen la probabilidad de ocurrencia del riesgo como si reducen su impacto.

Es la respuesta más común a los riesgos de una organización. Para mitigar los riesgos se pueden definir controles preventivos, controles correctivos, controles detectivos o controles directivos.

Transferir. Significa que la organización transfiere a un tercero los efectos adversos en caso de materializarse el riesgo y ese tercero es que el finalmente acaba afrontando dicho riesgo.

Evitar. Significa que la organización va a dejar de realizar las actividades que generan el riesgo y por tanto ya no va a afrontar dicho riesgo. Si una actividad presenta un riesgo demasiado alto para el apetito definido por una organización, ésta puede optar con cesar dicha actividad, evitando el riesgo.

Aceptar. Significa que la organización continúa con las actividades que generan el riesgo y que no tiene previsto realizar actividades de control que disminuyan el impacto o la probabilidad del riesgo identificado.

Reporte y comunicación

El reporte y la comunicación de riesgos tiene dos finalidades principales. Por un lado garantizar un seguimiento adecuado de los riesgos identificados y, por otro, asegurar que la gestión de los riesgos es adecuada y no se necesitan acciones adicionales para tratar los riesgos identificados.

El procedimiento de reporte y comunicación debe ser integral para que se reporten los riesgos nuevos, si se identifican. Asimismo, garantiza que se realiza un seguimiento de aquellos riesgos relevantes, en todos los niveles organizativos pertinentes.

NORMAS Y REGULACIONES EN MATERIA DE GESTIÓN DE RIESGOS

Existen numerosos estándares internacionales para la gestión de riesgos, algunos desarrollados bajo enfoques más específicos, como por ejemplo para la gestión de riesgos de salud y seguridad en el trabajo, o riesgos ambientales; y otros diseñados bajo un enfoque general, que pretenden servir para una gestión integral de los riesgos, en cualquier tipo de organización y para cualquier tipo de riesgo.

■ ISO 31000

El estándar ISO 31000, realizado dentro de la Organización Internacional de Normalización, fue emitido en 2009 y actualmente es un referente en materia de gestión integral de riesgos a nivel internacional.

Esta norma contempla intrínsecamente la complejidad y variedad de riesgos, aspirando a ser un documento genérico que se pueda aplicar a todos los sectores y organizaciones. Es importante indicar que no establece directrices para el tratamiento de riesgos concretos sino que da orientaciones para la implantación de un sistema de gestión del riesgo que sea compatible con los estándares de gestión de riesgos particulares de cualquier sector.

En concreto, esta norma permite la gestión de cualquier tipo de riesgos, de una manera sistemática, transparente y efectiva. Podemos detallar algunos objetivos para esta norma:

– Establecer un marco común lo suficientemente amplio que permita la gestión de todo tipo de riesgos y la implantación de dicho sistema de gestión en cualquier tipo de organización.

– Realizar una unificación de los estándares existentes en materia de gestión de riesgos.

– Dotar al proceso de gestión de riesgos de la consistencia necesaria para que sea efectivo y ayude a las organizaciones a lograr su estrategia.

– Desarrollar un enfoque integral que abarque todas las fases de la gestión de riesgos, desde la implantación inicial hasta su seguimiento y mejora continua.

En principio se trata de una norma no certificable, lo que, en cierta medida, es visto por algunos expertos, como una garantía para que dicho contenido sea lo más amplio y objetivo posible.

Entre los beneficios reconocidos de contar con un sistema de gestión de riesgos acorde con el estándar ISO 31000, podemos destacar, entre otros, los siguientes:

• Aumento de la probabilidad del logro de objetivos. Si se conocen los eventos que pueden afectar al logro de los objetivos marcados, es más sencillo que éstos se puedan gestionar, en caso de ocurrir, y posibilitar así el logro de los objetivos, o minimizar la desviación respecto a ellos.

• Es un aliciente para una gestión proactiva. Se reconoce un papel necesario e importante en todos los niveles organizativos, lo que implica a todas las personas e incentiva su participación.

• Hace a la organización sensible respecto a las necesidades de identificar y tratar los riesgos. Un sistema formal y explícito garantiza que los miembros de la organización conocen lo que se espera de ellos a la hora de identificar y gestionar la incertidumbre.

• Favorece la identificación de oportunidades y amenazas. La incertidumbre es un mero cambio que gestionado anticipadamente y de forma adecuada se puede transformar en oportunidad.

• Mejora el reporte financiero. Una parte importante del trabajo financiero se centra en elaborar planes de negocio, presupuestos y perspectivas a futuro, lo que implica el conocimiento adecuado de lo que puede ocurrir. Cuanto mayor sea la información de la que se dispone, más acertado será ese reporte.

• Mejora el control y gobernabilidad de las organizaciones. La gestión de riesgos implica en sus primeras fases un ejercicio de identificación de los puntos débiles de la organización, aquéllos que se ven afectados por la incertidumbre, y en sus últimas fases la identificación de responsables y la gestión mediante la implantación de controles adecuados y efectivos para los eventos identificados.

• Facilita la comunicación y la confianza de los grupos de interés, ya que éstos están implicados en la gestión de riesgos a través de los canales de comunicación.

• Establece un marco robusto para la toma de decisiones y la planificación. Las decisiones son mejores cuanto mayor es la información con que se cuenta. Evaluar los riesgos implica aumentar necesariamente la información manejada.

• Asigna recursos de manera eficiente. La evaluación de riesgos se realiza comparándolos con los objetivos marcados. La definición e implantación de estrategias de tratamiento de riesgos implica asignar recursos en función del impacto en los objetivos, aumentando la probabilidad de lograr los objetivos, por lo que la asignación de recursos a esas medidas será más eficiente.

• Mejora la eficiencia y eficacia de las operaciones. Al conocerse y comunicarse de manera clara los objetivos que se espera conseguir y al identificar los posibles riesgos para lograrlos, se consigue una operativa más segura y eficiente.

• Aumenta el aprendizaje organizativo y la capacidad de resiliencia de las organizaciones. Un sistema de gestión que proporciona foros de discusión abiertos y flexibles garantiza el intercambio efectivo de información y el aumento del conocimiento de los miembros de la organización.

• Minimiza las pérdidas ya que, según lo comentado anteriormente, asigna recursos a las medidas de control más eficientes.

■ COSO

Otro de los estándares internacionales de referencia para la gestión de riesgos es el Marco Integrado de Gestión de Riesgos Corporativos emitido por el Committee of Sponsoring Organizations (COSO). Este estándar surge con una vocación integral, habiendo sido diseñado bajo un enfoque general, y pretende servir para una gestión de los riesgos, en cualquier tipo de organización y para cualquier tipo de riesgo.

El documento fue emitido en el año 2004. En la práctica se trata de un estándar de gran relevancia y aplicación en los Estados Unidos de América y en su entorno de influencia. Asimismo, la regulación del mercado de valores estadounidense (Ley Sarbanes Oxley o SOA, por su acrónimo en inglés Sarbanes Oxley Act) referente al control interno de las sociedades cotizadas, lo sitúa como un estándar de referencia en la gestión de riesgos requerida a las empresas. El texto legal es abierto en relación con el estándar que las empresas pueden utilizar aunque menciona COSO de manera explícita. Al ser una regulación obligatoria para las empresas que coticen en los Estados Unidos de América, (exigido por la SEC, el equivalente a la española CNMV), ha contribuido a que dicho estándar se extienda de forma internacional y se considere una mejor práctica en el campo de la gestión de riesgos.

También el Marco Integrado considera de manera explícita la variedad de riesgos, su complejidad y su impacto en cada organización. Cada sector, cada acción y cada proceso afrontan unos riesgos específicos a los que hay que añadir los riesgos genéricos que tiene cualquier actividad. Asimismo, la implantación de un sistema de gestión en una organización debe responder y amoldarse a ciertos condicionantes particulares de la misma, como su contexto, composición, estructura y estrategia.

Al igual que el documento ISO 31000, el Marco Integrado de Gestión de Riegos, o COSO II (ya que COSO I es el Marco Integrado de Control Interno), está enfocado para que cualquier tipo de organización pueda utilizarlo en la gestión de riesgos de su actividad. Pretende ser un marco común.

GRÁFICO 2
ELEMENTOS QUE SE DEBEN CONSIDERAR EN LA DETERMINACIÓN DE UN RIESGO

FUENTE: Elaboración propia.

Las diferencias con ISO 31000 no son tan sustanciales, aunque es cierto que el Marco COSO II surge con una clara aspiración de mejora del control interno de las organizaciones, lo que condiciona las últimas fases de la gestión de riesgos, así como la necesidad explícita de que dicho marco quede:

✓ Alineado con los objetivos de la organización, para garantizar su viabilidad estratégica.

✓ Implantado en toda la organización, a todos los niveles, al igual que debe estarlo el control interno.

COSO II, consciente de esta misión, centra su labor en la falta de certeza y el reto que representa para los responsables el determinar cuánta incertidumbre se puede aceptar para incrementar el valor dado a los grupos de interés. El valor se maximiza cuando la dirección de una organización establece una estrategia y unos objetivos y se consigue un equilibrio óptimo entre las metas de crecimiento y rentabilidad y los riesgos asociados.

En este contexto, los eventos pueden tener un impacto positivo o negativo, o ambos tipos de efectos a la vez. Para COSO II, los riesgos son los eventos con un impacto negativo que impiden la creación de valor y el logro de los objetivos.

La siguiente figura muestra un detalle de los elementos que se deben considerar en la determinación de un riesgo:

■ La gestión de riesgos en la nueva ISO 9001:2015

La gestión de riesgos es una de las novedades principales de la norma ISO 9001. La organización tiene que tener en cuenta para la planificación de su sistema de gestión de calidad, los riesgos y oportunidades que necesitan ser tratados de forma que aseguremos que se alcanzan los resultados esperados o planificados.

Será necesario determinar los riesgos y oportunidades que se presentan en cada uno de los procesos que la organización haya definido, por supuesto, teniendo en cuenta los objetivos que se persiguen y los efectos que los posibles fallos o defectos tuvieran en la satisfacción de nuestros clientes.

Al introducir como un elemento clave en el sistema de gestión de calidad de la organización la gestión de los riesgos, la norma elimina las acciones preventivas. La determinación de estos riesgos y oportunidades en los procesos es en sí mismos una herramienta preventiva, pues tendremos que tomar las acciones oportunas que nos ayuden a evitar los riesgos, eliminarlos, reducir sus efectos o incluso que podamos asumirlos, compartirlos o mantenerlos.

CONCLUSIONES

En definitiva, tal y como podemos apreciar, la gestión de riesgos se ha revelado, más que nunca, como un aspecto esencial en la dirección de las organizaciones, siendo necesario que el gestor tenga la capacidad de anticipar los eventos desfavorables (riesgos) y obtener un aprovechamiento óptimo de los eventos favorables (oportunidades).

Se puede asegurar que, para que un sistema de gestión de control y gestión de riesgos resulte eficaz en una organización, deben establecerse ciertas condiciones:

1 Supervisión activa por parte de la dirección y la gerencia.

2 Desarrollo de políticas y procedimientos claros y globales, así como el establecimiento de límites adecuados de apetito al riesgo.

3 Medición y monitorización periódico de los riesgos y de los sistemas de control de dichos riesgos.

4 Revisiones y auditorías periódicas y controles internos integrales.

La gestión de riesgos es un campo de gerencia que se encuentra en auge y progresiva profesionalización y puede considerarse un componente transversal para la gestión de otros factores relevantes como la calidad, la inteligencia estratégica o el cambio organizativo.