

Nuevos modelos de gestión de riesgos

¿Un nuevo impulso para la gestión de riesgos en Chile?



Esteban David Olivares Arellano

Académico DCS, FEN Universidad de Chile.
Consultor en áreas de Auditoría, Gestión de
Riesgos y Control Interno.

Magíster en Finanzas, Universidad de Chile
Contador Auditor e Ingeniero en Información y
Control de Gestión, Universidad de Chile

La gestión de riesgos está cada vez más incorporada en las actividades y prácticas habituales de la organización alrededor del mundo. Considerada una práctica habitual en los países más desarrollados, sin embargo, en Chile, aún en empresas de mayor tamaño, tiene un desarrollo incipiente incluso en algunas entidades cuyos reguladores han generado normas con exigencias al respecto. Al parecer ha costado en nuestro país, más que en otros, reconocer el valor que genera y también que protege la adecuada administración de los riesgos más relevantes que enfrenta una organización.

Mostrar de manera clara y concreta los beneficios que trae aparejados esta disciplina, es evidentemente fundamental para que los directorios y las administraciones, adopten e incorporen la gestión de riesgos como una herramienta que puede facilitar el cumplimiento de los objetivos, incluso aquellos más agresivos. Hay varios motivos que pueden explicar por qué nuestro país muestra un relativo retraso en la adopción efectiva de esta herramienta, pero más que ahondar en los mismos (tema para otra ocasión), en esta oportunidad revisaremos las principales novedades de los dos modelos más reconocidos, en Chile al menos, respecto de la gestión de riesgos: COSO ERM e ISO 31000.

¿Por qué aparece la gestión de riesgos en las organizaciones? Esta tendencia obedece a variados factores, dentro de los cuales se destacan: el hecho de enfrentar escenarios más complejos e inciertos, asociados principalmente a grandes cambios tecnológicos,

Mostrar de manera clara y concreta los beneficios que trae aparejados esta disciplina, es evidentemente fundamental para que los directorios y las administraciones, adopten e incorporen la gestión de riesgos como una herramienta que puede facilitar el cumplimiento de los objetivos, incluso aquellos más agresivos.

pero también a evoluciones en lo social y cultural. No olvidemos lo que ha pasado con varias empresas que fueron borradas del mapa, debido a la irrupción de las nuevas tecnologías asociadas a internet, los microchips, la fibra óptica, la comunicación satelital, entre otros; incluso empresas que participaron de la revolución tecnológica tales como BlackBerry, Nokia; u otras que no reaccionaron a tiempo quedando rápidamente con productos obsoletos, tales como Kodak, Blockbuster o la industria discográfica incluso. Adicionalmente recordar, que, aunque lo tengamos muy internalizado, hoy contamos con productos y servicios que hasta hace muy poco tiempo podían haber parecido de ciencia ficción: Uber, Spotify, Netflix, WhatsApp, Waze o aplicaciones que resuelven complejos problemas matemáticos con solo enfocarlos con el teléfono móvil, están incorporadas en nuestra diaria rutina. Los cambios y avances han sido muy grandes y no solo afectan a las personas, sino que, a la sociedad como un todo, y por supuesto de manera importante a todas las organizaciones que forman parte de ésta.

En este contexto, muchas empresas están prestando más y más atención a los lineamientos entregados por los principales referentes en la materia. En este contexto, en meses recientes, los dos modelos más reconocidos, ISO 31000 y COSO ERM, han sido actualizados con distintos grados de cambio en sus propuestas.

Por una parte, el modelo ISO 31000 fue actualizado con cambios no tan significativos y con la idea de simplificarlo, mientras que COSO ERM presentó prácticamente un modelo distinto, aproximando la gestión de riesgos a la estrategia y desempeño de las organizaciones. A continuación, revisaremos y comentaremos las principales novedades que plantean ambos estándares.

El modelo ISO 31000 fue actualizado con cambios no tan significativos y con la idea de simplificarlo, mientras que COSO ERM presentó prácticamente un modelo distinto, aproximando la gestión de riesgos a la estrategia y desempeño de las organizaciones.

ISO 31000:2018

La Organización Internacional de Estandarización emitió en febrero de 2018, la actualización de la norma ISO 31000, Gestión del Riesgo - Directrices. De acuerdo a la propia organización: "Los principales cambios en comparación con la edición anterior son los siguientes:

- » **Se revisan los principios de la gestión del riesgo, que son los criterios clave para su éxito.**
- » **Se destaca el liderazgo de la alta dirección y la integración de la gestión del riesgo, comenzando con el gobierno de la organización.**
- » **Se pone mayor énfasis en la naturaleza iterativa de la gestión del riesgo, señalando que las nuevas experiencias, el conocimiento y el análisis pueden llevar a una revisión de los elementos del proceso, las acciones y los controles en cada etapa del proceso.**
- » **Se simplifica el contenido con un mayor enfoque en mantener un modelo de sistemas abiertos para adaptarse a múltiples necesidades y contextos."**

Los cambios más relevantes que pueden observarse, efectivamente, tienen relación con la reducción de los principios de la gestión de riesgos y la simplificación del modelo, lo que en estas materias siempre se agradece.

Definiciones

Se mantiene en esta versión la tendencia de entregar definiciones sucintas, pero a la vez muy claras, las que mayormente provienen de la versión anterior, entre las cuales se destacan:

Riesgo: Efecto de la incertidumbre sobre los objetivos.

El documento además agrega sobre este concepto que "Un efecto es una desviación respecto a lo previsto. Puede ser positivo, negativo o ambos, y puede abordar, crear o resultar en oportunidades y amenazas". También agrega sobre los objetivos, que éstos pueden tener distintos aspectos y categorías, pudiéndose aplicar en diferentes niveles de la organización. En este sentido podría aplicarse en niveles operativos con los objetivos del control interno (Eficiencia, Información y Cumplimiento) y también considerando una amplia gama de factores de riesgo de diversa naturaleza.

Gestión del Riesgo: Actividades coordinadas para dirigir y controlar la organización con relación al riesgo.

Como puede verse, una definición muy sencilla pero que hace referencia a lo relevante del concepto.

Control: Medida que mantiene y/o modifica un riesgo.

La norma complementa la definición señalando que “los controles incluyen, pero no se limitan a cualquier proceso, política, dispositivo, práctica u otras condiciones y/o acciones que mantengan y/o modifiquen un riesgo”. Además, a efectos de no sobreestimarlos, se indica que “los controles no siempre pueden producir el efecto de modificación previsto o asumido”, destacando, por tanto, que los controles pueden fallar.

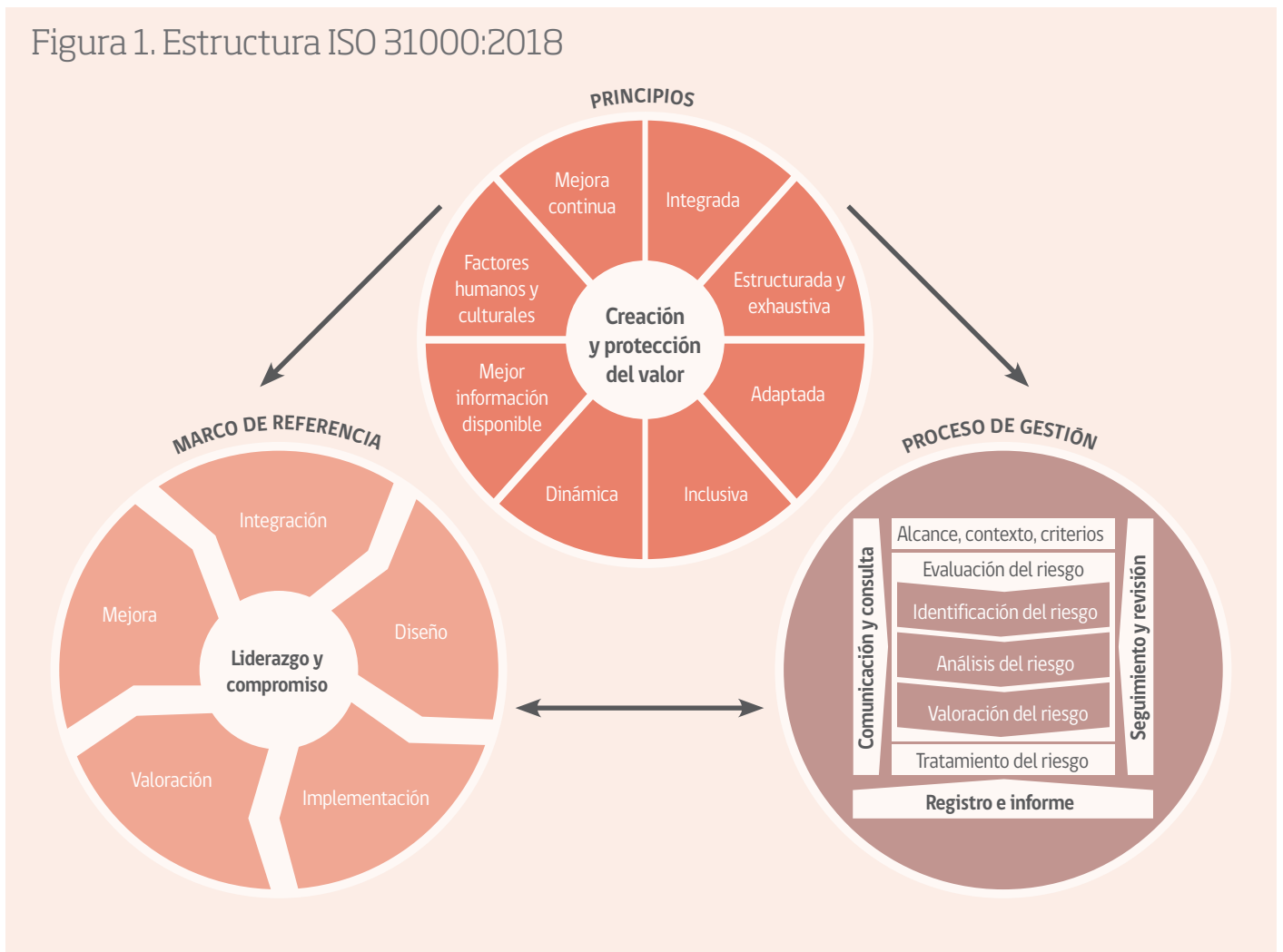
Esta definición no es nueva, viene de la versión anterior de la norma, con un pequeño agregado: en la versión anterior se definía control como, “medida que modifica un riesgo”.

Definir de este modo un control, puede llamar la atención, pues implica que éste no solo se concibe como una acción para reducir los riesgos, sino que también para mantenerlos en un límite determinado e incluso aumentarlos, lo que podría parecer contradictorio si se concibe el riesgo, solo como algo potencialmente negativo. Ahora bien, si se considera la definición de riesgo expuesta anteriormente, la definición tendrá mucho más sentido, pues se puede entender la mayor toma de riesgo en pos de mejorar los resultados obtenidos.

Estructura

En términos gruesos, se mantiene la estructura de tres pilares de la gestión de riesgos, que son: los principios de gestión de riesgos, el marco de referencia y el proceso (de gestión de riesgos), como puede observarse en la figura 1.

Figura 1. Estructura ISO 31000:2018



Fuente: "ISO 31000, Gestión del riesgo - Directrices", Segunda edición 2018-02. Traducción oficial

Principios

ISO 3100 establece que “el propósito de la gestión del riesgo es la creación y la protección del valor” complementando que la gestión de riesgos “mejora el desempeño, fomenta la innovación y contribuye al logro de objetivos”. Además, se establecen unos principios (ver figura 1) que señalan, cómo ésta debe ser implementada para cumplir su propósito de manera “eficaz y eficiente”.

Se indica también que “los principios son el fundamento de la gestión del riesgo” y que servirán de guía al establecer los otros dos pilares.

Marco de Referencia

El marco de referencia resulta fundamental, pues entrega lineamientos respecto de cómo integrar la gestión de riesgos en los distintos niveles la organización. La actualización refuerza la relevancia de integrar la gestión de riesgos dentro de las actividades inherentes a cada entidad.

La integración puede ser complicada, pues no siempre es fácil visualizar por parte de las personas que conforman la empresa, el aporte de la gestión de riesgos, por lo que podrían rechazar su adopción. Mostrar adecuadamente sus beneficios puede ser todo un desafío, pero es muy importante enfatizar que es un aspecto fundamental para lograr el compromiso de las personas.

Si no se establece este marco de manera adecuada, sin el total apoyo de la dirección y sin trabajar de manera relevante en la cultura de la entidad, los esfuerzos por adoptar la gestión de riesgos pueden ser realizados en vano.

Proceso

El proceso de gestión de riesgos, es el pilar del modelo en donde se lleva a cabo, en la práctica, la gestión de los riesgos más relevantes que enfrenta la organización. Implica el despliegue y aplicación de las metodologías desarrolladas para identificar, analizar, valorar, tratar, monitorear y comunicar los riesgos.

Todas las políticas, actividades y prácticas asociadas a la gestión de riesgos son integradas y aplicadas en las actividades normales de la entidad, en distintos niveles de la misma y de manera sistemática.

En resumen, la norma ISO 31000:2018 es más clara, breve y concisa, enfatizando la integración de la gestión de riesgos en las distintas actividades de las organizaciones, con el objeto de apoyarlas en la administración de la incertidumbre que enfrentan. Se considera un papel más relevante de la alta dirección en la implementación de esta herramienta, cuyo propósito es la creación y protección de valor, en especial liderando y apoyando el trabajo en la cultura de la entidad.

COSO ERM:2017

En septiembre de 2017, COSO (Committee of Sponsoring Organizations of the Treadway Commission) hizo pública la versión actualizada de su modelo en materia de gestión de riesgos, la que denominó “Enterprise Risk Management, Integrating with Strategy and Performance” (en adelante COSO ERM:2017). Con una imagen bastante distinta y un tratamiento de los riesgos que va desde la estrategia hasta la ejecución, COSO se inclinó por una administración de riesgos con un enfoque más integral.

Beneficios

De acuerdo a COSO ERM:2017, algunas de los beneficios de adoptar un modelo de gestión de riesgos son:

- » **Incrementar las oportunidades.**
- » **Identificar y gestionar los riesgos globales de la entidad.**
- » **Incrementar resultados positivos y ventajas, reduciendo sorpresas negativas y pérdidas.**
- » **Reducir la variabilidad del desempeño.**
- » **Mejorar la asignación de recursos.**

En suma, la gestión de riesgos, afirma COSO, está relacionada estrechamente con la capacidad de adaptarse, sobrevivir y prosperar de las organizaciones.

¿Qué cambia?

Hay varias modificaciones, de forma y fondo. El tradicional cubo empleado para representar el modelo se reemplaza por una estructura basada en cinco componentes y 20 principios (ver figura 2) alineados al ciclo del negocio.

Los cinco componentes son: Gobierno y Cultura, Establecimiento de Objetivos y Estrategia, Desempeño, Evaluación y Revisión, e Información, Comunicación y Reporte. Dentro de cada componente hay una serie de principios que representan los conceptos fundamentales asociados a cada componente. Los principios pueden

entenderse como las buenas prácticas que la organización debe cumplir en el ámbito de la gestión de riesgos.

Definiciones

Otro cambio relevante, dice relación con nuevas definiciones de algunos conceptos básicos o fundamentales. A continuación se señalan algunas definiciones consideradas relevantes:

Riesgo: La posibilidad de que se produzcan eventos y afecten el logro de la estrategia y los objetivos empresariales. Esta definición solo cambia en el sentido que se relaciona específicamente con el logro de la estrategia y los objetivos organizacionales. Adicionalmente se definen otros conceptos, en el entendido que los riesgos se relacionan a "eventos" potenciales y que normalmente se consideran en función de su severidad.

Figura 2. Estructura COSO ERM:2017



Fuente: "Enterprise Risk Management, Integrating with Strategy and Performance", COSO 2017.

- » **“Evento: Una ocurrencia o suceso o un conjunto de ellos”.**
- » **“Incertidumbre: El estado de no saber si los eventos potenciales pueden manifestarse o como pueden hacerlo”.**
- » **“Severidad: Una serie de consideraciones tales como la probabilidad e impacto de los eventos o el tiempo para recuperarse de los eventos”.**

En la última definición podría llamar la atención que dos conceptos, que usualmente se tratan como sinónimos en estas materias -severidad e impacto- en este caso no lo sean, y más bien, uno esté en función del otro.

Uno de los cambios significativos en este ámbito, es la nueva definición de gestión de riesgos (empresariales):

Gestión de Riesgos: La cultura, las capacidades, y las prácticas, integradas con la implementación de la estrategia, en las que una organización basa la gestión de sus riesgos en la creación, mantención, obtención de valor.

Esta definición, y el modelo en general, hacen referencia y énfasis especial en el trabajo que debe realizarse en la cultura de la organización, pues la gestión de riesgos debe incorporarse considerando la cultura de la entidad, teniendo así más posibilidades de funcionar adecuadamente y generar valor. Además, se señala los riesgos deben gestionarse desde la definición de la estrategia y también que deben relacionarse con el desempeño o retorno del negocio.

Estrategia, Objetivos y Desempeño

Otra de las novedades del COSO ERM:2017, es cómo se asocia de manera estrecha la gestión de riesgos con la estrategia, los objetivos y el desempeño de una organización.

De manera resumida, el modelo establece que la gestión de riesgos ayuda a la mejor comprensión de:

- » **Como la misión, visión y valores constituyen la base para determinar que tipo de monto y riesgos son aceptables cuando se establece la estrategia.**
- » **La posibilidad de que la estrategia y los objetivos no estén alineados con la misión, visión y valores.**
- » **Los tipos y cantidades de riesgo a los que la organización está expuesta por elegir una determinada estrategia.**

- » **Los tipos y cantidades de riesgo inherente al llevar a cabo su estrategia y lograr los objetivos y la aceptabilidad de este nivel de riesgo y valor asociado.**

COSO denomina “perfil de riesgo” a la relación entre los riesgos y el desempeño, y establece que ese concepto ayuda a la Administración a determinar cuál es la cantidad de riesgo aceptable y manejable, para poder cumplir con la estrategia y los objetivos. En este sentido, resulta interesante la importancia que se le otorga a la relación Riesgos-Desempeño, pues se destaca que los riesgos están asociados a un retorno o desempeño y que no pueden considerarse de manera aislada.

Otras “novedades”

En el cuerpo del documento se describen, analizan y ejemplifican, cada uno de los cinco componentes y sus respectivos principios, generándose algunas recomendaciones de buenas prácticas que permitirán optimizar el funcionamiento del modelo y por ende de sus resultados. Entre los aspectos más novedosos o llamativos podemos destacar los siguientes.

En el Principio 1 “Ejercicios de supervisión del riesgo del Directorio” pueden destacarse, las siguientes recomendaciones, muy atingentes por cierto a la realidad de nuestro país:

En el cuerpo del documento se describen, analizan y ejemplifican, cada uno de los cinco componentes y sus respectivos principios, generándose algunas recomendaciones de buenas prácticas que permitirán optimizar el funcionamiento del modelo y por ende de sus resultados. Entre los aspectos más novedosos o llamativos podemos destacar los siguientes.

Debe considerarse que los riesgos que se aceptan o toleran, están vinculados con el desempeño, por lo que, si no se cumple el desempeño requerido sin asumir todo el riesgo permitido, una respuesta podría ser: aumentar el riesgo hasta el umbral establecido para tratar de mejorar y alcanzar el nivel de desempeño establecido como meta.

- » **Ciber-seguridad.** Los directorios de organizaciones expuestas a riesgos tecnológicos o ciber-riesgos deben tener conocimientos ad hoc o bien contar con asesores expertos independientes.
- » **Causas e impactos.** Se sugiere que, para cada evento de riesgo, se identifiquen explícitamente sus causas, además de los impactos respectivos.

- » **Idoneidad en la Gestión de Riesgos.** Es relevante que el directorio conozca las complejidades de la entidad, y promueva prácticas y capacidades de gestión de riesgos que se correspondan con los riesgos asumidos.

- » **Sesgo Organizacional.** Los sesgos siempre existen y se manifiestan de diversas formas. Se espera que el directorio comprenda los posibles sesgos organizativos que existen y desafíe a la administración a superarlos. Este tema es fundamental, pues en muchas ocasiones son los sesgos los que pueden hacer fracasar o minimizar el efecto o aporte de una adecuada administración de los riesgos.

En el Principio 3 “Define la cultura deseada” en donde se establece que “la organización define los comportamientos deseados, los que caracterizan la cultura deseada para la entidad”, se señalan los siguientes aspectos.

- » **Alineando valores fundamentales, toma de decisiones y comportamientos.** Es relevante que los valores fundamentales permeen en la organización, que sean difundidos, comunicados y reforzados. Las acciones y decisiones del día a día, deben considerar y estar alineados con los valores fundamentales.

- » **Modificando la cultura.** La cultura esta siempre evolucionando y debe ser permanentemente trabajada, reforzada y difundida. Fusiones, adquisiciones y otras situaciones pueden afectarla.

En el Principio 10 “Identifica riesgos” se destaca la recomendación de describir adecuadamente los riesgos en función de su análisis, además de contar con una base o inventario de riesgos.

- » **Uso de un inventario de riesgos.** Se recomienda elaborar una lista de los principales riesgos que enfrenta la entidad, de distinta naturaleza y a distintos niveles.

En el Principio 12 “Prioriza riesgos” se establece de manera clara, que no pueden mitigarse todos los riesgos, siendo necesaria una priorización a efectos de gestionar aquellos más relevantes de manera prioritaria.

- » **Uso del apetito para priorizar riesgos.** En función de esto no todos los riesgos serán mitigados.

- » **Priorización en todos los niveles.** Los riesgos más relevantes deben asociarse a cada nivel o cada proceso que afecta.

En el Principio 13 “Implementación de mitigación de los riesgos” se señalan cuáles son las acciones que la organización lleva a cabo como respuesta a los riesgos más relevantes.

- » **Elección de respuesta a los riesgos.** Para los riesgos identificados, evaluados y priorizados deben definirse las respuestas más adecuadas para su prevención o mitigación. En este contexto se indica que las posibles respuestas frente a los riesgos son: **Aceptar - Evitar - Aumentar - Reducir - Compartir.**

En este sentido, puede llamar la atención que una alternativa sea aumentar los riesgos. No obstante, debe considerarse que los riesgos que se aceptan o toleran, están vinculados con el desempeño, por lo que, si no se cumple el desempeño requerido sin asumir todo el riesgo permitido, una respuesta podría ser: aumentar el riesgo hasta el umbral establecido para tratar de mejorar y alcanzar el nivel de desempeño establecido como meta.

En el Principio 14 “Desarrolla portafolio de riesgos” se sugiere la elaboración y evaluación permanente del portafolio de riesgos de la entidad.

- » **Portafolio de riesgos.** Un portafolio de riesgos permite a la Administración y el Directorio considerar el tipo, severidad e

interdependencia de los riesgos y cómo éstos afectan al rendimiento. Se identifican los riesgos más relevantes a nivel de entidad y a cada objetivo de negocio.

En el Principio 18 “Se apoya en la información y en la tecnología”, se hace referencia a que la organización debe apoyar la gestión de riesgos con sistemas de información y tecnología.

- » **Usar tecnología para apoyar la información.** Se comenta respecto a la evolución de la información tanto en su volumen como sus características y por tanto se recomienda usar tecnología para hacer un mejor y más eficiente uso de los datos o información disponibles.

Finalmente, en COSO ERM:2017, se destacan las ventajas respecto de integrar la gestión del riesgo dentro de las actividades habituales de las organizaciones, indicando que:

- » **Anticipa la identificación de los riesgos o los muestra de manera más explícita dando más posibilidades para gestionarlos adecuadamente.**
- » **Identifica y persigue oportunidades nuevas y existentes de acuerdo con el apetito de riesgo de la entidad y su estrategia.**

Trabajar la cultura de la organización, priorizar la gestión de los riesgos más relevantes, integrar las actividades de gestión de riesgos a las actividades normales de las entidades, asegurar que dichas actividades agregan valor en todos los niveles que son aplicadas, y otras consideraciones que con seguridad facilitarán la adecuada adopción de esta herramienta.


- » **Entiende y responde a las desviaciones en el rendimiento de manera más ágil y consistente.**
- » **Desarrolla y reporta portafolios de riesgos de manera más comprensible y consistente, distribuyendo de mejor forma los recursos finitos.**
- » **Mejora la colaboración, confianza y la información compartida a través de la organización.**

Como puede observarse, los cambios en este modelo son relevantes, modificándose definiciones, generándose una nueva estructura con componentes renovados y principios orientadores. Se incorporan, además, recomendaciones o buenas prácticas que van muy de la mano con el escenario que enfrentan las organizaciones en nuestros días. Este sentido el documento hace aportes importantes pues “refresca” en varios aspectos la gestión de riesgos.

¿Nuevos Paradigmas?

Conociendo el detalle de ambos modelos, puede observarse una evolución interesante, especialmente en la incorporación de algunas recomendaciones o buenas prácticas para el diseño, implementación y despliegue de los modelos de gestión de riesgos. Si bien, no se puede hablar de nuevos paradigmas en la gestión de riesgos, es destacable que para lograr que la gestión de riesgos sea una herramienta agregue valor de manera relevante, se hace énfasis en aspectos importantes que deben atenderse.

Trabajar la cultura de la organización, priorizar la gestión de los riesgos más relevantes, integrar las actividades de gestión de riesgos a las actividades normales de las entidades, asegurar que dichas actividades agregan valor en todos los niveles que son aplicadas, y otras consideraciones que con seguridad facilitarán la adecuada adopción de esta herramienta. La gestión de riesgos cada vez está más presente en el día a día de las organizaciones, las que deben enfrentar y sortear mayores complejidades e incertidumbres para el logro de sus objetivos.

Finalmente, está por verse que estas dos nuevas versiones de los referentes de la gestión de riesgos, impulsen el despegue de esta disciplina en nuestro país. Si bien, son claramente un aporte, se hacen necesarias otras varias condiciones o iniciativas, a efectos de conseguir que en Chile pase lo que ocurre en países más avanzados, en donde la gestión de riesgos tiene desde hace algunos años un papel relevante en las organizaciones de distinta naturaleza. 

◆ **CONTADOR AUDITOR**



*¡Ven a estudiar con
los MEJORES!*