

# OPTIMIZACIÓN DE RIESGOS.

## PARTE II

AUTOR: LUIS RAMÍREZ LORÍA

MARZO: 2021



**San Marcos**

## Tabla de contenido

Introducción .....	2
Contenido.....	3
Optimización del riesgo.....	3
El papel de los gobiernos .....	4
Relación del enfoque de gestión de riesgos con el cumplimiento legal y regulatorio .....	5
MEA03 Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos .....	5
Métodos para alinear la gestión de TI y la gestión de riesgos empresariales (ERM). .....	8
El entorno de riesgos.....	9
Gestión de riesgo empresarial. Perspectiva de Dirección .....	10
Gestión de riesgo empresarial. Perspectiva de Consejo de Administración.....	10
Gestión de riesgo empresarial. Logros.....	12
Gestión de riesgo empresarial. Beneficios de una gestión eficaz.....	13
Gestión de riesgo empresarial. Selección de estrategias .....	14
Marco de Gestión de Riesgo Empresarial .....	16
Conclusiones y recomendaciones .....	19
Referencias bibliográficas .....	20



## Introducción

Tal cual se mencionó en la lectura inicial del módulo con el estudio de los conceptos de gestión de riesgos de tecnologías de información y las normas, estándares y mejores prácticas se busca que el estudiante y futuro profesional en TI logre comprender como dentro de los marcos de Gobierno de TI la aplicación de la gestión de riesgos en la estrategia, carteras, proyectos, programas y operaciones puede generar ventajas significativas y con esto la formación profesional en los conceptos es un requerimiento que permitirá mejorar el desempeño de las organizaciones en el entorno donde se desempeñen.

Dando continuidad a estos nuevos conocimientos, para la segunda parte del módulo se abordará la relación del enfoque de gestión de riesgos con el cumplimiento legal y regulatorio que deben respetar las organizaciones, así como los métodos más aceptados para alinear la gestión de TI y la gestión de riesgos empresariales (ERM), aspectos también enfocados en las normas internacionales y estándares de mejores prácticas de TI

Tal cual se mencionó anteriormente en el país existen las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información, así como las Normas de Control Interno de la Contraloría General de la República, ambas brindando una serie de lineamientos a respetar por parte de las entidades del Gobierno o controladas por este ente regulador.

## Contenido

Inicialmente se requiere establecer la diferencia que existe en el concepto de normas y el de regulación. Telefónica, en su Guía completa de aplicación para la gestión de los servicios de tecnologías de la información, nos señala que:

- *“Una norma, según define la legislación española, es “una especificación técnica de aplicación repetitiva o continuada, cuya observancia no es obligatoria, establecida con la participación de todas las partes interesadas, que aprueba un organismo reconocido a nivel nacional o internacional”. Mientras que un reglamento técnico, se refiere a “una especificación técnica, relativa a productos, procesos o instalaciones industriales, establecidas con carácter obligatorio a través de una disposición de la Administración, para su fabricación, comercialización o utilización”.*
- *Por tanto, la norma en sí misma constituye una recomendación y no es de obligado cumplimiento por las organizaciones; su implantación y cumplimiento es voluntario. La regulación o reglamentación pueden exigir el cumplimiento de los requisitos definidos en una norma. Es en este caso cuando la norma pasa a ser de obligado cumplimiento para las organizaciones afectadas. Hay que recalcar que en el caso de las Normas ISO/IEC 20000, los requisitos que contienen son exigibles sólo al efecto de certificar la conformidad de una organización con ellas de manera voluntaria, no porque exista una ley o regulación lo exija” (Telefónica, 2009)*

Por tanto, adicional a los estándares y normas abarcados en la lectura anterior, es importante tomar en consideración aquellas recomendaciones y mejores prácticas que nos orientan al cumplimiento de requerimientos externos, de forma que las organizaciones de Tecnologías de la Información (TI) tengan lineamientos establecidos en su modelo de Gobernanza y Organización, para facilitar la gestión y cumplimiento legal y regulatorio.

## Optimización del riesgo

Tal cual se analizó en la lectura anterior, una adecuada gestión del riesgo de las TI, inicia por la identificación de la utilidad de su gestión por parte de la alta administración (conciencia del riesgo), de manera que se genere el apetito por el riesgo en la organización, y se logre comprender el beneficio del cumplimiento de objetivos de gestión de riesgos, establecer modelos de transparencia en el tratamiento de riesgos (al inicio lo más relevantes por impacto, visibilidad o criticidad del negocio), definir claramente las responsabilidades de su gestión en la organización, de forma que se puede administrar o gerenciar el riesgo (evaluar, mitigar, evitar o aceptar), abarcando desde los procesos críticos de negocio hasta la seguridad de la información (sumamente relevante en la actual revolución 4.0).

Aunado a lo anterior, en la presente lectura se abordarán dos aspectos adicionales que también son fundamentales dentro de la gestión y optimización de riesgos, lo cuales coadyuvan el buen accionar de las TI en las organizaciones y que aportan valor a la organización donde funcionan, el primero es la relación del enfoque de gestión de riesgos con el cumplimiento legal y regulatorio (requerimientos externos) y el segundo algunos métodos recomendados por las mejores prácticas para alinear la gestión de TI y la gestión de riesgos empresariales (ERM).

## El papel de los gobiernos

A nivel internacional, con la explosión de la era de la información y la mencionada cuarta revolución industrial o industria 4.0, el papel de los gobiernos, sus instituciones gubernamentales, reguladores de servicios y administración pública, deben desempeñar un papel fundamental en la definición de normas sobre gestión de riesgos, servicios de TI, así como realizan a nivel de la regulación del comercio y de los servicios.

**ENTRE LOS ORGANISMOS GUBERNAMENTALES DESTACA EL MINISTERIO DE COMERCIO BRITÁNICO (OGC, OFFICE OF GOVERNMENT COMMERCE) EN SU PAPEL DE CREADOR, IMPULSOR Y PROPIETARIO DE ITIL Y EL DEPARTAMENTO DE DEFENSA DE ESTADOS UNIDOS (DOD, DEPARTAMENT OF DEFENSE) COMO IMPULSOR DE CMMI. (Telefónica, 2009)**

Para Telefónica, (Telefónica, 2009), los tres papeles que debe desempeñar el Gobierno, en relación con la gestión de las TIC y su regulación son:

1. Establecer o sustentar la actividad de normalización mediante subvenciones a los organismos de normalización
2. Como impulsores de algunas iniciativas destacadas, y
3. Exigir el cumplimiento de la normativa, bien estableciendo una regulación o bien en su papel de cliente contratante de servicios al sector de las TIC.

En Costa Rica hemos destacado las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información, así como las Normas de Control Interno de la Contraloría General de la República.

Adicionalmente otros actores dentro de las instituciones de Gobierno como el Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT), institución que promueve el desarrollo de la Ciencia, Tecnología, Innovación y Telecomunicaciones, como elementos fundamentales para el desarrollo socioeconómico del país y para el mejoramiento de la calidad de vida de los ciudadanos, por medio de la articulación de las acciones de los sectores académico, privado y gubernamental, sin olvidar el papel de la academia y su formación de profesionales adentrados en materia, tal cual se realiza en la Universidad San Marcos.

## Relación del enfoque de gestión de riesgos con el cumplimiento legal y regulatorio

Dentro de los marcos que han sido analizado, el COBIT nos ofrece .dentro de sus objetivos en la Gobernanza de TI: “Asegurar la conformidad de TI con leyes y regulaciones”, (ISACA®, 2012), para esto dentro del Dominio MEA, Supervisar, Evaluar y Valorar, existe el proceso MEA 03 Supervisar, evaluar y valorar la conformidad con los requerimientos externos, cuyo enfoque apoya la gestión de riesgo y el cumplimiento legal y regulatorio.

### MEA03 Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos

Este proceso se describe como: “Evaluar el cumplimiento de requisitos regulatorios y contractuales tanto en los procesos de TI como en los procesos de negocio dependientes de las tecnologías de la información. Obtener garantías de que se han identificado, se cumple con los requisitos y se ha integrado el cumplimiento de TI en el cumplimiento de la empresa general.” (ISACA®, 2012)

El COBIT 5, nos señala que la organización de TI debe supervisar, evaluar y valorar la aceptación de requerimientos externos, garantizando que estos requisitos de conformidad externos se identifican, que los directivos establecen una dirección hacia su cumplimiento y que como tal se establecen procesos de supervisión, evaluación e informes para garantizar a nivel de TI su abordaje, como parte de la conformidad global que la empresa tiene con su requisitos legales, regulatorios o externos.

Según nos señala el COBIT 5:

*“La guía en elaboración COBIT 5 para el Aseguramiento explica cómo los auditores pueden proporcionar aseguramiento de conformidad de manera independiente y adhesión a las políticas internas derivadas de las directivas internas o de requisitos externos legales, regulatorios o contractuales, confirmando que se han tomado de manera oportuna, por parte del dueño y responsable de que se lleve a cabo el proceso, las acciones correctivas necesarias para solventar cualquier laguna en el ámbito de la conformidad.” (ISACA, 2012)*

Como tal las metas de este proceso señaladas por COBIT 5, procesos catalizadores son:

1. *“La totalidad de los requisitos externos de cumplimiento se han identificado.*
2. *Tratar adecuadamente los requisitos externos de cumplimiento.” (ISACA®, 2012)*

Para su ejecución el proceso MEA 03 de COBIT se compone de las siguientes prácticas claves:

### *MEA03.01 Identificar requisitos externos de cumplimiento.*

La cual no señala como práctica de gestión: *“Identificar y supervisar, de manera continuada, cambios en las legislaciones y regulaciones tanto locales como internacionales, así como otros requisitos externos de obligado cumplimiento en el área de TI.”* (ISACA®, 2012)

Estableciendo las siguientes actividades, en resumen:

1. Establecer un proceso responsable de identificar y supervisar los cambios legales y regulatorios (requisitos contractuales externos) aplicables al uso de recursos de TI y al procesamiento de información en las operaciones (TI y negocio)
2. Identificar la totalidad de requisitos de cumplimiento y su impacto en actividades de TI, en ámbitos como los flujos de datos, privacidad, controles internos, informes financieros, regulación sectorial, propiedad intelectual, seguridad e higiene.
3. Valorar requisitos legales y regulatorios y su impacto en contratos con terceros que afecten las operaciones de TI (proveedores y socios de TI/Negocio)
4. Obtener asesoramiento sobre modificaciones en legislación, regulación y estándares cuando proceda.
5. Mantener un inventario de requisitos legales, regulatorios y contractuales, su impacto y acciones de cumplimiento.
6. Mantener un registro general de requisitos externos de cumplimiento que afecten la empresa.

### *MEA03.02 Optimizar la respuesta a requisitos externos.*

La cual no señala como requisito: *“Revisar y ajustar políticas, principios, estándares, procedimientos y metodologías para asegurar la adecuada gestión y comunicación de los requisitos legales, regulatorios y contractuales. Considerar qué estándares sectoriales, códigos de buenas prácticas y guías de mejores prácticas pueden adoptarse y adaptarse.”* (ISACA®, 2012). Estableciendo las siguientes actividades, en resumen:

1. Revisar y ajustar políticas, principios, estándares, procedimientos, y metodologías para que mantengan su eficacia y asegurar el cumplimiento requerido, así como la gestión del riesgo empresarial (contar con experto internos y externos en materia).
2. Comunicar nuevos requisitos y modificaciones a los existentes al personal que corresponda.

### *MEA03.03 Confirmar el cumplimiento de requisitos externo.*

La cual no señala: *“Confirmar el cumplimiento de las políticas, los principios, los estándares, los procedimientos y las metodologías con los requisitos legales, regulatorios y contractuales.”* (ISACA®, 2012)

Y establece las siguientes actividades para su cumplimiento, en resumen:

1. Evaluar las políticas, estándares, procedimientos y metodologías de la organización para asegurar el cumplimiento de los requisitos legales y regulatorios aplicables al procesamiento de información.
2. Gestionar deficiencias de cumplimiento dentro de plazos razonables.
3. Evaluar procesos y actividades de TI y Negocio para asegurar el cumplimiento de requisitos legales, regulatorios y contractuales.
4. Detectar patrones reiterados de fallos de cumplimiento, mejorando políticas, estándares, procedimientos y metodologías, sus procesos y actividades.

*MEA03.04. Obtener garantía del cumplimiento de requisitos externos.*

La cual no señala como práctica de gestión: *“Obtener y notificar garantías de cumplimiento y adherencia a políticas, principios, estándares, procedimientos y metodologías. Confirmar que las acciones correctivas para tratar las diferencias en el cumplimiento son cerradas a tiempo.”* (ISACA®, 2012)

Estableciendo las siguientes actividades, en resumen:

1. Confirmar el cumplimiento de políticas internas con los propietarios de TI y negocio, y con los directores de las unidades.
2. Realizar revisiones internas y externas evaluando el nivel de cumplimiento.
3. Obtener declaraciones de proveedores de servicios de TI externos sobre el cumplimiento de leyes y regulaciones.
4. Obtener declaraciones de socios de negocio sobre el cumplimiento de leyes y regulaciones de transacciones electrónicas entre compañías.
5. Supervisar informar de incidentes de incumplimiento, investigar causa raíz.
6. Consolidar informes de requisitos legales, regulatorios y contractuales a nivel empresarial.

Como aclaración debe entenderse el concepto “Cumplimiento” como la función (ejercicio) en la empresa responsable de dirigir el cumplimiento legal, regulatorio y contractual. Así mismo.

De igual forma, para mayor profundidad en el tema es necesario aclarar que existen otros modelos y normas que permiten apoyar la aplicabilidad de los requisitos legales o regulatorios que apoyan la gestión de las organizaciones de TI y pueden ser de gran aporte al implementar modelos internos de gestión, por ejemplo, IT Control Objectives for Sarbanes-Oxley, IT Control Objectives for Basel II. Estos modelos tienen una gran relevancia en seguridad de la información (incluido el COBIT Security Baseline) y otros temas relacionados con gestión de riesgos.



Es por esta razón que *“COBIT ha sido mapeado otros marcos y estándares para ilustrar el cumplimiento completo del ciclo de vida de gestión de TI y para dar soporte para su uso en empresas que adopten múltiples marcos y estándares relacionados con TI”* (ISACA, 2012).

## **Métodos para alinear la gestión de TI y la gestión de riesgos empresariales (ERM).**

Para establecer los métodos de alineamiento de la gestión de TI y la gestión de riesgos empresariales se evaluará de forma ejecutiva los señalamientos del “Committee of Sponsoring Organizations of the Treadway Commission”, COSO por sus siglas, el cual es una organización que lidera en el desarrollo de marcos orientadores sobre control interno, gestión de riesgo empresarial, disuasión del fraude, todos dirigidos a mejorar el desempeño organizacional y la supervisión, reducir niveles de fraude en las organizaciones y la gestión de riesgo empresariales (ERM). Por lo cual analizaremos algunos aspectos claves señalados por COSO sobre la gestión de riesgos empresariales y su integración a la estrategia y desempeño (en base al resumen ejecutivo del Instituto de Auditores Internos de España y PwC).

## El entorno de riesgos

El entorno de riesgos es variado conforme con las organizaciones en las que se realicen los análisis y se busquen establecer los componentes para su gestión, sin embargo, toda empresa realiza actividades de gestión en sus procesos para la consecución de sus

**GESTIÓN DEL RIESGO EMPRESARIAL- INTEGRANDO ESTRATEGIA Y DESEMPEÑO CONSTITUYE UN MARCO DE TRABAJO PARA CONSEJOS DE ADMINISTRACIÓN Y EQUIPOS DE DIRECCIÓN DE ENTIDADES DE CUALQUIER TAMAÑO. ESTE MARCO PROFUNDIZA EN EL NIVEL ACTUAL DE GESTIÓN DE RIESGOS QUE EXISTE EN EL CURSO ORDINARIO DE LAS ACTIVIDADES DE NEGOCIO. ASIMISMO, DEMUESTRA CÓMO LA INTEGRACIÓN DE LAS PRÁCTICAS DE GESTIÓN DEL RIESGO EMPRESARIAL EN TODA LA ENTIDAD CONTRIBUYE A ACELERAR EL CRECIMIENTO Y A MEJORAR EL DESEMPEÑO. ADEMÁS, CONTIENE PRINCIPIOS QUE PUEDEN APLICARSE EN LA PRÁCTICA, DESDE LA TOMA DE DECISIONES ESTRATÉGICAS HASTA LA CONSECUCCIÓN DE RESULTADOS. (Instituto de Auditores Internos de España y PwC, 2017)**

objetivos y por tanto posee riesgos, los cuales están intrínsecos desde las decisiones operativas, hasta las decisiones claves, decisiones de consejos de administración y mandos medios, todas estas elecciones forman parte de riesgos en los que incurre una organización buscando conseguir los mejores resultados posibles, sin embargo, las decisiones rara vez son binarias, por lo cual, tanto por el ambiente en el que se desenvuelven las organizaciones como la constante toma de decisiones, la gestión de riesgos es una condición que debe acompañar a la organización en su cambiante entorno de riesgos.

Por tanto, la comprensión de riesgos, prácticas de gestión de riesgo empresarial, buscan reducir los márgenes de error en los procesos, permitiendo a las organizaciones

enfrentar los desafíos del entorno, creciente, volátil, complejo y ambiguo del mundo donde se desarrollan sus operaciones, sin mencionar la complejidad que las Tecnologías de la Información y Comunicación introducen como factor de evolución (y riesgo) constante, elementos que incorporan desafíos que pueden afectar la fiabilidad, relevancia y confianza de clientes, proveedores, acreedores y socios, pero a su vez, en la actualidad existe un mayor nivel de comprensión sobre como la gestión de riesgo y el alineamiento estratégico brindan elementos que aumentan los niveles de transparencia, rendición de cuentas, gestión de impactos, aprovechamiento de oportunidades, mejor toma de decisiones por los equipos de dirección entre otros.

## Gestión de riesgo empresarial. Perspectiva de Dirección

Por medio del proceso de dirección se deben considerar la fórmulas, objetivos, apetito y condicionantes de alto nivel sobre riesgos, su influencia en la toma de decisiones y en la elección de la estrategia.

**EL EQUIPO DE DIRECCIÓN TIENE LA RESPONSABILIDAD GENERAL DE GESTIONAR EL RIESGO PARA LA ENTIDAD, PERO ES IMPORTANTE QUE VAYA MÁS ALLÁ: MEJORANDO EL DIÁLOGO ENTRE EL CONSEJO DE ADMINISTRACIÓN Y LAS DISTINTAS PARTES INTERESADAS SOBRE EL USO DE LA GESTIÓN DEL RIESGO EMPRESARIAL PARA OBTENER UNA VENTAJA COMPETITIVA. PARA ELLO, HA DE EMPEZAR POR LA IMPLANTACIÓN DE CAPACIDADES DE GESTIÓN DEL RIESGO EMPRESARIAL COMO PARTE DE LA SELECCIÓN Y EL PERFECCIONAMIENTO DE LA ESTRATEGIA. (Instituto de Auditores Internos de España y PwC, 2017)**

Esta gestión de riesgos desde la perspectiva de dirección permite a la organización enriquecer el enfoque del equipo de dirección sobre las fortalezas y debilidades de la estrategia, su incidencia sobre la misión, visión, objetivos y metas, de forma que se pueda asegurar que se incluyen alternativas estratégicas, acciones de respuesta y principalmente que se toman en consideración los aportes de los responsables de implantar la estrategia como un factor fundamental para el alineamiento de los niveles operativo, táctico y estratégico.

Cuando se ha establecido la estrategia, la gestión del riesgo empresarial debe considerarse una herramienta que permite un efectivo desempeño de la dirección, por el control que incorpora al equipo de dirección y su trabajo administrativo en relación a los riesgos. Esta gestión de riesgo empresarial ERM, establece un vínculo de confianza y seguridad hacia las partes interesadas, sobre el tratamiento de las condiciones cambiantes del entorno actual, exigiendo una constante mejoría en el análisis y abordaje de riesgos, cómo se están gestionando y su trato de forma activa y consciente.

## Gestión de riesgo empresarial. Perspectiva de Consejo de Administración

La función que desempeña el Consejo de Administración es la de supervisar la creación de valor organizacional, mantener su desempeño y evitar su degeneración, por lo cual, la ERM (gestión de riesgo empresarial) habilita capacidades a nivel de consejo para establecer un apoyo sólido a la gestión de riesgos y por tanto se espera, cada vez más, que este nivel de la organización supervise la ERM.

El marco de gestión propuesto por COSO aporta una serie de funciones y recomendaciones prácticas para que en este nivel se definan y aborden responsabilidades de supervisión del riesgo, incluyendo aspectos de Gobierno (Negocio y TI), cultura, estrategia, establecimiento

de objetivos, desempeño, información, comunicación, reportes, revisión y monitorización de prácticas y técnicas que permitan mejorar el desempeño de las entidades.

Entre las funciones recomendadas por COSO tenemos:

- *“Revisar, cuestionar y acordar con la dirección:*
  - *La estrategia propuesta y el apetito al riesgo.*
  - *La alineación de la estrategia y los objetivos de negocio con la misión, visión y valores clave de la entidad.*
  - *Las principales decisiones de negocio, incluidos aspectos como fusiones, adquisiciones, asignaciones de capital, financiación y decisiones relacionadas con dividendos.*
  - *La respuesta a dar ante fluctuaciones significativas en el desempeño de la entidad o en la visión del riesgo a nivel de cartera.*
  - *Las respuestas ante casos de desviación con respecto a los valores clave.*

Los Consejos de Administración también pueden pedir a los miembros de la alta dirección que analicen no sólo los procesos de riesgo sino también la cultura. ¿En qué medida permite o impide la cultura una asunción responsable de riesgos? ¿Qué perspectiva adopta la dirección para efectuar un seguimiento de la cultura de riesgos y cómo ha cambiado dicha perspectiva? A medida que el entorno evolucione —y sin duda alguna evolucionará, independientemente de que lo detecte o no la entidad— ¿cómo puede el consejo de administración confiar en que el equipo de dirección será capaz de dar una respuesta adecuada y oportuna? (Instituto de Auditores Internos de España y PwC, 2017)

- *Aprobar los incentivos y remuneración del equipo de dirección.*
- *Participar en la relación con inversores y demás partes interesadas.”* (Instituto de Auditores Internos de España y PwC, 2017)

Adicionalmente entre los factores que puede mejorar la gestión de riesgos empresarial, ERM, en la empresa tenemos:

- Mejorar la resiliencia de la empresa sobre los riesgos.
  - Mejorar la capacidad de anticipar riesgos.
  - Mejorar la capacidad de responder ante el cambio.
- Identificar factores que representan riesgos y cambios que pueden afectar el desempeño y exigir modificación de las estratégicas organizacionales planteadas o bien en ejecución.
- Elaborar planes de respuesta oportunos, por ejemplo, retirar una inversión, redireccionar un negocio, cambiar una tecnología informática.



La ERM proporciona un marco adecuado para el nivel de Consejo de Administración, su evaluación de riesgos y adopción de una mentalidad de resiliencia.

## Gestión de riesgo empresarial. Logros

El Marco Integrado de Gestión del Riesgo Empresarial propuesto por COSO tiene el propósito de ayudar a las empresas a proteger y aumentar el valor interno y de las partes interesadas. Al igual que se ha señalado en otra normativa y estándares de gestión del riesgo, COSO busca que el valor se maximice cuando el equipo de dirección establezca la estrategia y los objetivos para lograr un equilibrio óptimo entre las metas de crecimiento y rentabilidad y los riesgos relacionados, y despliega los recursos de manera eficiente y efectiva para alcanzar los objetivos de la entidad.

Según el Instituto de Auditores Internos de España, este marco permite aplicarse a todo tipo de organizaciones y sectores, casi sin importar el tamaño de la organización, por lo cual, brinda una ventaja a quienes realicen su aplicación y requieran establecer principios para la identificación, gestión riesgos dentro de un apetito al riesgo definido y facilitar la consecución de objetivos, esto beneficia por incorporar un análisis de riesgos en profundidad y mejorando la comprensión, claridad y resultados de su gestión, generando vínculos fuertes entre la estrategia, el riesgo y el desempeño, sin olvidar en este proceso el alineamiento que debe realizarse con las organizaciones de TI mediante los mecanismo de Gobernanza previamente establecidos en las lecturas. En resumen, mediante su aplicación se pueden esperar logros tales como:

- *“Conectar más claramente la gestión del riesgo empresarial con una amplia serie de expectativas de las distintas partes interesadas.*
- *Posicionar el riesgo en el contexto del desempeño de una organización, en lugar de ser el objeto de un ejercicio aislado.*
- *Permitir a las organizaciones anticiparse mejor al riesgo para que puedan adelantarse a él, entendiendo que él.”* (Instituto de Auditores Internos de España y PwC, 2017)

## Gestión de riesgo empresarial. Beneficios de una gestión eficaz

Para asegurar los beneficios de la gestión de riesgo empresarial, toda organización debe establecer su estrategia y realizarle ajustes de forma periódica, conscientes de las oportunidades y desafíos que se presentan en la constante búsqueda de creación de valor, es por esto que tanto para la arquitectura empresarial como la para la gestión de riesgos ERM se requieren marcos que optimicen estrategia y desempeño. Acorde con PwC, las organizaciones que integran el ERM en todos sus niveles pueden optar por mayores beneficios, tales como:

### *Aumentar la gama de oportunidades disponibles:*

- *“Al tener en cuenta todas las posibilidades –tanto los aspectos positivos como negativos del riesgo– la dirección puede identificar nuevas oportunidades y desafíos únicos asociados con las oportunidades actuales.”* (Instituto de Auditores Internos de España y PwC, 2017)

La gestión del riesgo empresarial no es una “lista de verificación”. Es un conjunto de principios sobre los cuales se pueden construir o integrar procesos para una organización en particular, y es un sistema de seguimiento, aprendizaje y mejora del desempeño.

La gestión del riesgo empresarial puede ser utilizada por organizaciones de cualquier tamaño. Si una organización tiene una misión, una estrategia y unos objetivos —y la necesidad de tomar decisiones que tengan plenamente en cuenta el riesgo— podrá aplicar la gestión del riesgo empresarial. Puede y debe ser utilizada por todo tipo de organizaciones, desde pequeñas empresas hasta organizaciones no gubernamentales, pasando por organismos públicos y grandes compañías del Fortune 500. (Instituto de Auditores Internos de España y PwC, 2017)

### *Identificar y gestionar el riesgo en toda la entidad:*

- *“Cada entidad se enfrenta a innumerables riesgos que pueden afectar a muchas partes de la organización. A veces, un riesgo puede originarse en una parte de la entidad, pero puede afectar a otra parte diferente. En consecuencia, la dirección identifica y gestiona estos riesgos a nivel de toda la entidad para sostener y mejorar el desempeño.”* (Instituto de Auditores Internos de España y PwC, 2017)

### *Aumentar los resultados positivos y las ventajas a la vez que se reducen las sorpresas negativas:*

- *“La gestión del riesgo empresarial permite a las entidades mejorar su capacidad para identificar riesgos y establecer respuestas adecuadas, reduciendo las sorpresas y costes o pérdidas relacionados, al tiempo que se benefician de los nuevos desarrollos.”* (Instituto de Auditores Internos de España y PwC, 2017)

### *Reducir la variabilidad del desempeño:*

- *“Para algunas organizaciones, el verdadero desafío no tiene tanto que ver con las sorpresas y las pérdidas, sino más bien con la variabilidad del desempeño. Unos*

*resultados que superen las expectativas o se adelanten a los calendarios previstos pueden causar tanta preocupación como unos resultados inferiores a las expectativas o retrasos en los calendarios. La gestión del riesgo empresarial permite que las organizaciones se anticipen a los riesgos que afectarían al desempeño e implanten las medidas necesarias para minimizar los trastornos y maximizar las oportunidades.” (Instituto de Auditores Internos de España y PwC, 2017)*

#### *Mejorar el despliegue de recursos:*

- *“Todo riesgo puede considerarse una petición de recursos. Dado que los recursos son finitos, si se dispone de una información sólida sobre riesgos, la dirección puede evaluar las necesidades generales de recursos, establecer prioridades en su despliegue y mejorar su asignación.” (Instituto de Auditores Internos de España y PwC, 2017)*

#### *Mejorar la resiliencia de las empresas:*

- *“La viabilidad a medio y largo plazo de una entidad depende de su capacidad para anticiparse y responder al cambio, no sólo para sobrevivir sino también para evolucionar y prosperar. Esto es posible, en parte, gracias a una gestión eficaz del riesgo empresarial. Es cada vez más importante a medida que se acelera el ritmo de cambio y aumenta la complejidad en el entorno empresarial.” (Instituto de Auditores Internos de España y PwC, 2017)*

Estas consideraciones deben ser intrínsecamente relacionadas con la generación de valor por parte de la organización, de forma que la gestión de riesgos empresariales no se considere solamente un modelo de control interno sino también una fórmula para la creación, mantenimiento y aseguramiento del valor en la organización, lo cual se debe establecer desde el ámbito estratégico, identificando las oportunidades clave y las capacidades diferenciadoras, como fortaleza empresarial.

## **Gestión de riesgo empresarial. Selección de estrategias**

La selección de estrategias implica en la toma de decisiones, aceptar pros y contras de un determinado enfoque estratégico o de negocio sobre el cual es indispensable aplicar la gestión de riesgo empresarial como un componente de “arte” o de “ciencia” que entre intrínsecamente dentro de la toma de decisiones. Sobre este proceso, no solo debe aplicarse la ERM durante la formulación de estrategias, sino también sobre estrategias existentes y cursos de acción en los cuales se evalúe la relevancia y viabilidad de las acciones en curso.

Entre las principales preguntas para evaluar la ERM en relación con la estrategia y las organizaciones, a nivel de directivos diariamente se deben enfrentar cuestionamientos tales como:

- ¿Hemos modelado la demanda del cliente con precisión?

- ¿Cumplirá nuestra cadena de suministro las expectativas tanto en cuestiones de plazo como de presupuesto?
- ¿Emergerán nuevos competidores?
- ¿Está nuestra infraestructura tecnológica a la altura de las circunstancias?

El marco COSO establece dos aspectos fundamentales para la gestión de riesgos empresariales sobre la estrategia, la primera es la posibilidad de que la estrategia no esté alineada y las consecuencias o resultados de la estrategia elegida.

*Posibilidad de una estrategia no alineada:*

**UNA ESTRATEGIA QUE NO ESTÉ ALINEADA AUMENTA LA POSIBILIDAD DE QUE LA ORGANIZACIÓN NO CUMPLA SU MISIÓN Y VISIÓN, O PUEDA COMPROMETER SUS VALORES, AUN CUANDO LA ESTRATEGIA SE LLEVE A CABO CON ÉXITO. POR TANTO, LA GESTIÓN DEL RIESGO EMPRESARIAL CONSIDERA LA POSIBILIDAD DE QUE LA ESTRATEGIA NO ESTÉ ALINEADA CON LA MISIÓN Y LA VISIÓN DE LA ORGANIZACIÓN. (Instituto de Auditores Internos de España y PwC, 2017)**

- Un efecto inicial que debe controlarse es que de una estrategia de alto nivel (estratégico) subyace la selección de estrategias tácticas y operativas, lo cual genera árboles de decisión y de definición de acciones, objetivos, metas y funciones técnicas y de negocio
- Cada entidad tiene una misión, una visión y unos valores clave que definen lo que está tratando de conseguir y cómo quiere llevar a cabo sus actividades de

negocio, por esto en algunas organizaciones se presenta un escepticismo en adoptar verdaderamente una filosofía corporativa.

- No obstante, los fundamentos de la administración empresarial demuestran que la misión, la visión y los valores clave son un factor crítico de éxito para el alineamiento empresarial y por tanto cuando se trata de gestionar el riesgo y demostrar resiliencia en períodos de cambio también son imprescindibles.
- A nivel del abordaje de la ERM, la estrategia elegida debe apoyar la misión y la visión de la organización como principio de su generación de valor a la organización.

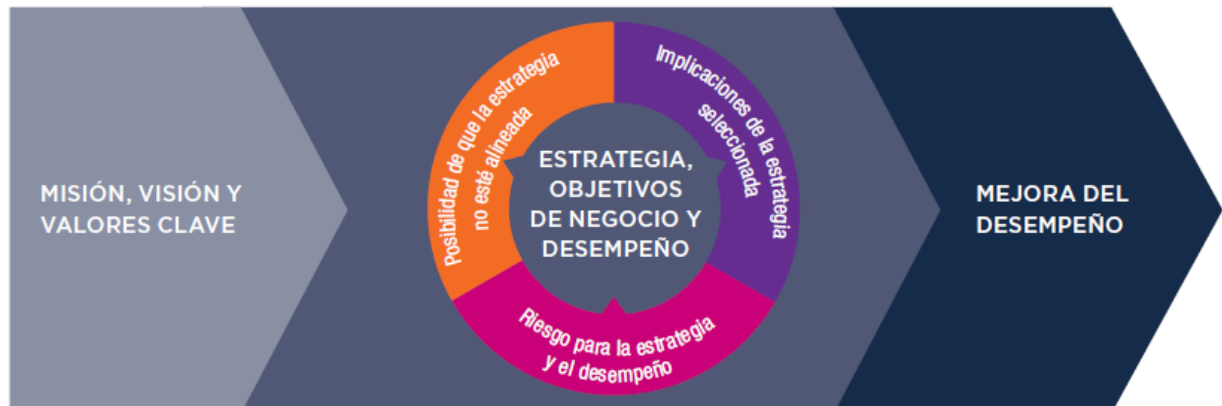
*Consecuencias resultantes de la estrategia elegida:*

- Acorde con PwC: “Cuando la dirección desarrolla una estrategia y baraja distintas alternativas con el consejo de administración, toman decisiones con respecto a los pros y los contras inherentes a dicha estrategia. Cada estrategia alternativa tiene su propio perfil de riesgos —esto es, las consecuencias que se derivan de la estrategia. El consejo de administración y la dirección deben determinar si la estrategia encaja con el apetito al riesgo de la organización y cómo ayudará a la organización a establecer objetivos y, en última instancia, a asignar los recursos de manera eficiente.” (Instituto de Auditores Internos de España y PwC, 2017)



Con base en lo anterior, la gestión del riesgo empresarial no solo implica su entendimiento y aplicación en la selección de estrategias sino también evaluar si las estrategias en formulación o en ejecución están desalineadas con la consecución de objetivos o de desalinean por cambios en el entorno, regulación, factores de mercado, tecnología u otros.

Estas consideraciones se muestran en la siguiente figura:



Fuente: (Instituto de Auditores Internos de España y PwC, 2017)

## Marco de Gestión de Riesgo Empresarial

El marco ERM destaca la importancia de la gestión de riesgo empresarial en la planificación estratégica y su integración o interrelación con todos los niveles organizacionales, ejerciendo influencia en sus planes, alineamiento estratégico y desempeño, lo cual implica a todos los departamentos y funciones, incluyendo los procesos de Tecnologías de Información y Comunicación TIC. Esto conjunto de principios es referenciado por COSO en la siguiente figura:



Fuente: (Instituto de Auditores Internos de España y PwC, 2017)

Para la implementación del marco COSO se deben respetar una serie de principios los cuales se organizan en los cinco componentes señalados en la figura, los cuales se encuentran interrelacionados y se definen de la siguiente forma:

**1. Gobierno y cultura:**

Acorde con PwC: *“El Gobierno marca el tono en la entidad, reforzando la importancia de la gestión del riesgo empresarial y estableciendo responsabilidades de supervisión al respecto. La cultura hace referencia a los valores éticos, a los comportamientos deseados y a la comprensión del riesgo en la entidad.”* (Instituto de Auditores Internos de España y PwC, 2017)

**2. Estrategia y establecimiento de objetivos:**

Acorde con PwC: *“La gestión del riesgo empresarial, la estrategia y el establecimiento de objetivos funcionan juntos en el proceso de planificación estratégica. Se establece un apetito al riesgo y se alinea con la estrategia; los objetivos del negocio ponen en práctica la estrategia al tiempo que sirven de base para identificar, evaluar y responder ante el riesgo.”* (Instituto de Auditores Internos de España y PwC, 2017)

**3. Desempeño:**

Acorde con PwC: *“Es necesario identificar y evaluar aquellos riesgos que puedan afectar a la consecución de los objetivos estratégicos y de negocio. Los riesgos se priorizan en función de su gravedad en el contexto del apetito al riesgo. Posteriormente, la organización selecciona las respuestas ante el riesgo y adopta una visión a nivel de cartera con respecto al nivel de riesgo que ha asumido. Los resultados de este proceso se comunican a las principales partes interesadas en el riesgo.”* (Instituto de Auditores Internos de España y PwC, 2017)

**4. Revisión y monitorización:**

Acorde con PwC: *“Al examinar el desempeño de la entidad, una organización puede determinar cómo funcionan los componentes de gestión del riesgo empresarial con el paso del tiempo en un entorno de cambios sustanciales, y qué aspectos son susceptibles de revisar y modificar.”* (Instituto de Auditores Internos de España y PwC, 2017)

**5. Información, comunicación y reporte:**

Acorde con PwC: *“La gestión del riesgo empresarial requiere un proceso continuo de obtención e intercambio de la información necesaria, tanto de fuentes internas como externas, que fluya hacia arriba, hacia abajo y a lo largo de todos los niveles de la organización.”* (Instituto de Auditores Internos de España y PwC, 2017)


Estos componentes del marco son respaldados por un conjunto de principios que cubren todos los aspectos señalados, desde aspectos de gobierno hasta aspectos de monitoreo los cuales describen las prácticas aplicables a las organizaciones, la adhesión a estos principios proporciona a la dirección y consejo, capacidades razonables sobre la gestión de riesgos, tanto en la estrategia como en los objetivos empresariales. Estos se resumen en la siguiente figura:





**Gobierno y Cultura**

1. Ejerce la Supervisión de Riesgos a través del Consejo de Administración
2. Establece Estructuras Operativas
3. Define la Cultura Deseada
4. Demuestra Compromiso con los Valores Clave
5. Atrae, Desarrolla y Retiene a Profesionales Capacitados




**Estrategia y Establecimiento de Objetivos**

6. Analiza el Contexto Empresarial
7. Define el Apetito al Riesgo
8. Evalúa Estrategias Alternativas
9. Formula Objetivos de Negocio



**Desempeño**

10. Identifica el Riesgo
11. Evalúa la Gravedad del Riesgo
12. Prioriza Riesgos
13. Implementa Respuestas ante los Riesgos
14. Desarrolla una Visión a nivel de Cartera



**Revisión y Monitorización**

15. Evalúa los Cambios Significativos
16. Revisa el Riesgo y el Desempeño
17. Persigue la Mejora de la Gestión del Riesgo Empresarial



**Información, Comunicación y Reporte**

18. Aprovecha la Información y la Tecnología
19. Comunica Información sobre Riesgos
20. Informa sobre el Riesgo, la Cultura y el Desempeño

Fuente: (Instituto de Auditores Internos de España y PwC, 2017)

## Conclusiones y recomendaciones

Con base en lo anterior la gestión del riesgo empresarial, tal y como se define en la lectura puede brindar un gran apoyo a las organizaciones para a identificar, evaluar y gestionar los riesgos de la estrategia y por tanto el alineamiento de las estrategia de los procesos de Tecnologías de la Información no pueden quedar excluidos en este proceso, Así mismo, señalan los autores referenciados que las causas más significativas de destrucción de valor están arraigadas en la posibilidad de que la estrategia no respalde la misión y visión de la entidad, y las consecuencias resultantes de la estrategia, incluyendo en esta dimensión a las áreas y al Gobierno de TI.

De igual forma la gestión del riesgo empresarial mejora la selección de estrategias tanto en las TI como en el Negocio y permite elegir estrategias mediante una toma de decisiones estructurada, que analice el riesgo y alinee los recursos con la misión y visión de la organización.

En estos procesos no pueden dejar de evaluarse tendencias importantes en tecnologías y su evolución tales como:

- La proliferación de datos: A medida que se disponga de más y más datos y aumente la velocidad a la que estos se puedan analizar, será necesario adaptar la gestión del riesgo empresarial.
- La inteligencia artificial y la automatización: Sobre lo cual se considera que hemos entrado en la era de los procesos automatizados y de la inteligencia artificial.
- El coste de la gestión de riesgos: Una preocupación frecuente expresada por muchos directivos es el coste de la gestión de riesgos, de los procesos de cumplimiento y de las actividades de control en comparación con el valor que generan.
- Construir organizaciones más fuertes: A medida que las organizaciones vayan integrando mejor la gestión del riesgo empresarial con la estrategia y el desempeño, se presentará una oportunidad para fortalecer la resiliencia.

## Referencias bibliográficas

- Alfaro Campos, J. C. (2017). *Metodología para la gestión de riesgos de TI basada en COBIT 5*. Cartago, Costa Rica: Instituto Tecnológico de Costa Rica.
- Alvarado Carpio, D. F., & Zumba Morales, L. A. (2015). *Elaborar un Plan de Gestión de Riesgos de las Tecnologías de Información y Comunicación basada en el Marco COBIT 5 para riesgos aplicado a la Universidad de Cuenca*. Cuenca - Ecuador: Universidad de la Cuenca. Obtenido de <http://dspace.ucuenca.edu.ec/handle/123456789/22342>
- Garbarino Alberti, H. (2014). *Marco de Gobernanza de TI para empresas PyMEs - SMEsITGF*. Madrid: Universidad Politécnica Madrid.
- Gasetta, E. R., Motta, A. C., & Boca Piccolini, J. D. (2016). *Fundamentos de gobierno de TI*. Obtenido de <https://cedia.edu.ec/dmdocuments/publicaciones/Libros/GTI2.pdf>
- González, P. (30 de Noviembre de 2018). *COBIT 2019 — El nuevo modelo de gobierno empresarial para información y tecnología*. Obtenido de <https://medium.com/https://medium.com/@ppglzr/cobit-2019-el-nuevo-modelo-de-gobierno-empresarial-para-informaci%C3%B3n-y-tecnolog%C3%ADa-a7bf92b7288b>
- Hamidovic, H. (2008). Gobierno de TI. Fundamentos del Gobierno de TI basados en ISO/IEC 38500. *ISACA Bogotá Chapter*, 1-9.
- Instituto de Auditores Internos de España y PwC. (2017). *Gestión del Riesgo Empresarial. Integrando Estrategia y Desempeño. Resumen Ejecutivo COSO*. España: PwC.
- ISACA. (2012). *Cobit 5. Un marco de negocio para el gobierno y la gestión de las TI de la Empresa*. Estados Unidos: ISACA.
- ISACA IT RISK. (2009). *Marco de Riesgos de TI*. Estados Unidos de América: ISACA.
- ISACA®. (2012). *Cobit 5. Procesos Catalizadores*. Estados Unidos: ISACA.
- Medina Cárdenas, Y. C., Areniz Arévalo, Y., & Rico Bautista, D. W. (2016). Alineación estratégica bajo un enfoque organizacional de gestión tecnológica: ITIL & ISO 20000. *Tecnura*, 82-94. Obtenido de <http://revistas.udistrital.edu.co/ojs/index.php/Tecnura/issue/view/805>
- Pacheco Garisoain, M. L. (2016). *Tecnologías de la información y la comunicación*. Obtenido de <https://elibro.net/es/ereader/usanmarcos/38062>
- Real Academia Española. (12 de 12 de 2020). *Diccionario de la Lengua Española*. Obtenido de <https://dle.rae.es/>
- Telefónica. (2009). *ISO/ICE 20000 Guía completa de aplicación para la gestión de los servicios de tecnologías de la información*. Madrid, España: Aenor Ediciones.
- *UNE-ISO/IEC 38500 Gobernanza Corporativa de la Tecnología de Información*. (2013). Madrid-España: AENOR.
- Valencia Duque, F. J. (Marzo de 2016). Gobierno y gestión de riesgos de tecnologías de información y aspectos diferenciadores con el riesgo organizacional. *Gerencia Tecnológica Informática*, 15(41), 65-77. Obtenido de <https://www.researchgate.net/publication/311206737>
- Vargas Bermúdez, F. A. (2014). Marcos de control y estándares para el gobierno de tecnologías de información (TI). *I+3 Investigación Innovación Ingeniería*, 31-44.



[www.usanmarcos.ac.cr](http://www.usanmarcos.ac.cr)

San José, Costa Rica