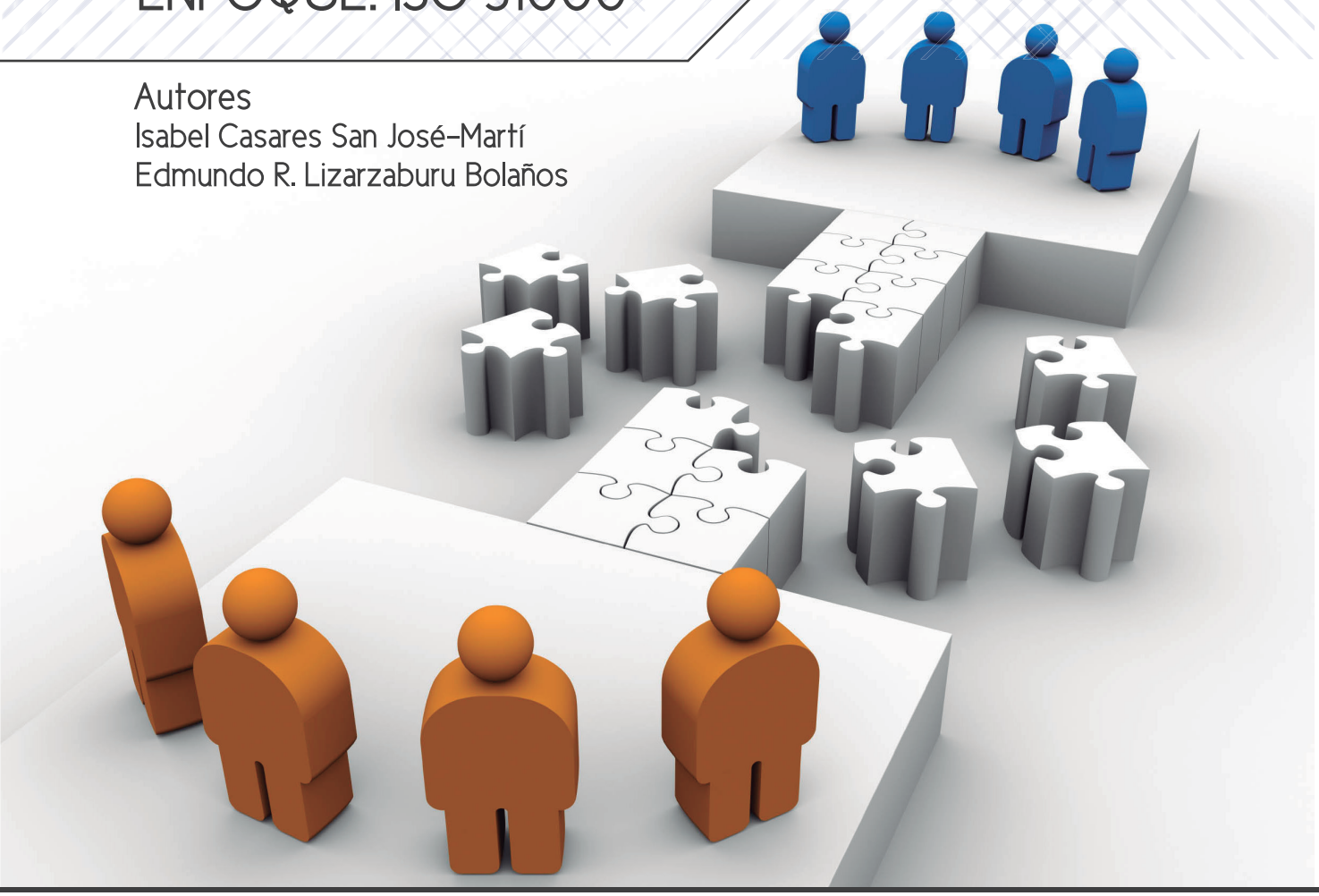
INTRODUCCIÓN A LA GESTION INTEGRAL DE RIESGOS EMPRESARIALES

ENFOQUE: ISO 31000

Autores
Isabel Casares San José-Martí
Edmundo R. Lizarzaburu Bolaños



Platinum
Editorial

INTRODUCCIÓN A LA GESTIÓN INTEGRAL DE RIESGOS EMPRESARIALES
ENFOQUE: ISO 31000

instituto de regulación & finanzas | UNIVERSIDAD esan

Platinum Editorial

CRÉDITOS

Introducción a la Gestión Integral de Riesgos Empresariales Enfoque: ISO 31000
Primera edición: Mayo del 2016 – Lima, Perú
ISBN: 978-612-47172-2-2

Editado por:
PLATINUM EDITORIAL S.A.C
Cal. San Lino Nro.148 Urb. Monterrico Chico Lima
Lima – Santiago de Surco
Tel. 511 – (01) 6440640
www.platinumeditorial.com

Autores
Isabel Casares San José-Martí, Economista, Actuario de Seguros y Asesora de empresas en Gestión de Riesgos y Seguros (España).

Edmundo R. Lizarzaburu Bolaños, Universidad ESAN (Perú).

Editor Responsable
Valery Motta Saenz

Corrección de texto
Isabel Arevalo Rufasto

Diagramación y diseño
Greyse Anais Morales Palacios

Publicación electrónica disponible en:
www.platinumeditorial.com
www.owlbook.org

Libro auspiciada por:

www.fri.com.pe

www.platinumeditorial.com

INTRODUCCIÓN A LA GESTIÓN INTEGRAL DE RIESGOS EMPRESARIALES
ENFOQUE: ISO 31000

Autores:

Isabel Casares San José-Martí, Economista, Actuario de Seguros y Asesora de empresas en Gestión de Riesgos y Seguros (España).

Edmundo R. Lizarzaburu Bolaños, Universidad ESAN (Perú).

Asistentes:

Javier Anderson Pagán , Rayko Zecevich, y Leonel Kevin Pacari alumnos de la Universidad ESAN

Miguel Cóndor, egresado de la Universidad ESAN.

Colaboradores:

Diego Cisneros, Exsuperintendente adjunto de banca y microfinanzas de la SBS (Perú)

Mónica Chávez, Universidad ESAN (Perú)

Hamilton Galindo, Universidad del Pacífico (Perú)

Julio Quispe, Universidad ESAN (Perú)

Luis Berggrun, Universidad ICESI (Colombia)

Roberto Santillán, EGADE Tecnológico de Monterrey (México).

Isabel Casares San José- Martí

Licenciada en Ciencias Económicas y Empresariales por la Universidad Autónoma de Madrid. Rama Ciencias Económicas (1988). Licenciada en Ciencias Económicas y Empresariales por la Universidad Complutense de Madrid. Rama Ciencias Actuariales y Financieras (1990). Doctorado en Economía Financiera y Actuarial por la Universidad Complutense de Madrid (1997). Título Profesional de Actuario de Fondos de Pensiones por el Ministerio de Economía – Dirección General de Seguros y Fondos de Pensiones de España. Diploma de Mediador de Seguros Titulado por el Ministerio de Economía – Dirección General de Seguros y Fondos de Pensiones.

Perito judicial actuarial. Presidenta de CASARES, Asesoría Actuarial y de Riesgos, S.L., Miembro de las comisiones de formación, investigación y actos de AGERS. Miembro del grupo de trabajo en España para la elaboración de las normas internacionales de gestión de riesgos de las empresas. ISO 31000 – ISO 31010 (GT 13). Miembro asociado número 1.668 del INSTITUTO DE ACTUARIOS ESPAÑOLES. Miembro de la Comisión de Asuntos Laborales y Sociales de la Confederación Empresarial de Madrid – CEOE. Miembro del Comité de Pensiones de la Comisión de Solvencia II y de la Comisión de Dependencia del Instituto de Actuarios Españoles.

Edmundo R. Lizarzaburu Bolaños

Profesor – Consultor en la Universidad ESAN. Director en GFI del Perú SAC, GFI Exchange de Colombia, Consultor Latinoamericano de GFI Group USA y Director en Empresas de los sectores de Tecnología, Servicios y Farmacéutico. Acreditado en Riesgos (CRA), Finanzas (RFS) y Proyectos. Experto en calidad (normas ISO) por AENOR. Vicepresidente del American Academy of Financial Management (AAFM) – Capítulo Peruano. Investigador acreditado por CONCYTEC.

Ha sido Gerente General desde el año 2003 hasta el 2011 en Datos Técnicos S.A. – Datatec, empresa subsidiaria de la Bolsa de Valores de Lima y SIF Icap Intercapital de México, dedicada a ofrecer soluciones para transacciones financieras OTC y venta de información para la intermediación financiera (áreas de finanzas, riesgos, tesorería entre otras). Además ha sido apoderado senior en Scotiabank (Ex – Banco Sudamericano).

Candidato a Doctor por UC3 de España (2012 a la fecha); Magister en Investigación – Programa Doctoral ESAN/UC3 (2012); Program of Negotiation PON – Harvard University (2012); Postgrado en Administración de Riesgos por el TEC – Tecnológico de Monterrey (2011); Global MBA de Thunderbird y EGADE – TEC de Monterrey (2008); Maestría en Dirección y Evaluación Financiera de USMP (2002) y Especializaciones en Riesgos, Finanzas, Proyectos y Calidad. Ingeniero Industrial (2000), Pontificia Universidad Católica del Perú. Ex alumno de La Inmaculada.

AGRADECIMIENTOS

A mi esposa Gabriela Barriga, mis hijos Macarena Lizarzaburu y Fausto Lizarzaburu así como a los alumnos de los diversos cursos impartidos.

Edmundo R. Lizarzaburu Bolaños

A mis alumnos de los distintos cursos y máster por la confianza y el apoyo incondicional que me dan en todo momento.

Isabel Casares San José-Martí

Al Sr. Diego Cisneros, por sus comentarios y por el prólogo escrito para el libro.

Los autores

PRÓLOGO

Los autores proponen un trabajo de aplicación sobre los principales marcos teóricos y de implementación de la gestión de los riesgos tomando como eje principal la norma ISO 31000, la cual nos permite contar con una aproximación a la gestión sistemática, ordenada y auditable de los riesgos de cualquier compañía.

La principal ventaja del camino escogido por los autores es las escalabilidad de las recomendaciones propuestas para distintos tamaños de empresa y niveles de complejidad del negocio, y casos prácticos para el desarrollo del lector.

La gestión del riesgo es antigua como la naturaleza de los negocios, existen registros de contratos sobre futuros del precio del arroz en el antiguo Japón del siglo XVII y los primeros contratos de seguros para cargamentos marítimos se empiezan a esbozar en la China del siglo II. Sin embargo, la gestión del riesgo como cuerpo teórico es relativamente nueva. Las primeras aplicaciones para gestionar riesgos surgen luego de la segunda Guerra Mundial, con la aplicación de los libros de teoría de juegos y probabilidades de John von Neumann y Oskar Morgenstern. No es hasta finales del siglo XX, que la industria financiera aplica de forma intensiva esta metodología para manejar los riesgos de manera integral, y los reguladores financieros introducen los conceptos de gestión de riesgos como mandatorios en todo su ámbito regulado (Dionne 2013: 147–166).

Los autores desarrollan los principios del estándar ISO 31000 como marco general para la gestión de los riesgos y control interno, pero también la implementación de la actualización del marco de trabajo de COSO en su versión 2013, dando énfasis en la gestión de la seguridad de la información y el desarrollo del riesgo de fraude como entidad separada de los otros riesgos. Esta actualización de principios permite una visión sistemática e integral de la gestión de riesgos y su evolución en los últimos veinte años.

Mg. Diego Cisneros

PRESENTACIÓN

Para iniciar un análisis de gestión de riesgos empresariales, es necesario tener claros los conceptos que se utilizarán y que todos conozcan el alcance del control y sus resultados, ya que existen muchas metodologías y muchos enfoques distintos.

El objetivo de este libro es ayudar a tener un buen comienzo, pues de eso depende que los resultados sean los esperados. También para entender la necesidad de gestionar los riesgos de una empresa, no solo reducirlos, y así generalizar un criterio para todo tipo de riesgos, incluidos los riesgos estratégicos, legales, operacionales, financieros, tecnológicos, reputacionales, etcétera.

Para una eficaz gestión de riesgos de una empresa es necesario no solo contemplar todas las etapas fundamentales: identificación, evaluación, respuesta y supervisión, sino también oportunidades de negocio. Es en la etapa de identificación de los riesgos donde podemos detectar, además de las amenazas para la empresa, oportunidades ocultas tras de estas que pueden ser aprovechadas. Con la aplicación de los principios explicados en estas páginas se puede confirmar que tanto la gerencia de los riesgos como un adecuado sistema de control interno pueden contribuir al logro de objetivos empresariales.

El buen gobierno de una sociedad en general exige el establecimiento de un control interno adecuado que permita a la alta dirección de la empresa la toma decisiones, por lo que las empresas deben analizar los riesgos que son propios de su actividad y mantener mecanismos específicos de control interno que aseguren la supervisión continuada de los mismos. Son modelos dinámicos que permiten evaluar la situación ante la aparición de riesgos, que incluso podrían ser objeto de aseguramiento con terceros.

Es necesario que exista transparencia en la información interna, de forma que pueda ser detectada cualquier amenaza lo antes posible para reducir o anular el impacto antes de que este se produzca. Nos encontramos ante una demanda creciente de información por parte de la empresa, a raíz de la aparición de nuevas exigencias que la afectan en materia de responsabilidad social, medio ambiente y sostenibilidad. La información se necesita en todos los niveles de la organización para, por una parte, identificar, evaluar y responder a los riesgos, y por otra, dirigir la entidad y conseguir sus objetivos.

Es importante el establecimiento de una comunicación eficaz en un sentido amplio, que facilite una circulación de la información (formal e informal). La alta dirección debe brindar un mensaje claro y preciso al personal sobre la importancia de compartir información veraz y oportuna, y la responsabilidad de cada uno en este objetivo, con el fin de lograr una adecuada administración y control.

ÍNDICE

ÍNDICE DE GRÁFICOS

ABREVIATURAS

AIR.- Administración Integral de Riesgos.

BCRP.- Banco Central de Reserva del Perú

COSO.- Committee of Sponsoring Organizations of Treadway Commission.

ERM.- Enterprise Risk Management – Gestión del riesgo empresarial.

IPPC.- Intergovernmental Panel on Climate Change.

ISO.- International Organization for Standardization.

MILA.- Mercado Integrado Latinoamericano.

OADS.- Órgano de administración, dirección o supervisión.

OCDE.- Organización para la Cooperación y el Desarrollo Económico.

OSHA.- Occupational Safety and Health Administration.

ORSA.- Own Risk and Solvency Assessment – Evaluación interna de los riesgos y de su solvencia.

PAS 99: Sistemas de Gestión Integrados.

PMI.- Project Management Institute.

RM.- Risk Management.

SBS.- Superintendencia de Bancos y Seguros.

SCI.- Sistema Control de Riesgos.

UNE-ISO 31000.- Gestión del riesgo. Principios y directrices.

INTRODUCCIÓN

En la actualidad, los profesionales de la gestión del riesgo tienen una labor importante en las empresas donde laboran, debido a que deben inculcar y fomentar la gestión del riesgo como parte de la cultura de su organización.

Es por ello que el reto al que se enfrentan hoy las empresas y los profesionales del riesgo no es solo romper el mito referido a que "la gestión del riesgo se relaciona con estar asegurados o coberturados", sino que tienen que involucrar a todo el personal en el manejo y administración de los riesgos de la empresa, de tal manera que puedan reducir el impacto y la probabilidad de ocurrencia de los mismos en las operaciones. Los sistemas de gestión de riesgos requieren una planificación y evaluación científica y rigurosa, que se cimenta en información veraz y oportuna.

Dentro de las empresas, los administradores de los riesgos son los responsables del manejo de los planes de acción y deben asegurar su efectividad al momento de implementarlos. Los riesgos están asociados a diversos conceptos, uno de ellos es la incertidumbre, situación que hace importante el uso de herramientas estadísticas para evaluarlos y sobre todo gestionarlos.

Ante todo esto, la gestión de riesgos aparece para dar solución a las necesidades que se presentan ante diversas amenazas, incertidumbres y eventos de riesgo a los que están expuestas todas las actividades que forman parte del desarrollo de una empresa u organización.

Diversos ejemplos de mala gestión del riesgo han atraído la atención de los medios de comunicación de todo el mundo y sus consecuencias son demasiado evidentes por su impacto en los trabajadores, los consumidores y la reputación de la empresa.

La gestión de riesgo es y ha sido objeto de un número significativo de publicaciones y trabajos académicos. Este libro proporciona una guía en el desarrollo de un mecanismo para la gestión eficiente de los riesgos basado tanto en las normas ISO 31000 e ISO 31010, como en el marco COSO 2013, incluyendo, donde sea necesario, las buenas prácticas descritas en BS 31100 y PAS 99 para la gestión de procesos de una manera integrada.

Lo importante de los riesgos es identificarlos. Si se identifican se pueden gestionar, si se gestionan se puede monitorear y establecer planes de acción y de mejora.

Capítulo I:

Introducción a los Riesgos

1.1 Normas y estándares internacionales aplicados a la gestión de riesgos

El análisis de oportunidades y amenazas, incertidumbres y los riesgos o eventos al riesgo a los que están sometidas todas las actividades de cualquier organización, sin importar su diligencia o tamaño, son conocidas en la actualidad como "Gestión de Riesgo", un término antes utilizado para referirse específicamente a accidentes operacionales, enfermedades, incendios o catástrofes naturales, entre otros, que pueden afectar el logro de los objetivos de cualquier tipo empresa y alterar los sistemas de gestión.

La gestión de riesgos es una etapa fundamental en la evaluación económica y financiera. Se trata de un enfoque riguroso y documentado en todos los niveles de desarrollo de los eventos analizados, lo que requiere información de todas las áreas de interés, internas y externas.

Por otro lado, la información de sus procesos es uno de los activos más importantes que poseen las empresas y tiene un valor para la organización, por lo tanto se deberían desarrollar mecanismos que aseguren una protección adecuada de los mismos. Es así como la seguridad de información, cuyo objeto o propósito consiste en mantener la continuidad de los procesos organizacionales, ha cobrado enorme importancia. Es necesario que los responsables de la seguridad de la información en las organizaciones tomen conciencia de su papel y contrasten los riesgos a los que están sometidos.

Finalmente, la globalización ha acelerado el ritmo de la innovación y el desarrollo tecnológico, generando una continua transformación en el mercado y un enorme crecimiento de la demanda por productos y servicios, lo que ha llevado a una mayor evolución de la gestión del conocimiento y los estudios de gestión de riesgos.

En los últimos años se ha incrementado la preocupación por la gestión de riesgos, y se ha identificado la necesidad de tener un marco de referencia sólido para identificar, evaluar y gestionar de manera efectiva los riesgos en las empresas. En este sentido, diversos estudiosos tales como: Robert I. Mesh, Bob A. Hedges, Clifford W. Smith y René M. Stulz se han enfocado en el *Enterprise Risk Management* (ERM) ccomo un proceso por el cual la empresa integra todas sus funciones de gestión de riesgos.

Una de las estrategias de reacción y soluciones puntuales para protocolizar y gestionar el riesgo, es la norma-guía técnica ISO 31000, emitida por la Organización Internacional de Normalización. Es una familia de normas sobre Gestión del riesgo con el propósito de proporcionar principios y directrices para la gestión de riesgos y el proceso implementado en el nivel estratégico y operativo.

La ISO 31000 permite a las organizaciones[1]:

- Fomentar una gestión proactiva libre de riesgo.

[1]Fuente: www.iso.org

- Mejorar la identificación de oportunidades y amenazas.
- Cumplir con todas las exigencias legales y reglamentarias, además de las normas internacionales.
- Aumentar la seguridad y confianza, así como mejorar la prevención de pérdidas y manejo de incidentes.
- Mejorar el aprendizaje organizacional.
- Mejorar la eficiencia y eficacia operacional.

Todas las actividades de una organización están sometidas de forma permanente a una serie de amenazas, lo cual las hace altamente vulnerables, comprometiendo su estabilidad. Accidentes operacionales, enfermedades, incendios u otras catástrofes naturales, son una muestra de este panorama, sin olvidar las amenazas propias de su negocio

Tradicionalmente, las organizaciones han tratado estos riesgos mediante estrategias de reacción y soluciones puntuales. No obstante, la experiencia ha demostrado que los elementos que conforman los riesgos y los factores que determinan el impacto de sus consecuencias sobre un sistema son los mismos que intervienen para todos los riesgos en una organización. Por ello, la tendencia moderna es utilizar un enfoque integral de manejo de los mismos conocido como "*Enterprise Risk Management*" (ERM), con el fin de evaluar, administrar y comunicar estos riesgos de una manera integral, basados en los objetivos estratégicos de la organización. En la actualidad, las estrategias preventivas resultan mecanismos importantes en la gestión de riegos. La ¨anticipación¨ puede permitir generar ahorros y reducir impactos en las empresas.

La gestión integral de riesgos ha ganado impulso en los últimos años, especialmente a partir de la década de los noventa, lo que ha conllevado a la aparición de "modelos de gestión de riesgos y control", algunos de ellos de carácter más específico, como por ejemplo: COSO, SRM, ISO 14000, ISO 22000, OHSAS, etcétera, y otros de carácter más global como la norma AS/NZS 4630 o la misma ISO 31000.

La gestión de riesgos está diseñada para ayudar a las organizaciones a:

- Incrementar la probabilidad de lograr los objetivos.
- Promover la gestión proactiva.
- Ser conscientes de la necesidad de identificar y tratar el riesgo en toda la organización.
- Mejorar en la identificación de oportunidades y amenazas.
- Cumplir con las exigencias legales y reglamentarias pertinentes, así como las normas internacionales.
- Mejorar la información financiera.
- Establecer una base confiable para la toma de decisiones y la planificación.
- Mejorar la gobernabilidad.
- Mejorar la confianza de los grupos de interés (*stakeholders*).
- Mejorar los controles.

- Asignar y utilizar con eficacia los recursos para el tratamiento del riesgo.
- Mejorar la capacidad de recuperación de la organización.
- Aumentar la eficacia y eficiencia operacional.
- Mejorar la salud y de seguridad, así como la protección del medio ambiente.
- Mejorar la prevención de pérdidas, así como la gestión de incidentes.
- Reducir las pérdidas.
- Mejorar el aprendizaje organizacional.

El éxito de la implantación de los sistemas de gestión basados en estándares internacionales comenzó con la difusión de las normas ISO 9000 (calidad) e ISO 14000 (medio ambiente), (estándares en proceso de cambio y actualización), diversificándose ahora con nomas más específicas. En efecto, en los últimos años se está produciendo, siguiendo la senda abierta por las exitosas normas, un importante proceso de emisión de nuevos estándares, tanto nacionales como internacionales. Se trata de estándares relacionados con ámbitos tan diversos de la gestión empresarial como la prevención de riesgos laborales y la seguridad y salud en el trabajo, la responsabilidad social corporativa o las actividades relacionadas con la gestión de recursos humanos, entre otros.

Por ejemplo, en el ámbito de la gestión y prevención de riesgos laborales ~~,~~que tiene por objeto mejorar la calidad de la seguridad, higiene y salud laboral de los trabajadores de la empresa~~,~~ está en evaluación la norma ISO 45001, el primer estándar internacional para salud y seguridad ocupacional.

1.2 Modelo COSO

El Comité de Organizaciones Patrocinadoras de la Comisión Treadway[2] (COSO), es una iniciativa de cinco instituciones del sector privado de los Estados Unidos (Institute of Management Accountants (IMA), American Accounting Association (AAA), American Institute of Certified Public Accountants (AICPA), Institute of Internal Auditors (IIA), Financial Executives International (FEI)) que se formó en 1985, para establecer un modelo común de control interno que sirva de norma para contrastar y evaluar los sistemas de control interno de las empresas.. Dicho modelo ha sido incorporado en las políticas y regulaciones dentro de organizaciones que buscan mejorar el control de sus actividades y el cumplimiento de sus objetivos.

En los últimos se ha intensificado la preocupación en la gestión de riesgos, y se identificó la necesidad de tener marco de referencia sólido para identificar, evaluar y gestionar los riesgos de manera efectiva. La necesidad de este marco de referencia para la Gestión de Riesgos que proporcione principios y conceptos clave, y un lenguaje común con una orientación clara resultaba imperioso. El COSO considera que este marco integrado de Enterprise Risk Management (ERM) cubre esta necesidad, y espera que sea ampliamente aceptado por las empresas y otras organizaciones.

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

El 14 de mayo de 2013, el COSO publicó una versión actualizada de su Marco Integrado de Control Interno (marco 2013) que proporciona unas mejoras a las entidades que utilicen el marco de 1992, COSO Control Interno – Marco Integrado (el "Marco de 1992") para cumplir con la Sección 404 de la Ley Sarbanes-Oxley[3] de 2002 (SOX), y la información sobre cómo hacer la transición del marco 1992 al marco 2013.

El marco 2013 de COSO, crea una estructura que puede ser considera más formal para el diseño y la evaluación de la efectividad del control interno a través de 17 principios para describir los componentes del control interno relevantes para todas las entidades, desarrolla los conceptos de evaluación de riesgos, riesgo inherente, tolerancia al riesgo, tratamiento de los riesgos y la vinculación entre riesgos en las actividades de evaluación y control.

Asimismo, a diferencia del Marco 1992, incluye explícitamente el concepto de riesgo de fraude al evaluar los riesgos para el logro de los objetivos de la organización, teniendo en cuenta::

- Sesgo de la administración.
- Nivel de juicios y estimaciones en informes externos.
- Fraudes y situaciones comunes a los sectores y mercados en los que opera la entidad.
- Las regiones o zonas geográficas en las que opera la entidad.
- Los incentivos que pueden motivar un comportamiento fraudulento.
- La naturaleza de la tecnología y la capacidad de la administración para manejar la información.
- Transacciones inusuales o complejas sujetas a la influencia significativa en su gestión.
- La vulnerabilidad de la administración y los posibles esquemas para eludir las actividades de control existentes.

Además, se añaden consideraciones respecto al uso de los proveedores de servicios externalizados y una mayor relevancia de la tecnología de la información.

Se anima a las empresas a la transición de sus aplicaciones y a realizar la documentación relacionada con la actualización al marco 2013 tan pronto como sea posible, dependiendo de las circunstancias particulares de las entidades. Durante el período de transición, establecido del 14 de mayo de 2013 al 15 de diciembre de 2014, se recomendó indicar la versión utilizada en los informes externos que se elaborasen.

El marco ERM y el marco 2013 tienen diferentes enfoques, pero los dos se complementan entre sí para el diseño, implementación, realización y evaluación de la gestión de riesgos empresariales.

Las empresas que utilizan COSO para informar sobre el control interno en la presentación de reportes externos podrían considerar:

[3] La Ley Sarbanes Oxley nace en Estados Unidos con el fin de monitorear a las empresas que cotizan en bolsa de valores, evitando que la valorización de las acciones de las mismas sean alteradas de manera dudosa, mientras que su valor es menor. Su finalidad es evitar fraudes y riesgo de bancarrota, protegiendo al inversor.

- Identificación de nuevos conceptos y cambios en la norma.
- La evaluación de su formación y las necesidades de capacitación.

El Marco 2013 afecta al diseño y evaluación del informe elaborado por las entidades debiendo establecer:

- Evaluación de la cobertura de los principios de los procesos existentes y los controles relacionados.
- Evaluación de los procesos actuales, actividades, y documentación disponible relacionada con la aplicación de los principios.
- Identificación de las deficiencias existentes en el marco anterior.
- Identificación de las medidas a tomar en la transición.
- Formulación de un plan para la transición para las empresas obligadas a ella.
- Confirmación de la divulgación del marco utilizado en cada momento.
- Coordinación y comunicación interna con todos los grupos que son responsables de la implementación, seguimiento y presentación de informes de la organización.
- Discutir y coordinar las actividades con la auditoría interna y externa.

El control interno es un proceso llevado a cabo por el consejo de administración, la gerencia y el resto del personal de la organización, diseñado para proporcionar una garantía razonable para lograr de objetivos relacionados con operaciones, reportes y cumplimiento.

En un sistema efectivo de control interno bajo el marco 2013, cada uno de los cinco componentes y principios están obligados a estar presentes y en funcionamiento. En relación a esto, tenemos las siguientes definiciones:

- Presente definido como *"la determinación de que existen componentes y principios pertinentes en el diseño e implementación del sistema de control interno para lograr los objetivos especificados".*

- Funcionamiento definido como *"la determinación de que los componentes y los principios pertinentes siguen existiendo en la realización del sistema de control interno para lograr los objetivos especificados".*

El marco de referencia integrado de control interno realizado por la Comisión Treadway publicado en 1992, que redefine el control interno, desarrollando un marco conceptual con herramientas para evaluar y mejorar los controles. En 1996 se establece un método comprensivo que describe 89 principios de las mejores prácticas para un manejo de riesgo eficaz dentro de una institución financiera, recogidos en los "Principios de riesgo generalmente aceptados" (GARP).

Según el video Financial Accounting: Fraud & Sarbanes-Oxley Act of 2000[4], la Ley Sarbanes-Oxley de 2002 aclara que este tema, que ha sido replicado en mayor o menor grado en diversos países, extiende

[4] Financial Accounting: Fraud & Sarbanes-Oxley Act of 2000. Recuperado de https://www.youtube.com/watch?v=KZpXlmlBtks

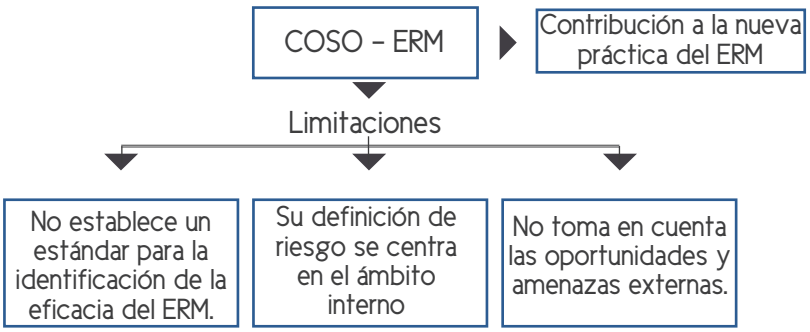
los requisitos a las empresas que cotizan en bolsa, para que implementen sistemas de control interno. Ello requiere de una Administración para la Certificación y de un auditor independiente para que dé fe de la eficacia de esos sistemas. El marco integrado de control interno sirve como el estándar ampliamente aceptado para satisfacer dichos requisitos.

En términos de evolución, el Enterprise Risk Management (ERM) ha sido ampliamente discutido por más de una década, pero fue desarrollado en un primer momento por grandes instituciones financieras. El interés se ha construido poco a poco desde mediados de los años 1990, cuando las unidades de inteligencia financiera crearon un marco extenso de ERM, lo que proporcionó una base sólida sobre la cual las empresas pueden mejorar el gobierno corporativo y entregar a los accionistas un mayor valor (Bowling y Rieger 2005).

Este marco de referencia integrado es la base para que el ERM se expanda al área de control interno, proporcionando un enfoque más sólido y amplio. Si bien con el ERM no se pretende reemplazar el marco de control interno, este no solo se circunscribe a necesidades de control interno sino que puede avanzar a un proceso de gestión de riesgos integral.

Por otro lado, si bien el marco de COSO–ERM hace una valiosa contribución a la nueva práctica del ERM, también tiene limitaciones. Por ejemplo, no puede establecer un estándar para la identificación de la eficacia del ERM. Su definición de riesgo se centra en el ámbito interno y no toma en cuenta las oportunidades y amenazas externas. Al adoptar un enfoque de comando y control, no se tiene en cuenta la gestión compartida de las amenazas con elementos externos ni las implicaciones sociales del ERM.

Gráfico 01: Limitaciones del COSO – ERM



Como resultado, la tendencia a no considerar las oportunidades se hace sistémica. Ello es hoy patente, ya que el ERM se ha institucionalizado dentro de la normativa, la práctica profesional y las normas esperadas de una buena gestión (Williamson 2007).

Capítulo II:
Gestión de Riegos

2.1 Introducción a la norma ISO 31000

En noviembre del 2009, la Organización Internacional de Normalización (ISO) publicó la norma ISO 31000: 2009 Gestión de Riesgos Principios y Directrices, una guía de implementación de la gestión de riesgos destinada a ayudar a las organizaciones de todos los tipos y tamaños a gestionar el riesgo, en vista de la diversidad de riesgos que enfrentan y las dificultades que existen en algunos casos para identificarlos. El objetivo de todas las organizaciones debe ser, además de la generación de valor con ética, la creación de un marco que:

- Ayude a gestionar los eventos de riesgos que se identifican.
- Proporcione una estructura para el control de riesgos, en especial para aquellos que no han sido identificados.
- Crear una organización más flexible, que permita responder a riesgos futuros de manera oportuna y logre una adecuada comunicación

La norma ISO 31000 para la gestión de riesgos tiene tres componentes relacionados:

Gráfico 02: Componentes para la gestión de riesgos

La norma ISO 31000 ofrece 11 principios para el proceso de la gestión del riesgo que pueden ser utilizados por cualquier organización, independientemente de su tamaño, actividad o sector. Su uso puede ayudar a las organizaciones a aumentar la probabilidad del logro de objetivos, mejorar la identificación de oportunidades y amenazas.

2.2 ¿Qué es la norma ISO 31000?

Es una guía de implementación que pretende ayudar a las organizaciones en el desarrollo de su propio enfoque de gestión del riesgo. Pero no es un estándar del que se pueda solicitar certificación. Mediante la implementación de la norma ISO 31000, las organizaciones pueden comparar sus prácticas de gestión de riesgos con un punto de referencia reconocido internacionalmente para conseguir una gestión eficaz de los riesgos y un buen gobierno corporativo. Es muy utilizada para programas de auditoría interna o externa de riesgos.

En muchas organizaciones ya están establecidos sistemas formales para gestionar los riesgos específicos basados en normas internacionales tales como calidad (ISO 9001), medio ambiente (ISO 14001), seguridad

de la información (ISO / IEC 27001), la seguridad alimentaria (ISO 22000), la continuidad del negocio (ISO 22301) y la salud y seguridad ocupacional (OHSAS 18001), que se han alojado en el sistema general de gestión de una organización. En algunos casos, se trata de un requisito reglamentario.

La gestión eficaz de riesgos permite mejorar potencialmente la gestión de las empresas, especialmente en aspectos como:

- Protección personal y material.
- Estrategias y tomas de decisiones.
- Mejora de la imagen de la empresa.
- Aumento de la competitividad frente a otras empresas.

El alcance de la norma ISO 31000 permite ser utilizada por todo tipo de empresa, sin importar su tamaño o sector, incluyendo entidades públicas o privadas y por grupos económicos, asociaciones, ministerios y compañías de todo tipo, pudiéndose aplicar para cualquier tipo de riesgo, buscando que la gestión sea transversal en la organización.

Centrándonos en la propia definición del riesgo, la ISO 31000 define el riesgo como "el efecto de incertidumbre sobre los objetivos", destacando además que:

- Un efecto es una desviación de lo esperado (positivo o negativo).
- Los objetivos pueden tener diferentes aspectos tales como financieros, económico, seguridad, metas medioambientales, entre otros, y pueden aplicarlos en diferentes niveles de la organización como los estratégicos, organizacionales, operativos o procesos de apoyo.
- El riesgo hace referencia a una combinación de las consecuencias de un evento o cambio en circunstancias, y la probabilidad de ocurrencia asociada.
- La incertidumbre es el estado, evento parcial, de deficiencia de información relacionada a, entendimiento o conocimiento de, un evento, su consecuencia, o probabilidad.

2.3 Principios de la gestión de riesgos

La ISO 31000 enumera once principios para una gestión eficaz del riesgo con el objetivo de informar y orientar todos los aspectos del enfoque de la organización en base a la gestión eficaz del riesgo. Además de implementar los principios, es importante que la organización los refleje en todos los aspectos del proceso de la gestión de riesgos, como indicadores del desempeño de la gestión eficaz.

Aunque todas las organizaciones gestionan el riesgo en alguna medida, los principios de la norma ISO 31000 proporcionan orientación sobre:

- La base para gestionar eficazmente el riesgo (por ejemplo, crea y protege el valor).
- Las características para una gestión eficaz de los riesgos (por ejemplo, integración de la gestión de riesgos en todos los procesos de la organización).

Al diseñar los objetivos de la gestión del riesgo de la organización, es importante y necesario considerar todos los principios, aunque cada uno de ellos puede variar según el marco de referencia considerado en la organización y su aplicación en la misma, por lo que es necesario conocer la implicación que tiene cada uno de ellos y aplicarlos de forma continua. La implementación eficaz de estos principios determinará tanto la eficacia como la eficiencia de la gestión del riesgo en la organización.

Posteriormente, los resultados de este tipo de análisis deben reflejarse en el diseño o la mejora (por ejemplo, en la asignación de responsabilidades, formación, comunicación con las partes interesadas y el diseño del seguimiento y revisión de los resultados de la gestión de riesgo).

Principio 1 : La gestión del riesgo crea y protege el valor

La gestión del riesgo contribuye de manera tangible al logro de los objetivos y a la mejora del desempeño, por ejemplo, en lo referente a la salud y seguridad de las personas, a la conformidad con los requisitos legales y reglamentos, a la aceptación por el público, a la protección ambiental, a la calidad del producto, a la gestión del proyecto, a la eficacia en las operaciones, y a su gobierno y reputación.

Aplicación del principio 1:

El principio explica que el propósito de la gestión del riesgo es crear y proteger el valor ayudando a la organización a lograr sus objetivos, ayudando a la organización a identificar y abordar los factores, tanto internos como externos, que dan lugar a la incertidumbre asociada con sus objetivos. El vínculo entre la eficacia de la gestión del riesgo y la contribución al éxito de la misma debe ser claramente demostrado y comunicado. El principio establece que el riesgo no debería ser gestionado para su propio bien, sino para lograr los objetivos y la mejora del desempeño.

Algunos atributos y valores son cualitativos y no se pueden medir en términos cuantitativos, pero también contribuyen considerablemente al desempeño, reputación y cumplimiento legal de la organización. Los valores humanos, sociales y ecológicos son particularmente importantes para gestionar los riesgos relacionados con la seguridad, la protección y el cumplimiento, así como los asociados con los activos intangibles, por lo tanto la creación de valor debe ser expresada usando medidas cualitativas y no cuantitativas.

Principio 2: La gestión del riesgo es una parte integral de todos los procesos de la organización

La gestión del riesgo no es una actividad independiente, separada de las actividades y procesos principales de la organización, sino que es parte de las responsabilidades de gestión y una parte integral de todos los procesos de la organización, incluyendo la planificación estratégica y todos los procesos de la gestión de proyectos y de cambios.

Aplicación del principio 2:

Las actividades de una organización, incluida la toma de decisiones, dan lugar a riesgos. Los cambios en el contexto externo van más allá de la influencia y el control de la organización, lo que da lugar a nuevos riesgos. Todas las actividades y procesos de la organización se llevan a cabo en un ambiente interno y externo en el cual existe incertidumbre. Por consiguiente:

a) El marco de referencia para la gestión del riesgo debe realizarse integrando sus componentes al sistema de global de gestión y a la toma de decisiones de la organización, independientemente de si el sistema es formal o informal.

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

c) Si no existe un sistema de gestión formal, el marco de referencia puede servir para este propósito.

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

Los dos métodos principales de aplicación de este principio son los siguientes:

- E n el desarrollo del marco de referencia de la gestión de riesgo (incluyendo mantenimiento y mejora).
- En la aplicación del proceso de gestión del riesgo para la toma de decisiones y actividades relacionadas.

El método seguido por la organización para el establecimiento del mandato y compromiso sobre la gestión del riesgo debe ser similar a la forma en que se establecen sus otras políticas, intentando incluir

los componentes del marco de referencia de gestión del riesgo en los componentes de sistemas de gestión ya existentes en la organización.

Los auditores internos y externos, pueden desempeñar un papel importante al cuestionar cómo la dirección ha llegado a una decisión, y comprobar si esto influye en una aplicación adecuada de los procesos de gestión de riesgo.

Principio 3: La gestión del riesgo es parte de la toma de decisiones

La gestión del riesgo ayuda a las personas que toman decisiones a realizar decisiones justificadas, a definir las prioridades de las acciones y a distinguir entre planes de acción diferentes.

Aplicación del principio 3:

Este principio establece que la gestión del riesgo proporciona la base para la toma de decisiones. La gestión del riesgo debe integrarse en las actividades para la consecución de los objetivos y el proceso de toma de decisiones, así como recoger las políticas de la organización sobre la gestión del riesgo y la forma en que se debe comunicar. El proceso de toma de decisiones debe evaluarse constantemente y, en caso necesario, proceder al tratamiento del riesgo. La toma de decisiones implica riesgos y es importante comprender los riesgos asociados en ambas situaciones.

La gestión del riesgo se debe aplicar de forma proactiva como parte de la toma de decisiones y nunca después de que la decisión se haya tomado (forma reactiva), por ejemplo:

- La toma de decisiones sobre objetivos estratégicos deber tener en cuenta los riesgos ambientales, al igual que los cambios en los recursos de la organización.
- El proceso de innovación debería tener en cuenta los riesgos humanos, sociales, de seguridad y ambientales, y tratarlos de acuerdo con las normas legales (por ejemplo, seguridad del producto). Los planes de inversión (I+D) deberían especificar las pautas de la toma de decisiones para la evaluación cuantitativa del riesgo.

Las otras partes del marco de referencia deberían tener en cuenta la forma en la que se toman las decisiones, de manera que el proceso sea eficaz y consistente en toda la toma de decisiones, por ejemplo, gestión de proyectos, valoraciones de inversiones, adquisiciones.

Los responsables de la toma de decisiones en toda la organización deben comprender la política de gestión del riesgo de la organización, y deben tener competencias para aplicar el proceso de gestión del riesgo para la toma de decisiones. Esto requerirá la asignación de responsabilidades, apoyada en la formación y en la revisión del desempeño.

Ejemplos prácticos: Con el fin de aplicar el principio, se presentan unas preguntas que deberían realizarse desde el principio del proceso:

- ¿Cómo puede ayudar a crear y proteger el valor?
- ¿Cómo y dónde se toman las decisiones en la organización?
- ¿Quién está involucrado en la toma de decisiones?
- ¿Qué conocimiento y habilidades son necesarios para que quienes toman las decisiones?
- ¿Cómo adquieren los conocimientos y habilidades necesarios quienes toman las decisiones?
- ¿Qué formación y apoyo es necesaria para el personal de la organización?
- ¿En el futuro, de qué manera se introducirá al personal a este método de toma de decisiones?
- ¿Cómo se verán afectadas las partes involucradas externas?
- ¿Qué decisiones se tendrían que cambiar dentro del proceso en la organización?
- ¿Cómo se establece el control del proceso al aplicar este principio?

Principio 4: La gestión del riesgo trata explícitamente la incertidumbre

La gestión del riesgo tiene en cuenta explícitamente la incertidumbre, su naturaleza y la forma de tratarla.

Aplicación del principio 4:

Lo que hace a la gestión del riesgo única entre otros tipos de gestión es que aborda específicamente el efecto de la incertidumbre sobre los objetivos. El riesgo solo se puede evaluar o tratar eficazmente si se conoce la naturaleza y el origen de esa incertidumbre, muy importante cuando se seleccionan tratamientos para el riesgo, y se consideran el efecto y la fiabilidad de los controles. Asimismo, habrá incertidumbre asociada con las medidas de apoyo del proceso de la gestión del riesgo, por ejemplo, si la información ha sido eficaz cuando hay comunicación o consultas con las partes involucradas, o si los intervalos seleccionados por los procesos de seguimiento son suficientes para detectar cambio.

Quienes están involucrados en la gestión del riesgo deberían tener una comprensión adecuada de la incertidumbre, y de los tipos y fuentes de incertidumbre:

- El número y tipos de métodos de evaluación del riesgo usados para abordar la incertidumbre deberían ser apropiados y pertinentes a la importancia de la decisión: se pueden justificar múltiples métodos.
- Las hipótesis recogidas en el proceso de gestión del riesgo reflejan generalmente alguna forma de incertidumbre, al igual que cualquier incertidumbre explícita que se haya considerado en los diversos pasos del proceso.

- Al evaluar el riesgo se considera la incertidumbre asociada con la estimación de las calificaciones de probabilidad y consecuencia.
- Al analizar el riesgo se proponen tratamientos. Se deberían usar análisis de sensibilidad para entender la influencia real de estas incertidumbres.

Ejemplos prácticos:

Para la aplicación de este principio deberíamos tener en cuenta:

- Respecto a quienes toman las decisiones: ¿cuáles son las hipótesis y cuáles son las incertidumbres asociadas con estas hipótesis?
- Respecto al ambiente interno y externo como parte del establecimiento del contexto: probabilidad asociada con una alta volatilidad, fuente de incertidumbre, contexto supervisado y revisado de forma continuada.
- Respecto a la incertidumbre: comunicación.

Principio 5: La gestión del riesgo es sistemática, estructurada y oportuna

Un enfoque sistemático, oportuno y estructurado de la gestión del riesgo contribuye a la eficacia y a resultados coherentes, comparables y fiables.

Aplicación del principio 5: Mediante tres enfoques:

1. Enfoque consistente: para gestionar el riesgo en el momento en que se toman decisiones, lo que creará eficiencia en una organización, y proporciona resultados que construyan confianza y éxito. Para esto se requieren prácticas organizacionales que consideren los riesgos asociados con todas las decisiones y el uso de criterios de riesgo consistentes que se relacionen con los objetivos de las organizaciones y el alcance de sus actividades.

2. Enfoque puntual: de tal forma que el proceso de gestión del riesgo se aplique en el punto óptimo del proceso de toma de decisiones, dependiendo del diseño del marco de referencia al que se aplica también este principio. Si se realizan las consideraciones de riesgo demasiado pronto o demasiado tarde, se pueden perder oportunidades o los costos de revisar la decisión pueden ser sustanciales. Las dependencias de tiempo deben ser evaluadas y entendidas para determinar el enfoque más eficaz de gestión de riesgo..

3. Enfoque estructurado: mediante la aplicación del proceso de gestión eficaz del riesgo coherente y consistente con un enfoque ascendente o descendente, con el fin de abordar el nivel apropiado de gestión del riesgo más eficaz.

Principio 6: La gestión del riesgo se basa en la mejor información disponible

Los elementos de entrada del proceso de gestión eficaz del riesgo se basan en fuentes de información tales como datos históricos, experiencia, retroalimentación de las partes interesadas, observación, previsiones y juicios de los expertos. No obstante, las personas que toman decisiones deberían informarse y tener en cuenta todas las limitaciones, los datos o modelos utilizados, así como las posibles divergencias entre los expertos.

Aplicación del principio 6:

Solo se puede comprender correctamente un riesgo si está basado en la mejor información disponible, por lo que las decisiones de la gestión del riesgo deberían incluir métodos para recoger o generar información, aunque esta puede estar limitada. Por ejemplo, prever lo que ocurrirá en el futuro puede estar limitado al uso de proyecciones estadísticas.

Se debería entender la sensibilidad de las decisiones de cualquier incertidumbre en la información. La fiabilidad de la evaluación del riesgo dependerá, en parte, de la claridad y precisión de los criterios de riesgo. La recopilación de datos relacionados con el riesgo (por ejemplo, la ocurrencia de eventos y otra información basada en la experiencia) puede ayudar a los análisis estadísticos.

Aunque el objetivo final es la toma de decisiones basada en evidencias, esto no siempre es posible con el tiempo y los recursos disponibles. En estos casos, se debería usar el juicio de expertos, en combinación con la información que está disponible.¬ Sin embargo, es necesario evitar sesgo en el grupo cuando se aplica este juicio. Además, la evidencia del pasado no puede predecir exactamente el futuro. En situaciones de eventos con impactos muy altos, la falta de información puede provocar acciones si hay evidencia de daño potencial, en lugar de una prueba definitiva de daños.

Este principio también es aplicable al diseño (o mejora) del marco de referencia de gestión del riesgo debido a que habrá aspectos del marco (por ejemplo, aquellos que proporcionan capacidad de investigación o que recopilan, analizan, actualizan y ponen a disposición información para apoyar la aplicación del proceso) que determinarán cómo se aplica este principio.

La fiabilidad y exactitud de la información deben ser evaluadas regularmente por relevancia, puntualidad y fiabilidad, mediante hipótesis documentadas. El marco de referencia debería prever la revisión periódica y la emisión de actualizaciones o correcciones.

Ejemplos prácticos:

- Cuestionarios: ¿quiénes son los usuarios finales presentes y futuros?, ¿cómo puede ser necesario

clasificar la información?, ¿cómo se puede mejorar la integridad?, y ¿cómo se puede acceder a esta información? Una vez que se ha hecho esto, se puede diseñar el cuestionario de presentación de informes, teniendo en cuenta que la calidad suministrada puede estar influenciada por el tiempo necesario para alimentarla.

- Contexto: como parte de las descripciones detalladas y documentadas de los riesgos clave enfrentados (por ejemplo, inscripción del riesgo). Esto permite a los usuarios tener en cuenta cualquier cambio en el contexto que pueda haber ocurrido posteriormente, con los cambios resultantes en el riesgo.

- Hipótesis: registrar y comprender claramente el fundamento y limitaciones de las hipótesis.

- Tratamientos del riesgo: se debería considerar cómo se hará el seguimiento del desempeño de los controles resultantes, y cómo se pondrán a disposición de las personas que tomarán las decisiones en el futuro, quienes serán responsables de estos controles.

Principio 7: La gestión del riesgo está adaptada

La gestión del riesgo se alinea con el contexto externo e interno de la organización y con el perfil del riesgo.

Aplicación del principio 7:

La ISO 31000 proporciona un enfoque genérico para la gestión del riesgo, que es aplicable a todo tipo de organizaciones y a todo tipo de riesgo. Todas las organizaciones tienen su propia cultura, características, criterios de riesgo y contextos de la operación. La gestión del riesgo se debería adaptar para satisfacer las necesidades de cada organización.

No hay una forma única y correcta de diseñar e implementar el marco de referencia y los procesos de gestión del riesgo, ya que requieren flexibilidad y adaptación en cada organización. El diseño se puede determinar por muchos aspectos, incluyendo estilo, tamaño, cultura, sector, configuración y gestión organizacional.

Diferentes áreas de riesgo pueden requerir procesos diferentes dentro de la misma organización.¬ Aunque todos los procesos deberían ser consistentes con la norma ISO 31000, habrá diferencias en los sistemas, modelos y nivel de juicio involucrado, por ejemplo, entre los involucrados en la evaluación de riesgos relacionados con la tecnología de la información, riesgos de tesorería y de inversiones, o riesgos de la competencia. Cada proceso se debería adaptar a su propósito específico.

Puesto que el propósito del marco de referencia es asegurar que el proceso de gestión del riesgo se aplique a la toma de decisiones en una manera que sea eficaz y que refleje la política, el diseño del marco de referencia debería reflejar cómo y en dónde se tomaron las decisiones, y debería tener en cuenta cualquier obligación legal u otras con la que esté comprometida la organización.

Este principio es importante durante el diseño y mejora del marco de referencia de gestión del riesgo, pero también será relevante en la forma en que los aspectos del proceso estén estructurados y la organización debe considerar cuestiones internas, por ejemplo, rotación de personal (que si es muy alta puede requerir mejoras en la formación con el fin de asegurar que los empleados nuevos sean capaces de cumplir lo que se les requiere en relación a la gestión del riesgo).

Es necesaria la adaptación del marco de referencia, para lograr la integración con los procesos de la toma de decisiones de la organización. También es posible que esos procesos de toma de decisiones necesiten modificarse o regularse para ajustarse a un marco de referencia de gestión del riesgo estructurado.

Ejemplos prácticos:

El diseño del marco de referencia de gestión del riesgo debería incluir los puntos de vista de quienes están involucrados en su implementación y deben darse a conocer los conceptos fundamentales para ayudar a asegurar que la adaptación, tanto del marco de referencia como del proceso, alcanzará los atributos de una gestión eficaz del riesgo.

Principio 8: La gestión del riesgo integra los factores humanos y culturales

La gestión del riesgo permite identificar las aptitudes, las percepciones y las intenciones de las personas externas e internas que pueden facilitar u obstruir el logro de los objetivos de la organización.

Aplicación del principio 8:

Consiste en obtener las opiniones de las partes interesadas, así como entender que esas opiniones pueden estar influenciadas por las características humanas y culturales. Los factores a considerar incluyen conceptos políticos y sociales, al igual que los conceptos de tiempo. Los tipos de error más comunes son los siguientes:

a) Falta de detección y respuesta a las alertas.
b) Indiferencia a los puntos de vista de otros, o falta de conocimiento de los mismos.
c) Sesgo debido a estrategias de procesamiento de información simplificadas para abordar temas complejos.

d) Incapacidad para reconocer la complejidad.

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

El diseño del marco de referencia y la comunicación acerca del riesgo debería tener en cuenta las características culturales y los niveles de conocimiento de los receptores.

Ejemplos prácticos:

- Los directores deberían actuar de manera que demuestren que promueven y apoyan el respeto y la comprensión de las diferencias individuales.
- Las personas aprecian que se les pregunte su punto de vista.
- Por regla general, las organizaciones recompensan lo que valoran. Si la selección, promoción y remuneración de los empleados no está vinculada abiertamente con el desempeño real de la gestión del riesgo, es improbable que este desempeño cumpla con los estándares esperados. Se deberían reconocer adecuadamente los esfuerzos individuales.
- Por regla general, no es prudente que el control dependa de una sola persona, para hacer una modificación considerable al riesgo.
- Las organizaciones transnacionales actuarán en forma sensata sí reconocen la importancia de la cultura para determinar el comportamiento de las personas.

Algunos ejemplos de preguntas útiles acerca de factores humanos y organizacionales son:

- ¿El marco de referencia de la organización es apropiado para sus necesidades?
- ¿Se han identificado claramente los individuos que deben rendir cuentas de manera formal?
- ¿Todas las descripciones de los cargos contienen especificaciones claras acerca de las autoridades y responsabilidades de los individuos?
- ¿Todos los canales de comunicación son claros y eficaces?
- ¿Ocasionalmente se verifica que las comunicaciones se entienden e interpretan correctamente a todos los niveles en la organización?
- ¿En la organización se monitorea el nivel de motivación?
- ¿Se revisan todas las interfaces entre los equipos?
- ¿Existen mecanismos para reconocer y responder a rumores dentro de la organización, antes de que causen un impacto negativo?
- ¿Existen políticas claras para contratación, remuneración y promoción?
- Si las políticas son dudosas, ¿existe un proceso para revisarlas?
- ¿Se observan políticas y procedimientos? Si no se observan, ¿se lleva a cabo una investigación?,

¿se hacen cumplir?
- ¿Los auditores internos y externos buscan en la organización comportamientos no seguros o no éticos?

Principio 9: La gestión del riesgo es transparente y participativa

La implicación apropiada y oportuna de las partes interesadas y, en particular, de las personas que toman decisiones a todos los niveles de la organización, asegura que la gestión del riesgo se mantenga pertinente y actualizada. La implicación también permite a las partes interesadas estar correctamente representadas y que sus opiniones se tengan en cuenta en la determinación de los criterios de riesgo.

Aplicación del principio 9:

Se puede aplicar a múltiples niveles y se puede reflejar en la política de gestión del riesgo de la organización (por ejemplo "Informar y consultar a las partes involucradas siempre que sea posible, con el fin de que comprendan nuestros objetivos y puedan contribuir con su conocimiento y puntos de vista a la toma de decisiones").

La consulta con las partes involucradas, como parte de la aplicación del proceso de gestión del riesgo, necesita una planificación cuidadosa para ser eficiente y fortalecer la confianza en los resultados, por lo que las partes involucradas pertinentes deberían participar en todos los aspectos del proceso de gestión del riesgo, incluido el diseño del proceso de comunicación y consulta.

La implementación de este principio debería considerar aspectos de confidencialidad, seguridad y privacidad, por ejemplo, puede requerir la limitación de accesos a alguna información en las inscripciones sobre los riesgos.

Ejemplos prácticos

- Se debería incluir el juego de roles en relación con comunicación y consulta en la formación en gestión del riesgo.
- Se debería llevar a cabo una evaluación acerca de cómo se percibe la información recibida.
- Se debería suministrar retroalimentación periódica para demostrar cómo se llevó a cabo en la práctica el desempeño prometido o proyectado.
- Los puntos de vista no solicitados se deberían estimular, reconocer y apreciar, y siempre que sea posible, se debería suministrar retroalimentación acerca de ellos.

Principio 10: La gestión del riesgo es dinámica, reiterativa y receptiva al cambio.

La gestión del riesgo es sensible de manera continuada a los cambios y responde a ellos: sucesos externos e internos, el contexto y los conocimientos cambian, se debe hacer un seguimiento y revisión de riesgos, pues surgen nuevos riesgos, algunos cambian y otros desaparecen.

Aplicación del principio 10:

Cualquier cambio en los objetivos de la organización o cualquier aspecto de las circunstancias internas oCualquier cambio en los objetivos de la organización o cualquier aspecto de las circunstancias internas o externas, inevitablemente cambiará el riesgo (por ejemplo, una reestructuración interna, un importante proveedor nuevo o un cambio en la normativa legal). Asimismo, los cambios en el contexto organizacional (por ejemplo, la adquisición de otra compañía o conseguir un nuevo contrato importante) pueden requerir cambios en el marco de referencia (por ejemplo, en formación, en especialistas de riesgos). Los procesos de gestión del riesgo deben diseñarse para reflejar la dinámica de la organización (por ejemplo, rapidez del cambio).

La ISO 31000 contiene dos regímenes de seguimiento y revisión (para el marco de referencia y para el proceso). Cada uno es específico para su propósito, y requiere reflexión e implementación.

El marco de referencia se debería supervisar y revisar para asegurar que puede continuar aplicándose a estos principios de gestión eficaz del riesgo, a la política de gestión del riesgo de la organización, y a apoyar la aplicación del proceso de toma de decisiones en toda la organización. La supervisión y la revisión se deberían incorporar a cada uno de los pasos fundamentales en el proceso de gestión del riesgo. Por ejemplo, los controles manuales no serían tan eficaces si hay cambios en el personal de la organización.

La supervisión y la revisión se deberían adaptar cuidadosamente, de manera que sean sensibles a los factores de cambio que pueden tener los mayores efectos, deberían evaluar la importancia continua de los indicadores supervisados, y si es necesario, los indicadores se adaptarán a los cambios o a las nuevas circunstancias.

La supervisión está relacionada con la observación continua de los parámetros clave para determinar si se siguen en la forma prevista o supuesta. Si la revisión ocurre de vez en cuando, se estructura en cuanto a su propósito, y generalmente se prevé para determinar si las hipótesis en base en las cuales se tomaron las decisiones (por ejemplo, el diseño del marco de referencia) permanecen vigentes, y por tanto si es necesario revisar las decisiones resultantes. La revisión también debería tener en cuenta los nuevos conocimientos y tecnologías.

Ejemplos prácticos:

- Cuando se aplica el proceso de gestión del riesgo y se desarrolla la declaración del contexto, se deberían identificar los componentes (por ejemplo, las características del entorno externo) que tienen más posibilidad de cambiar, y se deberían supervisar de cerca para determinar los cambios. Cualquier cambio podría requerir la reevaluación de todos o de algunos riesgos documentados.
- Se debería motivar a las personas a que reporten sus inquietudes acerca del estado de la situación actual (incluidas las reclamaciones internas).
- Incluso las organizaciones pequeñas deberían tener en mente cambios globales, ya que los eventos externos o circunstancias emergentes pueden requerir cambios proactivos al marco de referencia de gestión del riesgo.

Principio 11: La gestión del riesgo facilita la mejora continua de la organización

Las organizaciones deberían desarrollar e implementar estrategias para mejorar su madurez en la gestión del riesgo y en todos los demás aspectos de la organización.

Aplicación del principio 11:

La mejora continua del desempeño organizacional está interrelacionada con la mejora continua del desempeño de la gestión del riesgo. La mejora continua del riesgo, fundamentada en la toma de decisiones basadas en el mismo, puede reducir la incertidumbre en el logro de los objetivos, minimizar la volatilidad e incrementar la agilidad. Sin embargo, es conveniente no manipular excesivamente el riesgo de gestión, hasta el punto de reprimir la búsqueda de oportunidades y la flexibilidad de la respuesta. El objetivo central de este principio es que las organizaciones permanezcan alerta a nuevas oportunidades de mejora. Estas oportunidades pueden surgir internamente (por ejemplo, del aprendizaje de incidentes reportados) o externamente (por ejemplo, por la disponibilidad de nuevas herramientas y conocimientos que pueden mejorar la gestión del riesgo).

Este principio también es relevante para buscar continuamente mejoras en la eficiencia de la gestión del riesgo, por ejemplo, implementar nuevas tecnologías que conecten mejor la información con quienes toman las decisiones.

El objetivo de la mejora continua debería estar claro en la política de gestión del riesgo de la organización y se debería comunicar continuamente de manera formal e informal. La mejora continua puede incluir lo siguiente:

- Mejorar el grado de integración de la actividad de gestión del riesgo a la actividad general.
- Mejorar la calidad de las evaluaciones del riesgo.

- Mejorar el marco de referencia, por ejemplo, la calidad y el acceso a la información.
- Mejorar la rapidez en la toma de decisiones.

La mejora continua se basa en indicadores cualitativos y cuantitativos del progreso. Las organizaciones que usan modelos de madurez y enfoques por fases deberían diseñar estos como impulsores de la mejora continua basada en los recursos y cultura de la organización. El propósito de la gestión eficaz del riesgo se encuentra únicamente en incrementar la probabilidad de que una organización alcance sus objetivos en su totalidad. Cuanto más rápidamente la organización pueda llevar a cabo una gestión eficaz del riesgo, más eficientes serán sus objetivos. En términos prácticos, algunas mejoras pueden tomar tiempo para lograr, por ejemplo, la asignación de un presupuesto o una planificación y el lanzamiento al mercado. Los planes de mejora deberían considerar las prioridades y beneficios relativos, y deberían permitir el seguimiento del progreso.

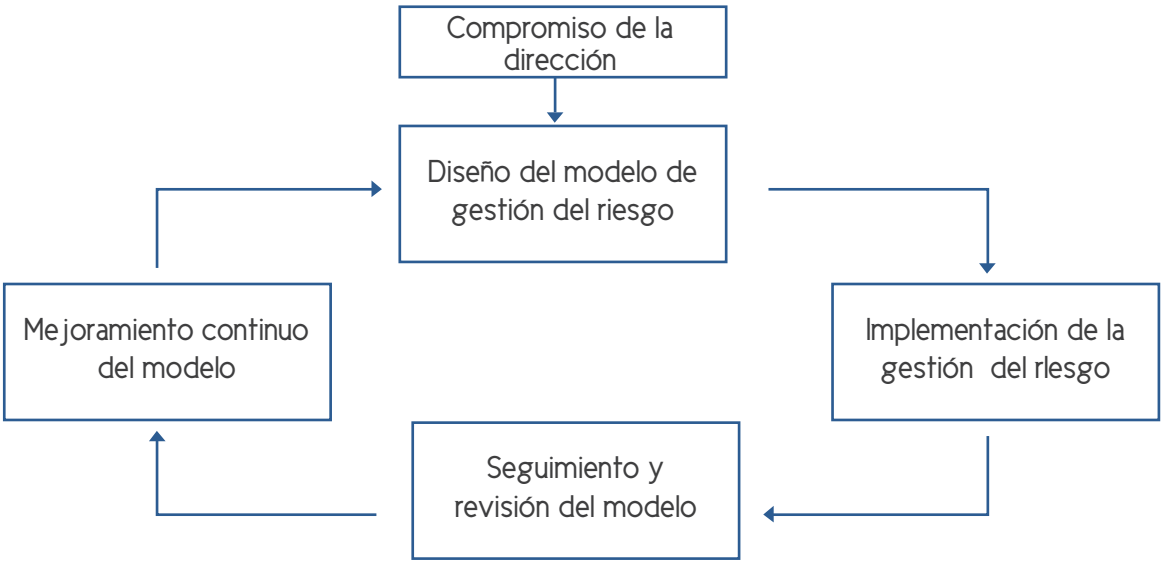
Ejemplos prácticos:

- Usando los elementos de supervisión y de revisión del marco de referencia, se debería llevar a cabo una revisión anual del desempeño con base en estas mejoras del diseño y principios de gestión del riesgo.
- La adecuación, idoneidad y eficiencia del marco de referencia de gestión del riesgo se deberían revisar y evaluar.
- El sistema de reporte de incidencias se debería usar para llevar a cabo el análisis de causa raíz, considerando no solamente las causas probables del incidente, sino también las características del marco de referencia de gestión del riesgo que hicieron posible que el incidente ocurriera.
- El éxito (por ejemplo, un proyecto a tiempo/dentro del presupuesto) se debería supervisar para comprender qué características del marco de referencia de gestión del riesgo facilitaron principalmente el éxito, y esto se debería comunicar para reforzar el valor.

2.4 El marco de trabajo para la gestión de riesgo

La selección del marco requiere una gestión por mandato y compromiso, describir el diseño del marco, proporcionar una guía de implementación, monitorear y revisar, así como la mejora continua del marco. El marco de trabajo tiene como objetivo estructurar las actividades para la implementación y mejora continua del proceso de gestión de riesgos. Las normas Internacionales recomiendan que las organizaciones, desarrollen, implementen y mejoren continuamente un marco de trabajo o estructura de soporte (framework) cuyo objetivo es integrar el proceso de gestión de riesgos en el gobierno corporativo de la organización, planificación y estrategia, procesos de información, políticas, valores y cultura.

Gráfico 03: Marco de la gestión de riesgo



Fuente: UNE-ISO 31000 (2009): Gestión del riesgo. Principios y directrices

El análisis de la investigación se basa en la estructuración de las actividades para la implementación y mejora continua del proceso de gestión de riesgos.

- Compromiso de la dirección:
  - La existencia de un compromiso firme y mantenido por la dirección de la organización, además de una planificación estratégica y rigurosa para lograr el compromiso de todos los niveles organizacionales.

- Diseño del modelo de gestión del riesgo:
  - Contextualización de la organización y el establecimiento de la política de gestión de riesgos.
  - Rendición de cuentas y recursos e integración en los procesos de la organización y establecimiento de la comunicación interna y externa, y mecanismos de información.

- Mejoramiento continuo del modelo
  - Establecimiento de una política y modelo de mejora continua, y plan de tratamiento de riesgos.

- Implementación de la gestión del riesgo
  - Implementación de un marco de Gestión de Riesgos e implementar el proceso de Gestión

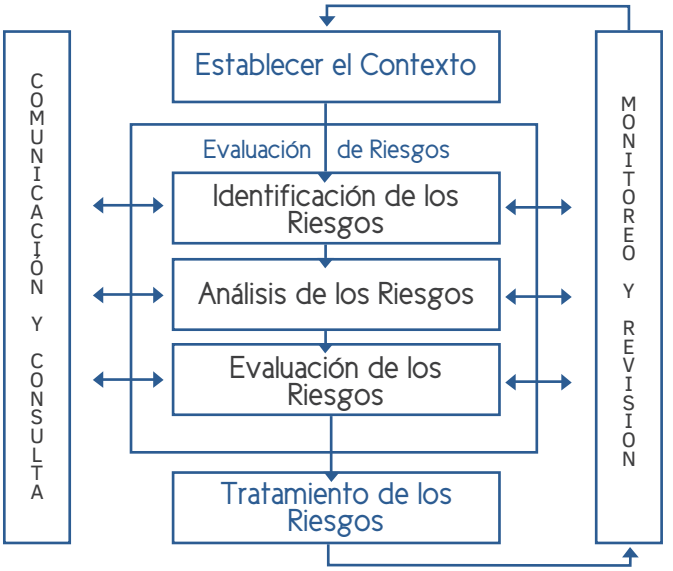
de Riesgos.

- Seguimiento y revisión del modelo
  - Uso de indicadores de evaluación para revisar las desviaciones y reportar efectividad del modelo.

2.5 El proceso de gestión del riesgo

El proceso de gestión de riesgo debería ser una parte integral de la gestión y estar adaptado al proceso de negocio de la organización, recogiendo la cultura y prácticas. Esto incluye los 5 componentes de establecimiento del contexto: evaluación de riesgo con la identificación, análisis y evaluación cualitativa y cuantitativa de los riesgos; el tratamiento del riesgo para la toma de decisiones; la comunicación y consulta; el monitoreo y revisión.

Gráfico 04: Actividades del proceso de gestión de riesgos



Fuente: UNE-ISO 31000 (2009): Gestión del riesgo. Principios y directrices.

- Establecimiento del contexto
  - Generar metas, objetivos y responsabilidades del proceso
  - Definir actividades, procesos y su respectivo alcance
  - Reconocer la relación con otros posibles proyectos
  - Determinar la metodología de valoración riesgo
  - Establecer criterios de decisiones y reconocer los estudios necesarios

- Contexto externo
  - Ambiente social y cultural
  - Ambiente político
  - Ambiente legal y reglamentario
  - Ambiente económico y financiero
  - Ambiente tecnológico
  - Relaciones con los grupos de interés (stakeholders) externos
  - Otros grupos que tengan impacto en los objetivos de la organización

- Contexto interno
  - Estructura de la organización, funciones y responsabilidades
  - Políticas, objetivos y estrategias implementadas para alcanzarlos
  - Capacidad y conocimientos de los recursos humanos
  - Relaciones con los grupos de interés o stakeholders internos
  - Otros grupos que tengan impacto en los objetivos de la organización

- Evaluación de riesgos
  - Identificar el riesgos y sus fuentes.
  - Reconocer las áreas de impactos
  - Determinar las causas y consecuencias de eventos no favorables.

- Análisis de riesgos

  Su realización se puede dar con diversos grados de detalle dependiendo de varios factores como el riesgo, propósito del análisis e información, datos y recursos disponibles.

  Puede ser cualitativo, semi-cuantitativo, cuantitativo o una combinación de los tres anteriores. Las consecuencias y posibilidad del riesgo se determinaran con los resultados del modelamiento del análisis, y estos pueden tener impactos tangibles e intangibles.

- Evaluación de Riesgos

  El propósito principal es facilitar la toma de decisiones basada en los resultados del análisis para determinar qué riesgos necesitan tratamiento y prioridad.

  Puede tener como resultado la decisión de no tratar el riesgo de ninguna manera distinta a los controles ya existentes. Las decisiones se toman de acuerdo a la legalidad, los reglamentos y otros.

- Tratamiento de riesgos

  Opciones:

  - Evitar el riesgo, si fuera posible, decidiendo no iniciar o continuar con la actividad que lo originó.
  - En caso de una oportunidad, tomar el riesgo o incrementarlo
  - Retirar la fuente del riesgo
  - Cambiar la probabilidad transfiriéndolo o mitigándolo
  - Cambiar las consecuencias
  - Compartir el riesgo
  - Retener el riesgo, tomando en cuenta la información que tenemos

- Comunicación y consulta
  - Comunicación y consulta con las partes involucradas en todas las etapas del proceso
  - Identificación de procesos y partes involucradas

- Monitoreo y revisión

  Comprende todos aspectos de la gestión de riesgos para:

  - Garantizar controles eficaces y eficientes, mediante el monitoreo del desempeño y obtener información adicional que mejore la valoración del riesgo
  - Analizar eventos, cambios, tendencias, éxitos y fracasos, y canalizar lo mejor de estos a la organización
  - Reconocer cambios en el contexto, tanto externo como interno, para determinar la revisión de los tratamientos del riesgo y su priorización
  - Identificar nuevos riesgos emergentes

Capítulo III:
Metodología Aplicada

3.1 Metodología aplicada[5]

El presente capítulo busca, entre otras cosas, dar una idea sólida acerca de los requerimientos exigidos en normativas legales a una organización, para implementar y desarrollar el sistema de evaluación y gestión de riesgos. Es importante mencionar que ningún sistema de control interno logra establecer niveles de seguridad absolutos en el desenvolvimineto de las operaciones, pues pueden existir diversas limitaciones intrínsicas a los procesos de control interno de dicha organización.

El sistema de control interno debe ser estructurado de tal forma que facilite a las organizaciones:

- Mejorar su gestión en toda circunstancia
- Cumplir con su plan de negocio y/o servicio de manera eficiente
- Evaluar anticipidamente los potenciales efectos adversos, ya sea, derivados de factores internos como externos
- Crear un valor agregado para la organización

Un fundamento de lo mencionado anteriormente tiene como base los avances de la Norma ISO 31000: 2009[4] y el marco COSO II[6] y ahora COSO III[7]. En consecuencia, se analizan tanto los principios como las directrices sobre la gestión eficaz de los riesgos que puedan ser implementados por las entidades aseguradoras dentro de las Normas de Buen Gobierno Coorporativo, las cuales son exigidas por el establecimiento de una gerencia de riesgos, y que a la vez, permiten la toma de desiciones en éste ámbito.

Este capítulo recoge la aplicación de la gestión eficaz de los riesgos para implementar y desarrolloar el sistema de evaluación y gestión integral de los riesgos de una organización que permita, a la dirección de la empresa, entender los riesgos y adoptar las medidas necesarias para identificarlos y mitigarlos a través de un sistema de control interno acorde a la naturaleza, complejidad y riesgos inherentes a las actividades desarrolladas.

Asimismo, busca servir de guía para la implementación de los procedimientos básicos de control que una organización debe establecer para el desarrollo de sus actividades en el marco del ordenamiento jurídico, y sentar las bases para la elaboración de mapas de riesgo que permitan evaluar los riesgos potenciales de la empresa por tipo de negocio, además de no perder la posición financiera conseguida, a la luz de la regulación legal presente y futura.

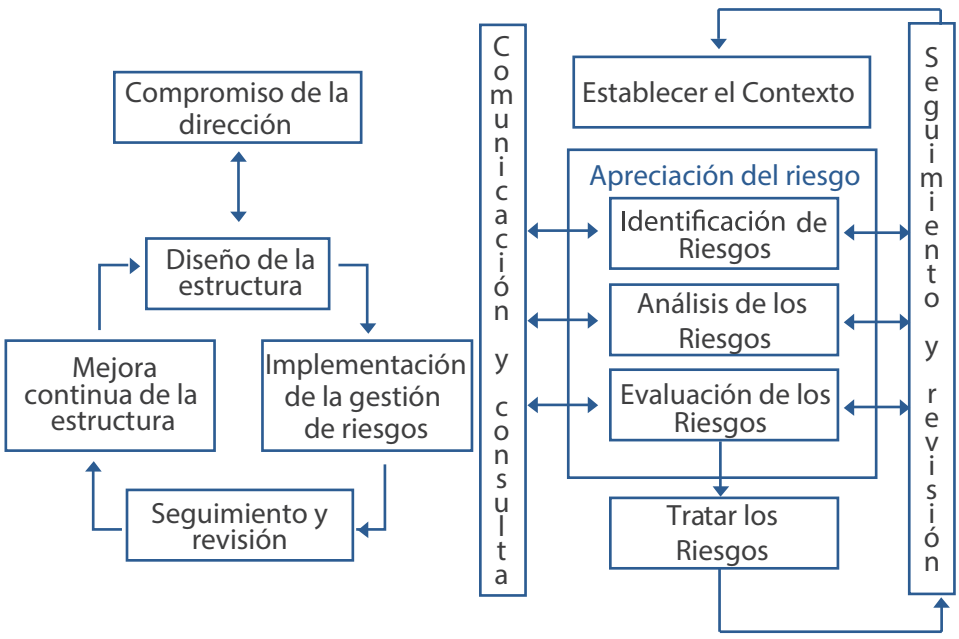
Para el desarrollo del proceso se mostrará las relaciones entre los principios de la gestión de riesgos, la estructura organizacional y el proceso que reúne la norma ISO 31000. La apreciación del riesgo está conformada por cuatro etapas: Identificar los riesgos, analizar los riesgos, evaluar los riesgos y tratar los riesgos.

[5] Casares San José-Martí, Isabel (2014): Implementación de la Gestión Integral de Riesgos en el Sector Asegurador bajo la Norma ISO 31000.
[6] UNE-ISO 31000:2010 Gestión del riesgo: Principios y directrices. Traducido por AENOR (Asociación Española de Normalización y Certificación). Julio 2010
[7] COSO II (2004): Gestión de Riesgos Corporativos-Macro Integrado: Técnicas de Aplicación Committee of Sponsoring Organizations of Treadway Commission, Septiembre. Asimismo COSO ha sido actualizado en el 2013.

Lo mencionado se implementa con una buena comunicación dentro de la organización junto con el seguimiento y revisión detallada de cada riesgos, así mismo como el compromiso y soporte de la supervisión continua del riesgo.

Gráfico 05: Principios y directrices de la gestión de riesgos

a) Crea valor.
b) Está integrada en los procesos de la organización.
c) Forma parte de la toma de decisiones.
d) Trata explícitamente la incertidumbre.
e) Es sistemática, estructurada y adecuada.
f) Está basada en la mejor información disponible.
g) Está hecha a la medida.
h) Tiene en cuenta a factores humanos y culturales.
i) Es transparente e inclusiva.
j) Es dinámica, iterativa y sensible al cambio.
k) Facilita la mejora continua de la organización.



Fuente: UNE-ISO 31000 (2009): Gestión del riesgo. Principios y directrices.

La metodología a aplicar en el proceso de implementación de riesgos contempla un extenso abanico de procedimientos de control, cuyo objetivo esencial es que sean empleados como una guía de consulta y referencia para la dirección de la empresa, el comité de administración integral de riesgos y/o de la unidad de riesgos, con el fin de:

- Establecer un desarrollo de los sistemas de control interno, en el que sea considerado el marco legal existente y la situación actual de la empresa.
- Establecer, por áreas de la empresa, una metodología práctica a seguir con las técnicas de

control.

- Proponer a los responsables de control de riesgos de la empresa: formatos, cuestionarios y calendarios de aplicación, los cuales permitirán su aplicación a la realidad diaria.

En este sentido, en el presente, nos hemos centrado en sentar las bases que permitan realizar en el futuro una gestión eficiente de los riesgos que pueden amenazar a la organización. Ello es posible a través de mapas de riesgos que la misma organización debería implementar a medio plazo, con el fin de garantizar sus objetivos estratégicos.

Así mismo, es importante mencionar la gestión estratégica con el fin de poder generar un rol importante en la gestión de riesgo mediante la responsabilidad y la supervisión, además del manejo, decisión y control operacional de toda una organización, como se ve en el gráfico 6.

Las actividades del gobierno corporativo están representadas como cuatro principales componentes: dirección, acción ejecutiva, supervisión y responsabilidad. La necesidad de la gestión de riesgo a emprender en el nivel estratégico de una organización es resaltada

Gráfico 06: Gestión estratégica

Fuente: UNE-ISO 31000 (2009): Gestión del riesgo. Principios y directrices.

¿Cuáles son los objetivos del sistema de evaluación y gestión de riesgos?:

Los principales objetivos del sistema de evaluación y gestión de riesgos son:

1. Analizar y enfrentar el riesgo en forma sistemática y permanente. Para ello, se identifican los

factores de riesgo y su exposición, y se cuantifica el posible efecto en la solvencia.

2. Anticipar posibles situaciones que afecten la viabilidad de la entidad, disminuyendo su probabilidad de solvencia.

3. Implementar políticas de responsabilidad de riesgos.

4. Proveer información para la toma de decisiones, que permita a la organización reaccionar a cambios del entorno en que se desarrollan los negocios, de manera rápida y eficiente.

5. Reducir el abanico de los resultados. En la normativa actual, no hay un desarrollo específico que sea considerado para determinar qué se entiende por control interno adecuado, lo que retrasa su puesta en marcha y crea inseguridad jurídica.

Este libro se ha diseñado con el objetivo de sentar las bases que permitan realizar los siguientes pasos en el proceso:

- Implementación y puesta en marcha de los controles y herramientas básicas por parte de la dirección de la empresa, el comité de administración de riesgos, unidad de riesgos y/o asesores externos.

- Revisión y validación del correcto funcionamiento de los controles básicos implementados por parte de la dirección de la empresa.

- Identificación del entorno de control actual y su consistencia con los objeticos estratégicos de la empresa.

- Descripción de los los procesos y procedimientos del negocio segun las principales actividades que realiza la empresa (relativos a sus informes financieros, división y segmento de negocio).

- Establecimiento de los criterios de materialidad e importancia del riesgo de todas las áreas de negocio y procesos de la entidad.

- Reconocimiento de las unidades de control o de negocio clave y los sistemas de información y recursos asociados a las mismas, lo cual se realizará por un análisis de mapa de riesgos (en relación a las estrategias y factores externos).

Todo lo mencionado debe estar de la mano con la gestión de riesgo, gestión integral de riesgos o también llamado *Risk Management*, A continuación se detalla la normativa sobre gestión de riesgos presentada por cada sector al que se aplica:

1. Documentos multisectoriales
   - Terminología: ISO IEC Guide 73
   - Requisitos: BS 8800
   - Directrices: OHSAS 18001

2. Sector Industrial
   - Terminología: ISO 12100-1
   - Requisitos: ISO 14121-2(2012)

3. Sector transporte
   - Requisitos: Procedimientos de EURO CONTROL
   - Directrices: ISO 17666

4. Sector Salud
   - Requisitos: ISO 14971
   - Directrices: EN 1441

5. Sector Tecnología
   - Requisitos: ISO/IEC 17799
   - Directrices: ISO/IEC 15408-1

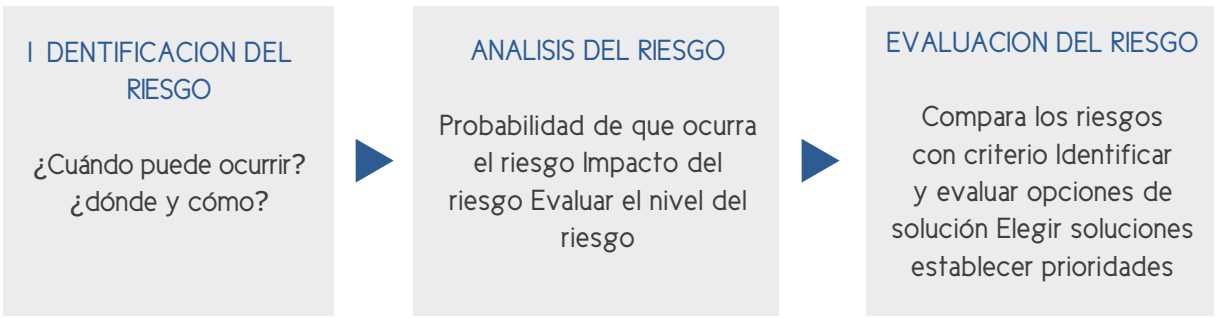
6. Sector Energía
   - Requisitos: ISO 17776
   - Directrices: ENV 14459

7. Sector Eléctrico
   - Requisitos: Principios ATEX
   - Directrices: IEC 62198, IEC 61508-2

8. Medio Ambiente
   - Requisitos: Directiva de la IPPC, ISO 14001,
   - Directrices: UNE 150008

El gráfico 07 muestra el flujo que deben seguir las empresas para implementar una gestión integral de riesgos.

Gráfico 07: Proceso del GIR



Fuente: Elaboración propia

Capítulo IV:

Estructura del Sistema y Área de Riesgos

4.1 Introducción a la estructura general del sistema

La creación de una estructura organizacional resulta importante para determinar las jerarquías necesarias y agrupación de actividades, con el fin de simplificar las mismas y sus funciones dentro de la organización.

Esencialmente, la organización nació de la necesidad humana de cooperar. Los hombres se han visto obligados a cooperar para obtener sus fines personales, por razón de sus limitaciones físicas, biológicas, sicológicas y sociales. En la mayor parte de los casos, esta cooperación puede ser más productiva o menos costosa si se dispone de una estructura de organización.

Personas, dentro de la organización, que deseen cooperar entre sí, trabajarán mucho más efectivamente si todos conocen el papel que deben cumplir y la forma en que sus funciones se relacionan unas con otras.

Este es un principio general, válido tanto en la administración de empresas como en cualquier institución. Así, una estructura de organización debe estar diseñada de manera tal que sea perfectamente claro para todos quien debe realizar determinada tarea y quien es responsable por determinados resultados; en esta forma se eliminan las dificultades que ocasiona la imprecisión en la asignación de responsabilidades y se logra un sistema de comunicación y de toma de decisiones que refleja y promueve los objetivos de la empresa.

Luis Cañas (2009) menciona que:

> La gestión de los riesgos implica cambios en la toma de decisiones, en la forma de gerenciar o gestionar, en la eliminación de ciertos paradigmas y creación de la cultura de gestión de riesgos, en todos los niveles de la entidad, iniciando en la alta dirección alcanzando hasta el último nivel de la entidad. Asimismo, gestionar los riesgos requiere del establecimiento formal de un proceso que permita de forma clara, técnica y sencilla la evaluación y análisis de los riesgos.

4.2 Conformación del comité de administración integral de riesgos

Un comité de administración integral de riesgos, está compuesto, al menos por:

- Presidente: Un vocal del directorio o del organismo que haga sus veces.
- Responsable: El máximo representante legal de la institución de que se trate.
- Gerente de riesgos: El empleado responsable de la unidad de riesgos.

El comité de administración de riesgos deberá contar con la participación de especialistas de cada uno de los riesgos, si los hubiere. Ninguno de estos miembros tendrá derecho a voto. Las designaciones y las sustituciones en la nómina de los miembros del comité deberán ser conocidas y aprobadas por el directorio o consejo de administración, lo cual debe quedar consignado en las respectivas actas.

Es importante señalar que la Superintendencia de Banca, Seguros y AFP del Perú en el 2015 trabajó un proyecto de cambio de reglamento de gobierno corporativo y la gestión integral de riesgos, que debe implementarse en el 2016, lo mismo fue trabajado por la superintendencia del mercado de valores. A continuación se toma la información de los reglamentos publicados por ambas entidades.

Entre las funciones que debe desarrollar el comité de administración integral de riesgos están las siguientes[8]:

- Diseñar y proponer estrategias, políticas, procesos y procedimientos de administración integral de riesgos o reformas, y, someterlos a la aprobación del directorio.
- Asegurase de la correcta ejecución tanto de la estrategia, como de la implantación de políticas, metodologías, procesos y procedimientos de la administración integral de riesgos.
- Proponer al directorio los límites específicos apropiados por exposición de cada riesgo.
- Informar oportunamente al Directorio respecto de la efectividad, aplicabilidad y conocimiento por parte del personal de la institución, de las estrategias, políticas, procesos y procedimiento fijados.
- Conocer en detalle las exposiciones de los riesgos asumidos en términos de afectación al patrimonio técnico y con relación a los límites establecidos para cada riego.
- Aprobar, cuando sea pertinente, los excesos temporales de los límites, tomar acción inmediata para controlar dichos excesos e informar inmediatamente tales asuntos al directorio u organismo que haga sus veces.
- Proponer al directorio u organismo que haga sus veces la expedición de metodologías, procesos, manuales de funciones y procedimientos para la administración integral de riesgos.
- Aprobar los sistemas de información gerencial, conocer los reportes de posiciones para cada riesgo y el cumplimiento de límites fijados, y adoptar las acciones correctivas según corresponda.
- Analizar y aprobar los planes de contingencia.
- Remitir al directorio u organismo que haga sus veces para su aprobación, la matriz de riesgo institucional.
- Informar oportunamente al directorio u organismo que haga sus veces, sobre la evolución de los niveles de exposición de cada uno de los riesgos de identificados.

[8] Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones (2014) Resolución S.B.S. N° 6253-2014

- Remitir al directorio u organismo que haga sus veces para su aprobación, los planes de continuidad de negocio.
- Poner en conocimiento del directorio, cambios repentinos en el entorno económico que genere un aumento en la exposición a alguno de los riesgos, o por cualquier asunto que en criterio del comité de administración integral de riesgos sea necesario tratar en dicho cuerpo colegiado.
- Aceptar las normas del directorio o de la Superintendencia de Bancos y Seguros."

Es importante señalar que diversos reguladores internacionacionales han desarrollado diversas definiciones con la finalidad de estandarizar los conceptos de riesgos y la gestión de los mismos, destacando[9]:

- Apetito por el riesgo
  El nivel de riesgo que una empresa está dispuesta a asumir dentro de su capacidad de gestión de riesgos, para alcanzar sus objetivos. Este es definido por la alta dirección tomando como base a los accionistas.

- Capacidad de riesgo
  El nivel máximo de riesgo que una empresa puede asumir sin incurrir en incumplimientos regulatorios o con sus acreedores y grupos de interés.

- Conflicto de interés
  Toda situación en la que una persona o un grupo de interés se enfrenta a distintas alternativas de conducta con intereses incompatibles entre sí debido, entre otras causas, a la falta de alineamiento entre sus intereses y los de la empresa u otros grupos de interés.

- Control interno
  Proceso realizado por el directorio, la gerencia y el personal, diseñado para proveer un aseguramiento razonable en el logro de objetivos referidos a la eficacia y eficiencia de las operaciones, confiabilidad de la información financiera, y cumplimiento de las leyes aplicables y regulaciones.

- Gobierno corporativo
  Conjunto de procesos, políticas, normas y procedimientos que determinan cómo una empresa o un grupo es dirigido, gestionado y controlado. Asimismo, la estructura del gobierno corporativo especifica la distribución de los derechos y responsabilidades entre los diferentes órganos de gobierno y grupos de interés. El gobierno corporativo también provee la estructura a través de la cual se establecen los objetivos de la empresa, los medios para alcanzar estos objetivos, así como la forma de hacer un seguimiento de su desempeño.

[9] Superintendencia del Mercado de Valores (2015). Resolución SMV Nº 037-2015-SMV/01

- **Grupo de interés**
  Persona, conjunto de personas, empresas o entidades organizadas que son afectadas (positiva o negativamente) por las actividades o la marcha de la organización. Asimismo, se considera si estos grupos pueden afectar las operaciones de la empresa.

- **Impacto**
  Consecuencias de un evento (en costo, tiempo, alcance, calidad, etcétera), expresado ya sea en términos cualitativos o cuantitativos. Usualmente se expresará en términos monetarios, como pérdidas financieras. Es un componente para calcular la severidad, el otro es la probabilidad, es decir la severidad es igual a la multiplicación de la probabilidad de ocurrencia con el impacto.

- **Manuales de gestión de riesgos**
  Documentos que contienen las funciones, responsabilidades, políticas, metodologías y procedimientos dispuestos para la identificación, evaluación, tratamiento, control, reporte y monitoreo de los riesgos de las empresas.

- **Manuales de organización y funciones**
  Documentos que detallan la estructura orgánica de las empresas, los objetivos y funciones de sus unidades, así como las obligaciones y responsabilidades de su personal.

- **Manuales de políticas y procedimientos**
  Documentos que contienen funciones, responsabilidades, políticas, metodologías y procedimientos establecidos por las empresas para la realización de las actividades de cada una de las unidades con las que cuenta, incluyendo las que corresponden a la gestión de riesgos.

- **Riesgo**
  La posibilidad de ocurrencia de eventos que impacten negativamente sobre los objetivos (cumplimiento de los mismos) de la empresa o su situación financiera.

- **Sistema de apetito por el riesgo**
  Conjunto de políticas, límites, procesos, procedimientos, roles y responsabilidades mediante los cuales el apetito por el riesgo es establecido, comunicado y vigilado.

4.3 Conformación de los especialistas de riesgos

El responsable último del establecimiento, de la actualización permanente y del control de riesgos es el consejo de administración o directorio de la organización, a pesar que dichos controles cuenten con diferentes niveles. Asimismo, el consejo debe presentar los informes estadísticos contables y los relacionados al control interno y gestión de riesgos.

El comité y la unidad de riesgos de la entidad responsable de la gestión de riesgos no deben tener relación con las funciones y áreas de gestión de la entidad (comercial y operativa). No obstante, el representante legal de la institución (o presidente ejecutivo) forma parte del comité de administración Integral de riesgos.

A continuación se muestra el modelo de funciones del comité de administración de riesgos:

- Proponer las políticas y la organización para la gestión integral de riesgos acorde a la naturaleza, tamaño y complejidad de las operaciones y servicios de la empresa.
- Proponer los límites de riesgo que la empresa está dispuesta a asumir en el desarrollo del negocio.
- Decidir las acciones necesarias para la implementación de las medidas correctivas requeridas, en caso existan desviaciones con respecto a los niveles de apetito, límites de riesgo y grados de exposición asumidos.
- Aprobar la toma de exposiciones que involucren variaciones significativas en el perfil de riesgo de la empresa o de los patrimonios administrados bajo responsabilidad de la empresa.
- Evaluar la suficiencia de capital y liquidez de la empresa para enfrentar sus riesgos y alertar de las posibles insuficiencias.
- Proponer mejoras en la gestión integral de riesgos.
- Informar a la gerencia y al directorio de los riesgos asociados a nuevos productos y cambios importantes en el ambiente de negocios, operativo o informático, de forma previa a su lanzamiento o ejecución, así como de las medidas de tratamiento propuestas o implementadas.

Funciones del comité de auditoría

El comité de auditoría tiene como propósito principal vigilar que los procesos contables y de reporte financiero sean apropiados, así como evaluar las actividades realizadas por los auditores internos y externos. Entre sus principales funciones están:

- Vigilar el adecuado funcionamiento del control interno.
- Informar al directorio sobre la existencia de limitaciones en la confiabilidad de los procesos contables y financieros.
- Vigilar y mantener informado al directorio sobre el cumplimiento de las políticas y procedimientos

internos y sobre la detección de problemas de control y administración interna, así como de las medidas correctivas implementadas en función de las evaluaciones realizadas por la unidad de auditoría interna, los auditores externos y de la Superintendencia.

- Definir los criterios para la selección y contratación de los auditores externos, evaluar su desempeño, así como determinar los informes complementarios que requieran para el mejor desempeño de sus funciones o el cumplimiento de requisitos legales, salvo en aquellos casos en los que el comité de auditoría de la casa matriz sea quien defina los criterios para la selección, contratación y evaluación de los auditores externos.
- Definir los criterios para la selección y contratación del auditor interno y de sus principales colaboradores, y evaluar su desempeño.
- Finalmente se debe precisar la estructura de control y el manual de implementación que debe presentar el especialista.

Las empresas deben identificar los grupos de interés que inciden en su gestión, organización o actividad, considerando principalmente aquellos que, de forma voluntaria o involuntaria, generan un impacto significativo en el cumplimiento de los objetivos de la empresa. Las empresas deben desarrollar políticas que tengan por objeto:

- Evaluar el impacto potencial que las actividades que realizan los grupos de interés pueden generar en la empresa y, en caso corresponda, establecer las medidas de mitigación necesarias.
- Desarrollar e implementar políticas que establezcan los principales lineamientos para la gestión y/o aprobación de operaciones con partes vinculadas.[10]

[10] El punto 4.2. tiene como fuente las normas de las siguientes superintendencias:
- Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones (2014) Resolución S.B.S. N° 6253-2014
- Superintendencia del Mercado de Valores (2015). Resolución SMV N° 037-2015-SMV/01

Gráfico 08: Estructura de control y manual de implementación

ESTRUCTURA DE CONTROL		MANUAL DE IMPLEMENTACIÓN
Componentes corporativos	Componentes	Estándares
De control estratégico	Ambientes de control	Acuerdos y compromisos éticos
		Desarrollo del talento humano
		Protocolos del buen gobierno
	Direccionamiento estratégico	Planes y programas
		Modelo de gestión de procesos
		Estructura organizacional
	Administración de riesgos	Contexto estratégico del riesgo
		Identificación de riesgos
		Análisis de riesgos
		Valoración de riesgos
		Políticas de administración de riesgos
De control de gestión	Actividades de control	Políticas de operación
		Procedimientos
		Controles
		Indicadores
		Manual de Operación
	Información	Información interna
		Información externa
		Sistema de Información
	Comunicación	Comunicación institucional
		Comunicación pública
		Rendición de cuentas
De control evaluación	Autoevaluación	Autoevaluación de control
		Autoevaluación de gestión
	Evaluación independiente	Evaluación de control interno
		Auditoría interna
	Planes de mejoramiento	Plan de mejoramiento institucional
		Plan de mejoramiento funcional
		Plan de mejoramiento individual

Fuente: Elaboración propia

Capítulo V:

Proceso de Gestión de Riesgos

5.1 Proceso de gestión del riesgo

El "proceso de gestión de riesgos" es uno de los tres pilares básicos de la Norma ISO 31000. Es precisamente este pilar el que consideramos más importante al ser el que realmente permite gestionar los riesgos cuando estos se materializan en el contexto de la empresa. Sin embargo, y aunque no sea objeto de este trabajo, no debemos olvidar que este último pilar debe estar precedido y apoyado en los dos primeros si se quiere que el conjunto de la gerencia de riesgos sea eficaz para el logro de los objetivos de la empresa.

Una organización debe integrar en los niveles estratégico y táctico la gestión de riesgos. Es parte fundamental de una gestión eficiente el considerar de forma integrada todos los factores que pueden afectar las operaciones, actividades y resultados de la empresa. El marco de la gestión de riesgos proporciona una forma de abordar cómo la organización enfrenta y supera las diferentes eventualidades a las que está expuesta, como mitiga las consecuencias de aquellos factores que no puede controlar y como evita que su supervivencia se vea afectada por la presencia de éstos.

En este proceso de gestión del riesgo existen beneficios que motivan la implementación del ISO 31000 en una organización:

- Aumenta la probabilidad de lograr los objetivos que se ha trazado la organización.
- Fomenta una gestión proactiva.
- Concientiza sobre la necesidad de identificar y tratar los riesgos en toda la organización.
- Mejora la identificación de las oportunidades y amenazas.
- Ayuda a realizar las exigencias legales y reglamentarias, y además las normas internacionales.
- Mejora los informes financieros.
- Mejora la confianza de los interesados.
- Establece una base confiable para la toma de decisiones y la planificación.
- Mejora los controles.
- Asigna efectivamente los recursos para el tratamiento del riesgo.
- Mejora la eficacia y eficiencia operativa.
- Mejora la prevención de pérdidas y de manejo de incidentes.
- Mejora el aprendizaje organizacional.
- Mejora la capacidad de resistencia de la organización.

Las empresas que desean implementar la norma ISO 31000 deben considerar que va a proveerles de un conjunto de directivas y criterios para el diseño, implementación, monitoreo, evaluación, revisión y mejora de la gestión de riesgo en la organización. Esta norma permitirá que una empresa aborde de forma ordenada el análisis de los diversos riesgos a los que está expuesta, tanto riesgos financieros,

operacionales, de salud, seguridad, etcétera, para luego definir las diferentes estrategias a desarrollar para la implementación de medidas de control. Empresas pertenecientes a cualquiera de los sectores productivos pueden obtener mejoras evidentes que se traducen en una mejor capacidad de respuesta ante situaciones imprevistas, mejor esquema de control de las operaciones, mayor conciencia del personal respecto a las amenazas y oportunidades del entorno interno y externo y finalmente, mejoras en los resultados.

Por otro lado, dentro de la gestión del riesgo hay dos factores importantes, los cuales son el apetito al riesgo y el riesgo en sí (o también llamado el riesgo aceptado).

El apetito al riesgo puede ser definido como el nivel de riesgo que una empresa está dispuesta a aceptar. Esto significa que no existen valores predefinidos, puesto que cada empresa puede estar dispuesta a considerar, en diferentes etapas de su ciclo de vida y en diferentes entornos o circunstancias, distintos niveles de riesgo.

En este contexto nos movemos entre diferentes márgenes. La tolerancia al riesgo mide los niveles de desviación del apetito de riesgo que pueden ser tolerados por la empresa mientras que la capacidad de riesgo es el nivel máximo que la empresa puede tolerar. Por cierto que tanto la capacidad y la tolerancia al riesgo podrán variar dependiendo del tipo de riesgo a asumir o de las condiciones particulares de cada organización. Por ello, resulta difícil establecer un parámetro que pueda servir a las organizaciones como referencia para cada una de sus operaciones. En algunos casos una empresa puede manejar un espectro amplio de tolerancia y en otros casos puede tener una tolerancia nula hacia cierto tipo de riesgos.

El gráfico 9 presenta un esquema de la exposición al riesgo y de los conceptos de apetito, tolerancia y capacidad de riesgo.

Gráfico 09: Exposición al riesgo

Exposición	Condición
ALTA	Capacidad de Riesgo
	Tolerancia al riesgo
	Apetito al riesgo
	Tolerancia al riesgo
BAJA	Capacidad de Riesgo

La implementación del apetito al riesgo puede hacerse de arriba hacia abajo, es decir desde la alta dirección hacia los demás estamentos jerárquicos de la empresa y de abajo hacia arriba, es decir la definición desde el mínimo nivel de la organización hacia los más altos niveles jerárquicos. Generalmente

el criterio de arriba hacia abajo suele tener mayor aceptación y uso pues es la alta dirección la que establece las pautas que definirán el apetito al riesgo a considerar y que están alineadas con los objetivos estratégicos. La segunda forma ~~-de~~ abajo hacia arriba~~-~~, funcionaría mejor en organizaciones más horizontales.

Dentro del primer factor que es el apetito al riesgo, se deben tomar varias recomendaciones con el fin de poder contrarrestarlo, las cuales son:

1. Alinear con la estrategia
2. Personalizar para cada entidad
3. Alinear con las expectativas de los grupos de interés o *stakeholders*.
4. Comunicar internamente
5. Revisar continuamente
6. Adecuar análisis coste/beneficio
7. Medir adecuadamente para toma de decisiones
8. Alinear con la capacidad y la cultura de riesgo

Gráfico 10: Apetito a riesgo de una organización

Alinear con estrategia	Apetito al riesgo
Personalizar para cada entidad	
Alinear con las expectativas de los *stakeholders*	
Comunicar internamente	
Revisar continuamente	
Adecuar análisis costo/beneficio	
Medir adecuadamente para toma de decisiones	
Alinear con la capacidad y la cultura de riesgo	

Fuente: Elaboración propia

En ciertos sectores como la banca y los seguros, la medición del apetito de riesgo se ha manejado tradicionalmente con el uso de métodos cuantitativos, además de que la regulación ha obligado a la realización de un cálculo exacto de los riesgos potenciales.

Podemos citar como ejemplo el trabajo del Comité de Basilea que forma parte del Banco de Pagos Internacionales (*Bank foro International Settlements* – BIS por sus siglas en inglés)[11], que fue creado por acuerdo entre los representantes de los bancos centrales de diez naciones industrializadas, con el objetivo de crear estándares para la supervisión bancaria. Estos estándares han sido asumidos por la mayoría de países en el mundo, con el propósito de mejorar la gestión de riesgos en el sector

[11] En la actualidad nos encontramos en proceso de implementación de Basilea III hasta el 2019, fuente: BIS.

bancario, ya que las crisis financieras han evidenciado la importancia y utilidad de contar con ellos. Estos estándares establecen, por ejemplo, criterios para la medición de riesgos en términos de solvencia y liquidez, así como aspectos relacionados con la supervisión y transparencia, para garantizar un mejor control de los riesgos.

En conclusión, desarrollar el apetito de riesgo permite a la organización un mejor proceso de evaluación de riesgos pues hay parámetros que permiten analizar las decisiones de negocio y límites para el establecimiento de estrategias y objetivos.

El segundo factor, el riesgo aceptado dentro de una organización, depende del grado en que ésta se encuentra dispuesta a tolerar la existencia de algo que supone una situación de riesgo o incertidumbre.

Sería ideal lograr niveles de riesgo nulo, pero en la mayoría de los casos este escenario es difícil de lograr o resulta asociado a un costo prohibitivo, por lo que casi cualquier actividad u operación está sometida a un determinado nivel de riesgo. Lo que las organizaciones definen es aquel nivel que les permite cumplir con sus obligaciones legales, con la política y valores que promueve la empresa y con el logro de sus objetivos. Aquellos riesgos que llevan a la empresa a salir de este marco suelen ser considerados inaceptables y por lo tanto, la organización definirá estrategias para reducir o eliminar tales riesgos.

El riesgo aceptado contiene ocho parámetros:

Gráfico 11: Riesgo aceptado en una organización

Riesgo Aceptado
Preparación y asunción de riesgos
Rendimiento
Ganancias en función de la confianza
Leyes de privacidad de la información
Objetivos paralelos y específicos
Calidad de productos y valor añadido
Proyectos de mayor o menor éxito
Indicador cualitativo o cuantitativo

Fuente: Elaboración propia

Capítulo VI:

Manuales e Informes de Riesgos

6.1 Elaboración de manuales e informes de riesgos[12]

Implementar un manual de administración de riesgos es fundamental para establecer todos los requerimientos concretos exigidos, tales como informes, listados, normas y procesos. El proceso de implementación exige de un esfuerzo de la organización y está asociado a un costo. En lo referente a los contenidos, se basan en el establecimiento de una norma abierta que incluya principios generales sobre lo que es el control interno y la medición de los riesgos, en donde la entidad tiene la capacidad de definir el control interno, de acuerdo a sus propias estrategias y objetivos. Resulta ventajoso poder utilizar parte de la estructura actual, teniendo en cuenta los requerimientos mínimos de control exigidos:

- La unidad de riesgos deberá estar formada por una o más personas, las cuales no deben contar con funciones operativas y comerciales de la organización.

- La unidad de riesgos se responsabilizará de la supervisión del cumplimiento de las normas que son evaluadas por el órgano supervisor. Asimismo, se realiza una constante revisión de los procesos y sistemas relativos al control interno contable y al seguimiento y gestión de riesgos y reclamaciones. El objetivo es poder vigilar el cumplimiento de todas las medidas y límites establecidos, además de verificar su validez. Para ello se plantean las modificaciones que se consideren apropiadas, de esta manera se puede informar al consejo de administración de las ineficiencias observadas.

6.2 Manuales de políticas y procedimientos[13]

Un resultado de la implantación de los sistemas de evaluación y gestión de riesgos en las empresas es determinar las políticas de gestión de riesgos, las cuales deben considerar principalmente los límites de exposición a los riesgos. Estos riesgos están asociados con la dirección de la estrategia, para cada parte de seguro. Las políticas deben ser adoptadas por el consejo de administración o directorio de la organización y la gerencia, y ser incorporadas en los manuales de administración de riesgos en forma escrita.[14]

Los límites operativos que establecen las organizaciones se basan en autorizaciones previas al procedimiento para la responzabilización de los riesgos de la entidad:

- Procesos a seguir si los resultados no estén dentro de los límites establecidos.
- En caso, se tenga previsto que las operaciones excederán los límites establecidos, se debe documentar y tener la autorización previa del consejo de administración o del gerente de riesgos.
- Implementar sistemas de control necesarios con el fin de que las operaciones se encuentren dentro de los límites establecidos.

12,13 Casares San José-Martí, Isabel (2014): Implementación de la Gestión Integral de Riesgos en el Sector Asegurador bajo la Norma ISO 31000.
14 Norma ISO 91000:2009.

- La unidad de control de riesgos deberá tener la seguridad que las operaiones estén realizándose correctamente, de tal manera que los clientes se encuentren satisfechos e informados de los riesgos reales o potenciales que aceptan con el fin de formarse una opinión fundada de dichos riesgos.
- Por último, se debe conseguir autorización expresa antes de realizar cualquiera de las operaciones anteriores.

La realización de ciertas funciones o tareas que signifiquen mayor riesgo operativo pueden ser realizadas desde la organización; ello se establece siempre y cuando quede asegurada la segregación entre dichas funciones.

Además, pueden ser asignadas diferentes tareas al personal externo, perteneciente a otras entidades del grupo o terceras empresas especializadas en administración y consultoría. Si se elige la última opción, el consejo de administración debe estar seguro del profesionalismo, capacidad y experiencia de estos. Los procedimientos y controles establecidos en la organización deben ser informados a los servicios subcontratados.

6.3 Manual de tareas y responsabilidades

La empresa debe asegurarse de que el recurso humano sea suficiente y esté capacitado para:

- Una eficiente y eficaz gestión de los riesgos asumidos y del negocio.
- Realizar el control de las operaciones y del registro contable.
- Contrastar criterios de valoración del patrimonio y las provisiones técnicas de la empresa.
- La gestión de requerimientos apropiada.

Las entidades deben establecer planes de formación y evaluación continuada para asegurar la capacitación técnica del personal y que este pueda alcanzar las competencias requeridas, tales como:

- Realizar funciones comerciales o de venta.
- Gestionar (monitorear) los riesgos.
- Actualización constante en las actividades que realice.
- Realizar actividades "core" de la empresa (claves).

En resumen, el personal podrá llevar a cabo tareas de administración, control y gestión de reclamaciones ya que cuenta con conocimientos informáticos y los medios materiales necesarios, lo que a su vez permitirá brindar garantías suficientes de seguridad y capacidad, manteniendo la calidad de los procesos.

Entonces, las organizaciones deben conocer todos los riesgos que está asumiendo el personal para

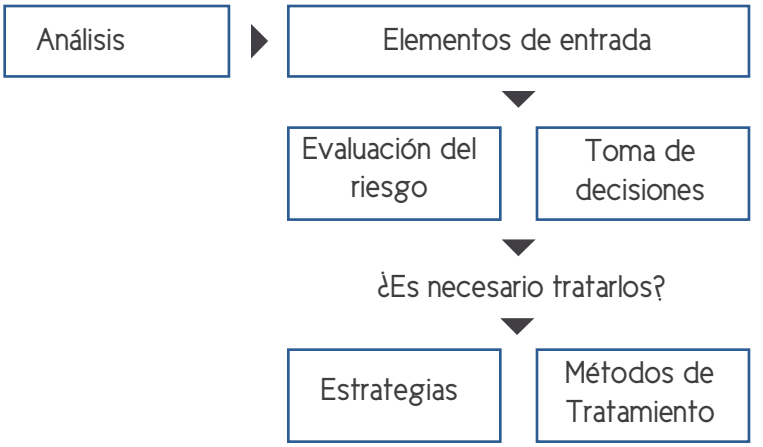
poder evaluar su capacidad de realizar las operaciones anteriormente mencionadas. Asimismo, los sistemas de información para la gestión y las bases de datos de la mismas estarán orientados a la evaluación de riesgos y la toma de decisiones, en relación con los objetivos planteados por el consejo de administración.

En consecuencia, se deberá establecer un sistema eficaz y eficiente de comunicaciones para asegurar que la información relevante (procedimientos a seguir antes de la operaración de nuevos productos o servicios) de la gestión y el control de riesgos llegue a todos los involucrados.

6.4 Manual de administración de riesgos

El manual de administración de riesgos debe ser descriptivo y, a la vez, debe solicitar el análisis de los principales riesgos mediante el estudio del grado de exposición especifico de la entidad a los mismos. Asimismo, debe ser exigido a través de un control ordenado de los límites marcados como tolerables, los cuales serán relativos al resto de factores aplicados a la solvencia de la entidad.

Gráfico 12: Análisis de riesgo



El análisis del riesgo proporciona elementos de entrada para la evaluación del riesgo y para tomar decisiones acerca de si es necesario tratar los riesgos, así como sobre las estrategias y los métodos de tratamiento del riesgo más apropiados.

Es por ello que para un correcto analsis de riesgos se deben tomar en cuenta los siguientes procedimientos y acciones:

- Contar con un sistema de medición y control de riesgos financieros. Estos se deben basar en sensibilidades, modelos estadísticos y duraciones para realizar la valoración de pérdidas potenciales.
- Deben realizarse habitualmente simulaciones de escenarios específicos de crisis. Ello con el fin de evaluar los probables efectos de cada escenario.
- Deben realizarse acuerdos sistemáticamente, por personal distinto al que contabiliza las operaciones, los cuales serán evaluados con información externa a la entidad.
- Debe quedar evidencia de la realización de dichos acuerdos. Se debe erificar el cumplimiento periódico del proceso (partidas conciliatorias y las diferencias registradas) por una persona distinta a quien efectúa dicho acuerdo. Asimismo, se debe emitir un informe sobre las incidencias más relevantes.
- Se debe establecer criterios del registro de las participaciones significativas y sus incidencias.
- Se debe revisar perodicamente si la contabilización y valoración se están realizando correctamente.
- Se debe realizar un seguimiento de las participaciones y la estructura de la entidad, es decir, verificar la información de la variación porcentual de participación y existencia de vinculaciones no accionariales.
- Se deben seguir procesos adecuados de implementación de los procedimientos y controles para evitar posibles quebrantos derivados de riesgos legales, reputacionales y operacionales o, incluso la realización de actividades fraudulentas en las relaciones con clientes, proveedores, distribuidores y cualquier tercero.
- Se deben implementar procedimientos formales de autorización, control y seguimiento de límites de operaciones, otros saldos deudores con clientes, canales de distribución y proveedores, los cuales serán necesarios para la clasificación de saldos morosos, dudosos o fallidos, para obtener expedientes individualizados que contengan toda la documentación relativa a su entidad, contratos firmados y otras informaciones necesarias, además de datos acerca de capacidad financiera.
- Se debe contrastar toda la información de forma habitual. De esta manera, se cumplirán con los criterios establecidos en la normativa. Además, esto ayudará a que se mantenga actualizada la información de los saldos contabilizados.
- Si se opera por medio de sucursales, se deben asignar las herramientas necesarias para que se pueda desarrollar la actividad. Asimismo, deben estar afiliadas en los procedimientos de control interno establecidos por la entidad."[15]

[15] Fuente: Normas, circulares referidas a riesgos de la SBS y SMV.

Capítulo VII:

Control Interno y COSO

7.1 Descripción COSO III

COSO *(Committee of Sponsoring Organizations of the Treadway Commission)* se define como un proceso efectuado por la dirección y el resto del personal de una entidad, diseñado con el objeto de proporcionar un grado de seguridad razonable en cuanto a la consecución de los objetivos dentro de las siguientes categorías:

- Eficacia y eficiencia de las operaciones.
- Confiabilidad de la información financiera.
- Cumplimiento de las leyes, reglamentos y normas (que sean aplicables).

A continuación se presentan los 5 componentes del informe COSO III (actualizado recientemente) que sirvirán de base para el desarrollo de la implementación de la gestión eficiente de los riesgos a través de la norma ISO 31000:2009:

I) Entorno de control

1. Debe demostrar su compromiso con la integridad y los valores éticos.
2. El consejo de administración debe demostrar independencia en la gestión y ejercer la supervisión del desarrollo y ejecución del control interno.
3. La alta dirección debe establecer, con la supervisión del consejo de administración, la estructura, líneas de reporte, autoridad y responsabilidad en la consecución de objetivos.
4. Debe demostrar su compromiso para atraer, desarrollar y retener personas competentes.
5. En la consecución de los objetivos, debe disponer de personas responsables para atender sus responsabilidades de control interno.

II) Evaluación de riesgos

6. Debe especificar los objetivos para permitir la identificación y evaluación de los riesgos relacionados.
7. Debe identificar y evaluar sus riesgos.
8. Debe gestionar el riesgo de fraude.
9. Debe identificar y evaluar los cambios que podrían impactar en el sistema de control interno.

III) Actividades de control

10. Debe seleccionar y desarrollar actividades de control que contribuyan a la mitigación de los riesgos para el logro de sus objetivos.

11. Debe seleccionar y desarrollar controles generales sobre tecnología de la información.
12. Debe implementar sus actividades de control a través de políticas y procedimientos adecuados.

IV) Información y comunicación

13. Debe generar la información relevante para respaldar el funcionamiento de los otros componentes de control interno.
14. Debe compartir internamente la información, incluyendo los objetivos y responsabilidades para el control interno, necesarios para respaldar el funcionamiento de los otros componentes de control interno.
15. Debe comunicar externamente las materias que afecten al funcionamiento de los otros componentes de control interno.

V) Actividades de monitorización

16. Debe comunicar externamente las materias que afecten al funcionamiento de los otros componentes de Control Interno.
17. Debe evaluar y comunicar las deficiencias de control interno.

Los principios introducen ciertos cambios en los componentes del control interno, destacando la evaluación de los riesgos que, a partir que ahora, ha de incluir los conceptos de velocidad y persistencia de los riesgos como criterios para evaluar la criticidad de los mismos.

- Velocidad de riesgo se refiere a la rapidez con la que impacta un riesgo en la organización una vez este se ha materializado.
- Persistencia de un riesgo se refiere a la duración del impacto después de que le riesgo se haya materializado.

Adicionalmente, el marco de COSO 2013, ha modificado la información acerca de las tareas y responsabilidades de los distintos participantes en el proceso, tales como:

- Responsabilidades del CEO (gerente general) y CFO (gerente de finanzas) para que formalmente asuman la efectividad del control interno en ciertas jurisdicciones.
- Actividad a desarrollar por los distintos tipos de comités y su campo de actuación.
- Necesidad de incorporar, además de los auditores externos, a otros proveedores de servicios externalizados (evaluadores) para completar los diferentes tipos de revisión que puede realizar una entidad sobre su control interno (riesgos medioambientales, prácticas de comercio justo o seguridad laboral, etcétera).
- Exigencias reguladoras y legislativas para certificar la eficacia del control interno de la compañía

sobre el reporte financiero.

- Responsabilidad en la gestión de los riesgos de los procesos externalizados, debiendo implementar un programa para evaluar dichas actividades realizadas por terceros en su nombre, y evaluar la eficacia del sistema de control interno sobre las actividades realizadas por dichos proveedores externos de servicios.

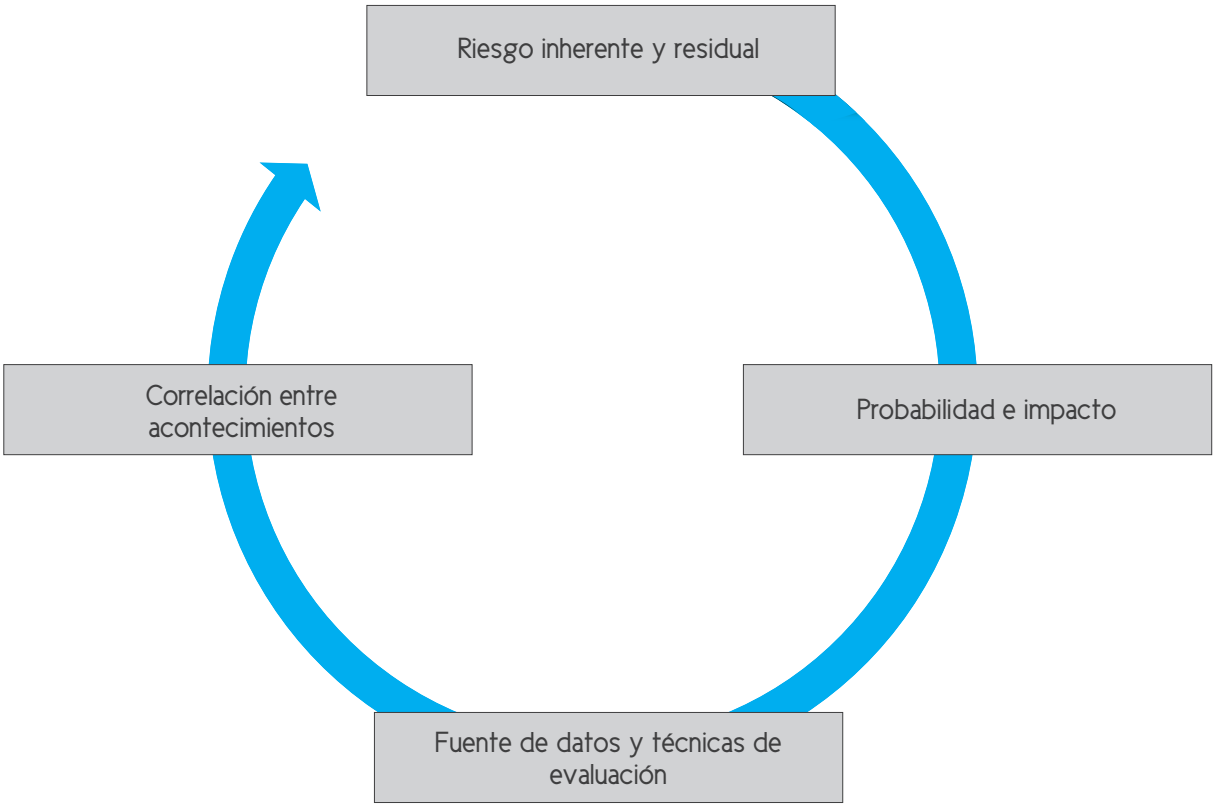
Gráfico 13: Establecimientos del entorno de control de una organización

Fuente: Elaboración propia

Una vez identificados los acontecimientos importantes dentro de una organización, hay que tener en cuenta la evaluación de riesgos. En este paso tenemos cuatro puntos a tomar en cuenta:

1. Riesgo inherente y residual
2. Probabilidad e impacto
3. Fuente de datos y técnicas de evaluación
4. Correlación entre acontecimientos

Gráfico 14: Evaluación de riesgo de una organización

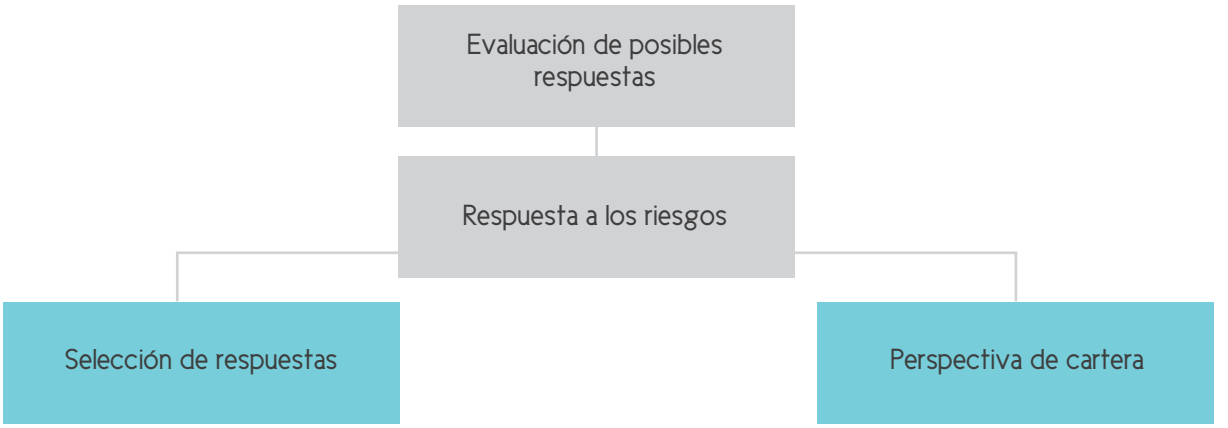


Fuente: Elaboración propia

Luego de evaluar los riesgos a groso modo, debemos tener respuestas de los riesgos mencionados anteriormente, con el objetivo de poder abarcarlos con una evaluación independiente; en este libro mencionaremos tres respuestas que mayormente se encuentran:

1. Evaluación de posibles respuestas
2. Selección de respuestas
3. Perspectiva de cartera

Gráfico15: Respuesta a los riesgos de una organización

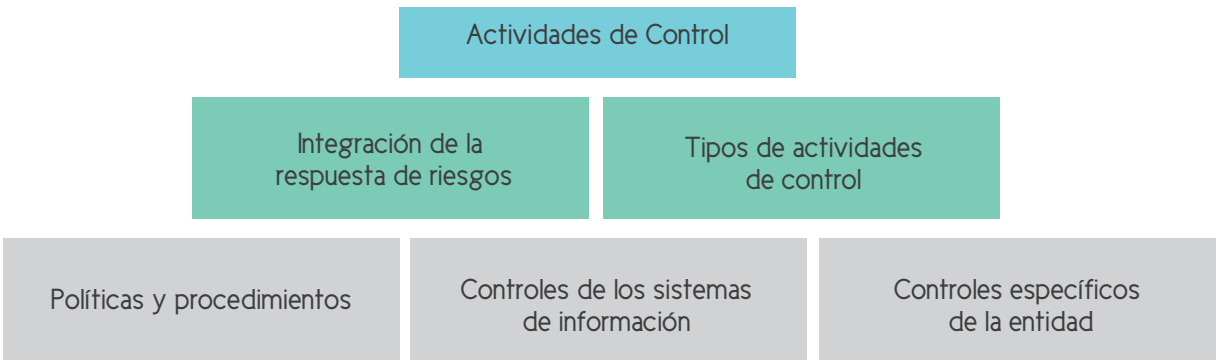


Fuente: Elaboración propia

Posteriormente, luego de hallar las respuestas a los riesgos, hay que enfocarnos en las activdades de control, dentro de este control hay cinco actividades:

- Integración de la respuesta de riesgo
- Tipos de actividades de control
- Políticas y procedimientos
- Controles de los sistemas de información
- Controles específicos de la entidad

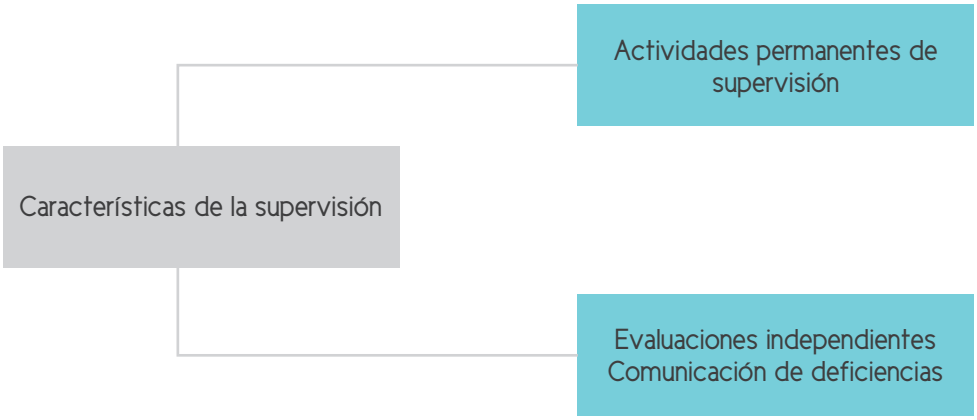
Gráfico16: Actividadesde control de una organización



Fuente: Elaboración propia

Finalmente debemos recopilar la información de las actividades de control para realizar la supervisión correspondiente. En este libro se mencionarán dos características principales de una supervisión de riesgos eficiente y eficaz, las cuales se mostraran en el siguiente gráfico:

Gráfico 17: Supervisión de una organización



Fuente: Elaboración propia

Para resumir el capitulo introductorio se debe entender que hay muchas definiciones que se utilizan en el área de gestión de riesgos. Los lectores pueden encontrar útil consultar otras definiciones específicas en la norma ISO 31000, BS 31100 y la guía ISO 73 si necesitan más aclaraciones.

Para aquellos que están empezando a abarcar el tema, hay una necesidad de ayudarlos a entender con solo siete palabras en que consiste la gestión de riesgos. El riesgo se define como "el efecto de la incertidumbre en los objetivos" [16]

7.2 Definición y evolución del *Enterprise Risk Management*

Dentro de la evolución que ha tenido el interés de las organizaciones por mejorar la administración de los riesgos y su ámbito de control el Enterprise Risk Management (ERM) maneja riesgos y oportunidades que afectan la creación o preservación de valor. La Comisión Treadway (1992) define el ERM como: Esta definición desarrolla conceptos fundamentales como:

> {...} un proceso afectado por la junta directiva, administración y personal de una entidad, aplicado en el establecimiento de la estrategia a lo largo de la organización, diseñado para identificar eventos potenciales que puedan afectar a la entidad y gestionar el riesgo para que se encuentre dentro del perfil de riesgo establecido que proporcione seguridad razonable en

[16] SO Guide 73, Clause 1.1

la consecución de los objetivos de la organización.

Esta definición desarrolla conceptos fundamentales como:

- Proceso que se desarrolla a través de toda una organización
- Realizado por las personas en todos los niveles jerárquicos
- Aplicado en el establecimiento de la estrategia
- Diseñado para identificar eventos potenciales que, de producirse, afectarán a la organización
- Manejar el riesgo de acuerdo al perfil de la organización
- Capaz de proporcionar seguridad razonable a la gestión de la entidad y la junta directiva
- Orientadas a la consecución de los objetivos en una o más categorías separadas pero superpuestas.

Esta definición es muy amplia porque involucra conceptos fundamentales para el manejo de riesgos en las empresas, proporcionando una base para su aplicación dentro de las organizaciones, industrias y sectores. Se enfoca directamente en el logro de los objetivos establecidos por una entidad particular y proporciona una base para la definición de la eficacia del ERM.

La integración del ERM y la gestión de control interno aún no ha dado mayores resultados, siendo a la fecha una agregación de riesgos, creación formal de estrategias o planes de ejecución para enfrentar los riesgos, dejando de lado el desarrollo de marcos de referencia que puedan realizar pruebas de riesgo o tomar medidas correctivas.

En este sentido, el momento de la aplicación generalizada de ERM finalmente se ha establecido por dos razones:

- Ley Sarbanes-Oxley (2002):
  Se busca llevar a un nivel superior la aplicación de esta Ley, en la que las instrucciones financieras públicas aplican, en particular la sección 404 de la ley. El énfasis creciente en el gobierno corporativo y el relacionado con los crecientes costos de cumplimiento están motivando a los líderes de las empresas a revisar si efectivamente los enfoques transversales para la gestión de riesgos van a generar un mayor valor de sus inversiones en el cumplimiento de la SOA (*Society of Actuaries*)[17]. Ellos ven al ERM como el siguiente paso en una progresión lógica para el desarrollo de sus actividades de administración de riesgos. En su plenitud, el ERM tiene el potencial de reducir los costos de cumplimiento, mejorar el rendimiento operativo, mejorar la gobernabilidad corporativa y ofrecer un mayor valor para los accionistas.

- Publicación del nuevo marco COSO:
  El modelo describe los componentes clave y los principios de gestión de riesgos para las organizaciones sin importar su tamaño. El ERM tiene una visión amplia sobre riesgo, un avance

[17] Es la mayor organización profesional dedicada a servir a 24.000 miembros actuariales y a público en todo el mundo. Está dirigido a profesionales líderes en la medición y gestión del riesgo.

importante en comparación con la fragmentación de la gestión de los riesgos en muchas organizaciones.

El ERM se centra en las causas y los efectos que pueden mantener a las empresas en el logro de sus objetivos de negocio estratégicos. Finalmente, en 2013 el comité publicó un nuevo marco de gestión integral de riesgo "COSO Enterprise Risk Management – Integrated Framework", el cual constituye una guía para la gestión de riesgo y está conformado por ocho componentes interrelacionados entre sí: i) entorno de control, ii) establecimiento de objetivos, iii) identificación de eventos, iv) evaluación de riesgos, v) respuesta al riesgo, vi) actividades de control, vii) información y comunicación, y viii) monitoreo; de esta manera permite lograr los objetivos estratégicos, operacionales, de reporte y cumplimiento de cualquier organización, en todas sus entidades, unidades y áreas funcionales (Roisenzvit y Zárate 2006).

7.3 Cumplimento de objetivos

En el contexto de la misión o visión de una institución, la administración establece objetivos estratégicos, selecciona la estrategia y fija objetivos jerarquizados a través de la empresa. Este marco de referencia está orientado al logro de los objetivos de la entidad, establecidos en cuatro categorías:

- Estratégicos: Objetivos de alto nivel, en concordancia y respaldo de su misión.
- Operacionales: El uso eficaz y eficiente de sus recursos.
- Financieros: Confiabilidad de la información
- De cumplimiento: Cumplimiento de las leyes y reglamentos aplicables.

Esta categorización de los objetivos en una entidad permite centrarse en distintos aspectos de la gestión del ERM. Estas categorías distintas pero superpuestas (un objetivo particular puede pertenecer a más de una categoría) dirigen las necesidades de la organización y pueden ser responsabilidad directa de diferentes ejecutivos. Esta categorización también permite distinguir entre lo que se puede esperar de cada categoría de objetivos.

Debido a que los objetivos relacionados con la fiabilidad de la información y el cumplimiento de las leyes y regulaciones están dentro del control de la organización, se espera que la gestión del ERM pueda proporcionar la seguridad razonable para el logro de dichos objetivos. El logro de los objetivos estratégicos y operacionales, sin embargo, está sujeto a eventos externos no siempre dentro del control de la organización, en consecuencia, para estos objetivos, la gestión de riesgos empresarial puede proporcionar la seguridad razonable de que la administración y la junta en su función de supervisión, tengan conocimiento, de manera oportuna, de la medida en que la entidad se está moviendo hacia el logro de los objetivos.

7.4 Los cinco componentes del Modelo COSO

Estos son los cinco componentes:

a. Control interno

a.1) Ambiente interno: El ambiente interno abarca el estilo de la organización, y busca influenciar la conciencia de las personas con respecto al riesgo. Incluye la filosofía de gestión del riesgo, la integridad y valores éticos, y el entorno en que operan.

El ambiente interno es la base para el sistema de control interno en su conjunto porque establece la disciplina y estructura, además de un clima que influye en la calidad del control interno dentro de la organización. Tiene una influencia general en la manera en la que se establecen las estrategias y objetivos, así como en el modo en que las actividades de control son diseñadas.

Gráfico 18: Indicadores de ambiente Interno (I)

Integridad y valores éticos	Directorio/Comité de auditoria	Compromiso con la competencia	
Código de conducta	Directorio y comité integrados por personas independientes y competentes	Procedimientos eficaces de contratación y evaluación de dempeño por parte de RRHH.	Filosofía y estilo operativo de la gerencia
Capacitación sobre ética	Participación activa en las principales decisiones de la gerencia	Funciones y responsabilidades definidas claramente	Políticas y procedimientos de RRHH
Políticas con énfasis en las normas éticas	Supervisión del desempeño de la gerencia	Capacitación	Estructura de la organización
Buenas prácticas en relación a la contratación del personal			Asignación de responsabilidades

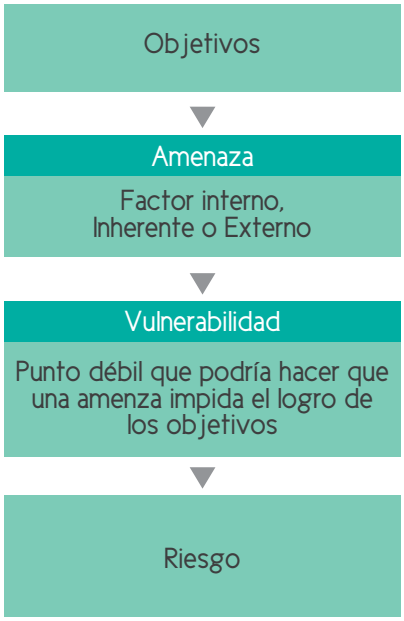
Fuente: Elaboración propia

b. Evaluación de riesgos

b.1) Establecimiento de objetivos: Los objetivos deben existir antes de que la administración pueda identificar eventos potenciales que afecten su rendimiento. El ERM asegura que la administración ha puesto en marcha un proceso para establecer objetivos y que los objetivos seleccionados respaldan y coinciden con las metas de la organización y son consistentes con su perfil de riesgo.

La importancia que tienen los objetivos para la evaluación de los riesgos en una organización es indiscutible porque representa la orientación básica de todos los recursos y esfuerzos, y proporciona una base sólida para un control interno efectivo.

Gráfico 19: Indicadores de ambiente interno (II)



b.2) Identificación de eventos: Los eventos (internos y externos) que afectan el logro de los objetivos de la organización deben ser identificados, diferenciando entre riesgos y oportunidades. Las oportunidades son canalizadas de vuelta a la estrategia de gestión o a los procesos de establecimiento de objetivos.

Gráfico 20: Categorización de los riesgos

Origen de las amenazas		Efecto de la organización
Externa	Eficiencia y eficacia de las operaciones	Entidad
Interna	Integridad de la información financiera	Procesos
Inherente	Cumplimiento de leyes y reglamentos	Actividades
COSO		

Fuente: Elaboración propia

La organización debe identificar los riesgos internos y externos que podrían impedir el logro de los objetivos de negocio críticos, además de los factores internos y externos de riesgo inherentes a toda actividad, independientemente del rubro o la organización.

Gráfico 21: Riesgos internos y externos

Categoría	Descripción
Externos	Riesgos que provienen de las condiciones del entorno y sobre los que no puede influir la organización.
Internos	Riesgos que provienen de las decisiones tomadas por la organización y del empleo de recursos internos y externos.
Inherentes	Riesgos propios de la actividad empresarial, suelen ser independientes del sector o tipo de organización.

Fuente: Elaboración propia

Los riesgos pueden variar según el efecto que tengan en determinados niveles de la organización. Los que afectan a toda la entidad son más amplios y suponen consideraciones macroeconómicas y más estratégicas. Por el contrario, los riesgos que afectan a los procesos y las actividades son más específicos y pueden asociarse fácilmente con actividades de control tangibles dentro de

un proceso.

Gráfico 22: Riesgos por niveles de la organización

Categoría	Descripción
Entidad	Riesgos más amplios que afectan a toda la organización. La alta dirección asume la responsabilidad de remediarlos.
Proceso	Riesgos específicos de un proceso determinado. La solución suele quedar para los responsables de los procesos.
Actividad	Riesgo provenientes de la ejecución de las tareas o actividades particulares.

Fuente: Elaboración propia

b.3) Evaluación de riesgos: Los riesgos son analizados, teniendo en cuenta la probabilidad de ocurrencia y el impacto, lo que permitirá determinar su tratamiento. Se evalúan los riesgos inherentes y residuales.

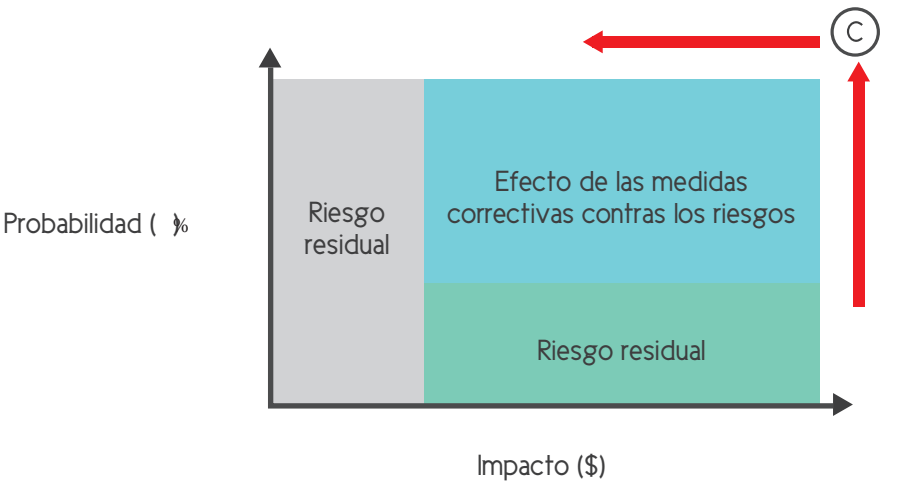
La evaluación de riesgos es el proceso de análisis y priorización de los riesgos relevantes para el logro de los objetivos de la entidad y para determinar una respuesta apropiada.

Mediante la identificación y análisis de los riesgos relevantes y de la capacidad institucional de gestionarlos, se evalúa la vulnerabilidad de la organización preparándose la respuesta necesaria para enfrentarlos y resguardándose la consecución de los objetivos y resultados previstos por la empresa. Criterios de evaluación de riesgos:

- Impacto (I): Nivel de exposición financiera de la empresa ante un riesgo o cuantía de la pérdida financiera que se generaría si ocurriera un evento de riesgo.

- Probabilidad (P): Grado de posibilidad de que ocurra el evento de riesgo en un periodo de tiempo determinado. Puede ser estimado en función a cuántas veces históricamente ha ocurrido el evento de riesgo en la organización y la posibilidad que vuelva a ocurrir en el futuro.

Gráfico 23: Riesgo residual



Fuente: Elaboración propia

Severidad = Probabilidad por el Impacto (C)

Gráfico 24: Evaluación del nivel de riesgo

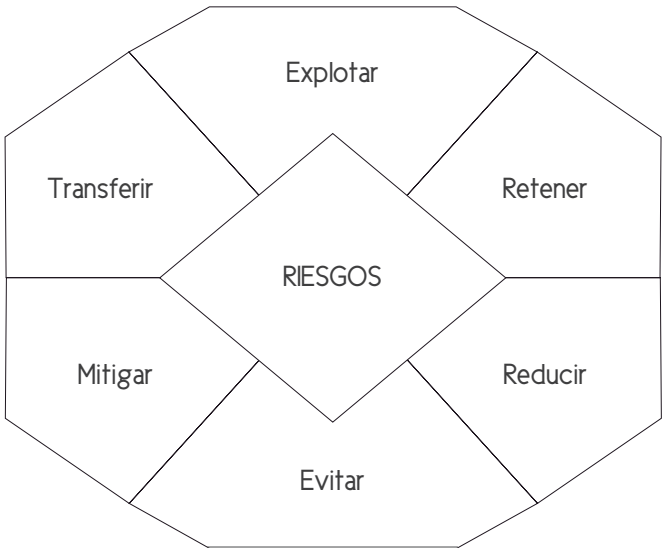
Impacto	(5) Impacto severo	Alto	Extremo	Extremo	Extremo	Extremo
	(4) Impacto	Alto	Alto	Extremo	Extremo	Extremo
	(3) Impacto	Moderado	Moderado	Alto	Alto	Extremo
	(2) Impacto	Bajo	Bajo	Moderado	Alto	Alto
	(1) Impacto	Bajo	Bajo	Bajo	Moderado	Alto
		(1) Raro	(2) Improbable	(3) Posible	(2) Probable	(1) Cierto
Probabilidad						

Fuente: Elaboración propia

Se recomienda iniciar con una matriz 3x3, para luego pasar a una 5x5 a los 6 meses o al año y luego una de 7x7, lo importantes es poder generar la base de datos de información. *Lo importante es tener la información, procesarla e iniciar la medición.*

b.4) Respuesta a riesgos: La administración selecciona las respuestas al riesgo: evitar, aceptar, reducir o compartir los riesgos, desarrollando una serie de medidas para adaptar los riesgos al perfil de riesgo de la entidad.

Gráfico 25: Estrategias para el tratamiento de los riesgos



Fuente: Elaboración propia

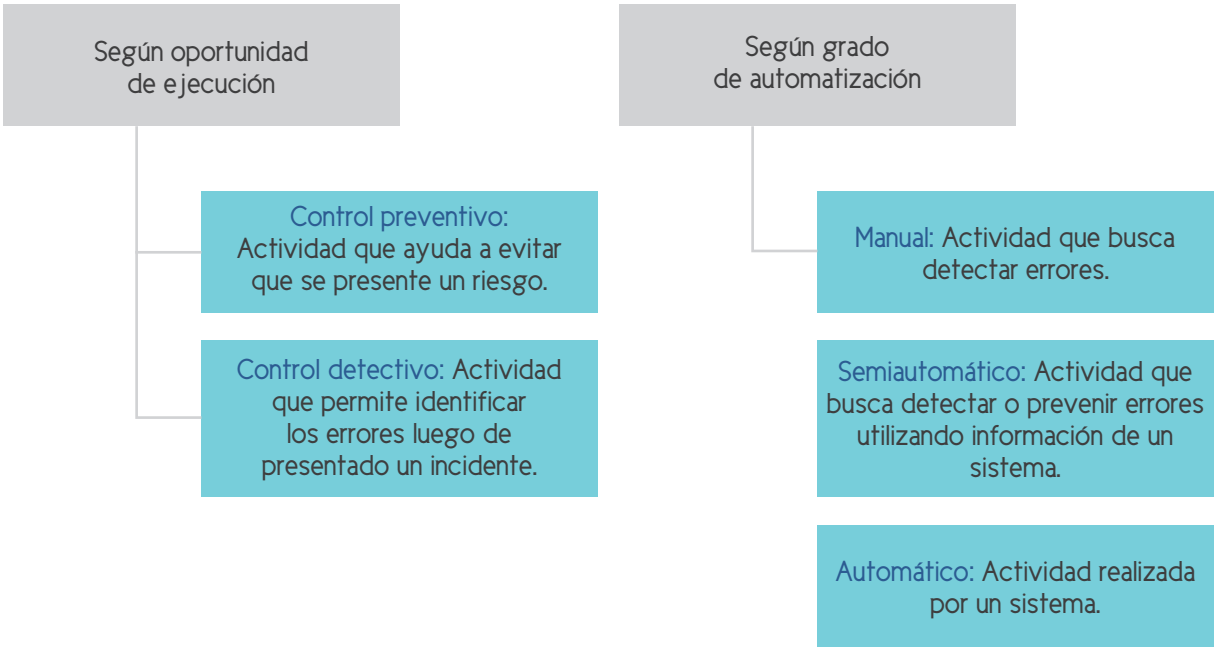
- Explotar: Aceptar altos niveles de riesgo para aprovechar oportunidades.
- Transferir: Traspasar a un tercero la administración de un riesgo determinado.
- Retener: Conservar el riesgo y realizar un adecuado monitoreo del mismo.
- Mitigar: Establecer controles para disminuir el impacto del riesgo.
- Reducir: Establecer controles que permitan disminuir la probabilidad de ocurrencia de un riesgo determinado.
- Evitar: No realizar una determinada actividad para que el riesgo no se genere.

c. Actividades de Control

Se establecen e implementan políticas y procedimientos para ayudar a garantizar que las respuestas al riesgo se lleven realmente a cabo. Se define control como toda medida tomada

para mitigar o gestionar el riesgo y para que la probabilidad de que un negocio / procesos logre sus metas y objetivos sea mayor.

Gráfico 26: Tipos de control (I)



Fuente: Elaboración propia

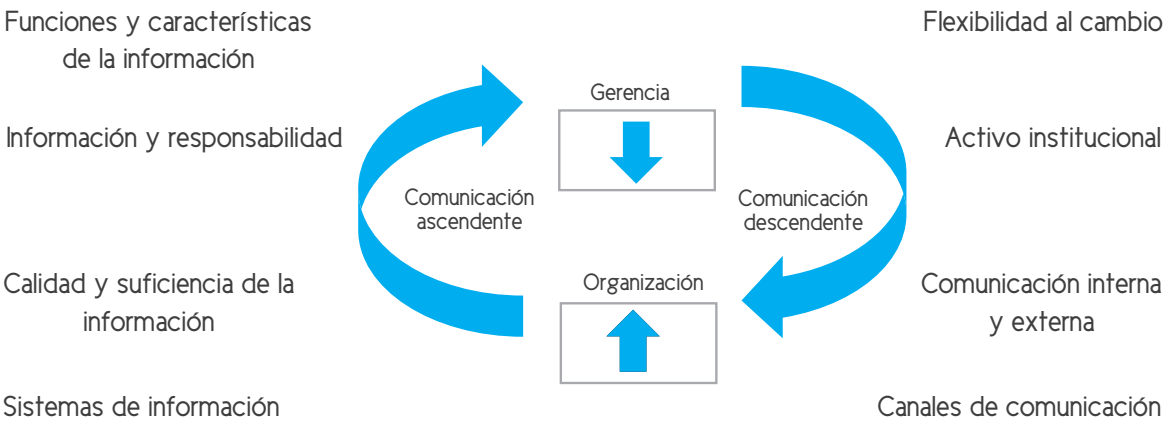
Algunos aspectos a considerar sobre los controles:

- Los controles ayudan a lograr los objetivos y mitigar riesgos.
- Los controles deben tener un responsable, una periodicidad definida de ejecución de la actividad y una evidencia de que se ejecutó

d. Información y comunicación

d.1) Información y comunicación: La información pertinente es identificada, almacenada, y comunicada en la forma y plazos que permitan a las personas llevar a cabo sus responsabilidades. La comunicación efectiva también se produce en un sentido más amplio, fluyendo a lo largo de la entidad.

Gráfico 27: Tipos de control (II)



Fuente: Elaboración propia

e. Actividades de monitorización

e.1) Supervisión: El ERM se controla y se realizan las modificaciones que sean necesarias. El monitoreo se realiza a través de las actividades de gestión en curso, evaluaciones separadas, o ambas cosas. La gestión del riesgo no es estrictamente un proceso en serie, donde uno de los componentes afecta solo al siguiente. Se trata de un proceso multidireccional e iterativo en el que casi cualquier componente puede y tiene influencia sobre otro.

La prevención y monitoreo se deben efectuar sobre los diferentes documentos que regulen y sustenten el desarrollo de las actividades de la organización –sean estos de gestión, operativos o de control–con la finalidad de tener una seguridad razonable de que se van a cumplir con los objetivos así como aquellos relacionados con el control interno.

7.5 Relación de los objetivos y componentes[18]

Existe una relación directa entre los objetivos que la entidad desea lograr y los componentes de la gestión de riesgos corporativos, que representan lo que hace falta para lograr aquellos. La relación se representa con una matriz tridimensional, en forma de cubo.

[18] Committee of Sponsoring Organizations of the Tradeway Commission, Enterprise Risk Management Integrated Framework, 2004.

Gráfico 28: Evolución de COSO (2013)

CUBO COSO ACTUALIZADO

CUBO COSO ORIGINAL

Fuente: COSO

Las cuatro categorías de objetivos (estrategia, operaciones, información y cumplimiento) están representadas por columnas verticales, los ocho componentes lo están por filas horizontales y las unidades de la entidad, por la tercera dimensión del cubo. Este gráfico refleja la capacidad de centrarse sobre la totalidad de la gestión de riesgos corporativos de una entidad o bien por categoría de objetivos, componente, unidad o cualquier subconjunto deseado.

a. Eficacia:

La afirmación de que la gestión de riesgos corporativos de una entidad es eficaz es un juicio resultante de la evaluación de si los ocho componentes están presentes y funcionan de modo eficaz. Así, estos componentes también son criterios para estimar la eficacia de dicha gestión.

Para que estén presentes y funcionen de forma adecuada, no puede existir ninguna debilidad material y los riesgos necesitan estar dentro del nivel de riesgo aceptado por la entidad. Cuando se determine que la gestión de riesgos es eficaz en cada una de las cuatro categorías de objetivos, respectivamente, el consejo de administración y la dirección tendrán la seguridad razonable de que conocen el grado de consecución de los objetivos estratégicos y operativos de la entidad, que su información es fiable y que se cumplen las leyes y la normas aplicables.

Los ocho componentes no funcionan de modo idéntico en todas las entidades. Su aplicación en las pequeñas y medianas empresas, por ejemplo, puede ser menos formal y estructurada.

Sin embargo, estas entidades podrían poseer una gestión eficaz de riesgos corporativos, siempre que cada componente esté presente y funcione adecuadamente.

b. Limitaciones:

Aunque la gestión de riesgos corporativos proporciona ventajas importantes, también presenta limitaciones. Además de los factores comentados anteriormente, las limitaciones se derivan de hechos como que el juicio humano puede ser erróneo durante la toma de decisiones, que las decisiones sobre la respuesta al riesgo y el establecimiento de controles necesitan tener en cuenta los costes y beneficios relativos, que pueden darse fallos por error humano, que pueden eludirse los controles mediante connivencia de dos o más personas y que la dirección puede hacer caso omiso a las decisiones relacionadas con la gestión de riesgos corporativos. Estas de los objetivos de la entidad.

c. Incorporación del control interno:

El control interno constituye una parte integral de la gestión de riesgos corporativos. Este marco lo incluye, constituyendo una conceptualización y una de las herramientas más sólidas para la dirección. El control interno se define y describe en el documento Control interno: Marco integrado. Dado que este ha perdurado a lo largo del tiempo y es la base para las reglas, normas y leyes existentes, se mantiene vigente para definir y enmarcar el control interno.

d. Roles y responsabilidades:

Todas las personas que integran una entidad tienen alguna responsabilidad en la gestión de riesgos corporativos. El consejero delegado es su responsable último y debería asumir su titularidad. Otros directivos apoyan la filosofía de gestión de riesgos de la entidad, promueven el cumplimiento del riesgo aceptado y gestionan los riesgos dentro de sus áreas de responsabilidad en conformidad con la tolerancia al riesgo. El director de riesgos, director financiero, auditor interno u otros, desempeñan normalmente responsabilidades claves de apoyo. El restante personal de la entidad es responsable de ejecutar la gestión de riesgos corporativos de acuerdo con las directrices y protocolos establecidos.

El consejo de administración desarrolla una importante supervisión de la gestión de riesgos corporativos, es consciente del riesgo aceptado por la entidad y está de acuerdo con el. Algunos terceros, como los clientes, proveedores, colaboradores, auditores externos, reguladores y analistas financieros, proporcionan a menudo información útil para el desarrollo de la gestión de riesgos corporativos, aunque no son responsables de su eficacia en la entidad ni forman parte de ella.

7.6 Fortalecer el gobierno corporativo

"El gobierno corporativo abarca un conjunto de relaciones entre la administración de la empresa, su consejo de administración, sus accionistas y otras partes interesadas. También proporciona la estructura a través de la que se fijan los objetivos de la compañía y se determinan los medios para alcanzar esos objetivos y supervisar el desempeño" (OECD 2004).

El concepto de gobierno corporativo se refiere al conjunto de principios y normas que regulan el diseño, integración y funcionamiento de los órganos de gobierno de la empresa, como son los tres poderes dentro de una sociedad: los accionistas, directorio y alta administración. En el mundo, el mercado de valores, los fondos de pensiones, sociedades mutualistas, compañías de seguros, sociedades de capital de riesgo y otros similares, forman parte importante del sistema financiero y las necesidades de información sobre sus inversiones han sido definitivas para la incorporación en las empresas de las llamadas mejores prácticas corporativas.

> En su sentido más amplio, el gobierno corporativo consiste en mantener el equilibrio entre los objetivos económicos y los sociales entre los objetivos individuales y los comunitarios. El marco de gobierno se establece con el fin de promover el uso eficiente de los recursos y, en igual medida, exigir que se rindan cuentas por la administración de esos recursos. Su propósito es lograr el mayor grado de coordinación posible entre los intereses de los individuos, las empresas y la sociedad. El incentivo que tienen las empresas y sus propietarios y administradores para adoptar las normas de gestión aceptadas a nivel internacional es que ellas los ayudarán a alcanzar sus metas y a atraer inversiones. En el caso de los Estados, el incentivo es que esas normas fortalecerán sus economías y fomentarán la probidad de las empresas. (Cadbury 2013)

El ERM (Enterprise Relationship Management) puede ser una fuente para el fortalecimiento del gobierno corporativo. El gobierno corporativo se compone de los sistemas y procesos que utiliza una organización para proteger los intereses de sus distintos grupos de interés. La forma ideal responde a las necesidades de todos los interesados, ya sean accionistas, empleados, clientes, proveedores y la comunidad, ya que todos comparten un interés común en la continuidad y éxito del negocio.

Las organizaciones con un buen Gobierno Corporativo reconocen que la satisfacción de los intereses de las partes interesadas resulta fundamental para el sostenimiento de la organización en el largo plazo y lo que le permite prosperar a través del tiempo.

Gráfico 29: El ERM fortalece el gobierno corporativo

Fuente: Bowling D. Y Rieger, L (2010)

El ERM – gestión del riesgo empresarial entra en escena, porque el buen gobierno corporativo requiere, entre otras cosas:

- Seguimiento de los riesgos con los procedimientos adecuados.
- Garantizar una comprensión adecuada de la forma del manejo de los riesgos.
- Aprender a detectar oportunidades en los riesgos presentes.

El modelo COSO – ERM reconoce sus limitaciones (Williamson 2007) que se derivan de los errores de juicio de las personas al momento de tomar decisiones, estas pequeñas fallas pueden resultar en errores al momento de dar una respuesta frente al riesgo. También la dirección mantiene la capacidad de omitir las decisiones de ERM. Tampoco el fraude desaparecerá mientras sean las personas quienes dirigían los negocios, ya que se pueden burlar controles. La definición de COSO ERM, como se mencionó anteriormente, incluye el término "certeza razonable"[19]

[19] Committee of Sponsoring Organizations of the Tradeway Commission, Enterprise Risk Management Integrated Framework, 2004.

7.7 Definición de control interno partiendo de bases para el establecimiento de un sistema de gestión de riesgos

En general, del informe COSO III se recoge que el control interno es entendido como *"un proceso diseñado por un cuadro de directores, gerentes y otro tipo de personal, para obtener una visión razonablemente segura en el alcance de los objetivos"*[20]

Los objetivos de este control interno se agrupan en tres categorías:

1. Efectividad y eficiencia en las operaciones.
2. Veracidad en la información financiera.
3. Cumplimiento de las leyes aplicables y regulaciones.

En resumen, el control interno pretende agregar en cada entorno determinado los riesgos del negocio, flujos de información y comunicación de forma similar a lo representado en el siguiente gráfico, donde se resume:

- Los riegos
- Flujos de información
- La comunicación deseada

Gráfico 30: El ERM fortalece el gobierno corporativo

Así, el objetivo de los controles internos y los procesos que se proponen en este manual es garantizar que la entidad cuente con elementos de juicio necesarios para ofrecer una razonable seguridad en cuanto a que:

- Las transacciones que realiza la empresa estén debidamente autorizadas.
- Los activos de la entidad estén a salvo del uso no autorizado o fraudulento.
- Las transacciones de la compañía sean registradas y archivadas correctamente para permitir la elaboración de los estados financieros en concordancia con los principios contables en vigor, y sentar las bases para el desarrollo de un sistema de control dinámico a alto nivel.

[20] COSO II (2004): Gestion de Riesgos Corporativos– Marco Integrado: Técnicas de Aplicación, Committe of Sponsoring Organizations of Treadway Comission, Septiembre.

7.8 Elección de las bases técnicas[21]

La administración eficaz de los riesgos va a permitir hacer frente a factores internos y externos que generan incertidumbre para:[22]

- Mejorar la probabilidad de alcanzar los objetivos fijados.
- Promover una gestión empresarial proactiva y ética.
- Entender la necesidad de identificar y evaluar los riesgos en todas las áreas de la empresa.
- Identificar las oportunidades, fortalezas, debilidades y amenazas.
- Realizar las actividades de acuerdo a las normativas legales y reglamentarias aplicables y las normas internacionales.
- Mejorar el gobierno.
- Mejorar en la prestación de los informes financieros.
- Brindar confianza y transparencia a todo el personal de la empresa.
- Establecer un punto de partida para la toma de decisiones.
- Conocer los controles internos y externos.
- Asignar los recursos necesarios para el tratamiento del riesgo.
- Aumentar la eficacia y eficiencia operacional.
- Mejorar la prevención y gestión de siniestros.
- Minimizar las pérdidas.
- Mejorar la información para toda la organización.

El proceso de administración de riesgos se inicia con la identificación y análisis de los riesgos de la empresa y continua con la reducción, asunción, transferencia o retención y financiación de los riegos económicos y sociales. Dicha metodología permite identificar, analizar y evaluar los riesgos, a la vez que los minimiza, controla y hace un tratamiento financiero de los mismos.

Las bases técnicas que se emplean para identificar y cuantificar los riesgos se basan en las relaciones entre los principios de gestión del riesgo, la estructura organizacional y el proceso.

7.9 Identificación de los riesgos

Se deben identificar los riesgos relevantes que enfrenta un organismo en la persecución de sus objetivos, ya sean de origen interno como externo. La identificación del riesgo es un proceso iterativo, generalmente integrado a la estrategia y planificación. En este proceso es conveniente "partir de cero", esto es no basarse en el esquema de riesgos identificados en estudios anteriores.

Su desarrollo debe comprender la realización de un "mapeo" del riesgo, que incluya la especificación de los dominios o puntos claves del organismo, la identificación de los objetivos generales y particulares,

[21] Casares San José-Martí, Isabel (2014): Implementación de la Gestión Integral de Riesgos en el Sector Asegurador bajo la Norma ISO 31000.
[22] UNE-ISO 31000:2010 Gestión de riesgo: Principios y directrices. Traducido por AENOR (Asociación Española de Normalización y Certificación). Julio 2010

y las amenazas y riesgos que se pueden tener que afrontar. Un dominio o punto clave del organismo, puede ser:

- Un proceso que es crítico para su sobrevivencia;
- Una o varias actividades que impliquen la entrega de porciones importantes de servicios a la ciudadanía;
- Un área que está sujeta a leyes, decretos o reglamentos de estricto cumplimiento, con amenazas de severas puniciones por incumplimiento;
- Un área de vital importancia estratégica para el gobierno.

Al determinar estas actividades o procesos claves, fuertemente ligados a los objetivos del organismo, debe tenerse en cuenta que pueden existir algunos que no estén formalmente expresados, lo cual no debe ser impedimento para su consideración. El análisis se relaciona con la criticidad del proceso o actividad y con la importancia del objetivo, más allá que este sea explícito o implícito.

Existen muchas fuentes de riesgos, tanto internas como externas. A título puramente ilustrativo se pueden mencionar, entre las externas:

- Desarrollos tecnológicos que en caso de no adoptarse, provocarían obsolescencia organizacional.
- Cambios en las necesidades y expectativas del ciudadano/usuario.
- Modificaciones en la legislación y normas regulatorias que conduzcan a cambios forzosos en la estrategia y procedimientos.
- Alteraciones en el escenario económico que impacten en el presupuesto del organismo, sus fuentes de financiamiento y su posibilidad de expansión.

Entre las internas, podemos citar:

- La estructura organizacional adoptada, dada la existencia de riesgos inherentes típicos tanto en un modelo centralizado como en uno descentralizado.
- La calidad del personal incorporado, así como los métodos para su instrucción y motivación.
- La propia naturaleza de las actividades del organismo.

Una vez identificados los riesgos a nivel del organismo, deberá practicarse similar proceso a nivel de programa y actividad. Se considerará, en consecuencia, un campo más limitado, enfocado en los componentes de las áreas y objetivos claves identificados en el análisis global del organismo. Los pasos siguientes al diagnóstico realizado son los de la estimación del riesgo y la determinación de los objetivos de control.

En general, las entidades están sometidas a un conjunto de riesgos por su actividad económica, por

lo que debe realizarse un diagnóstico de la exposición y control de riesgos con independencia de la organización que tenga. El objetivo de esta etapa consiste en generar una lista exhaustiva de riesgos denominada "decálogo de riesgos" basada en aquellos sucesos que podrían crear, mejorar, prevenir, degradar, acelerar o retrasar el logro de los objetivos.

A continuación detallaremos algunos riesgos[23] que podrían afectar a las organizaciones, aunque cabe mencionar que cada organización cuenta con su decálogo de riesgos de acuerdo a la industria donde se encuentre, por lo que no todos los riesgos podrían ser tomados en cuenta.

Riesgo de desviación.– Se refiere a la posibilidad de pérdida en caso de que el desarrollo actual de las frecuencias de reclamaciones, mortalidad, tasas de interés e inflación, no correspondan a las bases con las que se calcularon las primas cobradas, ocasionando un aumento no esperado en el índice de siniestralidad.

Riesgo de tarifas o comisiones.– Corresponde a la probabilidad de pérdida como consecuencia de errores en el cálculo de las tarifas, al punto que resulten insuficientes para cubrir los costos de atención actuales y futuros, los gastos administrativos y la rentabilidad esperada.

Riesgo de políticas inadecuadas de venta.– Se refiere a la probabilidad de incurrir en pérdidas por políticas inadecuadas de selección de riesgos, de intermediación y de otorgamiento de descuento.

Riesgo técnico.– La posibilidad de pérdidas por siniestros y gastos mayores a los esperados, insuficiencia de las reservas técnicas y deficiente cobertura de reaseguros. Se le conoce también como riesgo de seguro.

Riesgo operacional.– La posibilidad de pérdidas debido a procesos inadecuados, fallas del personal, de la tecnología de información, o eventos externos. Esta definición incluye el riesgo legal, pero excluye el riesgo estratégico y de reputación.

Riesgo de concentración y hechos catastróficos.– Se refiere a la probabilidad de pérdida en que puede incurrir la organización como consecuencia de una concentración de los riesgos asumidos, bien sea por franjas de edades, por regiones o por la ocurrencia de hechos catastróficos.

Riesgos de lavado de activos y del financiamiento del terrorismo.– La posibilidad de que la empresa sea utilizada para fines de lavado de activos y/o financiamiento del terrorismo. Esta definición excluye el riesgo de reputación y el operacional.

Riesgo de insuficiencia de provisiones técnicas.– Se refiere a la probabilidad de pérdida como consecuencia de una subestimación en el cálculo de las provisiones técnicas y otras obligaciones

[23] RESOLUCIÓN No. JB-2011-2066 de la junta Bancaria del Ecuador de la Superintendencia de Bancos y Seguros. 29 de Noviembre de 2011

contractuales tales como beneficios garantizados o rendimientos garantizados, entre otros.

Los riesgos de crédito, liquidez y mercado generalmente se encuentran asociados al valor de los activos de las empresas, es decir, están referidos a los movimientos de las tasas de mercado y los precios como tasas de interés, tasas de cambio o precios de las acciones, las cuales afectan adversamente el valor reportado o el valor de mercado de las inversiones. Están incluídos también el riesgo de liquidez en sus dos aceptaciones, calce y convertibilidad en efectivo de las inversiones, y el de crédito.

Riesgo de crédito.– Se refiere a la probabilidad de incurrir en pérdidas por el no pago, el pago parcial o pago importuno de las obligaciones a cargo de otras compañías, clientes o proveedores, otros prestadores de servicios o a cargo de cualquier otra persona que determine una acreencia a favor de la empresa. Además, se incluye la posibilidad de incurrir en pérdidas por el riesgo de insolvencia de los emisores de títulos en los cuales se encuentran colocadas las inversiones de la organización.

Riesgo de mercado.– Está asociado al valor de los activos de las empresas en la industria. Es la posibilidad de incurrir en pérdidas derivadas del incremento no esperado en el monto de sus obligaciones con acreedores externos, pérdida en el valor de activos a causa de los movimientos en las tasas de mercado, incremento de tasas de interés, tasas de cambio o precios de las acciones o cualquier otro parámetro de referencia, que afectan adversamente el valor reportado o el valor de mercado de las inversiones.

Riesgo de liquidez.– Es la probabilidad de pérdida que se manifiesta por la incapacidad de la entidad para enfrentar una escasez de fondos y cumplir sus obligaciones a corto plazo, y que determina la necesidad de conseguir recursos alternativos o de realizar activos en condiciones desfavorables, bien sea para el pago de siniestros o para el ajuste de reservas inadecuadamente calculadas.

Riesgo operativo.– Es la probabilidad de que se produzcan pérdidas debido a eventos originados en fallas o insuficiencia de procesos, personas, sistemas internos, tecnología, y en la presencia de eventos externos imprevistos. Incluye el riesgo legal pero excluye los riesgos sistémico y de reputación, estrategia y el de ambiente de los negocios. El riesgo operativo no trata sobre la posibilidad de pérdidas originadas en cambios inesperados en el entorno político, económico y social.

Riesgo legal.– Es la probabilidad de que una empresa sufra, por disposiciones legales o normativas, pérdidas directas o indirectas, que sus activos se encuentren expuestos a situaciones de mayor vulnerabilidad, que sus pasivos y contingentes puedan verse incrementados más allá de los niveles esperados o que el desarrollo de sus operaciones enfrente la eventualidad de ser afectado negativamente debido a error, negligencia, impericia, imprudencia o dolo. Dichas disposiciones legales o normativas pueden ser instrucciones de carácter general o particular que son emanadas

de los organismos de control en las competencias particulares de las entidades, sentencias o resoluciones jurisdiccionales o administrativas adversas, deficiente redacción de los textos, deficiente formalización o ejecución de actos, contratos o transacciones, inclusive distintos a los del giro ordinario de negocio y derechos de las partes contratantes no claramente estipulados.

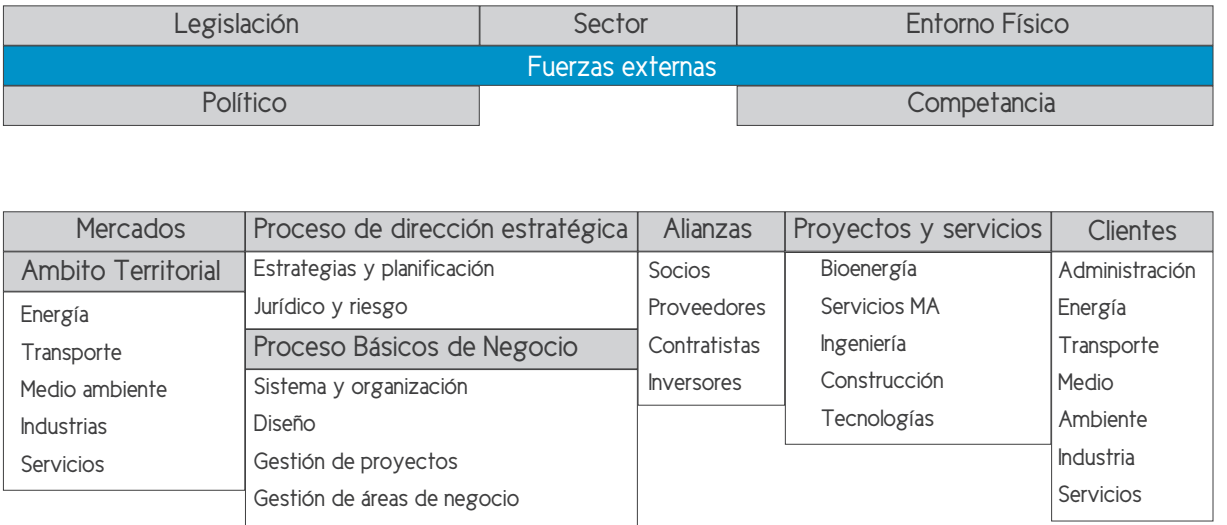
Riesgo estratégico.– Se refiere a la probabilidad de pérdida tras la imposibilidad de definir los objetivos y estrategias de la entidad. Por ejemplo, implementar apropiadamente los planes de negocio, las decisiones de mercado, la asignación de recursos y la incapacidad para adaptarse a los cambios en el entorno de los negocios. Se debe considerar, en este tipo de riesgo, el derivado del crecimiento acelerado y desordenado que pueda ocasionar incapacidad de atender adecuadamente a los usuarios o demandar un alto valor de inversiones en la expansión de los servicios.

Riesgo reputacional.– Se refiere a la posibilidad de afectación del prestigio de una entidad por algún evento externo, tal como: fallas internas hechas públicas, participación en negocios ilícitos. Estos eventos pueden generar pérdidas y ocasionar un deterioro de la situación de la entidad.

Es importante mencionar que estos riesgos son de difícil pronóstico, e incluso exógenos a la operatividad de la entidad; sin embargo, realizar una adecuada aplicación de los controles permitirá una mejor administración de dichos riesgos. Por ello, es fundamental que la evaluación de cada grupo de riesgos sea validada por el sistema o departamento implicado.

Los riesgos que están asociados a la actividad que la compañía realiza se clasifican de acuerdo a la importancia a priori de los mismos. A continuación presentamos algunos ejemplos clave de interpretación según importancia, que puede ser baja, media o alta:

Gráfico 31: Ejemplo de clasificación del riesgo



Fuente: Elaboración propia

7.10 Tipos de técnicas de apreciación del riesgo

Las técnicas de apreciación del riesgo se pueden clasificar de varias maneras para ayudar a comprender sus cualidades relativas de solidez y de debilidad. Además, cada una de las técnicas se desarrolla según la naturaleza de la apreciación que proporcionan, y se dan directrices para su aplicabilidad en determinadas situaciones.

La primera clasificación muestra cómo se aplican las técnicas en cada etapa del proceso de apreciación del riesgo, como sigue:

- Identificación del riesgo.
- Análisis del riesgo y análisis de las consecuencias.
- Análisis del riesgo y estimación de la probabilidad cualitativa, semicuantitativa o cuantitativa.
- Análisis del riesgo y evaluación de la eficacia de todos los controles existentes.
- Análisis del riesgo y estimación del nivel de riesgo.
- Evaluación del riesgo.

Para cada etapa del proceso de apreciación del riesgo, la aplicación del método se describe como muy aplicable, aplicable o no aplicable.

A continuación se describen los atributos de los métodos, en función de:

- La complejidad del problema y de los métodos que se necesitan para analizarlo.
- La naturaleza y el grado de incertidumbre de la apreciación del riesgo, ba-sados en la cantidad de información requerida que está disponible para sa-tisfacer los objetivos.
- La amplitud de los recursos requeridos en función del tiempo y del nivel de conocimientos técnicos, de las necesidades de datos o de los costes.
- Si el método puede proporcionar un resultado cuantitativo.

Gráfico 32: Atributos de una selección de herramientas de evaluación de riesgo

Tipos de técnicas de apreciación de riesgos	Herramientas y Técnicas	Descripción	Relevancia de los factores			¿Puede proporcionar resultados cuantitativos?	Proceso de evaluación del riesgo				
								Análisis del riesgo			
			Recursos y capacidades	Naturaleza y grado de incertidumbre	Complejidad		Identificación del riesgo	Consecuencia	Probabilidad	Nivel de riesgo	Evaluación del riesgo
METODOS DE BÚSQUEDA	Lista de verificación (Check-lists)	Método simple de la identificación de riesgos, Una técnica que proporciona una lista de las incertidumbres típicas que deben considerarse. Los usuarios consultan una lista previamente desarrollada, códigos o normas.	B	B	B	NO	FA	NA	NA	NA	NA
	Análisis preliminar de riesgos	Un método inductivo simple de análisis cuyo objetivo es identificar los riesgos, situaciones peligrosas y sucesos que puedan causar daño para una actividad determinada, instalación o sistema.	B	A	M	NO	FA	NA	NA	NA	NA
METODOS DE APOYO	Intercambio de ideas (Brainstorming) / Entrevistas estructuradas o semiestructuradas	Un método para recopilar un amplio conjunto de ideas, su evaluación y clasificación por un equipo. Las ideas pueden ser recibidas por mensajes o entrevistas individuales o colectivas.	B	B	B	NO	FA	NA	NA	NA	NA
	Técnica Delphi	Un método para combinar las opiniones de los expertos que pueden apoyar la identificación de los riesgos y su influencia, la estimación de la probabilidad y su consecuencia y la evaluación del riesgo. Es una técnica de colaboración para la creación de consenso entre los expertos. Requiere de un análisis independiente y votación por los expertos.	M	M	M	NO	FA	NA	NA	NA	NA
	¿Que pasaría si? What if? » (SWIFT)	Un método para que un equipo identifique los riesgos. Normalmente se utiliza dentro de un grupo de trabajo. Habitualmente se utiliza vinculado a un análisis de riesgos y a una técnica de evaluación.	M	M	M	NO	FA	FA	FA	FA	FA
	Análisis de fiabilidad humana (HRA)	Evaluación de la fiabilidad humana (HRA) por el que se trata el impacto de los seres humanos sobre el funcionamiento del sistema y puede utilizarse para evaluar la influencia del error humano sobre el sistema.	M	M	M	SI	FA	FA	FA	FA	A

Gráfico 32: Continuación

Tipos de técnicas de apreciación de riesgos	Herramientas y Técnicas	Descripción	Relevancia de los factores			¿Puede proporcionar resultados cuantitativos?	Proceso de evaluación del riesgo				
								Análisis del riesgo			
			Recursos y capacidades	Naturaleza y grado de incertidumbre	Complejidad		Identificación del riesgo	Consecuencia	Probabilidad	Nivel de riesgo	Evaluación del riesgo
ANÁLISIS DE ESCENARIOS	Análisis de causa	La única pérdida producida es analizada para comprender las causas que la ocasionan y poder mejorar el sistema o proceso para evitar pérdidas futuras. El análisis deberá considerar cuáles eran los controles en el lugar y en el momento en que se produjo la pérdida y cómo podrían mejorarse los controles.	M	B	M	NO	NA	FA	FA	FA	FA
	Análisis de escenario	Se imaginan o extrapolan posibles escenarios futuros de los diferentes riesgos actuales suponiendo que cada uno de estos escenarios puedan producirse. Esto puede hacerse formal o informalmente y cualitativa o cuantitativamente.	M	A	M	NO	FA	FA	A	A	A
	Valoración de riesgo medioambiental	Se identifican y analizan las fuentes de riesgo y las posibles vías de migración por las cuales un receptor podría estar expuesto al riesgo. La información sobre el nivel de exposición y la naturaleza del daño causado se combinan para dar una medida de la probabilidad de que se produzca el daño especificado.	A	A	M	SI	FA	FA	FA	FA	FA
	Análisis del impacto en el negocio	Proporciona un análisis de los riesgos de interrupción del negocio como punto clave que podría afectar a las operaciones de una organización, identificando y cuantificando las capacidades que se necesitarían para gestionarlo.	M	M	M	NO	A	FA	A	A	A
	Análisis de árbol de fallos	Una técnica que comienza con un suceso no deseado (máximo suceso) determinando todas las maneras en que podría ocurrir. Se muestran gráficamente en un diagrama de árbol lógico. Una vez que se ha desarrollado el árbol de fallos, deben considerarse las formas de reducir o eliminar las posibles causas y orígenes.	A	A	M	NO	A	NA	FA	A	A
	Análisis de árbol de sucesos	Utilización de un razonamiento inductivo para determinar las probabilidades de los diferentes sucesos iniciadores de los posibles resultados.	M	M	M	SI	A	FA	A	A	NA
	Análisis de causa y consecuencia	Una combinación de análisis de árbol de fallos y sucesos que permite su diferimiento en el tiempo. Se consideran causas y consecuencias de un suceso iniciador.	A	M	A	SI	A	FA	FA	A	A
	Análisis de causa y efecto	Un efecto puede tener un número de factores que pueden agruparse en diferentes categorías. Los factores son identificados a menudo a través de intercambio de ideas y se muestran en un diagrama de estructura o troncal.	B	B	M	NO	FA	FA	NA	NA	NA

Gráfico 32: Continuación

Tipos de técnicas de apreciación de riesgos	Herramientas y Técnicas	Descripción	Relevancia de los factores			¿Puede proporcionar resultados cuantitativos?	Proceso de evaluación del riesgo				
			Recursos y capacidades	Naturaleza y grado de incertidumbre	Complejidad		Identificación del riesgo	Análisis del riesgo			Evaluación del riesgo
								Consecuencia	Probabilidad	Nivel de riesgo	
ANÁLISIS DE FUNCIONES	"Análisis modal de fallos potenciales y sus efectos (ANFE/FMEA FMECA)"	ANFE es una técnica que identifica los potenciales modos de fallos y sus efectos. Existen varios tipos:	M	M	M	SI	FA	FA	FA	FA	FA
	Mantenimiento centrado en la confiabilidad "Análisis de errores de diseño (SNEAK)"	Un método para identificar las políticas que se deben implementar para gestionar errores a fin de lograr de forma eficiente y eficaz la seguridad necesaria, la disponibilidad y la economía de funcionamiento para todos los tipos de equipos.	M	M	M	SI	FA	FA	FA	FA	FA
	"Estudios de riesgos operacionales (HAZOP)	Método para identificar errores de diseño. Una condición insidiosa es una condición latente de hardware, software o integrada que pueda ser el origen de un suceso indeseable o puede evitar un evento deseado no siendo causada por el fallo de un componente. Estas condiciones se caracterizan por su carácter aleatorio y su capacidad para escapar a la detección incluso durante la más rigurosa de las pruebas de sistema normalizado. Las condiciones insidiosas pueden causar un funcionamiento incorrecto, pérdidas de disponibilidad del sistema, retrasos en la programación, o incluso la muerte o lesiones personales.	M	M	M	NO	A	NA	NA	NA	NA
	Estudios de peligros y operabilidad"	Proceso general de identificación de riesgos para definir posibles desviaciones del rendimiento esperado o deseado. Utiliza un sistema basado en palabras clave. Se evalúa la criticidad de las desviaciones.	M	A	A	NO	FA	FA	A	A	A
	"Análisis de peligros y puntos de control críticos (HACCP)"	Un método sistemático, proactivo y preventivo para asegurar la calidad del producto, la fiabilidad y la seguridad de los procesos de medición y control de características específicas que deben estar dentro de los límites definidos.	M	M	M	NO	FA	FA	NA	NA	FA

Gráfico 32: Continuación

Tipos de técnicas de apreciación de riesgos	Herramientas y Técnicas	Descripción	Relevancia de los factores			¿Puede proporcionar resultados cuantitativos?	Proceso de evaluación del riesgo				
								Análisis del riesgo			
			Recursos y capacidades	Naturaleza y grado de incertidumbre	Complejidad		Identificación del riesgo	Consecuencia	Probabilidad	Nivel de riesgo	Evaluación del riesgo
EVALUACIONES DE CONTROL	Análisis de niveles de protección (LOPA)	(Análisis por capas o de barrera). Permite evaluar los controles y su eficacia.	M	M	M	SI	A	FA	A	A	NA
	Análisis del nudo de pajarita	Sencillo croquis para describir y analizar los caminos de un riesgo desde sus orígenes hasta los resultados incluyendo la revisión de los controles. Puede considerarse como la combinación de un árbol de fallos, que permite analizar la causa de un suceso (representado por el nudo de una pajarita) y un árbol de sucesos analizando las consecuencias.	M	A	M	SI	NA	A	FA	FA	A
MÉTODOS ESTADÍSTICOS	Análisis de Markov	Análisis de Markov, a veces llamado análisis estado-espacio, es utilizado en el análisis de sistemas complejos reparables que pueden existir en múltiples estados, incluyendo varios estados degradados.	A	B	A	SI	A	FA	NA	NA	NA
	Simulación Monte Carlo	La simulación de Monte Carlo se utiliza para establecer la variación total en un sistema como consecuencia de variaciones en el sistema, para un número de entradas, donde cada entrada tiene una distribución definida y las entradas están relacionadas con la salida a través de relaciones definidas. El análisis puede utilizarse para un modelo específico donde pueden ser definidas matemáticamente las interacciones de las distintas entradas. Las entradas pueden basarse en una variedad de tipos de distribución de acuerdo con la naturaleza de la incertidumbre que pretenden representar. Para la evaluación del riesgo, se utilizan habitualmente las distribuciones triangulares o distribuciones de beta.	A	B	A	SI	NA	NA	NA	NA	FA
	Estadísticas y redes Bayesianas	Un procedimiento estadístico que utiliza datos de una distribución previa para evaluar la probabilidad de un resultado. El resultado preciso del análisis Bayesiano depende de la precisión de la distribución previa. El modelo de redes Bayesianas tiene un impacto en una variedad de dominios mediante la captura de relaciones probabilísticas de variables de entrada para obtener un resultado.	A	B	A	SI	NA	FA	NA	NA	FA

Tipos de técnicas de apreciación de riesgos	Herramientas y Técnicas	Descripción	Relevancia de los factores			¿Puede proporcionar resultados cuantitativos?	Proceso de evaluación del riesgo				
								Análisis del riesgo			
			Recursos y capacidades	Naturaleza y grado de incertidumbre	Complejidad		Identificación del riesgo	Consecuencia	Probabilidad	Nivel de riesgo	Evaluación del riesgo
ANÁLISIS DE FUNCIONES	Árbol de decisión	Representa alternativas de decisión y sus resultados de manera secuencial, teniendo en cuenta los resultados inciertos. Es similar a un árbol de eventos en que se parte desde un evento o una decisión inicial y se indican diferentes vías y resultados como consecuencia de eventos que pueden producirse y decisiones diferentes que pueden realizarse.					NA	FA	FA	A	A
	Curvas FN	Son una forma de representar los resultados del análisis de riesgos. Muchos eventos tienen una alta probabilidad de resultado de consecuencia baja y una baja probabilidad de resultado de gran consecuencia. Proporcionan una representación del nivel de riesgo que es una línea que describe este rango en lugar de hacerlo en un par de probabilidad único punto que representa una de las consecuencias. Pueden utilizarse para comparar los riesgos, por ejemplo para comparar los riesgos previstos contra criterios definidos como una curva de FN, o para comparar los riesgos previstos con datos de incidentes históricos, o con los criterios de decisión. Pueden utilizarse para el diseño de sistema o proceso, o para la gestión de los sistemas existentes. No son un método de evaluación de riesgo, sino una forma de presentar los resultados de la evaluación del riesgo. Son un método bien establecido para la presentación de resultados de la evaluación de riesgo pero requieren preparación por parte de analistas cualificados y a menudo son difíciles para los no especialistas interpretar y evaluar.					A	FA	FA	A	FA
	Índice de riesgos	Es una medida semicuantitativa de riesgo, una estimación derivada usando un enfoque de puntuación utilizando escalas ordinales. Pueden utilizarse para evaluar una serie de riesgos utilizando criterios similares, por lo que ellos pueden ser comparados. Las puntuaciones se aplican a cada componente de riesgo, por ejemplo características de contaminantes (fuentes), el rango de los caminos de la posible exposición y el impacto sobre los receptores. Son esencialmente un enfoque cualitativo para la clasificación y comparación de los riesgos. Mientras que se utilizan números, esto es simplemente permitir la manipulación. En muchos casos donde el sistema o modelo subyacente no es conocido o no pueden estar representados, es mejor utilizar un enfoque cualitativo más abiertamente.					A	FA	FA	A	FA

Gráfico 32: Continuación

Tipos de técnicas de apreciación de riesgos	Herramientas y Técnicas	Descripción	Relevancia de los factores			¿Puede proporcionar resultados cuantitativos?	Proceso de evaluación del riesgo				
								Análisis del riesgo			
			Recursos y capacidades	Naturaleza y grado de incertidumbre	Complejidad		Identificación del riesgo	Consecuencia	Probabilidad	Nivel de riesgo	Evaluación del riesgo
MÉTODOS ESTADÍSTICOS	Matriz de consecuencia/ probabilidad	Es un medio de valoraciones cualitativas o semicuantitativos de consecuencia y la probabilidad de combinar para producir un nivel de riesgo o clasificación de riesgos. El formato de la matriz y las definiciones aplicadas dependen del contexto en el que se utiliza y es importante que se utiliza un diseño apropiado para las circunstancias.					FA	FA	FA	FA	A
	Análisis Coste beneficio	Pueden utilizarse para la evaluación de riesgo donde se espera que los costos totales sopesen los beneficios esperados totales con el fin de elegir la opción mejor o más rentable. Es una parte implícita de muchos sistemas de evaluación de riesgo. Puede ser cualitativa o cuantitativa o implican una combinación de elementos cuantitativos y cualitativos. CBA cuantitativo agrega el valor monetario de todos los gastos y de todos los beneficios a todos los interesados que se incluyen en el ámbito de aplicación y se ajusta a diferentes periodos de tiempo en el que se acumulan los costos y beneficios. El valor neto actual (VNA) que se produce se convierte en un insumo para las decisiones sobre el riesgo. Un valor actual neto positivo asociado a una acción normalmente significaría que se produzca la acción. Sin embargo, para algunos riesgos negativos, especialmente aquellos que impliquen riesgos para la vida humana o de daños al medio ambiente el principio ALARP podrán aplicarse. Esto divide los riesgos en tres regiones: • Un nivel por encima del cual los riesgos negativos son intolerables y no deben tomarse excepto en circunstancias extraordinarias. • Un nivel inferior que los riesgos son insignificantes y sólo tiene que controlarse para asegurarse de siguen siendo bajas. •Una banda central donde los riesgos son hechos tan bajos como sea razonablemente posible (ALARP). Hacia el extremo inferior de riesgo de esta región, puede solicitar un análisis de coste beneficios estricto pero donde los riesgos son cerrar a intolerable, la expectativa del principio ALARP es que el tratamiento se producirá a menos que los costos de tratamiento son manifiestamente desproporcionado en relación con el beneficio obtenido.					A	FA	A	A	A

Gráfico 32: Continuación

Tipos de técnicas de apreciación de riesgos	Herramientas y Técnicas	Descripción	Relevancia de los factores			¿Puede proporcionar resultados cuantitativos?	Proceso de evaluación del riesgo				
			Recursos y capacidades	Naturaleza y grado de incertidumbre	Complejidad		Identificación del riesgo	Análisis del riesgo			Evaluación del riesgo
								Consecuencia	Probabilidad	Nivel de riesgo	
EVALUACIONES DE CONTROL	Análisis de decisión multicriterio	El objetivo es utilizar una gama de criterios de manera objetiva y transparente, evaluar el valor global de un conjunto de opciones. En general, el objetivo general es producir una preferencia de orden entre las opciones disponibles. El análisis consiste en el desarrollo de una matriz de opciones y criterios que son clasificados y agregados para proporcionar una calificación general para cada opción.					A	FA	A	FA	A

FA: Fuertemente aplicables.
NA: No se aplica.
A: Aplicable
B: baja, M: media
A: alta

Capítulo VIII:

Identificación de Controles

8.1 Identificación de los controles

Ramírez y Ortiz (2011) mencionan que es importante tener en cuenta, como parte de la identificación de controles, las dependencias entre activos y procesos, la cadena de valor, y el valor mismo por activo y proceso. Los procesos deben ser jerarquizados con el objetivo de establecer sus niveles de criticidad. Las vulnerabilidades pueden ser determinadas, por ejemplo, por realización de pruebas y listas de chequeo. Las amenazas se deben clasificar de forma acorde y analizar su impacto con respecto a la frecuencia de ocurrencia, que es importante para la determinación correcta de los riesgos. Por último, para la valoración se pueden usar técnicas cuantitativas y/o cualitativas para la estimación de riesgos (ibíd.: 56-66)..

Estas se clasifican en controles preventivos, de detección, correctivas, manuales o de usuario, de cómputo o de tecnología de información y administrativos, sin embargo, solo nos enfocaremos en los controles que tienen un impacto relevante en los resultados de las entidades:

- Controles para prevenir, detectar y corregir incorrecciones de importancia en los estados financieros.
- Controles básicos para gestionar los riesgos de negocio más significativos para la entidad.

8.2 Indicadores de control

El concepto de indicadores de gestión, remonta su éxito al desarrollo de la filosofía de calidad total, creada en los Estados Unidos y aplicada acertadamente en Japón. Al principio su utilización fue orientada más como una herramienta de control de los procesos operativos que como instrumentos de gestión que apoyaran la toma de decisiones. En consecuencia, establecer un sistema de indicadores debe involucrar tanto los procesos operativos como los administrativos en una organización, y derivarse de parámetros de desempeño basados en la misión y los objetivos estratégicos.

Todas las actividades que se realizan en una empresa pueden medirse con parámetros, que si se enfocan bien con la toma de decisiones gerenciales, nos pueden servir para monitorear por qué camino va la gestión, si es el sentido correcto y si gracias a estos parámetros se pueden evaluar los resultados de la gestión frente a sus objetivos, responsabilidades y metas. Todas estas señales son conocidas como indicadores de gestión.

Los indicadores son una forma clave para retroalimentar un proceso y monitorear el avance o la ejecución de un proyecto y de los planes estratégicos, entre otros. Los indicadores son más importantes todavía si su tiempo de respuesta es inmediato, o muy corto, ya que de esta manera las acciones correctivas son realizadas sin demora y en forma oportuna.

Con frecuencia se dice que no se puede administrar lo que no se puede medir, por lo cual es importante

señalar las principales razones por las que se necesita la medición, y su papel clave en la mejoría de la calidad y de la productividad:

1. Para asegurar que se han satisfecho las expectativas de los clientes.
2. Para estar en posibilidad de establecer objetivos sensibles y cumplirlos.
3. Para proporcionar normas para establecer comparaciones.
4. Para proporcionar visibilidad y un tablero de resultados para que las personas supervisen sus propios niveles de desempeño.
5. Para resaltar los problemas de calidad y determinar qué áreas necesitan atención prioritaria.
6. Para resaltar los problemas de calidad y determinar qué áreas necesitan atención prioritaria.
7. Para proporcionar una indicación de los costos de la calidad y servicio deficiente.
8. Para justificar el uso de los recursos.
9. Para proporcionar retroalimentación para impulsar.

Indicador clave de rendimiento: Son métodos de medida financiera y no financiera que son elegidos por las empresas en general, de forma puntual o permanente. A la vez, suelen ser empleados por la gerencia de riesgos de la empresa con el fin de analizar el progreso hacia la consecución de los objetivos marcados. Estos son:

a) Indicador de calidad en la gestión: Uno de los indicadores más importantes para las empresas que quieren implementar la ISO 31000, es la calidad de servicio y es importante ver que hay dos posiciones distintas por las cuales verlas, la primera es por los clientes que la perciben y la segunda por quienes la ofrecen. Los clientes tienen diferente percepción de la calidad de servicio que están recibiendo de una empresa (es subjetiva); lo que para unos es un servicio de calidad, para otros resulta un servicio normal o correcto. Sin embargo, para estas organizaciones es más una inversión a largo plazo que se mide por resultados.

   Las principales razones por las que calidad de servicio tiene especial importancia son:

   - Las empresas están orientadas finalmente a un gran público, el cual tiene una percepción personal y directa del producto o servicio que estas les ofrecen.
   - Las medidas adoptadas tienen un impacto a mediano y largo plazo.

La identificación de los riesgos, la generación de controles y su clasificación en riesgos económicos, del entorno, estratégicos y operacionales, nos permite contar con un panorama para definir las acciones a seguir.

A manera de ejemplo analizaremos un hospital para reconocer cuales riesgos son de naturaleza exógena para los cuales la gestión de una empresa no puede hacer mucho para su reducción, pero si para mitigar

el impacto de su ocurrencia~~, y~~ aquellos de naturaleza endógena, que pueden ser tratados y minimizados con acciones apropiadas. La mejora de las condiciones de trabajo y la reducción de la exposición de las personas que prestan servicios en el hospital a riesgos biológicos, serán el aspecto a analizar en este ejemplo hipotético que se ha desarrollado para el Hospital El Buen Samaritano. Se trata de un hospital de complejidad alta, ubicado en una zona céntrica de Lima, para el cual se ha preparado una matriz para el análisis de los riesgos biológicos, que estarían catalogados dentro del esquema de riesgo operacional.

En principio, al realizar una evaluación de riesgos es importante definir y catalogar cual es la naturaleza del riesgo que se va a evaluar y por ello se inicia definiendo qué es un riesgo biológico.

Riesgo biológico es un evento adverso relacionado con el uso de agentes biológicos, que puede afectar al hombre, la comunidad y el medio ambiente. El personal de salud enfrenta el riesgo de contraer una infección por numerosos agentes patógenos que se encuentran en diferentes formas diseminados en el ambiente hospitalario. Se trata de un riesgo que el personal de todas las organizaciones de salud debe afrontar.

Tomamos como base una norma, la Directiva 2000/54/EC, que clasifica los agentes biológicos en cuatro grupos de riesgo, según su diferente índice de riesgo de infección:

- Grupo 1: agente biológico que resulta poco probable que cause enfermedad en el hombre.
- Grupo 2: un agente patógeno que pueda causar una enfermedad en el hombre y puede suponer un peligro para los trabajadores, pero es poco probable que se propague a la colectividad. Existen generalmente una profilaxis o un tratamiento eficaces.
- Grupo 3: un agente patógeno que puede causar una enfermedad grave en el hombre y presenta un serio peligro para los trabajadores. Existe el riesgo de que se propague en la colectividad, pero existen generalmente una profilaxis o un tratamiento eficaces.
- Grupo 4: un agente patógeno que pueda causar una enfermedad grave en el hombre y supone un serio peligro para los trabajadores. Existen muchas probabilidades de que se propague en la colectividad y no existen generalmente una profilaxis o un tratamiento eficaces.

Como se observa en esta clasificación, en los hospitales existen diferentes tipos de agentes biológicos que están comprendidos entre los diferentes grupos de la clasificación anterior. En la matriz que expondremos a continuación, se analiza el riesgo por infecciones de transmisión hemática o a través de la sangre.

Gráfico 33: Infecciones de transmisión hemática

1. Nombre del riesgo	Infecciones de transmisión hemática (blood-borne infections)
2. Alcance del riesgo	Se produce en: · Exámenes clínicos efectuados a los pacientes (extracción de muestras de sangre y fluidos del cuerpo) · Procedimientos quirúrgicos · Tratamientos y procedimientos de atención dental. · Tratamiento de heridas · Cuidado de pacientes incapaces de atenderse a sí mismos o que son violentos.
3. Naturaleza del riesgo	Operacional.
4. Interesados	Trabajadores de salud: enfermeras, técnicos, médicos, internos de medicina.
5. Cuantificación del riesgo	Importancia : Alta , probabilidad : alta, sobre todo si no se siguen los protocolos establecidos.
6. Tolerancia del riesgo/ apetito	Potencial de pérdida e impacto financiero: Alta · Probabilidad y tamaño de las pérdidas potenciales. · En el caso que se trate de agentes biológicos de los grupos 1 y 2 la pérdida potencial es limitada. · En el caso que se trate de agentes biológicos pertenecientes al grupo 3 la pérdida es alta. · En el caso que se trate de agentes biológicos del grupo 4, se enfrentan consecuencias catastróficas. Objetivo del control del riesgo y nivel deseado de rendimiento · Se pretende minimizar los riesgos de contaminación por agentes del grupo 2 y proteger al personal de salud y a los pacientes de dichos riesgos. En el caso de producirse, se deben adoptar las medidas inmediatas para contener la infección y dar tratamiento a los afectados. · Se pretende mantener bajo control los riesgos de contaminación derivados de los agentes del grupo 3 y evitar bajo cualquier circunstancia la contaminación por agentes del grupo 4 teniendo en cuenta la repercusión de dicha contaminación.
7. Tratamiento del riesgo y mecanismos de control	Medios primarios por los que se gestiona el riesgo actualmente · Guías de actuación para el trabajo con agentes biológicos para el personal de salud. · Capacitación para el personal de salud. · Uso de equipos de protección. · Protocolos de limpieza y desinfección especiales para centro quirúrgico, laboratorios, áreas de consulta externa, hospitalización, etcétera. · Supervisión del cumplimiento por parte del personal de jefatura en todas las áreas. · Protocolos para la gestión de los desechos hospitalarios.

Gráfico 33: Continuación

	Niveles de confianza en el control existente · A nivel de centro quirúrgico: Alta · A nivel de laboratorios: Media · A nivel de hospitalización y consulta externa: baja (el ingreso de visitantes a las zonas de consulta y hospitalización reduce la efectividad de los controles) · A nivel de gestión de desechos hospitalarios: Media Identificación de protocolos de supervisión y revisión · Existencia de protocolos para la supervisión del personal de enfermería y técnico. · Existencia de protocolos para la aplicación de inyecciones y para extracción, custodia, procesamiento y desecho de muestras biológicas. · Existencia de protocolos para la gestión de desechos hospitalarios. · Existencia de guías de supervisión para el personal médico. · Información fragmentada y diseminada en diferentes departamentos por lo que dificulta que la dirección pueda tener control sobre la situación global en un momento determinado.
8. Acciones potenciales de mejora	· Diseño de un protocolo de cuarentena en caso de infecciones con agentes del grupo 3 y 4. · Uso de equipos de protección: guantes, ropa esterilizada, mascarillas, gafas de seguridad. · Desinfección de las superficies y objetos en contacto con los agentes biológicos. · Capacitación continua al personal de salud sobre el manejo de los agentes biológicos. · Chequeos médicos periódicos al personal de salud · Evitar consumo de alimentos en zonas de posible contaminación de agentes biológicos · Vacunación al personal de atención en salud. (difteria, influenza, hepatitis A, hepatitis B, tétanos, virus del papiloma humano, TBC).
9. Política y estrategia a desarrollar	A este nivel, la responsabilidad recae principalmente en la gerencia general del hospital para la implementación de las políticas y recomendaciones así como de los planes de acción. Además en las jefaturas de departamento, especialmente las de emergencia, centro quirúrgico, banco de sangre, laboratorios, hospitalización y en la de servicios generales: lavandería hospitalaria, esterilización y en gestión de desechos sanitarios para la implementación de los planes y la ejecución de las acciones de control y seguimiento. Estas políticas deben recoger las mejores prácticas y directivas creadas a nivel de la Organización Mundial de la Salud, Organización Panamericana de la Salud, Ministerio de Salud y autoridades sanitarias del país y del mundo.

Como se observa, en una organización compleja puede abordarse el análisis de cada riesgo con gran profundidad, lo que permite determinar cuáles serán las estrategias a realizar, las áreas que estarán involucradas y las acciones a desarrollar en cada caso.

Como quiera que un riesgo tiene impacto en diferentes áreas de una organización, resulta importante comprometer a los diferentes estamentos involucrados y contar con instrumentos que permitan organizar la información disponible y permitir el diseño de estrategias para el control eficaz de los riesgos, pues solo es posible controlar aquello que se conoce.

8.3 Tipos de controles

Los controles son, según Estupiñán y Cano (2006), políticas y procedimientos que ayudan a garantizar que la administración se lleve a cabo y que se direccione el riesgo con las acciones anteriormente estipuladas para cumplir los objetivos de la compañía. Aquellas ocurren en todas las funciones y niveles de la organización.

Este libro se enfocara solo en tipos de control preventivos y detectivos. En el control preventivo se explicará que alcance tiene y que técnicas se pueden utilizar para el desarrollo completo de este tipo de control.

Todas las categorías mencionadas se detallaran en cuadros dinámicos que facilitaran el entendimiento. Sin embargo empezaremos por los tipos de controles, con el fin de poder ir desagregando cada alcance, técnica y categoría según el tipo de control.

Gráfico 34: Tipo de controles preventivos

Controles	Alcance	Ejemplos de técnicas
Preventivos	Proporcionar una seguridad razonable de que únicamente se reconocen y procesan transacciones válidas	Autorización de todas las transacciones.
		Procedimientos de validación de datos previa a su proceso.
		Doble verificación de los datos introducidos en el sistema informático.
		Segregación y rotación de funciones.
		Normas y procedimientos claramente definidos.

Caso contrario ocurre con el tipo de control detectivo. Mencionaremos el alcance que este presenta, junto con algunos ejemplos de técnicas para desarrollar. Las categorías que presenta son:

- De autorización.
- De configuración del sistema.
- Informes de gestión de riesgos
- Controles sobre el "volcado de datos"
- Indicadores clave de rendimientos.
- Supervisión de la dirección.
- Conciliaciones.
- Segregado de tareas.
- Controles de acceso al sistema.

Gráfico 35: Tipo de controles detectivos

Controles	Alcance	Ejemplos de técnicas	Categorías
Detectivos	Aquellos tendentes a proporcionar certeza razonable de que se descubren los errores e irregularidades	Inventarios físicos de las existencias. Utilización de documentación prenumerada. Comparaciones de datos reales con presupuestos. Conciliaciones bancarias. Auditoría interna.	a. De autorización
			b. De configuración del sistema.
			c. Informes de gestión de riesgos
			d. Controles sobre el "volcado" de datos
			e. Indicadores clave de rendimiento.
			f. Supervisión de la dirección.
			g. Conciliaciones.
			h. Segregación de tareas.
			i. Controles de acceso al sistema.

Categorías de controles detectivos

Un control detectivo está diseñado para detectar un acontecimiento o resultado no intencionado. El siguiente gráfico detalla cada una de las categorías de controles detectivos con algunos ejemplos de cuestionarios y las acciones de evaluación.

Gráfico 36: Categoría de controles detectivos: Control de autorización

Controles	Alcance	Ejemplo de cuestionario	Acciones para su evaluación
Controles de autorización	Procedimientos destinados a la aprobación de las transacciones realizadas y de los accesos a activos y expedientes de acuerdo con las directrices de la dirección o con políticas específicas y procedimientos	¿Quién desarrollará la autorización? ¿Existe un manual de procedimiento y es facilitado informáticamente? ¿Hay varios niveles de autorización? ¿Qué directivas son usadas para determinar si la autorización es apropiada (por ejemplo: políticas contables, procesos, manuales, delegación de autoridad)? ¿Son estas seguidas actualmente? ¿Hay alguna posibilidad de saltarse la autorización bien sea manualmente o a través del sistema? ¿Cómo puede ser detectada? ¿Hay algún procedimiento de revisión de la dirección para asegurar que esas autorizaciones se están produciendo (por ejemplo: revisión desde auditoría interna o unidad de control)?	Inspeccionar la documentación de la autorización. Si la autorización es facilitada por el ordenador, desarrollar un sistema que prohíba los procesos desautorizados. Si la supervisión de la dirección se está desarrollando por auditoría interna o por la unidad de control, deberíamos considerar sus conclusiones

Gráfico 37: Categoría de controles detectivos: Controles basados en la configuración del sistema

Categoría	Alcance	Ejemplo de riesgos	Ejemplo de Cuestionario	Acciones para su evaluación
Controles basados en la configura-ción del sistema	Incluyen aquellos filtros establecidos sobre las bases de datos para proteger la información contra procesos inapropiados, según las normas y políticas de la organización, controlando así la integridad de los procesos de generación de información financiera, permitiendo detectar y evitar posibles resultados erróneos en la misma. Estos controles pueden ser estándares (incorporados por defecto en el aplicativo) o hechos a medida (desarrollados por la propia entidad). Dichos controles son contrastados por la entidad antes de su implementación y soportados por este tipo de controles (autorización, diversificación de tareas y auditoría interna).	Límites de envío a proceso. Límites de tolerancia al riesgo. Concordancia con estrategias establecidas. Márgenes de fluctuación de resultados. Validación y chequeo respecto a otros datos. Diseño de campos de entrada. Grupo de autorización. Uso de parámetros de identificación de usuario. Configuraciones de seguridad. Opciones de configuración (por ejemplo, bloqueo del sistema).	¿Cuál es el volumen de transacciones que fluyen a través de este elemento configurado y que tipo de errores/excepciones deben ser detectados? ¿Qué directivas han sido usadas para establecer la configuración? ¿Cómo fue la configuración "original" en esa área? ¿Tiene la entidad documentación sobre los procesos llevados a cabo? Si fuera así, ¿podemos ver dicha documentación? ¿Están los cambios del control de procesos formalizados? ¿Quién será responsable de la configuración? ¿cuál es su experiencia? ¿Están autorizados los cambios? ¿Están las autorizaciones y los deberes de acceso debidamente repartidos?	Comprensión de los cambios y confirmar que el mantenimiento está desarrollado de una forma regularizada. Desarrollar procesos para probar su eficacia. Auditoría informática.

Gráfico 38: Categoría de controles detectivos: Controles basados en informes de gestión de riesgos

Categoría	Alcance	Ejemplo de cuestionario	Acciones para su evaluación
Controles basados en informes de gestión de riesgos	Incluyen la generación de informes dirigidos a los diversos responsables designados tras la supervisión de un proceso desde su inicio hasta su conclusión. Dichos informes suelen recoger las violaciones de las normas establecidas ocurridas durante la ejecución del proceso, o bien, en otras ocasiones se limitan a ofrecer información sobre el mismo (como, por ejemplo: listados de la antigüedad de los saldos mantenidos con agentes y tomadores, de siniestros punta acaecidos, etcétera).	¿Con qué frecuencia se generará? ¿Qué desencadena su ejecución? ¿Será oportuno en el tiempo para la toma de decisiones? ¿Se archivará regularmente? ¿Qué pretenderá detectar la organización cuando obtenga el informe? ¿Se minimiza el riesgo de error en su elaboración?	Revisión del informe relativo a la frecuencia de elaboración y seguimiento de acciones correctivas posteriores. Valorar el conocimiento de los responsables para elaborar el informe. Si el informe se realizó por ordenador, auditoría informática.

Gráfico 39: Categoría de controles detectivos: Controles sobre volcado de datos o interface

Categoría	Alcance	Ejemplo de cuestionario	Acciones para su evaluación
Controles sobre el volcado de datos o interface	Comprende la transferencia de datos de información entre dos sistemas informáticos, usando métodos manuales o automatizados o una combinación de ambos. Los controles sobre el volcado de datos estarían diseñados para asegurar la precisión, exactitud e integridad de los datos que han sido transferidos. Estos controles deberían estar diseñados para poner de manifiesto cualquier error. El proceso de volcado puede ser en dos fases (ir y volver entre los dos sistemas) o en una fase (de un sistema a otro), y puede relacionar un sistema nuevo con los sistemas antiguos o sistemas antiguos con los nuevos.	Aspectos del negocio, como por ejemplo: ¿Cuándo puede el sistema llevar a cabo la interface? ¿Cada cuánto tiempo se puede realizar? ¿Cuántos datos y cuántas transacciones serían procesados? ¿Cuál es el impacto del proceso de interface en las operaciones del negocio habitual? ¿Está sincronizado el sistema antiguo con el nuevo? Aspectos técnicos, como por ejemplo: El método utilizado en la interface (importación/ importación de características del sistema antiguo y/o del nuevo, programa de clientes desarrollados, intermediación del sistema/utilidad–lugar de interés, entrada manual de los datos de interface), Proceso técnico (lote, tiempo real, paralelo). Los contenidos de los datos deben ser llevados a interface (puesta al día de los archivos, resumen de las transacciones, balances).	Los datos y procesos de la interface necesitan ser preparados, es decir: Diseñados. Probados. Realizados (manual o automáticamente). Propios. Mantenidos. Reenviados si es necesario. Revisados. Localizables. Del mismo modo, los cambios deberán ser autorizados, comprobados y documentados. La interface debería velar por la integridad de los datos, su gestión, su elaboración (sin pérdida, ni duplicados ni redundancia de datos y asegurar la exactitud y precisión), su validación y conciliación y la detección y corrección de las excepciones y errores.

Gráfico 40: Categoría de controles detectivos: Controles de indicadores

Categoría	Alcance	Ejemplo de cuestionario	Acciones para su evaluación
Controles de indicadores	Son métodos de medida financiera y no financiera. Son elegidos por la entidad aseguradora y reasegura-dora, de manera puntual o permanente Son empleados por la gerencia de riesgos con el fin de analizar el progreso hacia la consecución de los objetivos marcados. Elegimos aquellos indica-dores que son relevantes para los estados financieros y cuyo nivel de precisión es el adecuado para detectar desequilibrios de una cuantía o naturaleza predefinidos.	¿Con qué frecuencia se preparan los indicadores clave? ¿Quién se encarga de preparar los indicadores? ¿Estos son automáticos o manuales? ¿Cada cuánto tiempo se revisan los indicadores? ¿Las personas que elaboran y revisan los indicadores son las mismas? ¿La elaboración se revisa de acuerdo a los niveles de supervisión? Si fuera así ¿Existe constancia de revisión? ¿Qué puntos de referencia son escogidos en la elaboración de indicadores para la ulterior realización de comparaciones? ¿De qué manera se identifica un punto de referencia elegido como el más adecuado? En caso los puntos de referencia estén basados en datos internos, como presupuestos ¿Quién se encarga de reunirlos? ¿Están eficientemente recopilados? ¿Los indicadores son empleados por el supervisor para medir las expectativas? ¿De qué manera son establecidas las expectativas en relación a las fluctuaciones del indicador? ¿Qué medidas se deben tomar si el supervisor observa que las fluctuaciones del indicador están por encima de lo esperado? ¿Quiénes deben contar con la información sobre los indicadores y las correcciones propuestas? ¿Solo se encarga una persona o un comité de la revisión de indicadores? ¿Cómo son acordadas las diferencias de expectativas? ¿Se elaboran informes sobre los resultados para un auditor externo? ¿El análisis y acciones correctivas de los indicadores externos pueden ser de uso interno?	Valoración de competencias y conocimiento. Identificación del documento, fechas, resumen de revisiones y seguimiento de las acciones realizadas. Inspección de la documentación de los indicadores clave según: - Fecha de preparación. - Documentación sobre las aclaraciones de las fluctuaciones inusuales. - Concordancia con los libros/registros

Gráfico 41: Categoría de controles detectivos: Controles de supervisión de la dirección

Categoría	Alcance		Acciones para su evaluación
Controles de supervisión de la dirección	Supone una supervisión realizada por alguien distinto de quien prepara la información.	En muchos casos, es el propio director que controla el trabajo de un subordinado. De todas formas, no estará limitado a esto. También se contempla que compañeros de trabajo se controlen y revisen mutuamente.	Dicha supervisión debería estar suficientemente documentada con fechas, resumen de revisiones y seguimiento de las acciones realizadas.

Gráfico 42: Categoría de controles detectivos: Controles de conciliaciones

Categoría	Alcance	Ejemplo de cuestionario
Controles de conciliacio-nes	Una conciliación es un control diseñado para comprobar si los asuntos son consistentes.	¿Con qué frecuencia la entidad preparará las conciliaciones? ¿Se preparan manualmente, por sistema informático, o mediante una combinación de ambos? ¿Cómo se confirma si la base de datos ha sido capturada en el proceso de conciliación? ¿Están los procedimientos relativos a la preparación de la conciliación enmarcados dentro de la política de la entidad sobre normas y manual de procedimientos? ¿Con qué fuentes cuenta la entidad para preparar la conciliación? La conciliación, ¿sigue la política de la entidad y los procedimientos de los manuales? ¿Las conciliaciones se preparan conjuntamente con las bases de datos? ¿Qué se considera un error en una conciliación y cómo identifica los errores la entidad? ¿Con qué frecuencia se encuentra un error? ¿Cómo realiza la entidad el seguimiento del control? ¿Está evidenciando de alguna forma? ¿Puede verse algún ejemplo de dicha evidencia? ¿La entidad encuentra errores en los informes que pongan de manifiesto que la información relevante no es correcta?

Gráfico 43: Categoría de controles detectivos, Controles de segregación de tareas

Categoría	Alcance	Ejemplo de cuestionario
Controles de segregación de tareas	Comprende la separación de deberes y responsabilidades para autorizar transacciones, mantener la custodia de los activos o para evitar que los individuos estén en situación de perpetrar y ocultar algún error o irregularidad.	Los procedimiento a segregar, ¿están descritos en las políticas y en los manuales de procedimiento? ¿Hay sistemas de control de acceso que limitan al personal la capacidad de realizar ciertas funciones? ¿Están documentadas las bases para asignar responsabilidades (por ejemplo la descripción del puesto de trabajo? ¿Hay rotación en las responsabilidades? ¿Hay procedimientos en la supervisión de la gerencia para asegurar que la segregación de deberes es adecuada y ha ocurrido como se ha deseado?
Controles de acceso al sistema	Limitarían la capacidad que los usuarios individuales o los grupos de usuarios tienen en un entorno de tratamiento de datos informatizado.	Quedaría reflejado en los derechos de acceso configurados en el sistema.

8.4 Controles básicos sobre el ciclo de producción[24]

Las funciones del ciclo de producción comienzan con el reconocimiento de las necesidades del mercado, siguen con la distribución de la demanda al equipo productivo y la creación de nuevos productos.

Funciones típicas:

- Determinación del precio de los productos (*Pricing*)
- Cálculo de provisiones.
- Valoración de carteras.
- Desarrollo de nuevos productos (I+D).
- Información estadística contable que debe ser remitida al organismo de control.
- Cálculos de margen de solvencia y estados de cobertura de provisiones técnicas incluidos en el análisis patrimonial.

[24] Casares San José-Martí, Isabel (2014): Implementación de la Gestión Integral de Riesgos en el Sector Asegurador bajo la Norma ISO 31000.

Asientos contables comunes:

- Obtención de financiamiento, incluyendo el calendario de pago.
- Compra y venta de inversiones en valores.
- Emisión de acciones y control de autocartera.
- Devengos, cobros y pagos de intereses y dividendos.
- Amortización de empréstitos, descuentos, gastos y primeras diferidos, en relación con deuda e inversiones.
- Compra y venta de monedas extranjeras.
- Cambios en los valores según libros de las inversiones financieras.

Documentos o formatos importantes:

- Listado de tarifas.
- Recibos.

Bases usuales de datos:

Están representadas por aquellos documentos que contienen información necesaria para procesar las transacciones dentro de un bien. Esta información se produce como resultado del proceso de las transacciones. Se clasifican de acuerdo a su uso:

- Bases de referencia como notas técnicas.
- Bases dinámicas, por ejemplo: auxiliares de tarifas, márgenes por productos listados de valoración de cartera, relación de activos afectos a productos y análisis de estados de cobertura de provisiones técnicas, margen de solvencia e información estadístico contable.

Enlaces con otros ciclos:

- Desembolsos de efectivo con el ciclo de prestaciones.
- Pagos al personal con el ciclo de planillas.
- Conciliaciones de efectivo con los ciclos de prestaciones.

8.5 Controles básicos sobre el ciclo de tesorería[25]

Las funciones del ciclo de tesorería empiezan con el reconocimiento de las necesidades de efectivo, siguen con la distribución del efectivo disponible a las operaciones productivas y otros usos y se termina con los cobros y pagos a los deudores y acreedores. Dentro del ciclo de tesorería se pueden distinguir los siguientes asientos contables comunes:

[25] Casares San José-Martí, Isabel (2014): Implementación de la Gestión Integral de Riesgos en el Sector Asegurador bajo la Norma ISO 31000.

- Obtención de financiación y su calendario de pago.
- Amortización de empréstitos, descuentos, gastos y primas diferidos, en relación con deuda e inversiones.
- Emisión de acciones y control de autocartera.
- Cambios en los valores según libros de las inversiones financieras.
- Compra y venta de inversiones en valores.
- Devengos, cobros y pagos de intereses y dividendos.
- Compra y venta de monedas extranjeras.

Algunos ejemplos de los documentos y formatos importantes del ciclo de tesorería pueden ser:

- Contratos de seguro de cambio de moneda extranjera.
- Certificados de acciones.
- Acciones, bonos y otros instrumentos adquiridos como inversiones.
- Acciones emitidas.
- Obligaciones, bonos, papel comercial.
- Títulos de crédito como cheques, pagarés, cartas de crédito, etcétera.

Bases usuales de datos

- Bases de referencia, por ejemplo: libros de registro de accionistas, cuadros de amortización de principal e interés y cuestionario de cumplimiento de estipulaciones de préstamos.
- Bases dinámicas, por ejemplo: saldos de las cuentas bancarias, cartera de inversiones, saldos de mayores auxiliares deudores y acreedores.

Dentro del ciclo de tesorería podríamos distinguir los siguientes enlaces normales con otros ciclos:

- Conciliaciones de efectivo con los ciclos de prestaciones y primas.
- Desembolsos de efectivo con el ciclo de prestaciones.
- Pagos al personal con el ciclo de nómina.
- Ingresos de efectivo con el ciclo de primas.

8.6 Controles básicos sobre el ciclo de planillas

Todas aquellas actividades que se deben llevar a cabo para contratar la mano de obra, pagar y clasificar, resumir y procesar los registros que corresponden al ciclo de planillas.

Este ciclo involucra la contratación, utilización y pago de servicios del personal, tales como: mano de obra directa, mano de obra indirecta, ejecutivos, administrativos, etcétera.

Dado que existen diferencias de tiempo entre la recepción de los servicios del personal y el pago de los mismos, son consideradas también las cuentas por pagar y los pasivos devengados derivados de la obtención de dichos recursos en el ciclo de planillas.

Las funciones de planillas que podrían considerarse como típicas de este ciclo se muestran más adelante. Sin embargo, se debe mencionar que las mismas deberán servir tan solo como una guía general de orientación a la dirección en el proceso de implementación o revisión del control interno. Esto se debe a que la identificación y determinación de estas funciones, asientos contables y documentos importantes, etcétera, se deberán efectuar considerando las circunstancias particulares de la empresa.

Las funciones típicas de planillas podrían ser:

- Promoción y evaluación de personal
- Selección de personal
- Contratación de personal
- Desembolso de efectivo
- Llevar las relaciones laborales
- Registro, información y control de la nómina
- Preparar informes de asistencia

Dentro del ciclo de planillas también se pueden distinguir los siguientes asientos contables comunes:

- Pago de planillas
- Distribuciones de gastos de personal
- Anticipo de sueldos y préstamos al personal
- Otras prestaciones al personal

Algunos ejemplos de formatos y documentos importantes del ciclo de planillas pueden ser:

- Contrato de trabajo
- Informes de tiempo
- Recibos de planillas
- Solicitud de empleo
- Tarjetas de asistencia
- Autorización de ajustes de nómina
- Autorización de pagos especiales
- Cheques

Las bases usuales de datos contienen la información necesaria para poder procesar las transacciones dentro de un ciclo o bien. Esta información se produce como resultado de un proceso de transacciones. Por lo general, están representadas por archivos, catálogos, listas, auxiliares, etcétera.

Estas bases de datos se pueden clasificar según el uso que se les asigne:

- Bases de referencia, se refieren a la información que se utiliza para el proceso de transacciones
- Bases dinámicas, relacionadas con la información resultante del proceso de las transacciones, las cuales se están modificando constantemente.

Las bases usuales de datos para planillas podrían ser las siguientes:

- Archivo de personal, que incluya: nombres e información de referencia del empleado, tipos de retribución, prestaciones a empleados, etcétera.
- Registro de sueldos o salarios de los empleados.

Por otro lado, se pueden distinguir los siguientes enlaces con otros ciclos:

- Asignación de servicios del personal que se enlaza con el ciclo de producción.
- Desembolsos de efectivo que se enlazan con el ciclo de tesorería.
- Resumen de actividades que se enlaza con el ciclo de información financiera.

8.7 Esquema de la normativa interna[26]

En este apartado se ha realizado un primer esquema que servirá de base para el desarrollo del control interno deseado. El objetivo principal es el de poder avanzar en el planteamiento específico de la presente normativa.

El mencionado esquema que contiene los posibles aspectos a regular es:

1. Exposición de motivos
2. Definición de control interno
3. Ámbito de aplicación: Límites de cumplimiento considerando el tamaño de negocio, tipo de negocio, riesgos asumidos, y petición de autorización.
4. Normas generales:
    - Aspectos generales de la organización
    - Responsables del control interno
    - Aspectos de los medios necesarios

[26] Casares San José-Martí, Isabel (2014): Implementación de la Gestión Integral de Riesgos en el Sector Asegurador bajo la Norma ISO 31000.

5. Mecanismos de control
   - Control contable: normas y procedimientos contables, controles sistemáticos de verificación de la aplicación de los procedimientos y de saldos.
   - Aceptación de riesgos: estructuración de manuales de aceptación de riesgos, selección, límites, etcétera; controles sistemáticos sobre la aceptación de riesgos y de saldos con mediadores.
   - Políticas de reaseguro: establecimiento de políticas de retención de riesgos y utilización de reaseguro, controles sobre la calidad del reasegurador, sobre los límites establecidos y sobre la exposición al riesgo.
   - Tramitación de siniestros: desarrollo y diseño de normas y procedimientos de tramitación de siniestros y autorizaciones de pagos, dotaciones de reservas, etcétera; controles sistemáticos de verificación de la aplicación de las normas, de saldos con tomadores, de reservas, etcétera.
   - Control de riesgos financieros: mecanismos de control de exposición a riesgos financieros, riesgos de contraparte asumidos, riesgos en las variaciones en los tipos de interés y análisis de pérdidas potenciales, de las operaciones con derivados, medición de los riesgos asumidos y análisis de escenarios que puedan conducir a pérdidas potenciales.
   - Control de riesgos: verificaciones actuariales de riesgos y posibles desviaciones revisiones sistemáticas de cuantía de provisiones; contrastes sistemáticos de hipótesis utilizadas, realización de simulaciones de evolución de resultados con variaciones en las hipótesis biométricas, estadísticas, de gastos y de escenarios financieros utilizadas. Análisis sistemático del grado de exposición de las aseguradoras a una combinación de factores desfavorables.

Capítulo IX:

Mapa de Riesgos

9.1 Mapas de riesgos por actividades de negocio

Debido a que los riesgos identificados tienen un impacto claro en los procesos básicos de negocio en las entidades aseguradoras y reaseguradoras, ya sea individualmente o conjuntamente, es necesario diseñar controles de alto y bajo nivel que sean preventivos y detectives. Estos controles también deben permitir a la organización enfrentarse a diferentes riesgos estratégicos que puedan afectar al negocio, y garantizar el correcto funcionamiento del proceso establecido.

9.2 Estructura del mapa de procesos de una organización

La definición de los mapas de procesos de una compañía u organización se contempla durante la elaboración de su plan estratégico corporativo, con el objetivo de conocer mejor y más profundamente el funcionamiento y el desempeño de los procesos y las actividades en los que se halla involucrada, prestando una atención especial a aquellos aspectos clave de los mismos.

Los mapas de procesos se definen gráficamente, en lo que se conoce como diagramas de valor, combinando la perspectiva global de la compañía con las perspectivas locales del departamento respectivo en el que se inscribe cada proceso. Su desarrollo, por lo tanto, debe tratar de consensuar la posición local y el desempeño concreto de dichos procesos con los propósitos estratégicos corporativos, por lo que resulta imprescindible identificarlos y jerarquizarlos en función de su definición específica.

A grandes rasgos, podemos identificar 3 tipos de procesos en cualquier compañía u organización. Consiguientemente, la definición de los correspondientes mapas de procesos deberá adaptarse a las peculiaridades que reviste cada caso:

1. Procesos estratégicos: su definición corresponde a los cargos de dirección y gerencia, y atiende principalmente a procesos de gran calado estratégico que condicionan la definición y la consideración de los demás procesos y actividades con vistas a ofrecer un soporte para la toma de decisiones acertadas, fortalecer la operativa del negocio y contribuir a mejorar la perspectiva del cliente.

2. Procesos clave: aportan valor a la relación de la compañía o la organización con sus clientes y usuarios, persiguiendo como fin principal la satisfacción de sus necesidades. En este tipo de procesos hallamos, por ejemplo, los implicados en el diseño, la planificación y la supervisión de la estrategia comercial, de las cadenas de suministros y de los proyectos logísticos, entre otros. El desarrollo y la definición del mapa de procesos para esta tipología debe realizarse de un modo especialmente meticuloso, identificando cada proceso en el punto final de su recorrido

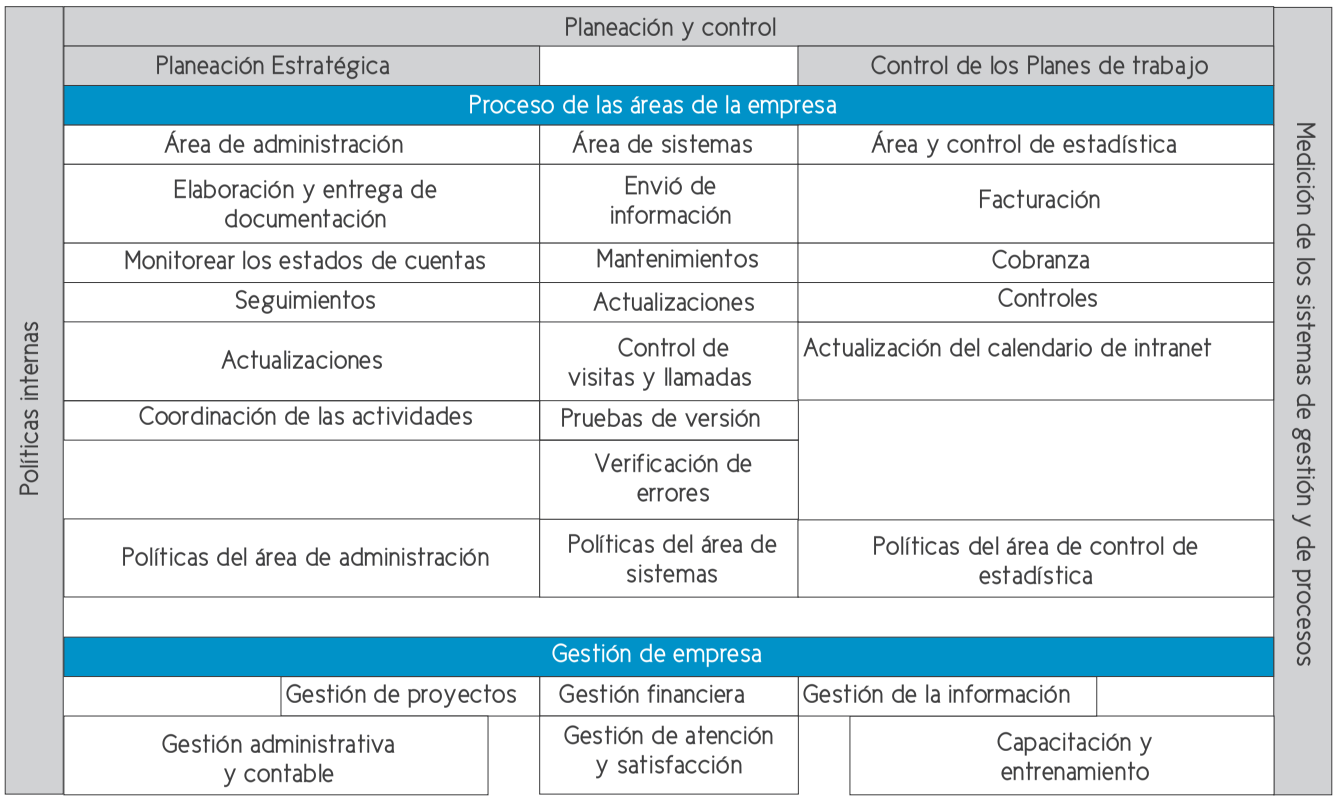
(la prestación del servicio o producto al cliente), y trazando en sentido inverso una línea que nos lleve hasta su punto de inicio, indicando tareas, actividades y subprocesos que directa o indirectamente dependan de él.

3. Procesos complementarios: también llamados procesos de apoyo, complementan a los procesos definidos anteriormente. Pese a ser procesos menores desde un punto de vista estratégico y corporativo, condicionan enormemente el desempeño de procesos superiores y determinan en muchos casos el éxito o el fracaso de los mismos. Las actividades y los procesos relacionados con el abastecimiento de materias primas, con las herramientas, las aplicaciones y los equipos informáticos o con la formación del personal son algunos ejemplos que encajan en esta consideración.

La definición de un mapa de procesos culmina en la elaboración de una ficha por cada proceso identificado, en la que se relacionan los aspectos clave del mismo y los elementos principales que lo conforman, el establecimiento de indicadores de desempeño que permitan monitorizarlo y evaluarlo, y un diagrama que lo sitúe en el lugar que le corresponde según importancia, peso específico y relevancia estratégica dentro del entramado corporativo general.

En el gráfico 43 se desarrolla un ejemplo de mapa de procesos de una organización que empieza en las necesidades del cliente y termina con la satisfacción del mismo. Además del proceso de dirección prestación del servicio, de apoyo y de control junto la evaluación.

Gráfico 44: Ejemplo de mapa de procesos



9.3 Estructura del mapa de riesgos[27]

Se ha establecido un mapa de riesgos general de acuerdo a como está definida la estructura organizativa de la entidad aseguradora:

- Actividad:
  Conjunto de acciones realizadas para alcanzar los objetivos del proceso en el que intervienen.

- Objetivo:
  Se refiere a lo que se consigue por la actividad realizada, la cual debe ir en consonancia con los objetivos estratégicos establecidos por la entidad.

- Riesgo:
  Se refiere a los eventos que pueden acaecer e impedir el correcto desarrollo de la actividad y con ello, el incumplimiento del objetivo establecido.

- Normativa:
  Son las normas de carácter externo (legislación) o interno (manuales de procedimiento o directivas de actuación) que especifican las pautas a seguir en el desarrollo de una actividad.

- Control:
  Se refiere al mecanismo establecido para contrarrestar o anular el impacto del riesgo que afecta al proceso.

- Periodicidad:
  Se refiere a la frecuencia con la que debe ser realizado el control.

- Responsable:
  Es la persona encargada de supervisar el cumplimiento del proceso.

- Recomendaciones:
  Es la evaluación de los controles establecidos.

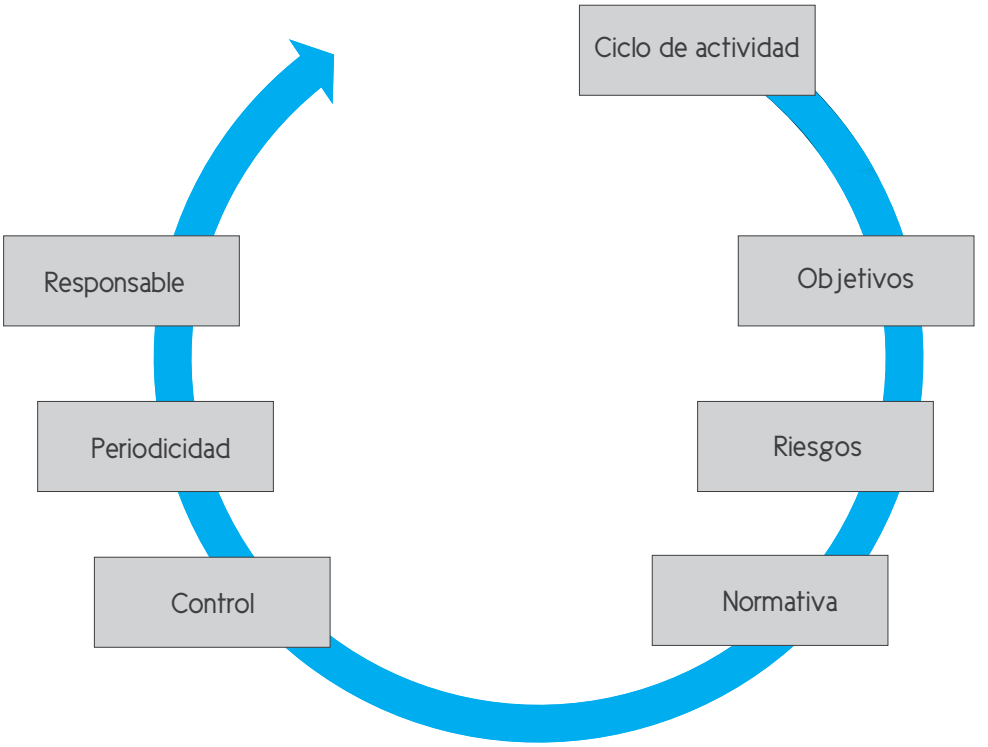
El gráfico 44 resume el mapa de riesgos por actividades de negocio que recoge la información de los ciclos de actividad por cada área o departamento. Para entender mejor debemos definir que es un riesgo. Celaya y López (2004) mencionan, que por riesgo se entiende cuál es la probabilidad de que la empresa no pueda enfrentar alguna situación inherente a su actividad. Esta definición es muy general pero, como veremos más adelante, son por lo menos tres riesgos los que nos permiten evaluar la

[27] Casares San José-Martí, Isabel (2014): Implementación de la Gestión Integral de Riesgos en el Sector Asegurador bajo la Norma ISO 31000.

situación, los resultados y el entorno de la empresa:

a. Riesgo operativo, financiero y total.
b. Riesgo sobre el comportamiento de la rentabilidad.
c. Riesgo del entorno o riesgo-país.

Gráfico 45: Mapa de Riesgo



A continuación se presentan algunos ejemplos que resultan útiles en el momento de elaborar el mapa de riesgos por actividades de negocio de las empresas.

Gráfico 46: Ejemplo de mapa de riesgos del área de administración

Actividad	Objetivo	Riesgo	Normativa	Control	Periodicidad	Responsable
Fijación de objetivos y evaluación del grado de cumplimiento	Establecer directrices de actuación con arreglo a los objetivos estratégicos de la entidad.	Establecimiento de objetivos inalcanzables o en contradicción con los fijados por el consejo de administración.	Normativa legal	Reuniones con el directorio para evaluar el grado de cumplimiento.	Trimestral	Responsable de administración
Selección de riesgos	Aceptación de altas.	Incorrecta selección de riesgos y posibles desviaciones importantes de la siniestralidad.	Normas de contratación interna	Elaboración de estadísticas de siniestralidad y evaluación de las normas existentes	Trimestral	Responsable de administración
Emisión de pólizas	Calidad y rapidez del proceso.	Errores en la introducción de los datos, en la entrega de la documentación.	Manual de procedimientos de emisión	Revisiones de una muestra de pólizas.	Trimestral	Responsable de administración

Gráfico 47: Ejemplo de mapa de riesgos del área de siniestros (I)

Actividad	Objetivo	Riesgo	Normativa	Control	Periodicidad	Responsable
Gestión de expedientes	Asignación adecuada de los expedientes. Eficacia y eficiencia en la gestión (velocidad de liquidación, calidad, control de costes, etcétera). Valoración adecuada.	Falta de fiabilidad de la documentación facilitada o pérdida de información. Insuficiencia de provisiones. Inadecuada asignación de siniestros. Inadecuada valoración.	Normativa legal	Control de los movimientos en cada expediente. Revisión de expedientes.	Relación global de forma anual. Con la periodicidad del evento.	Responsable de del área de seguridad.
Aceptación	Velocidad y agilidad en la realización de tareas. Evitar fraude.	Retraso en la apertura. Falta detección fraude. Insatisfacción del asegurado, tomador del seguro o beneficiario.	Protocolo de apertura. Política de rechazos.	Comprobación de altas. Parte firmado.	Con la periodicidad de la siniestralidad.	Responsable del área de riesgos.

Gráfico 48: Ejemplo de mapa de riesgos del área de siniestros (II)

Actividad	Objetivo	Riesgo	Normativa	Control	Periodicidad	Responsable
Apertura	Velocidad y agilidad en la realización de tareas administrativas.	Escasa o nula información inicial y retrasos en la remisión de datos adicionales. Falta detección fraude. Error en la grabación de datos. Futuras desviaciones producidas por una inadecuada estimación de las provisiones de apertura.	Normativa internas	Establecimiento automático de las provisiones de apertura en función de la garantía. Apertura de expediente. Establecimiento de un modelo de parte de siniestro.	Con la periodicidad del evento	Responsable del área de riesgos y seguridad
Gestión de pagos, recobros y cierre del expediente.	Mejorar la velocidad de liquidación. Calidad de la gestión y satisfacción del mutualista. Reducir el posible coste del siniestro.	Incorrecta selección de riesgos y posibles desviaciones importantes de la siniestralidad.	Normativa legal	Límites de pago. Requerimiento de confirmaciones de pago. Control del número de expedientes.	Mensual	Responsable de siniestros

Gráfico 49: Ejemplo de mapa de riesgos del área técnica

Actividad	Objetivo	Riesgo	Normativa	Control	Periodicidad	Responsable
Bases técnicas: elaboración y adquisición	Garantizar una tarifa adecuada de acuerdo con la siniestralidad y estructura de gastos de la entidad. Cumplimiento de la normativa aplicable	Insuficiencia de prima con el correspondiente desequilibrio técnico y financiero e impacto en resultados. Vulneración de la legalidad vigente en relación con el contenido mínimo exigido.	Normativa legal.	Elaboración y análisis de estadísticas de siniestralidad por factores de riesgo. Análisis de la suficiencia de los recargos para gastos de gestión con respecto a los reales.	Como mínimo una vez al año	Área Comercial
Elaboración de estadísticas	Obtener y analizar ratios de gestión que permitan la toma de decisiones.	Carencia de información para elaborar tales parámetros cálculos erróneos, elaboración de ratios inadecuados.	Protocolo de apertura. Política de rechazos.	Estadísticas de siniestralidad, frecuencia y crecimiento de la cartera.	Mensual (mínimo).	Área de Finanzas

Gráfico 50: Ejemplo de mapa de riesgos del área fiscal y contable

Actividad	Objetivo	Riesgo	Normativa	Control	Periodicidad	Responsable
Gestión de impuestos directos e indirectos	Cumplir con la legislación en vigor en cuanto a plazos y seguridad de la información y ficheros generados.	Sanciones fiscales que supongan gastos extraordinarios para la entidad con el correspondiente efecto en el resultado.	Normativa legal	Revisiones y cuadres.	Según los períodos de declaración.	Área legal de la empresa.
Contabilización de las operaciones	Registrar de acuerdo con la normativa aplicable la totalidad de las operaciones realizadas por entidad.	Incorrecto registro de las operaciones. Manipulación de cuentas. Retrasos	Plan contable.	Formación del personal. Existencia de controles informáticos. Claves de acceso a las aplicaciones.	Aleatoria	Área de contabilidad.
Información a terceros (Información estadístico contable, memoria, etc.).	Proporcionar a tiempo y con la calidad exigida la información requerida por el órgano de control.	Incumplimiento de la legislación vigente. Inexactitud y falta de fiabilidad de la información.	Normativa legal	Controles automáticos. Revisiones por terceros. Auditorías externas.	Trimestral y anual	Área de contabilidad.

Gráfico 51: Ejemplo de mapa de riesgos del área de inversiones

Actividad	Objetivo	Riesgo	Normativa	Control	Periodicidad	Responsable
Gestión de inversiones financieras y materiales.	Obtener una rentabilidad y un nivel de inversiones adecuados a efectos de mantener el margen de solvencia y cobertura de provisiones técnicas. Mantener la liquidez necesaria para dar servicio a los compromisos de la entidad.	Errores de inversión con el correspondiente impacto en la cuenta de resultados. Incumplimiento de la normativa aplicable a efectos de valoración, cobertura y margen de solvencia.	Directrices de inversión dadas al inicio de cada ejercicio (objetivos del año). Plan contable. Leyes y reglamentos. Directrices de la información estadístico contable.	Política de inversiones. Actualización de información respecto a la normativa existente. Registro de inversiones individualizado. Informe de gestión.	Con arreglo a la periodicidad de las compras y ventas. Trimestral y anual (valoración, cobertura y margen).	Responsable de inversiones.

En resumen, se pueden analizar los procedimientos de control encargados a cada área o departamento, cuya finalidad es analizar a través de ellos los controles establecidos, para que puedan estar bien definidos, y obtener los mapas de actividades sobre los que se puedan centrar los riesgos que amenazan el negocio. Esta aproximación debe ser posterior a la ejecución de un conjunto de comprobaciones para analizar la exposición específica a los riesgos generales de una entidad.[28]

[28] Casares San José-Martí, Isabel (2014): Implementación de la Gestión Integral de Riesgos en el Sector Asegurador bajo la Norma ISO 31000.

Capítulo X:

Matriz de Evaluación de Riesgos

10.1 Matriz de evaluación de los riesgos[29]

La matriz de evaluación de riesgos surge de la necesidad de accionar proactivamente los efectos de eliminar o reducir significativamente la gran cantidad de riesgos que puedan afectar los distintos tipos de organizaciones ya sean públicos o privados.

La cantidad de normas y reglamentaciones de carácter laboral, ecológico, impositivo, de consumidores, contable, bancario, societario, bursátil, entre otras, provenientes de organismos nacionales, provinciales y municipales, obligan a las administraciones de las organizaciones a mantenerse muy alerta ante los riesgos que la falta de cumplimiento de las mismas significan para sus patrimonios. Además, debe agregarse la necesidad de constatar el cumplimiento tanto de las normativas internas, como de diversas normas en materia de seguridad y control interno, como verificar la sujeción de las diversas áreas o sectores a las políticas de la empresa.

Sin embargo, debemos tener en cuenta tres definiciones claves para un mejor entendimiento del capítulo.

Impacto: Toda organización debe ser consciente de que su actividad tiene repercusiones en el ambiente en el que opera. Los entornos donde están ubicadas las empresas pueden sufrir tanto externalidades negativas como positivas, que pueden causar un riesgo para la organización.

Características del impacto:

a) Expresan los cambios ocasionados a partir de las acciones de formación. Deben permitir la comparación con la situación anterior a la implementación del programa y en los sucesivos cortes evaluativos programados. Para ello es necesario disponer de la llamada "línea de base" y los momentos de evaluación intermedia, final y de impacto.

b) Reflejan cambios observados en la población objetivo (salarios, empleo, protección social) así como de situaciones expresadas cualitativamente (satisfacción, salud, bienestar).

c) Se definen desde el diseño de las acciones de formación37 y de esa manera se garantiza su solidez y confiabilidad.

d) Deben buscar el retorno económico de las acciones de formación para poder demostrar la utilidad del esfuerzo realizado.

e) Deben ser válidos, es decir comprobar efectivamente aquello que se pretende medir.

[29] Casares San José-Martí, Isabel (2014): Implementación de la Gestión Integral de Riesgos en el Sector Asegurador bajo la Norma ISO 31000.

f) Deben ser confiables. Su valor no depende de quien lo mida pues las variaciones que refleja son efectivamente encontradas en la realidad.

g) Pueden ser cuantitativos y cualitativos, estos últimos están basados en la percepción o el grado de convicción del participante sobre una cierta situación.

Probabilidad (CACPECO: 2008): Es la posibilidad que existe entre varias posibilidades, que un hecho o condición se produzca. La probabilidad, entonces, mide la frecuencia con la cual se obtiene un resultado en oportunidad de la realización de un experimento sobre el cual se conocen todos los resultados posibles gracias a las condiciones de estabilidad que el contexto supone de antemano.

Severidad: Es otra métrica clave en el análisis cuantitativo del riesgo y se define como el porcentaje sobre la exposición en riesgo que no se espera recuperar en caso de incumplimiento.

Gráfico 52: SEVERIDAD = PROBABILIDAD X IMPACTO

Ejemplo 1:

Probabilidad		Impacto				
		Insignificante	Menor	Moderado	Mayor	Catastrófico
		1	2	3	4	5
Casi cierto	Entre 81 y 100—	A	A	E	E	E
Probable	Entre 61 y 80—	M	A	A	E	E
Posible	Entre 41 y 60—	B	M	A	E	E
Improbable	Entre 21 y 40—	B	B	M	A	E
Raro	Entre 1 y 20—	B	B	M	A	A

E: Extremo A: Alto M: Medio B: bajo

Ejemplo 2:

Frecuencia	Consecuencia			
	Catastrófico	Crítico	Marginal	Despreciable
Frecuente	I	I	I	II
Probable	I	I	II	III
Ocasional	I	II	III	III
Remoto	II	III	III	IV
Improbable	III	III	IV	IV
Increíble	IV	IV	IV	IV

El constante avance en el contexto de los riesgos, ha incentivado a buscar herramientas o instrumentos que permitan, como se expresó al inicio, "eliminar o reducir significativamente la gran cantidad de riesgos que puedan afectar los distintos tipos de organizaciones".

Por una parte, una empresa está expuesta a errores internos de buena fe, pero también a acciones que de manera accidental o no, representan pérdidas a la misma. Por ejemplo, si una entidad bancaria se encuentra expuesta al accionar de mala fe de su personal (o incluso, de sus clientes o proveedores), la posibilidad de cometer incumplimientos de normativas legales es mayor por la falta de previsiones en materia de seguridad interna (como pueden ser incendios, o las pérdidas de archivos en el sistema informático). En consecuencia, este tipo de sucesos origina para la entidad pérdidas económicas, pérdidas que, inclusive, pueden poner en riesgo la continuidad de la empresa.

Ahora bien, pensemos en lo que implica la sustracción de fórmulas o planos concernientes a procesos fabriles o productos, o bien la venta ilegal de bases de datos de clientes a la competencia.

Las pérdidas resultantes de defectos en los procesos productivos afectan la calidad de los productos y servicios, y con ello los costos (reprocesamiento, garantías, desperdicios) y la reputación de la empresa. Muy pocas empresas tienen políticas, planes y metodologías sistemáticamente conformadas para evitar los riesgos antes comentados. Generalmente accionan por experiencia, intuición o planifican de manera parcializada.[30]

[30] Casares San José-Martí, Isabel (2014): Implementación de la Gestión Integral de Riesgos en el Sector Asegurador bajo la Norma ISO 31000.

Capítulo XI:

Norma Complementaria: ISO 27001

11.1 Introducción a la norma ISO 27001

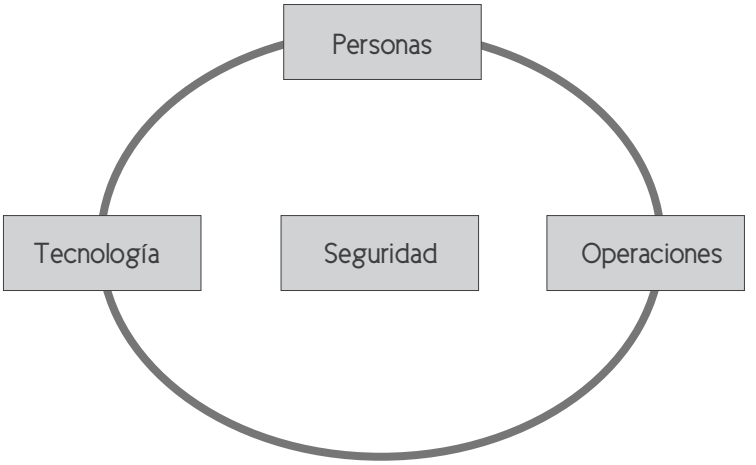
En la actualidad, existe mayor conciencia sobre la importancia de la seguridad de la información en las organizaciones, ya que los sistemas de información constituyen un soporte para los negocios porque contribuyen con la toma de decisiones y manejan, en sí mismos, su activo más importante: la información.

De esta manera, la seguridad de la información debe ser considerada como una forma de proteger los activos del negocio y al mismo tiempo un elemento estratégico para agregarle valor a las empresas y mantenerlas competitivas en el mercado.

Dada la naturaleza de su actividad económica y bajo la premisa que destaca la importancia de la información dentro de las organizaciones, surge la necesidad de diseñar mecanismos que permitan garantizar la confidencialidad, integridad y disponibilidad de la información que se maneja, y proteger los activos de información a través de la implementación de procesos convenientes dentro de una empresa.

En general, los elementos que interactúan dentro de la seguridad de una organización son personas, tecnología y operaciones o procesos. Es así como la seguridad de la organización es el resultado de operaciones realizadas por personas y soportadas por tecnología. La razón principal de la seguridad de la información es la de proteger los activos de información a través de la implementación de los procesos convenientes dentro de la organización.

Gráfico 53: Elementos de la seguridad en la organización



Fuente: OR Perú 2011

En este sentido, se desarrollarán algunos conceptos básicos relacionados con la seguridad de la información (Aenor 2011):

- Seguridad en la organización: Resultado de las operaciones realizadas por personas y soportadas por tecnología.
- Personas: Deben garantizar la seguridad de la información y concientizarse en la necesidad de gestionar la misma en la dirección de la organización.
- Tecnología: Sin un sistema global de gestión de la seguridad, resulta ineficaz.
- Operaciones: Deben sostener la seguridad que la organización requiere a través de una serie de acciones diarias.
- Activos: Elemento que compone los procesos de la comunicación, partiendo desde la generación de la información.
- Activo de información: Elementos que la seguridad de la información busca proteger. Contienen información registrada en medios electrónicos o físicos que se utilizan para la automatización de procesos.

Principios fundamentales del SGSI: Son los pilares sobre los cuales se fundamenta un SGSI.

- Confidencialidad: Su propósito es asegurar que únicamente las personas idóneas accedan a la información que se quiere distribuir.
- Integridad: Consiste en garantizar que los datos, objetos y recursos no han sido alterados en su contenido y son fiables. Se busca que solo las personas autorizadas puedan hacer modificaciones en la forma y contenido de una información.
- Disponibilidad: Asociada a la adecuada estructuración de un ambiente tecnológico y humano que permita la continuidad de las actividades de la organización, la información deberá ser accesible en forma segura para que se pueda usar en el momento en que se solicita.
- Amenazas: Agentes capaces de explotar fallos de seguridad y en consecuencia pueden causar pérdidas o daños a los activos de una empresa, afectando sus negocios. Se considera una amenaza a cualquier evento accidental o intencionado que pueda ocasionar algún daño en un sistema informático o de información, provocando pérdidas materiales, financieras o de otro tipo a una organización.
- Vulnerabilidad: Punto en el cual un activo de información o recurso es susceptible de ataque.
- Impacto: El resultado de un incidente de la seguridad de la información. Efecto de una amenaza en la misión de una organización y objetivos del negocio.
- Sistema de seguridad de la información: Diseñado para proteger los activos de información de la organización al nivel de seguridad necesario mediante el establecimiento y mantenimiento de un conjunto de políticas, procedimientos, controles y bunas prácticas.

11.2 Antecedentes de la norma

En los últimos tiempos, de alguna manera, las organizaciones han visto necesario trabajar bajo los lineamientos de las normas ISO. Por ejemplo, la ISO 9000 desarrolla los temas de calidad, mientras que la norma ISO 14000 tiene un enfoque dentro de la gestión y respeto por el medio ambiente.

Además, existe otra serie de normas ISO que están empezando a desempeñar un papel más importante en el ámbito de la gestión del riesgo. Estas normas son, respectivamente, el código de prácticas para la gestión de seguridad de la información (ISO 17799) y los requisitos de seguridad de los sistemas de seguridad de la información (ISO 27001). Se ha aceptado que hay una relación muy estrecha entre la seguridad de la información y la gestión de riesgos, y esas normas contribuyen a esta relación.

Tanto la ISO 17799 y las norma 27001 se derivan de los múltiples cambios del Estándar Británico BS7799. Originalmente esta norma constaba de dos partes. La primera parte fue adoptada como ISO 17799. En 2005 La segunda parte fue más adoptada como ISO 27001.

La ISO 17799 es un conjunto de pautas que una organización puede utilizar en el desarrollo de un sistema de gestión de seguridad de la información (SGSI). Estas directrices se han desarrollado durante muchos años y han pasado por muchas revisiones. Las directrices son aceptadas internacionalmente como buenas prácticas para la gestión de la seguridad de la información. No existe certificación ISO 17799, ya que es un conjunto de directrices que pueden ser utilizadas para ayudar a garantizar la aplicación y el cumplimiento exitoso de las especificaciones de la ISO 27001.

ISO 27001 es el conjunto de requisitos para el desarrollo de un sistema de gestión de seguridad de la información (SGSI). Esta es la norma de que una organización tendrá que cumplir a fin de recibir la certificación ISO 27001.

11.3 Cumplimiento de normativas y gestión de riesgos

El cumplimiento de la ISO 27001 proporcionará controles para los recursos de tecnología de información que también ayudarán a satisfacer los requerimientos de normas reglamentarias. La profundidad de la norma ISO 27001 puede ayudar a lograr el cumplimiento de otras normas de regulación dependiendo del tipo de controles que se seleccionen y la forma de su implementación.

Uno de los valores más fuertes que aporta la ISO 27001 es un enfoque en el que no hay ningún requisito para un tipo de tecnología específica, es decir, el cumplimiento de la norma puede lograrse teóricamente sin siquiera tener una computadora. Lo que requiere la norma es la selección e implementación de controles relacionados con la TI. De esta manera, este estándar se relaciona estrechamente con la

gestión del riesgo.

Los siguientes son tres puntos clave de la norma en referencia a la gestión de riesgos:

a) Las organizaciones deben definir y documentar su enfoque de evaluación del riesgo {4.2.1c}.

b) "La metodología de evaluación de riesgo seleccionada debe asegurar que las evaluaciones de riesgos produzcan resultados comparables y reproducibles". {4.2.1c}

c) Las evaluaciones de riesgos deben ser revisadas regularmente en intervalos planificados {4.2.3d}.

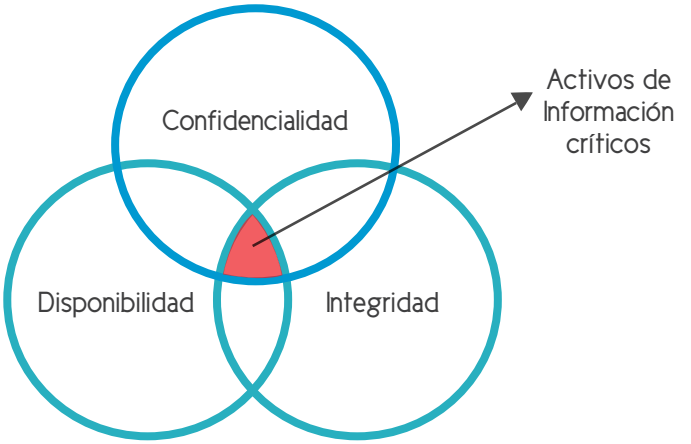
d) Además de lo anterior, la norma también exige que en la selección de los controles, debe haber una relación demostrada entre ellos y los resultados del proceso de tratamiento del riesgo y evaluación de riesgos: "Los objetivos de control y los controles serán seleccionados e implementados para satisfacer las requerimientos identificados por la evaluación del riesgo y el proceso de tratamiento del riesgo. Esta selección tendrá en cuenta los criterios de aceptación de riesgos, así como los requisitos legales, reglamentarios y contractuales." {4.2.1g}.

La norma también incluye las alternativas para el tratamiento del riesgo. Estas alternativas incluyen la prevención de riesgos, aceptación de riesgos, mitigación de riesgos (mediante la aplicación de los controles) y la transferencia de riesgo.

11.4 Sistema de gestión de seguridad de la información (SGSI)

Como se mencionó anteriormente, la norma ISO 27001 es el conjunto de requisitos para el desarrollo de un SGSI. La evaluación, manejo y tratamiento del riesgo se relacionan a lo largo de todo el proceso.

Gráfico 54: Principios fundamentales del SGSI



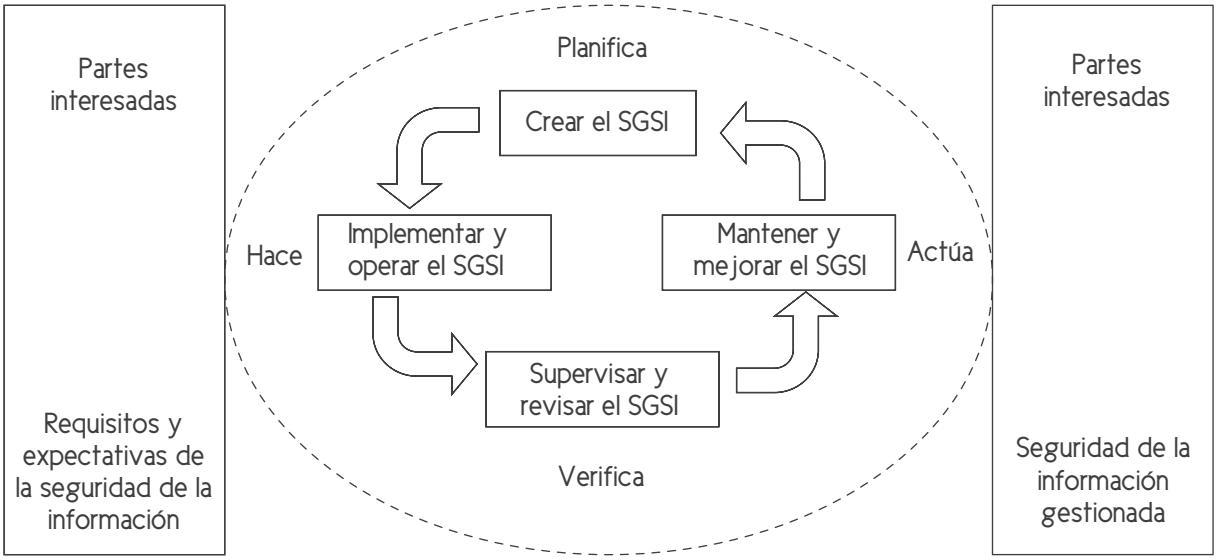
Fuente: Calder, A. Information Security base on ISO27001/27002: A Management Guide

El SGSI se basa en el modelo PHVA: Planificar, Hacer, Verificar y Actuar. Es un proceso cíclico que se debe seguir para asegurarse de que el SGSI y, por defecto, la gestión del riesgo no sean procesos estáticos.

La norma ISO 27001 contribuirá a desarrollar un enfoque de gestión de riesgos que se basa en la selección, implementación, revisión y seguimiento de controles estrictos. El desarrollo de un SGSI y un "enfoque basado en riesgo" son procesos que requieren una importante inversión de tiempo.

La siguiente es una breve descripción de los pasos dentro del ciclo PHVA para la implementación de un SGSI.

Gráfico 55: El ciclo de PHVA aplicado al SGSI



Fuente: AENOR Perú 2011

- Etapa 1 – Planificar: crear el SGSI

  - Definir método de evaluación de riesgos.
  - Identificar los riesgos.
  - Analizar y evaluar los riesgos.
  - Identificar y evaluar las opciones de tratamiento del riesgo.
  - Seleccione el objetivo de control y controles.
  - Gestión de los riesgos residuales.
  - Implementación del SGSI.

- Etapa 2 – Hacer: implementar y operar el SGSI

  - Definir las acciones de gestión, recursos, prioridades, funciones y responsabilidades.
  - Se correlacionan con el plan de tratamiento para la gestión de los riesgos identificados.
  - Implementar los controles.
  - Definir cómo medir la eficacia de los controles.

– Desarrollar e implementar procedimientos para la detección de incidentes.

- Etapa 3 – Verificar: supervisar y Revisar el SGSI

  – Ejecutar procedimientos de seguimiento y revisión.
  – Revisar periódicamente la eficacia del SGSI.
  – Medir la eficacia de controles.
  – Revisar periódicamente las evaluaciones de riesgos y actualización de los riesgos residuales.

- Etapa 4 – Actuar: mantener y mejorar el SGSI

  – Implementación de las mejoras identificadas por SGSI.
  – Adoptar medidas preventivas y correctivas apropiadas.
  – Comunicar las acciones tomadas.
  – Cumplir con los requisitos de documentación.
  – Asegurar el control de documentos.
  – Asegurar el control

Capítulo XII:

Gestión de Proyectos: Enfoque en Riesgos

12.1 Gestión de proyectos

Gestión de proyectos es una forma especializada de gestión, al igual que otras estrategias funcionales, que se utiliza para lograr objetivos de negocio, estrategias y actividades dentro de un programa y presupuesto definidos. La esencia de la gestión del proyecto es apoyar la ejecución de la estrategia competitiva de una organización para ofrecer un resultado deseado (Milosevic 2003). En comparación con el estereotipo tradicional, la literatura reciente reconoce la gestión de proyectos como un proceso clave de negocio (Jamieson y Morris 2004). Este enfoque define una organización como un proceso en lugar de en forma funcional o matricial, y describe la gestión de proyectos como uno de los procesos clave de negocio que permiten a las empresas implementar sistemas que entregan valor. Por lo tanto, cuando las organizaciones vinculan sus proyectos a su estrategia de negocio, están en mejores condiciones para lograr sus metas organizacionales (Srivannaboon 2006).

El enfoque de gestión de proyectos del PMI[31] identifica los elementos que las organizaciones deben alinear con su estrategia de negocios para poder gestionar de manera adecuada los riesgos.

12.2 Conceptos generales (De los Ríos 2009)

El PMI define un proyecto como un esfuerzo temporal que se lleva a cabo para crear un producto, servicio o resultado único.

De esta definición se pueden desprender tres conceptos fundamentales:

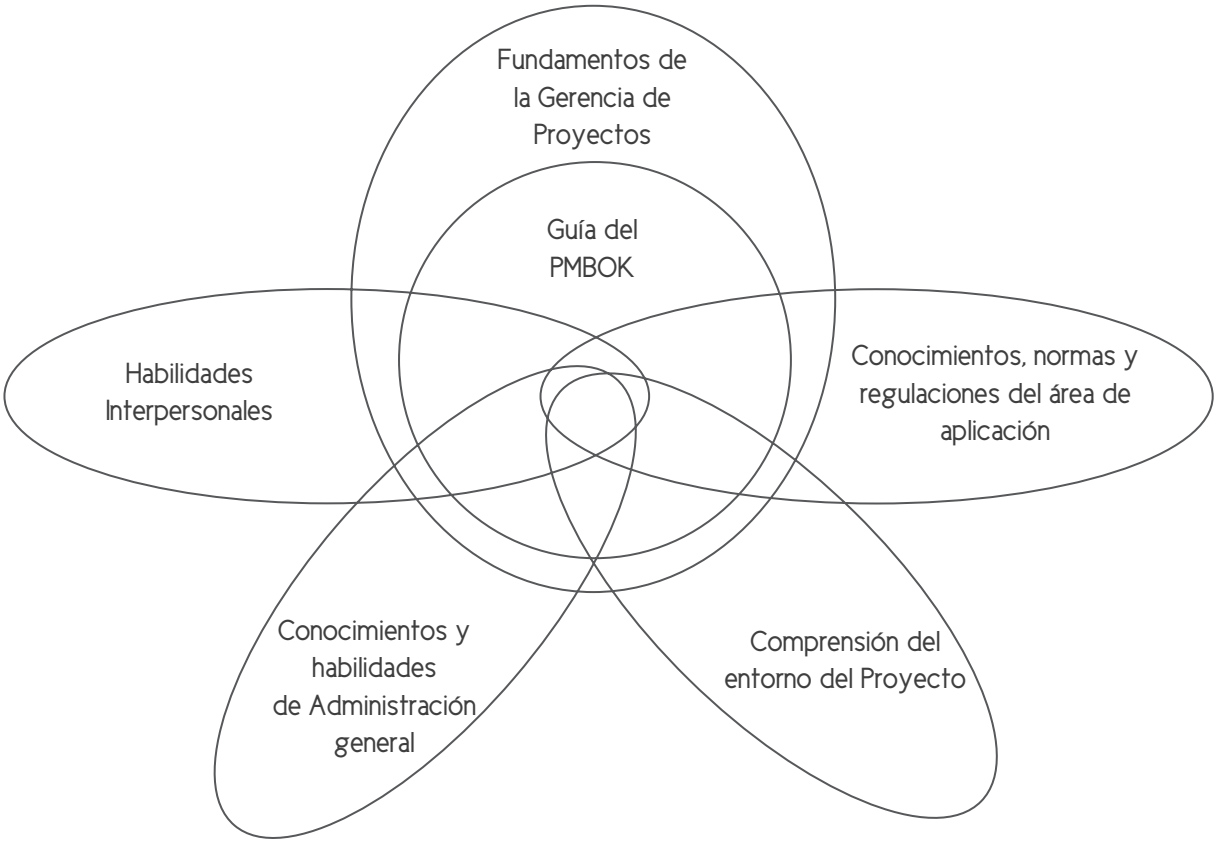
- Tiempo: Un proyecto tiene un inicio y un fin determinado, es decir, no se considera un esfuerzo continuo.
- Resultado: Un proyecto genera un resultado único (producto o servicio).
- Elaboración: Los proyectos se desarrollan de manera gradual de acuerdo al alcance.
- Impacto: Los proyectos se desarrollan en un entorno determinado (económico, político, social, etcétera)

El *Project Risk Management Institute* propone mediante el PMBOK[32] identificar los fundamentos de la dirección de proyectos, reconocido como el resultado de un compendio de buenas prácticas.

[31] El Project Management Institute (PMI) es una organización internacional sin fines de lucro que asocia a profesionales relacionados con la Gestión de Proyectos (tiene una sucursal peruana: www.pmi.org.pe).

[32] "Project Management Body of Knowledge" o "Guía de los Fundamentos de Gestión de Proyectos" es un libro en el que se presentan estándares, pautas y normas para la gestión de proyectos. La quinta edición del libro fue publicada en 2013, bajo la supervisión del Project Management Institute.

Gráfico 56: Guía de PMBOK®



Fuente: PMBOK®

El PMBOK® menciona que estas prácticas pueden aplicarse a la mayoría de proyectos y existe consenso sobre su valor y utilidad. Sin embargo dependerá de cada proyecto la forma en que deban aplicarse, es por esto que se debe contar con un equipo de dirección de proyecto capacitado para responder a cada proyecto de la mejor manera.

El PMBOK® divide la dirección de proyectos en nueve áreas de conocimiento[33], que mediante la gestión de la integración del proyecto son debidamente unificadas para generar el plan de gestión del proyecto.

Una de estas áreas de conocimiento, es la gestión de los riesgos del proyecto, área que se analizará en el presente documento. La gestión de los riesgos, posee seis procesos básicos según el PMI, los cuales son:

a. Planificación
b. Identificación

[33] Gestión de la integración, gestión del alcance, gestión del tiempo, gestión de los costos, gestión de la calidad, gestión de los recursos humanos, gestión de las comunicaciones, gestión de los riesgos y gestión de las adquisiciones del proyecto.

c. Análisis cualitativo
d. Análisis cuantitativo
e. Planificación de la respuesta
f. Seguimiento y control

12.3 Dirección de proyectos

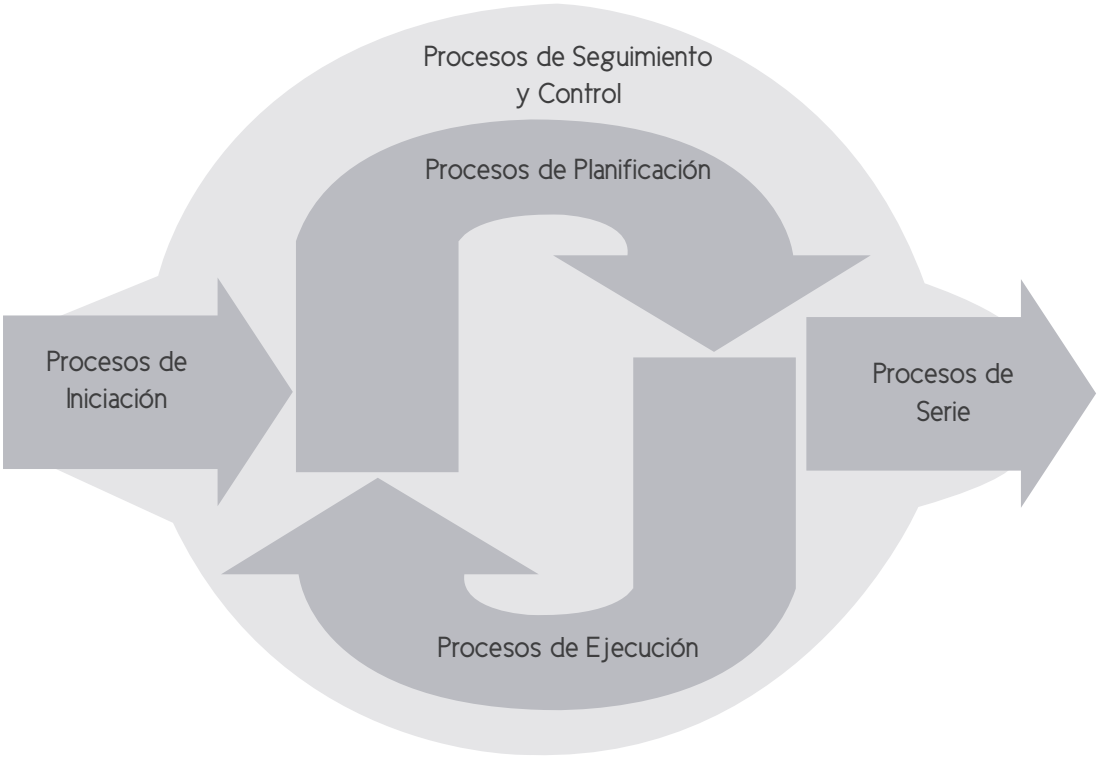
Por otro lado, la dirección de proyectos se define como la aplicación de conocimientos, habilidades, herramientas y técnicas a las actividades del proyecto para satisfacer los requisitos del mismo. La dirección de proyectos se logra mediante la ejecución de procesos, usando conocimientos, habilidades, herramientas y técnicas de dirección de proyectos que reciben entradas y generan salidas (PMBOK).

Así, para asegurar el éxito en la dirección de proyectos es necesario realizar una gestión activa de conocimientos, habilidades, herramientas y técnicas para cumplir con los requisitos interpuestos por los grupos interesados, se definen los llamados "grupos de procesos de la dirección de proyectos".

a) Grupo de procesos de iniciación: Define y autoriza el proyecto o una fase del mismo.
b) Grupo de procesos de planificación: Define y refina los objetivos, y planifica el curso de acción requerido para lograr los objetivos y el alcance pretendido del proyecto.
c) Grupo de procesos de ejecución: Integra a personas y otros recursos para llevar a cabo el plan de gestión del proyecto del proyecto.
d) Grupo de procesos de seguimiento: Mide y supervisa regularmente el avance, a fin de identificar las variaciones respecto del plan de gestión del proyecto, de tal forma que se tomen medidas correctivas cuando sea necesario para cumplir con los objetivos del proyecto.
e) Grupo de procesos de cierre: Formaliza la aceptación del producto, servicio o resultado, y termina ordenadamente el proyecto o una fase del mismo.

A continuación se muestran las áreas de conocimiento de la dirección de proyecto definidas por el PMI:

Gráfico 57: Proceso de seguimiento y control



Fuente: PMBOK ®

El gráfico 57, tomado del PMBOK versión 2013 muestra la relación entre las áreas del conocimiento y las etapas de un proyecto:

Gráfico 58: Grupo de procesos de la dirección de Proyectos

Áreas del conocimiento	Grupo de procesos de la dirección de Proyectos				
	Grupo de procesos de iniciación	Grupo de procesos de planificación	Grupo de procesos de ejecución	Grupo de procesos de monitores y control	Grupo de procesos de cierre
4. Gestión de la integración del proyecto	4.1. Desarrollar el Acta de constitución del proyecto	4.2. Desarrollar el plan para la dirección del proyecto	4.3. Dirigir y gestionar el trabajo del proyecto	4.4. Monitorear y controlar el trabajo del proyecto 4.5 Realizar el control integrado de cambios	4.6. Cerrar el proyecto o fase
5. Gestión del alcance del proyecto		5.1 Planificar la gestión del alcance 5.2 Recopilar requisitos 5.3 Definir el alcance 5.4 Crear la EDT		5.5 Validar el Alcance 5.6 Controlar el alcance	
6. Gestión del Tiempo del Proyecto		6.1 Planificar la gestión del cronograma 6.2 Definir las actividades 6.3 Secuenciar las actividades 6.4 Estimar la duración de las actividades 6.5 Estimar la duración de las actividades 6.6 Desarrollar el cronograma		6.7 Controlar el Cronograma	
7. Gestión del costo del proyecto		7.1 Planificar la gestión de los costos 7.2 Estimar los costos 7.3 Determinar el presupuesto		7.4 Controlar los costos	
8. Gestión de la calidad del proyecto		8.1 Planificar la gestión de la calidad	8.2 Realizar aseguramiento de la calidad	8.3 Controlar la calidad	

Gráfico 58: Continuación

Áreas del conocimiento	Grupo de procesos de iniciación	Grupo de procesos de planificación	Grupo de procesos de ejecución	Grupo de procesos de monitores y control	Grupo de procesos de cierre
9. Gestión de los recursos humanos del proyecto		9.1 Planificar la gestión de los recursos humanoslos Recursos Humanos	9.2 Adquirir el equipo de proyecto 9.3 Desarrollar el equipo del proyecto 9.4 Gestionar el equipo del proyecto		
10. Gestión de las comunicaciones del proyecto		10.1 Planificar la gestión de las comunicaciones		10.3 Controlar las comunicaciones	
11. Gestión de los riesgos del proyecto		11.1 Planificar la gestión de riesgos 11.2 Identificar los riesgos 11.3 Realizar análisis cualitativo de los riesgos 11.4 Realizar análisis cuantitativo de los riesgos 11.5 Planificar la respuesta a los riesgos		11.6 Controlar los riesgos	
12. Gestión de las adquisiciones del proyecto		12.1 Planificar la gestión de las adquisiciones	12.2 Realizar adquisiciones	12.3 Controlas las adquisiciones	12.4 Cerrar las adquisiciones
13. Gestión de los interesados del proyecto	13.1 Identificar intersados	13.2 Planificar la gestión de los interesados	13.3 Gestionar el compromiso de los interesados	13.4 Controlar el compromiso con los interesados	

Fuente: PMBOK ®

En marzo del presente año el PMI publicó el "Exposure Draft" con los cambios propuestos para el PMBOK 5ta edición, con el objetivo de que profesionales miembros del PMI lo revisen y generen sus comentarios. A continuación se comentan los cambios más importantes, como se señala en el gráfico 58.

Cambios más relevantes:

- Creación de una nueva área de conocimiento denominada "Gestión de los interesados del proyecto" (Project Stakeholder Management). En la versión actual del PMBOK, algunos procesos de esta nueva área de conocimiento se encontraban contemplados con un menor alcance en el área de conocimiento "Gestión de las comunicaciones del proyecto". En la nueva edición del PMBOK lo que propone el PMI es expandir el alcance de la "Gestión de los interesados del proyecto" dada su importancia, creando así un nuevo capítulo (el número 13).

  El área de conocimiento contempla los siguientes procesos:

  13.1 Identificar a los interesados (Identify Stakeholders)
  13.2 Planificar la gestión de los interesados (Plan Stakeholder Management)
  13.3 Gestionar el compromiso de los interesados (Manage Stakeholder Engagement)
  13.4 Controlar el compromiso de los interesados (Control Stakeholder Engagement)

- Formalización de los planes de "Gestión de los alcances, tiempos y costos"
- Se incorporaron como procesos la planeación de los alcances, tiempos y costos. Si bien se hacía referencia a estos planes en la 3era edición del PMBOK en las introducciones de sus respectivas secciones (5, 6 y 7) y en "Gestión del alcance" existía un proceso dedicado a la planificación del mismo, en "Tiempos y costos" no habían existido como procesos particulares.

  El área de conocimiento contempla los siguientes procesos:

  6.1 Planificar la gestión del cronograma (Plan Schedule Management)
  7.1 Planificar la gestión de los costos (Plan Cost Management)

- Creación de la sección 1.6 denominada "Valor del negocio" (Business Value). Esta sección incluye un tema que el PMI viene tratando en otros estándares desde hace tiempo como por ejemplo el del OPM3 y es la importancia de que los proyectos que se lleven adelante en las organizaciones generen valor para ellas. Es sumamente importante que las organizaciones desempeñen proyectos alineados a sus objetivos estratégicos.

- Algunos otros ajustes propuestos del PMBOK 2014 son:
  - El proceso "Verificar alcance" se renombra como "Validar el alcance"
  - La cantidad de procesos crece de 42 a 47
  - Se realizan ajustes para asegurar armonía y coherencia con otros estándares del PMI (elaboración de cronogramas, gestión de portafolios, de programas, etcétera)

Gráfico 59: Dirección de proyectos

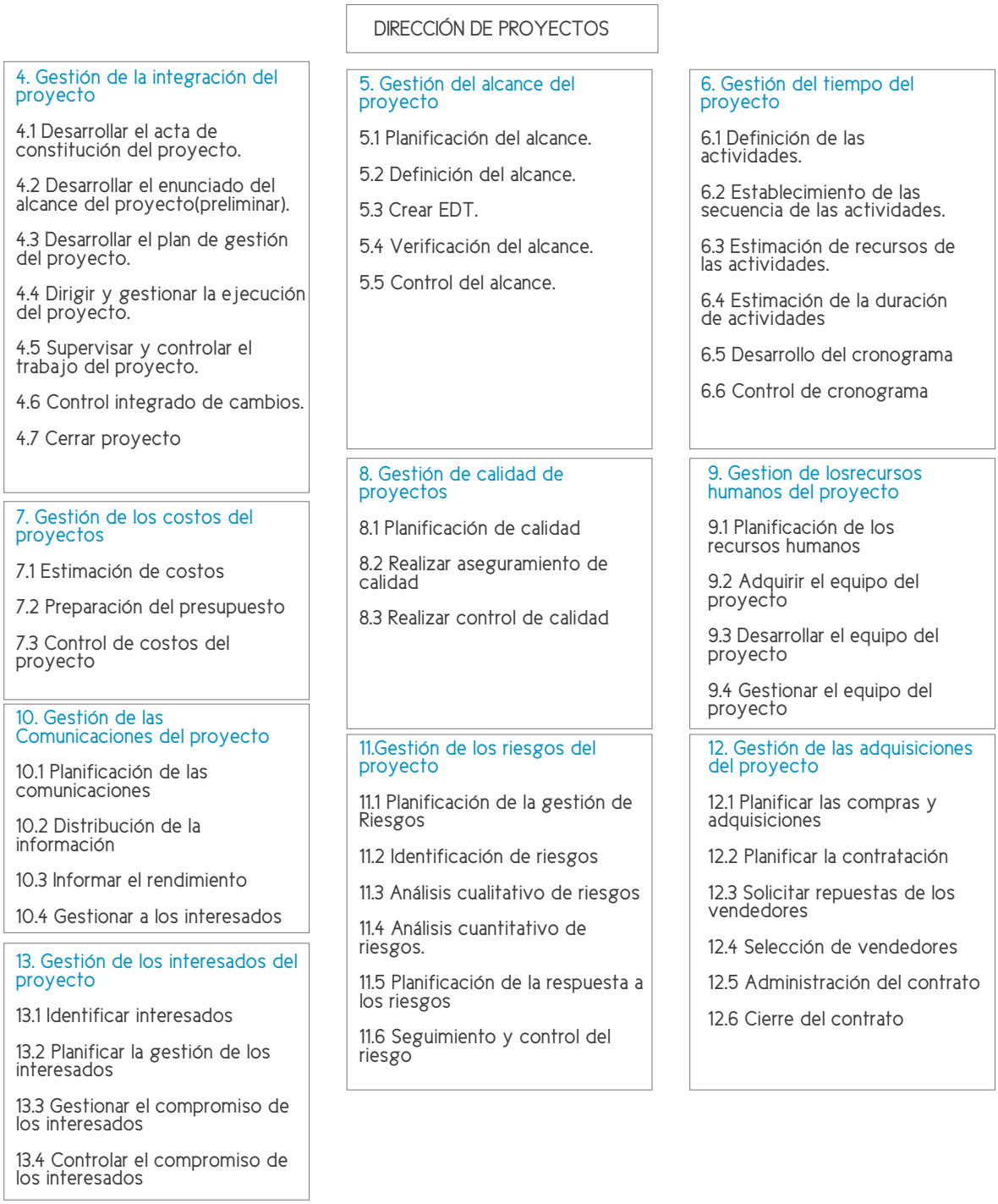


Gráfico 60: Tomado de PMBOK® 5ta edición

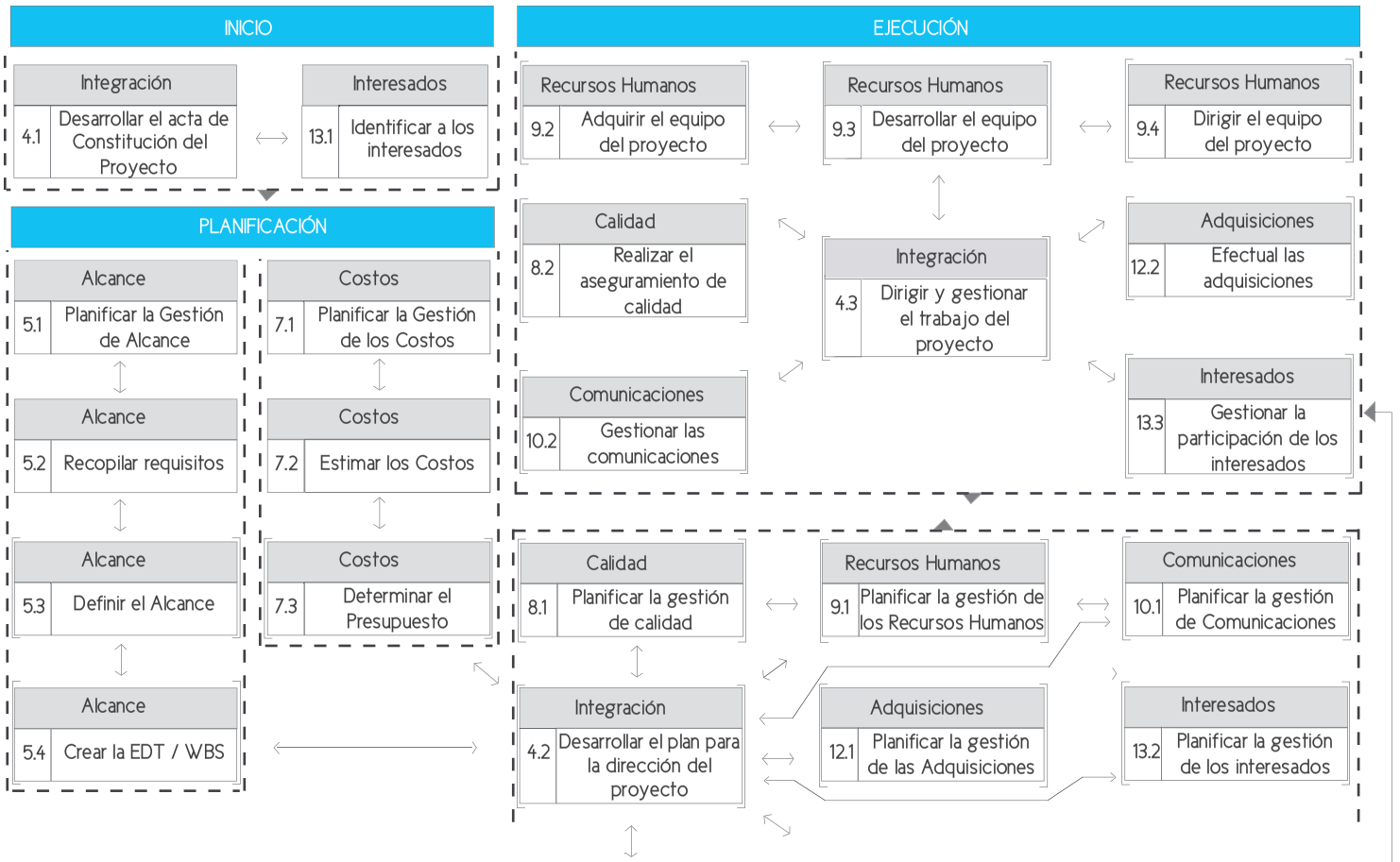
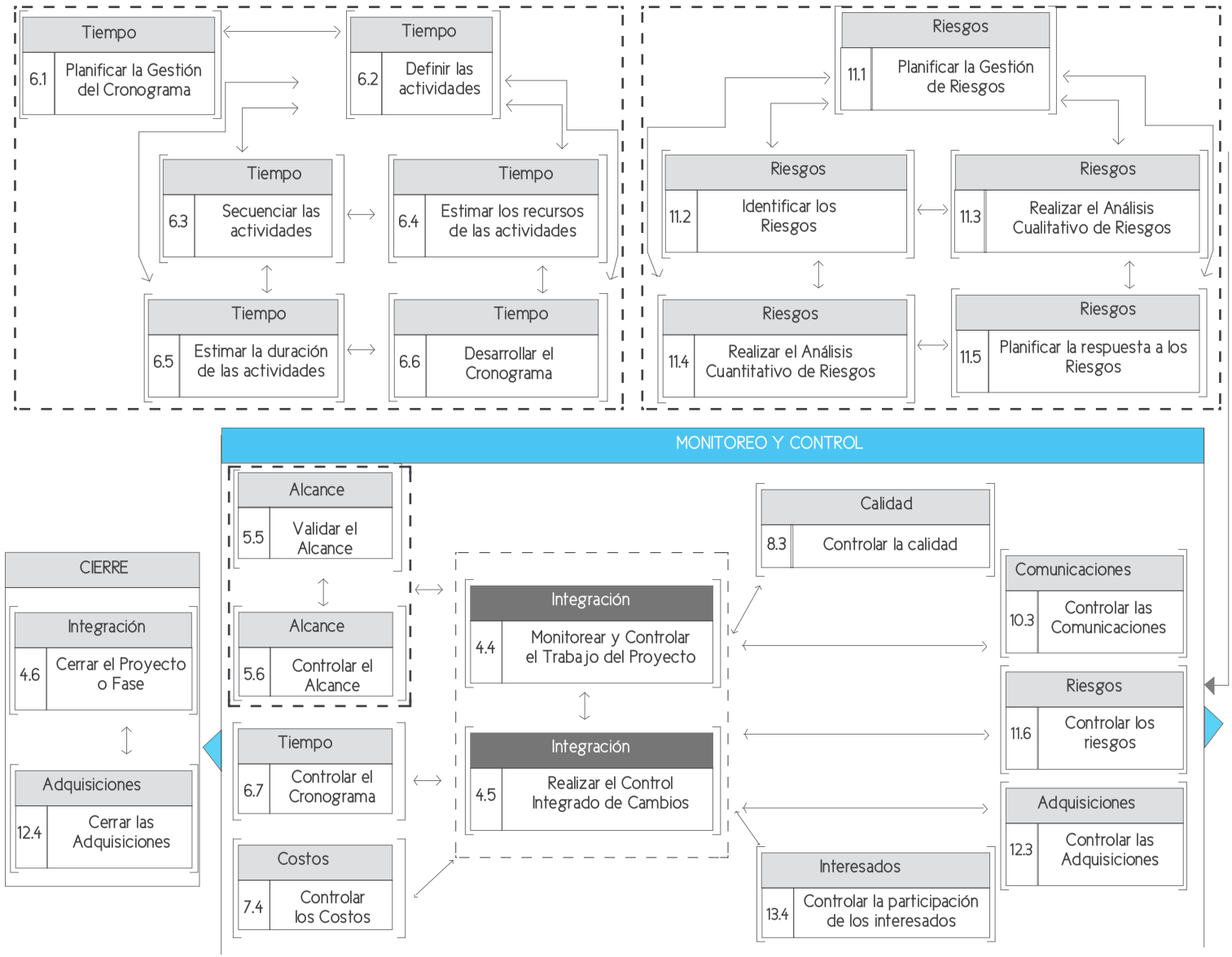


Gráfico 60: Continuación



Y se desarrollan de la siguiente manera:

a) Gestión de la integración: Incluye los procesos y actividades necesarios para identificar, definir, combinar, unificar y coordinar los distintos procesos y actividades de dirección de proyectos dentro de los "Grupos de procesos de dirección de proyectos".

b) Gestión del alcance: Incluye los procesos necesarios para asegurarse que el proyecto incluya los requerimientos para completarlo de manera satisfactoria. La gestión del alcance se relaciona principalmente con la definición y el control de lo incluido y no incluido dentro del proyecto.

c) Gestión del tiempo: Incluye los procesos necesarios para lograr la conclusión del proyecto a tiempo.

d) Gestión de los costos: Incluye los procesos involucrados en la planificación, estimación, preparación del presupuesto y control de costos de forma que el proyecto se desarrolle dentro del presupuesto.

e) Gestión de la calidad: Incluye todas las actividades de la organización ejecutora que determinan las políticas, los objetivos y las responsabilidades relativas a la calidad, de tal forma que el proyecto satisfaga las necesidades por las que se desarrolló.

f) Gestión de los recursos humanos: Incluye los procesos que organizan y dirigen el equipo del proyecto, compuesto por las personas con roles y responsabilidades específicas que permitirán concluir el proyecto.

g) Gestión de las comunicaciones: Incluye los procesos necesarios para asegurar la generación, registro, distribución, almacenamiento, recuperación y distribución de la información del proyecto en tiempo y forma.

h) Gestión de los riesgos: Incluye los procesos relacionados con la planificación de la gestión de riesgos, la identificación y el análisis de riesgos, las respuestas a los riesgos, y el seguimiento y control de riesgos de un proyecto. Los objetivos de la "Gestión de los riesgos del proyecto" son aumentar la probabilidad y el impacto de los eventos positivos, y disminuir la probabilidad y el impacto de los eventos adversos para el proyecto.

i) Gestión de las adquisiciones: Incluye los procesos para comprar o adquirir los insumos necesarios para realizar el proyecto.

j) Gestión de los interesados: Los interesados del proyecto son un conjunto de personas,

organizadas por un interés en común, con el fin de actuar conjuntamente en defensa de ese interés, queriendo dar a conocer sus pretensiones. Se denomina grupo de presión a los que utilizan los medios a su alcance buscando la manera de dominar a la opinión pública. A menudo los grupos de interés son de conocimiento público, como los sindicatos, las organizaciones patronales, las grandes empresas, las asociaciones de profesionales, las ONG, etcétera.

La mayoría de la sociedades modernas reconocen legitimidad a los grupos de interés y regulan las modalidades de su accionar, de modo que no afecten la forma en que se encuentra regulada en cada país la toma de decisiones políticas. Una modalidad característica de la canalización institucional de los grupos de interés son los consejos económicos y sociales que existen en varios países. Es habitual que los grupos de interés realicen sobre los poderes públicos una actividad particular denominada lobby, con el fin de tratar de incidir a su favor en el proceso de toma de decisiones públicas.

Todas estas áreas del conocimiento poseen entradas bien definidas, técnicas y herramientas identificadas, las cuales varían considerablemente en función del alcance, tipo de proyecto y salidas, que se convierten en el entregable final de cada área de conocimiento. Todos los planes de gestión definidos brevemente se integran para conformar el plan de gestión del proyecto, herramienta de la dirección y del equipo de proyecto para realizarlo en forma exitosa. La gestión de riesgos de proyectos según el PMI consiste en el proceso de identificar y analizar los riesgos, así como la respuesta, seguimiento y control de los mismos[34].

12.4 Gestión de riesgos en proyectos

Entre los conceptos fundamentales[35] dentro de la gestión de riesgo de proyectos se deben tener en cuenta:

- Riesgo de proyecto: Cualquier evento o condición que puede impactar de manera negativa los objetivos de un proyecto. Si el impacto es positivo, se refiere a una oportunidad.
- Evento de riesgo: Hecho aislado que puede impactar al proyecto de manera positiva o negativa.
- Condición de riesgo: Situación en que se encuentra presente el riesgo.

a) Planificación de la gestión de riesgos: Establecer el entorno del proyecto para definir el enfoque que se utilizará para evaluar y analizar las actividades de gestión de riesgo del proyecto.

b) Identificación de riesgos: Determinar los riesgos que pueden afectar al proyecto y documentar sus características. La identificación se realiza seleccionando una herramienta para su detección como: entrevistas a expertos, checklists, brainstorming, etcétera.

c) Análisis cualitativo de riesgos: Priorizar los riesgos identificados para realizar un análisis

[34] Fuente: PMBOK 2015
[35] Project & Process Management Consulting International, Risk Management for Project Manager, PMI, 2013.

de acuerdo a la probabilidad o frecuencia de ocurrencia y a la significancia del impacto de los mismos. A partir de la clasificación obtenida se debe desarrollar una matriz de evaluación de riesgos, de acuerdo a las combinaciones probabilidad-impacto resultantes.

d) Análisis cuantitativo de riesgos: Analizar de manera objetiva el efecto de los riesgos identificados de acuerdo a los datos recolectados.

e) Planificación de la respuesta a los riesgos: Desarrollar estrategias de acuerdo al perfil de riesgo de la organización. Es decir, escoger alternativas para aprovechar las oportunidades y reducir las amenazas que pueden presentar los riesgos detectados en el proyecto.

f) Seguimiento y control de riesgos: Realizar el seguimiento de los riesgos identificados, supervisar los riesgos residuales de acuerdo a los controles seleccionados, identificar nuevos riesgos, ejecutar planes de respuesta y evaluar su efectividad a lo largo del ciclo de vida del proyecto.

Se definen tres estrategias básicas para enfrentar los riesgos, cuyos efectos podrían impactar de manera negativa los objetivos de un proyecto:

a) Evitar: Implica eliminar la amenaza que representa un riesgo adverso, aislar los objetivos del proyecto del impacto del riesgo o hacer más realista el objetivo en cuestión considerando el riesgo.

b) Transferir: Trasladar el impacto negativo de una amenaza a un tercero, es decir, simplemente se cambia la responsabilidad de la gestión del riesgo.

c) Mitigar: Reducir la probabilidad y/o el impacto de un evento de riesgo adverso a niveles aceptables. Anticipar acciones para reducir la probabilidad de la ocurrencia de un riesgo y/o su impacto sobre el proyecto.

Gráfico 61: Gestión de los riesgos del proyecto

GESTIÓN DE LOS RIESGOS DEL PROYECTO

11.1 Planificación de la Gestión de Riesgos

1. Entradas
   - 1 Factores ambientales de la empresa.
   - 2 Activos de los procesos de la organización.
   - 3 Enunciado del alcance del proyect o.
   - 4 Plan de gestión del proyecto.
2. Herramientas y Técnicas
   - 1 Reuniones y análisis de planificación.
3. Salidas
   - 1 Plan de gestión de riesgos.

11.2 Identificación de Reisgos

1. Entradas
   - 1 Factores ambientales de la empresa.
   - 2 Activos de los procesos de la organización.
   - 3 Enunciado del alcance del proyecto.
   - 4 Plan de gestión de riesgos.
   - 5 Plan de gestión del proyecto.
2. Herramientas y Técnicas
   - 1 Revisiones de documentaciones
   - 2 Técnicas de recopilación de información.
   - 3 Análisis de listas de control.
   - 4 Análisis de asunciones.
   - 5 Técnicas de diagramación.
3 Salidas
   - 1 Registro de riesgos.

11.3 Análisis Cualitativo de Reisgos

1 Entradas
   - 1 Activos de los procesos de la organización.
   - 2 Enunciado del alcance del proyecto.
   - 3 Plan de gestión de riesgos.
   - 4 Registro de riesgos.

2 Herramientas y Técnicas
   - 1 Evaluación de probabilidades e impacto de los riesgos.
   - 2 Matriz de probabilidades e impacto de los riesgos.
   - 3 Evaluación de la calidad de los datos sobre riesgos.
   - 4 Categorización de riesgos.
   - 5 Evaluación de la urgencia del riesgo.

3 Salidas
   - 1 Registro de riesgos (actualizaciones)

Gráfico 61: Continuación

11.4 Análisis Cuantitativo de Reisgos

1. Entradas

1 Activos de los procesos de la organización.

2 Enunciado del alcance del proyecto.

3 Plan de gestión de riesgos.

4 Registro de riesgos.

5 Plan de gestión del proyecto

– Plan de gestión del cronograma del proyecto

– Plan de gestión de los costes del proyecto

2. Herramientas y Técnicas

1 Técnicas de recopilación y representación de datos

2 Técnicas de análisis cuantitativo de riesgos y de modelado.

3. Salidas

1 Registro de riesgos (actualizaciones)

11.5 Planificación de la Respuesta a los Riesgos

1. Entradas

1 Plan de gestión de riesgos.

2 Registro de riesgos.

2. Herramientas y Técnicas

1 Estratégias para riesgos negativos o amenazas.

2 Estratégias para riesgos positivos u oportunidades.

3 Estratégia común ante amenazas y oportunidades.

4 Estrategia de respuesta para contingencias.

3. Salidas

1 Registro de riesgos (actualizaciones)

2 Plan de gestión del proyecto (actualizaciones)

3 Acuerdos contractuales relacionados con el riesgo.

11.6 Seguimiento y Control de Riesgos

1. Entradas

1 Plan de gestión de riesgos.

2 Registro de riesgos.

3 Solicitudes de cambio aprobadas.

4 Información sobre el rendimiento del trabajo.

5 Informes de rendimiento.

2. Herramientas y Técnicas

1. Reevaluación de los riesgos.

2. Auditorías de los riesgos.

3. Análisis de variación y de tendencias.

4. Medición del rendimiento técnico.

5. Análisis de reserva.

6. Reuniones sobre el estado de la situación.

3. Salidas

1 Registro de riesgos (actualizaciones)

2 Cambios solicitados.

3 Acciones correctivas recomendadas.

4 Acciones preventivas recomendadas.

5 Activos de los proecesos de la organización. (actualizaciones)

6 Plan de gestión del proyecto. (actualizaciones)

Fuente: PMBOK®

Capítulo XIII:

Gestión Integral de Riesgos Financieros

13.1 Otros temas asociados al riesgo

- Gestión integral de riesgos financieros: Una empresa es afectada en su gestión por la incertidumbre, el principal reto de la alta gerencia es determinar cuál es el nivel de incertidumbre que debe aceptar para cumplir con su objetivo de generar valor para sus grupos de interés o *stakeholders*[36]. Según PwC[37], "la Gerencia moderna que debe afrontar escenarios con incertidumbre, maximiza su valor cuando logra un balance óptimo entre crecimiento, retorno de inversión, riesgo, oportunidades, eficacia y eficiencia" (Espiñeira et al. 2008).

La alta gerencia debe detectar los eventos internos y externos que pueden afectar el cumplimiento de los objetivos y los riesgos asociados a ellos, para que de esta manera se puedan tomar decisiones conociendo la criticidad que se debe enfrentar y no basadas en el azar, es decir, *"Take Risk by Choice, not by Chance".*

Uno de los factores claves de éxito que debe cumplir la gerencia se refiere a la organización funcional que soporta la gestión integral de riesgos (GIR). Se entiende en la práctica que la GIR es "efectuada por todo el personal en los diversos niveles de la institución".

Por ejemplo, la industria bancaria está experimentando un profundo cambio en lo relativo a las prácticas de gestión del riesgo gracias a los progresos registrados en la teoría de las finanzas y en las tecnologías de la información. (Basilea II y Basilea III) Esta evolución en la gestión del riesgo ayuda a conseguir ventajas competitivas en los diferentes niveles de la gestión.

De esta manera, la Gestión Integral de Riesgos (GIR) permite gestionar el negocio maximizando la creación de valor, ser conscientes del nivel de rentabilidad esperada, eliminando actividades que no generen el adecuado valor y tener un grado adecuado de transparencia respecto al verdadero valor del negocio, tema de relevancia para los accionistas e inversionistas.

A continuación se dividirá en cuatro partes la administración integral de riesgos para su mejor comprensión:

La primera parte se refiere al riesgo de eventos, por ejemplo el riesgo político y el riesgo exógeno, entre otros, como se puede ver en el gráfico 61.

La segunda parte se refiere al riesgo operacional, que según el Comité de Basilea[38] es el riesgo de pérdidas resultantes de la falta de adecuación, fallas en los procesos internos, de la actuación del personal o de los sistemas, o bien aquellas que sean producto de eventos externos.

En una visión simplificada, es el riesgo que incurre un banco por su operatoria, que no está ya clasificado

[36] Individuo u organización que está directa o indirectamente involucrada o se ve afectada por las actividades o decisiones de una organización en particular.
[37] Nombre abreviado de la empresa PricewaterhouseCoopers.
[38] El Comité de Basilea es la denominación usual con la que se conoce al Comité de Supervisión Bancaria de Basilea, la organización mundial que reúne a las autoridades de supervisión bancaria, cuya función es fortalecer la solidez de los sistemas financieros.

como riesgo de crédito o de mercado o los otros ya tradicionales, y que ha cobrado gran notoriedad dada la mayor participación de operatorias tercerizadas, sistemas tecnológicos complejos, productos derivados y estructurados, y una mayor diversidad de negocios financieros.

La tercera es riesgo de negocio, que puede ir incluido dentro de los riesgos estratégicos de una organización. Los riesgos estratégicos son aquellos que surgen derivados de la posición estratégica que la organización toma en el entorno en que desarrolla su actividad, por tanto tienen una doble fuente: por un lado las propias decisiones estratégicas que toma la organización y por otro el entorno en el que dichas decisiones se materializan. Es todo lo que afecta a la organización en su macroentorno. En ese sentido, se pueden distinguir:

- Riesgos de negocio: Riesgos de las decisiones estratégicas sobre los productos y servicios o sobre la propia organización.

- Riesgos no de negocio: Riesgos externos derivados del entorno de la organización, por ejemplo de sus competidores, reguladores, autoridades públicas, sociedad, etcétera.

El cuarto es el riesgo financiero, que es la probabilidad de un evento adverso que tenga consecuencias financieras negativas para una organización. El concepto debe entenderse en sentido amplio, incluyendo la posibilidad de que los resultados financieros sean mayores o menores de los esperados. De hecho, habida la posibilidad de que los inversores realicen apuestas financieras en contra del mercado, movimientos de estos en una u otra dirección pueden generar tanto ganancias o pérdidas en función de la estrategia de inversión.

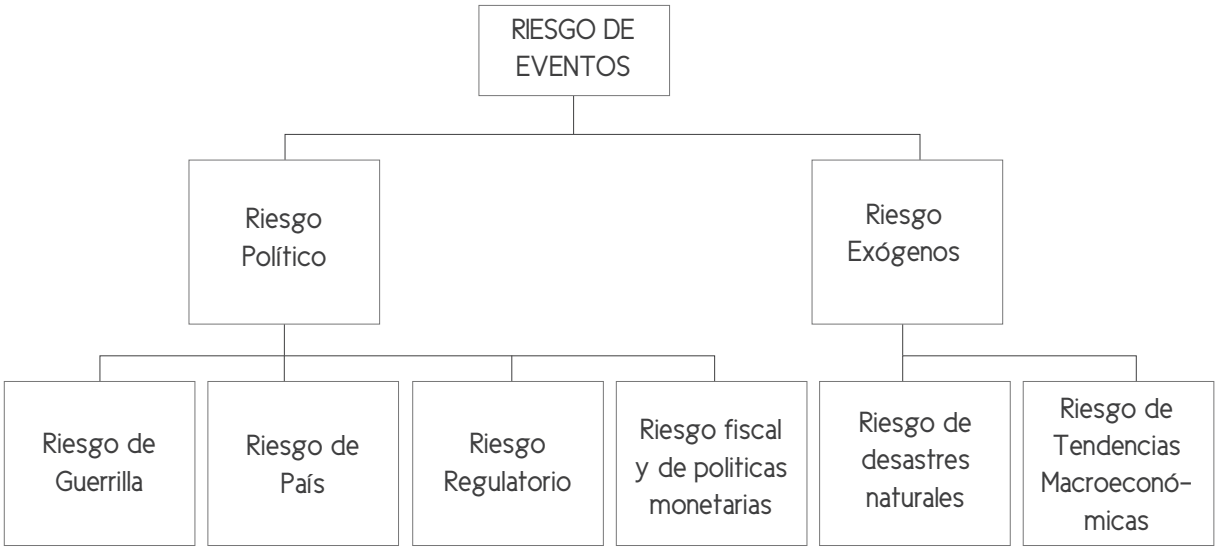
Más allá de la definición de los cuatro riesgos mencionados, lo importante para los bancos respecto del riesgo operacional es contar con un proceso de gestión de riesgos operativos o riesgos operacionales. Este proceso de análisis de riesgo operacional es el que va a garantizar al banco la buena administración de los riesgos en el marco de los estándares internacionales.

Según el Comité de Basilea, tanto en los principios básicos para una supervisión bancaria efectiva como en Basilea II y III, en un adecuado proceso de gestión del riesgo operacional se entiende por "gestión" al proceso de "identificación, evaluación, seguimiento y control o cobertura" del riesgo operacional. Estos cuatro elementos reflejan un enfoque comprehensivo de gestión de riesgos presentes en los Tres Pilares de Basilea II, y en todos los documentos y mejores prácticas del Comité de Basilea, y por ende en todas las normativas sobre riesgo operacional de todos los países avanzados del mundo.

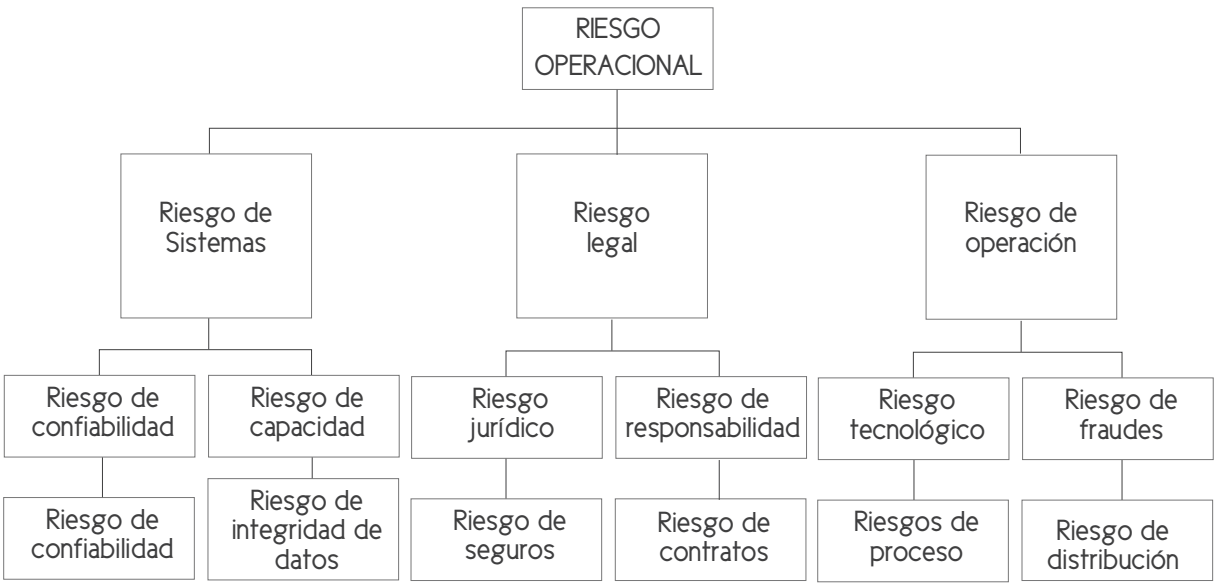
De la misma forma, se puede mencionar al riesgo del negocio que se divide en riesgo administrativo, riesgo estratégico y riesgo financiero.

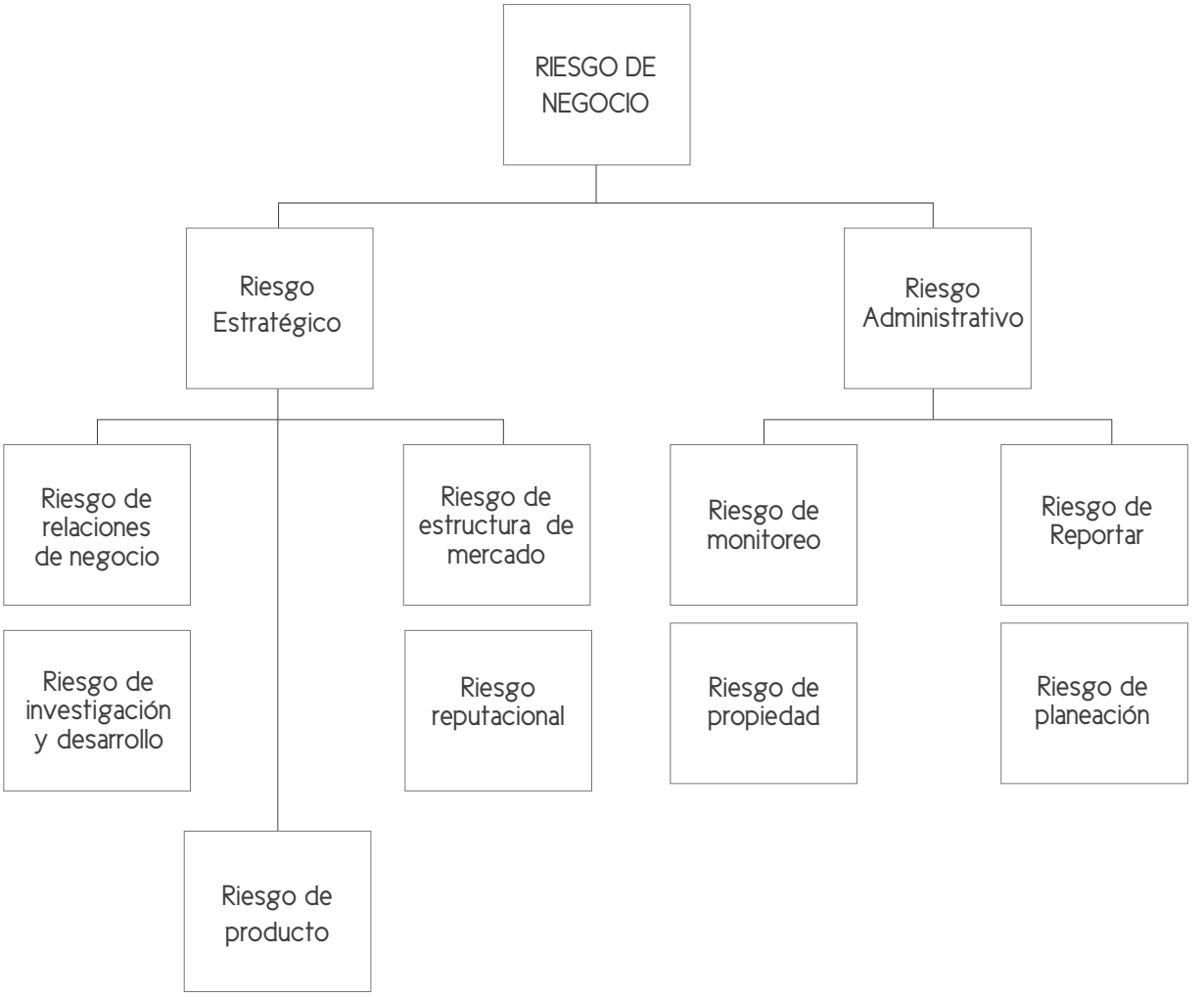
Gráfico 62: Administración integral de riesgos

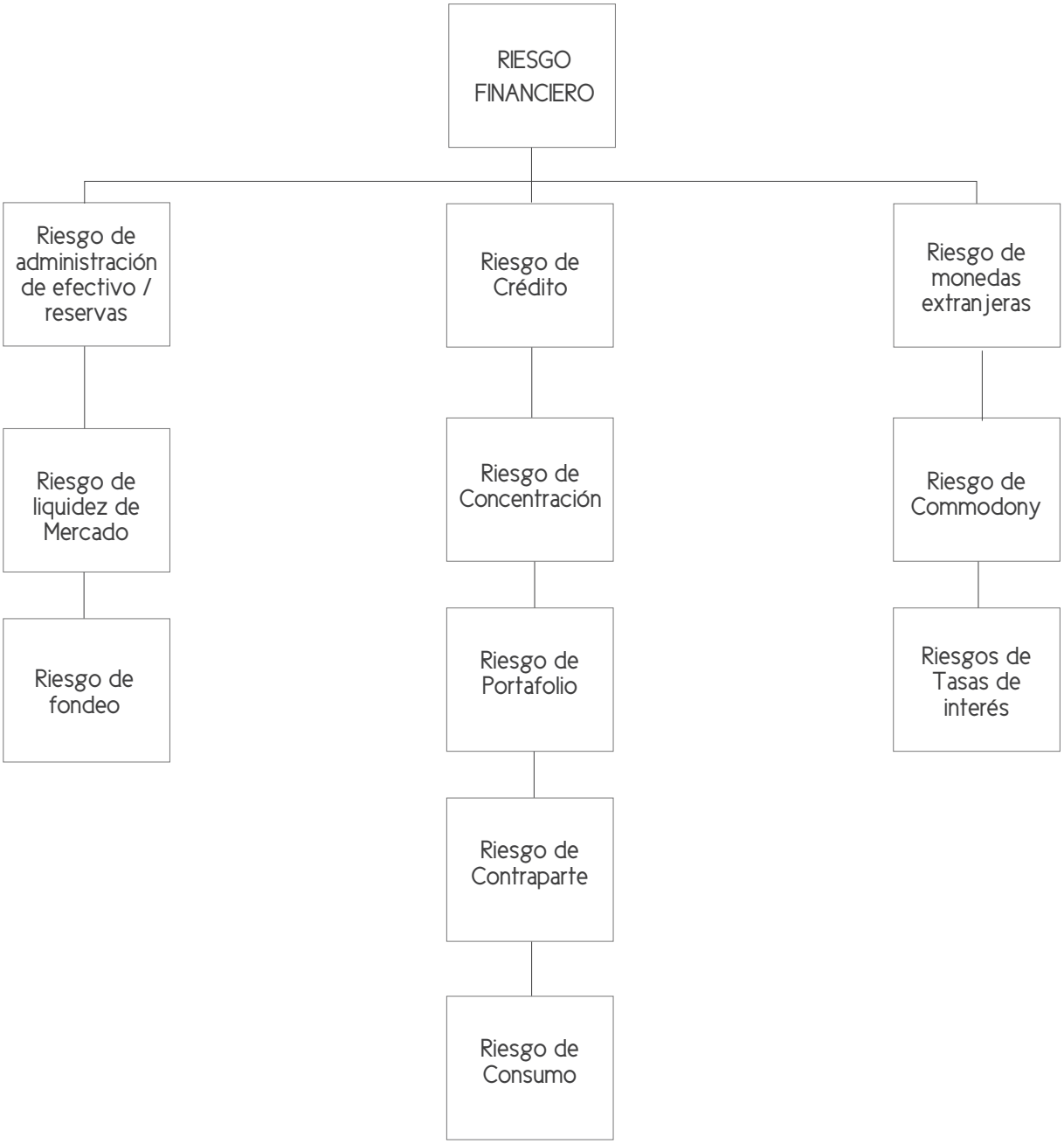
PARTE I



PARTE II




RIESGO DE NEGOCIO
Riesgo Estratégico
Riesgo Administrativo
Riesgo de relaciones de negocio
Riesgo de estructura de mercado
Riesgo de monitoreo
Riesgo de Reportar
Riesgo de investigación y desarrollo
Riesgo reputacional
Riesgo de propiedad
Riesgo de planeación
Riesgo de producto


RIESGO FINANCIERO
Riesgo de administración de efectivo / reservas
Riesgo de liquidez de Mercado
Riesgo de fondeo
Riesgo de Crédito
Riesgo de Concentración
Riesgo de Portafolio
Riesgo de Contraparte
Riesgo de Consumo
Riesgo de monedas extranjeras
Riesgo de Commodony
Riesgos de Tasas de interés

13.2 Introducción a los riesgos financieros

Los riesgos financieros son los riesgos asociados a los mercados financieros –donde las empresas obtienen sus recursos o los colocan—asociados, entre otras cosas, a realizar estrategias que permitan reducirlos o mitigarlos, siendo, los principales el riesgo de mercado, el riesgo de crédito, el riesgo de liquidez y el riesgo operacional.

Las entidades financieras tienen como objetivo principal el control de los riesgos financieros a los que se enfrentan, siendo el riesgo de crédito y el riesgo de mercado los de mayor importancia. Sin embargo, la evolución de los estudios sobre la medición y control de estos riesgos es desigual, ya que mientras los estudios sobre el riesgo de mercado se encuentran muy avanzados, ocurre todo lo contrario con respecto al riesgo operacional y de liquidez (Berggrun y Alonso 2015).

Riesgo es una medida de la magnitud de los daños frente a una situación peligrosa. El riesgo se mide asumiendo una determinada vulnerabilidad frente a cada tipo de peligro. Si bien no siempre se hace, debe distinguirse adecuadamente entre peligrosidad (probabilidad de ocurrencia de un peligro), vulnerabilidad (probabilidad de ocurrencia de daños dado que se ha presentado un peligro) y riesgo (propiamente dicho). Informalmente se habla de riesgo para hablar de la ocurrencia ante un potencial perjuicio o daño para las unidades, personas, organizaciones o entidades (en general "bienes jurídicos protegidos").

Cuanto mayor es la vulnerabilidad, mayor es el riesgo, pero cuanto más factible es el perjuicio o daño, mayor es el peligro. Por tanto, el riesgo se refiere solo a la teórica "posibilidad de daño" bajo determinadas circunstancias, mientras que el peligro se refiere solo a la teórica "probabilidad de daño" bajo esas circunstancias. Por ejemplo, desde el punto de vista del riesgo de daños a la integridad física de las personas, cuanto mayor es la velocidad de circulación de un vehículo en carretera mayor es el "riesgo de daño" para sus ocupantes, mientras que cuanto mayor es la imprudencia al conducir mayor es el "peligro de accidente" (y también es mayor el riesgo del daño consecuente).

Es importante indicar que en finanzas, suele entenderse el riesgo como la probabilidad de enfrentar pérdidas. Sin embargo, en sentido estricto debe entenderse como la probabilidad de observar rendimientos distintos a los esperados, es decir, "...la dispersión de resultados inesperados ocasionada por movimientos en las variables financieras" (Jorion 1997: 63). Si se observan rendimientos extraordinariamente positivos o negativos, la probabilidad de enfrentar rendimientos distintos a los esperados en el futuro, es decir, el riesgo, crece. Si no se considera como una señal de alerta el observar rendimientos muy superiores a los esperados, se omite el análisis de las causas de tal desempeño extraordinario y, por lo tanto, se construyen las bases para enfrentar en el futuro pérdidas también extraordinarias.

Dado que la única forma de evitar por completo el riesgo es no existir, la necesidad de administrarlo es tácita. Por lo tanto, primero deben identificarse, en finanzas, todos los factores que pueden ocasionar

la obtención de rendimientos distintos a los esperados, es decir, los factores de riesgo. Cada factor distinto define en sí mismo un tipo particular de riesgo, dentro de los cuales nos interesan los riesgos financieros.

Existen diversas formas de identificar y clasificar los riesgos financieros. En general, entenderemos como riesgo financiero la probabilidad de obtener rendimientos distintos a los esperados como consecuencia de movimientos en las variables financieras. Los principales tipos de riesgo revisados por diversos autores, incluyendo el comité de Basilea II y Basilea III, son:

Gráfico 63: Principales categorías de riesgos financieros

Principales categorías de riesgos financieros
Riesgo de mercado
Riesgo de crédito
Riesgo de liquidez
Riesgo país
Riesgo de taza de interés
Riesgo cambiario
Riesgo legal
Riesgo operacional
Riesgo reputacional

Fuente: En aproximación a diversos autores:
(Park. S. 1997; Jorion O. 1999; Portillo Tarragona 2001; Soldevilla E. 1996).

1. Riesgo de mercado: Resultado de la variación de los precios o valores de mercado (tasa /precio) de un instrumento o transacción financiera.

2. Riesgo de crédito: Es la posibilidad de pérdida debido al incumplimiento del prestatario o la contraparte, en operaciones directas, indirectas o contingentes que conlleva el no pago, el pago parcial o la falta de oportunidad en el pago de las obligaciones pactadas, generando pérdida o reducción de valor (calidad) de la cartera o portafolio.

3. Riesgo de liquidez: Asociado al stock, cantidad o liquidez de los activos en donde se desea invertir. Es decir, cuando una transacción no se realiza a precios de mercado debido a su baja operatividad.

4. Riesgo país: Riesgo de una eventual insolvencia comercial o financiera por parte de un vendedor o prestamista, a causa de problemas de carácter político o derivados de las graves perturbaciones

económicas que pueden darse, de forma relativamente frecuente en los países en desarrollo. El riesgo país obliga a contratar seguros especiales, con primas muy elevadas, así como a hacer previsiones en la cuenta de pérdidas y ganancias de los prestamistas. Tiene dos vertientes que son el riesgo soberano y el riesgo de transferencia.. Se mide por el spread de los bonos del "país" contra los bonos del tesoro de E.U.A. de similar maduración.

5. Riesgo de tasa de interés: Se refiere a la posibilidad de pérdidas futuras en el conjunto del balance, como consecuencia de descalces en los vencimientos de las operaciones activas, pasivas y de fuera de balance, ante movimientos adversos en el tipo de interés.

6. Riesgo cambiario: Afecta a la posición competitiva de la empresa frente a sus rivales, sea en su mercado doméstico o en los mercados internacionales. Asimismo, puede generar importantes pérdidas o ganancias a empresas importadoras o exportadoras de acuerdo de su estructura de financiamiento y forma de ventas.

7. Riesgo legal: Es el riesgo de pérdidas que podrían generarse por cambios en las leyes, regulaciones e incumplimiento de compromisos de pago de obligaciones contractuales de una contraparte.

8. Riesgo operacional: Es el riesgo de obtener pérdidas derivados de riesgos de operación (fraude), riesgo tecnológico (fallas en el sistema o plataforma), riesgo legal (contratos) y riesgo regulatorio.

9. Riesgo reputacional: Es la probabilidad de deterioro de la relación con los grupos de interés como resultado de una percepción negativa sobre el comportamiento de la empresa.

Según Gary L. Gastineau, dentro de los riesgos financieros encontraremos otros tipos más específicos de factores de riesgo como: riesgo cambiario, riesgo commodity, riesgo accionario, riesgo tasa, entre otros, y propone la siguiente clasificación:

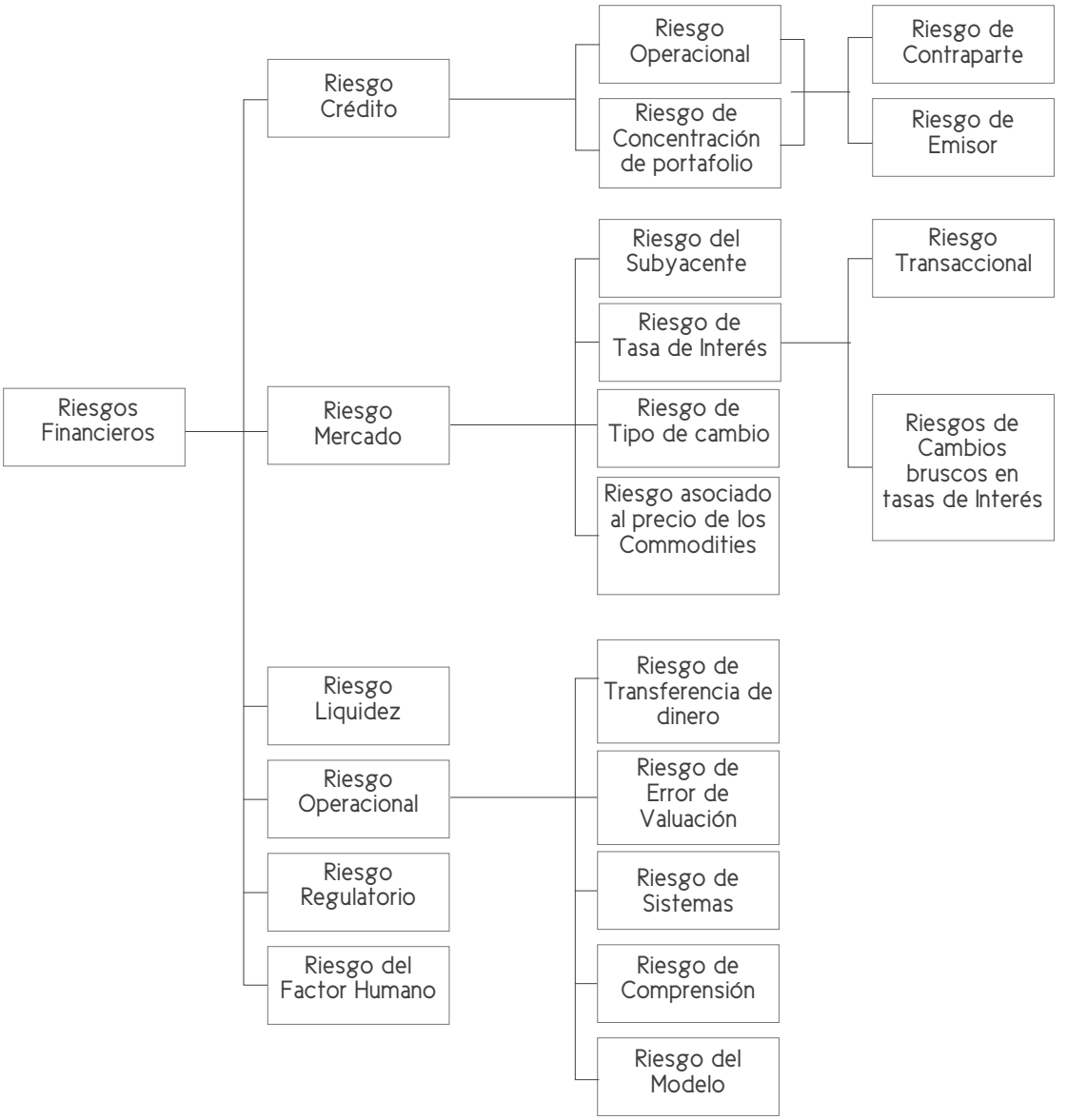
Gráfico 64: Tipo de riesgo mercado e impacto negativo

Tipo de Riesgo	Impacto negativo
Mercado	Variación de precios.
Crédito y Contraparte	– Incumplimiento de la contraparte en una operación. – Disminución en el valor de los instrumentos por reducción en la calificación crediticia.
Legal	– Incapacidad legal de la contraparte para pactar contratos y obligaciones. – Cambios legales repentinos que entren en conflicto con posiciones vigentes. – Demandas legales por no cubrir riesgos medibles.
Moral Hazard	– Mala fe de la contraparte desde que se pacta la transacción. – La contraparte proporciona información falsa sobre su capacidad financiera o crediticia. – La contraparte tiene incentivos para exponerse a riesgos excesivos.
Modelo	– Incorporación de sesgos sistemáticos u ocasionales en los criterios, supuestos, metodologías, bases de información o modelos de valuación, que conducen a decisiones erróneas.
Liquidez	– Costo implícito en la falta de liquidez del mercado: spread amplio o inexistente de compra – venta, variaciones abruptas de los precios operados. – Costo o penalización por retiros anticipados de depósitos. – Incapacidad para enfrentar requerimientos ocasionales de liquidez (llamadas de margen).
Fiscales	– Alto costo fiscal de operaciones de cobertura. – Esquema fiscal que obstaculice una eficiente administración de riesgos.
Contables	– Incertidumbre sobre el reporte financiero de la administración de riesgos. – Oposición reglamentaria al neteo de pérdidas y ganancias generado por una posición de cobertura.

Fuente: En aproximación a diversos autores:
(Park. S. 1997; Jorion O. 1999; Portillo Tarragona 2001; Soldevilla E. 1996).

Otra clasificación, específica para los tipos de riesgos asociados con los productos derivados es propuesta por Ezra Zask (1996), en el artículo "The Derivatives Risk Management Audit".

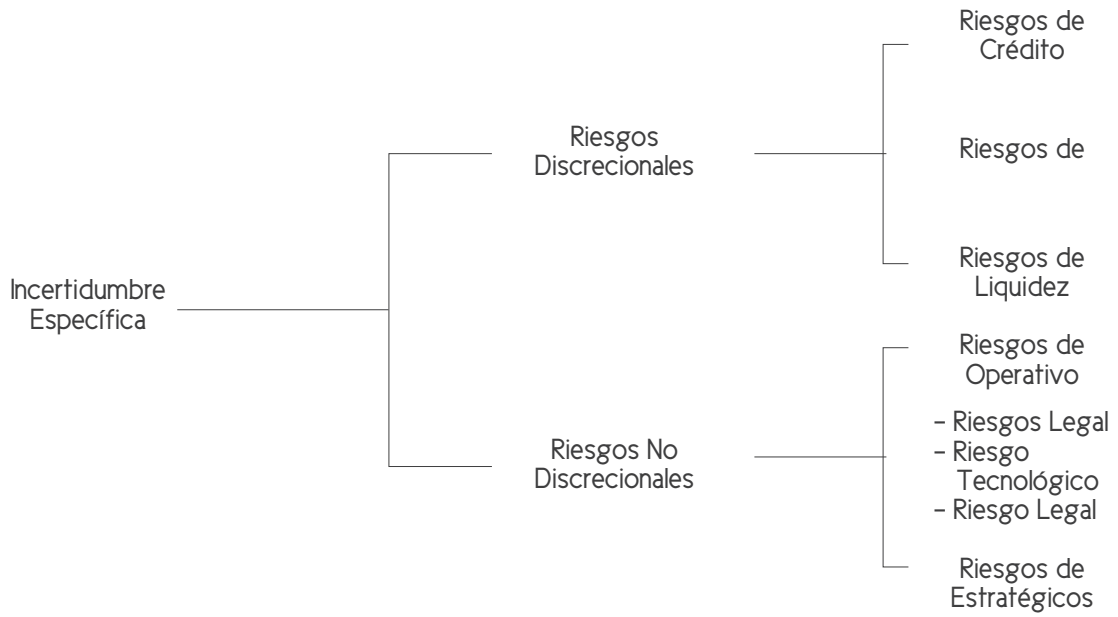
Gráfico 65; Riesgos financieros



Fuente: The Derivatives risk management audi (1996). Zask, E., Klein, R., & Lederman, J.

Por otro lado, en base a la incertidumbre específica que los riesgos presenten se pueden clasificar en riesgos discrecionales y los no discrecionales:

Gráfico 66: Incertidumbre específica



Fuente: Autores diversos (Jorion O. 1999)

Capítulo XIV:
Casos prácticos

Caso I : Gestión de procesos – Don Pizza

El siguiente trabajo tiene como objetivo proporcionar las herramientas necesarias a los lectores de la gestión de procesos, que forman parte de las operaciones de una empresa de bienes o servicios. Por ello, se presentara una parte teórica de manera que se comprendan a detalle ciertos conceptos básicos, y ejemplos aplicados para la explicación del mismo. Para dicho caso se explicaran temas como mapa de proceso, swimline, diagrama causa-efecto y punto de equilibrio. Para finalizar se presentará un caso donde se describirán los procesos y características de la empresa "Don Pizza" encargada de ofrecer pizzas al estilo peruano e italiano, con la finalidad de que se utilicen todas las herramientas presentadas en el marco teórico para que se apliquen a la empresa en mención y así mejorar sus procesos internos.

MARCO TEÓRICO

1. Mapa de procesos

Se habla actualmente de varios mecanismos para optimizar tiempo y tareas dentro de las empresas. Pero existe un enfoque basado en procesos, el cual contribuye de manera importante a gestionar todas las actividades o tareas características que desempaña la empresa bajo procesos indicados en cada área determinada, logrando así realizar una buena y eficiente gestión de las funciones y los recursos que se requieren e identificar qué tipos de procesos concuerdan con la estructura que tiene cada empresa. Puede parecer una idea compleja, sin embargo podemos encontrar procesos que se acomoden de manera significativa al tipo de estructura que maneja una empresa.

Una vez identificados los procesos que se realizan en la organización, es importante determinar de qué manera están relacionados, con el fin de que cada proceso identificado pueda entenderse e integrarse a un sistema interactivo de toda la empresa, donde intervienen los empleados, la alta gerencia, clientes, proveedores y grupos de interés.

Para la elaboración paso a paso del proceso, se debe comprender que cada parte posee elementos que van a permitir su integración dentro de la operación general de la empresa. A su vez, se van dar casos donde cada proceso va a estar dividido en subprocesos. Es decir procesos que están contenidos en otros procesos, pero que todos trabajan por un objetivo en común que viene a ser la eficiencia en la empresa.

A continuación se presentará la clasificación de los procesos en tres tipos (Amordazaran 1999):
Procesos estratégicos o de dirección:

Son todas aquellas actividades realizadas por los gestores para mantener los procesos de apoyo y los

operativos. Entre ellas tenemos:

- El establecimiento de metas
- El presupuesto y la distribución de los recursos.
- Las auditorías y revisiones del sistema de la calidad.
- Los procesos formales de planificación.
- Otras actividades.

Procesos operativos:

Son aquellos en que los productos resultantes son recibidos por una persona u organización externa a la empresa. Constituyen la secuencia de valor añadido con que la organización satisface las necesidades de los clientes:

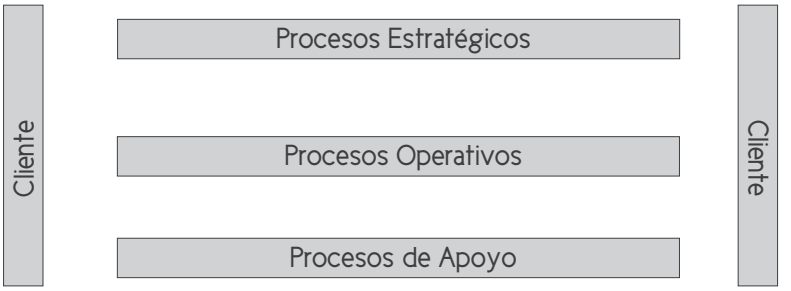
- Conocimiento del mercado y de los clientes (necesidades, deseos y expectativas)
- Diseño de productos y servicios.
- Comercialización y venta.
- Producción y ejecución de los servicios.
- Facturación y servicio a los clientes.
- Compras a proveedores.

Procesos de apoyo o soporte:

Son aquellos procesos esenciales para una gestión de los procesos operativos. Como ejemplos tenemos:

- Reclutamiento del personal.
- Formación.
- Mantenimiento.
- Información y sistemas tecnológicos.
- Compras.

Gráfico 67: Modelo de mapa de procesos.



Fuente: Beltrán y Carmona (2012).

Dentro de este modelo se puede ver que uno de los objetivos principales es satisfacer al cliente, por ello es que los procesos ayudan a que las distintas áreas puedan interactuar y desempeñar sus actividades con el fin de satisfacer los requerimientos del cliente y de esa manera entregar valor por parte de la empresa.

El nivel de detalle de los mapas de proceso dependerá del tamaño de la propia organización y de la complejidad de sus actividades. En este sentido, es importante alcanzar un adecuado punto de equilibrio entre la facilidad de interpretación del mapa o los mapas del proceso y el contenido de la información.

A continuación se mostrará el mapa de procesos de una industria.

Gráfico 68: Modelo de mapa de una industria

Procesos estratégicos			
Planificación estratégica	I + D	Mejora contínua	Investigación de mercado
Procesos operativos			
Producción	Diseño	Comercial	Entrega
Procesos de apoyo			
RR HH	Mantenimiento	Sistemas de información	

Fuente: Pérez, J. (1996)

2. Swimline

Se refiere a la creación de una representación gráfica de un proceso de transformación, el cual es útil para documentar lo que sucede dentro de un proceso de transformación. Esta documentación incluye las ediciones del proceso y puede ayudar a identificar la manera de mejorarlo cambiando alguno de los elementos si es necesario.

Estos diagramas facilitan la interpretación de las actividades en conjunto. Uno de los aspectos importantes que deberían recoger estos diagramas es la vinculación de las actividades con los responsables de su ejecución, ya que esto permite reflejar cómo se relacionan los diferentes actores que intervienen en el proceso. Se trata por tanto de un esquema "quién-qué", donde en la columna quién muestra las responsabilidades de cada departamento y muestra la transmisión de mando.

Para la representación de este tipo de diagramas, la organización puede recurrir a una serie de símbolos que proporcionan un lenguaje común y que facilitan la interpretación de los mismos (Schroeder et al. 2011).

Gráfico 69: Significado de la simbología

Inicio o fin de procesos	Se suele utilizar este símbolo para representar el origen de una entrada o el destino de una salida. Se emplea para expresar el comienza o el fin de un conjunto de actividades.
Actividad	Dentro del diagrama de proceso, se emplea para representar una actividad, si bien también puede llegar a representar un conjunto de actividades.
Decisión / Evaluación	Representa una decisión. Las salidas suelen tener al menos dos flechas (opciones).
Documento	Representan un documento. Se suele utilizar para indicar expresamente la existencia de un documento relevante.
Base de datos	Este símbolo representa a una base de datos y se suele utilizar para indicar la introducción o registro de datos en una base de datos, habitualmente informática.

Fuente: Beltrán, J. & Carmona, M. (2012)

3. Diagrama causa – efecto

Es una forma de organizar y representar las diferentes teorías propuestas sobre las causas de un problema. Se conoce también como el diagrama de Ishikawa (por su creador, el Dr. Kaoru Ishikawa en 1943), o diagrama de espina de pescado y se utiliza en las fases de diagnóstico y solución de la causa.

Este diagrama te permite en general ordenar todas las causas que supuestamente pueden contribuir a un determinado efecto. En otras palabras se puede lograr un conocimiento completo de un problema complejo ya sea dentro o fuera de la empresa. A su vez debe quedar claro que el diagrama causa-efecto no es una herramienta para resolver un problema, sino únicamente sirve para explicarlo y así analizar sus causas, siendo esto paso previo para corregirlo en caso se dé un problema.

Como se sabe este diagrama también es llamado "Espina de pescado" por la forma en que se van colocando cada una de las causas o razones que originan un problema. A su vez permite visualizar de manera rápida la relación de las causas con el origen del problema. En este diagrama se deben incluir los siguientes elementos:

- El problema principal que se va a analizar se debe colocar en el extremo derecho del diagrama (la cabeza del pescado). Se debe encerrar en un rectángulo para visualizarlo con facilidad.

- Se identifican los factores o grupos de causas en que estas pueden clasificarse. A cada uno de estos se les asigna una flecha que entronca en la "espina" principal del pez. Habitualmente, estos factores suelen estar predefinidos como las "4 M" o "5 M" como:

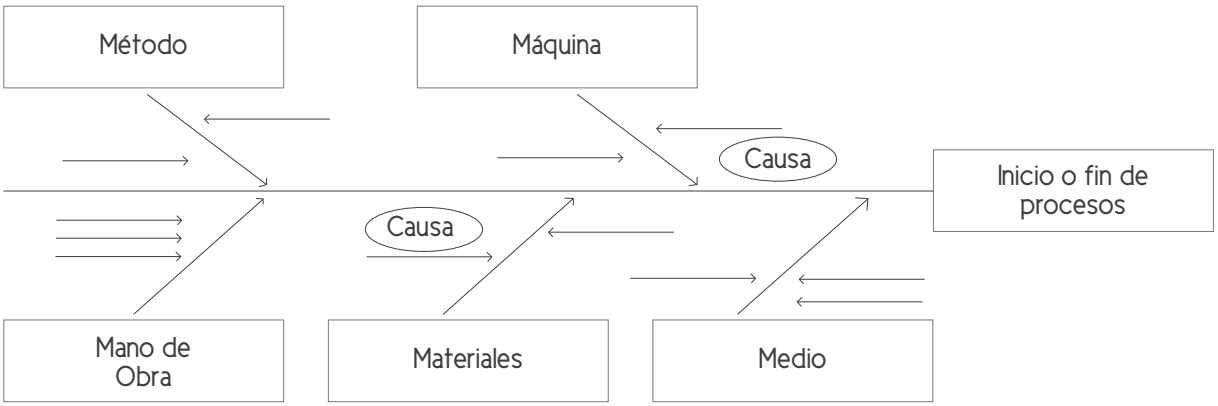
  - 1° M : Máquinas
  - 2° M : Mano de obra
  - 3° M : Método
  - 4° M : Materiales
  - 5° M : Medio (entorno del trabajo)

- Se asigna cada una de las causas identificadas a cada uno los títulos o conjuntos definidos, utilizando flechas paralelas a la "espina" central y escribiendo de nuevo la causa al lado de cada flecha.

- Se determina cuál es el orden de importancia de las causas identificadas. Para ello, puede someterse a votación de parte de los integrantes que están realizando el diagrama.

- Finalmente se encierran en un círculo las 2 o 3 causas más votadas, las cuales serán las primeras contra las que se deberá actuar y así corregir el problema.

Gráfico 70: Diagrama causa – efecto



Fuente Martínez, M. (2005)

4. Punto de equilibrio

También es conocido como punto crítico y se define como la situación donde el valor de las ventas o el volumen de un producto y los gastos son iguales, es decir si se vende o producen cantidades de productos por debajo de esa cantidad la empresa operará con pérdidas, mientras que si se vende o producen productos por encima de ese valor la empresa operará con utilidades.

Para calcularlo puede usarse la ayuda de formulaciones matemáticas o empleando gráficos que contribuyen a una mejor compresión del concepto, donde intervienen costos fijos y costos variables.

Costos fijos:
Son aquellos gastos que permanecen inalterables en su magnitud independientemente de la variación de las ventas en unidades monetarias o del volumen físico de producción.

Costos variables:
Son los costos que fluctúan en correspondencia con la variación de las ventas en unidades monetarias o de los volúmenes de productos en unidades físicas. Están dentro de esta categoría los materiales para la producción, los servicios productivos recibidos.

La utilidad a la que se refiere el punto de equilibrio es lo que resulta de la siguiente operación:

$$PV^* \text{ Unidades} = CF + (CV^* \text{Unidades})$$

PV: precio de venta CF: costos fijos CV: costos variables.

CASO I: Empresa Don Pizza

Don Pizza es una pizzería que se encuentra en la avenida Aviación (San Borja) que se diferencia por ofrecer productos comestibles y deliciosos en un ambiente cómodo para todos sus clientes. Actualmente, Don Pizza ofrece pizzas y pastas con ese sabor italiano auténtico con calidad y la buena atención hacia el cliente. Por ello tienen como objetivo dentro de cuatro años lograr ser la empresa peruana líder en ventas de pizza y pastas, capacitando a su personal de manera asertiva y así lograr ventaja frente a la cadena extranjera de Pizza Hut.

Dentro de su misión es brindar productos de alta calidad y atención personalizada a cada cliente de modo que tengan una buena experiencia de servicio. Con el fin de que el cliente se vaya muy satisfecho por la atención de sus capacitados colaboradores.

Por el momento, la empresa Don Pizza cuenta con las siguientes áreas:

- Gestión estratégica: la cual se encarga de la planificación estratégica de la empresa.
- Marketing: encargada de realizar las estrategias de publicidad, marketing digital y fidelidad del cliente.
- Cocina: encargada de la preparación de las pizzas y pastas
- Punto de venta: que se encarga de atender a todos los clientes que asisten al restaurante así como de registrar sus órdenes y también de la caja.
- Domicilios: que se encarga de realizar los envíos a domicilio de los productos.
- Compras: encargados de realizar los pedidos a los proveedores con el fin de obtener los mejores productos para la preparación de las pizzas y las pastas.
- Tecnología: encargado de establecer sistemas de información para mejorar el servicio y gestionar mejor las ventas de modo que se logre una mejora continua en la empresa.
- Limpieza: encargada de la limpieza del local y de los servicios utensilios del restaurante.

Adicionalmente, Don Pizza tiene diversos procesos dentro de toda su empresa. De los cuales lo más importantes son los siguientes:

Realizar una orden:

Esto comienza cuando el cliente ingresa al establecimiento y solicita una mesa. El área de punto de venta revisa sus mesas, si hay mesas se procede a situar al cliente en la mesa y brindar la carta, si no se le lleva al lugar de espera con la carta para que vaya revisándola.

Cuando el cliente se sitúa en la mesa procede a generar el pedido. El área de punto de venta recibe el pedido y procede a registrar el pedido y ordena el pedido al área de cocina, donde el cocinero se

encarga de la preparación y ejecución del pedido. Previamente revisa si sus insumos están completos para proceder a preparar, si no procede a llamar al área de compras para solicitar el insumo que falta y este le envía a la brevedad posible, ya que tiene un lugar de venta cercano a la pizzería. Finalmente, prepara el pedido y envía el pedido al área de punto de venta. Este registra la preparación y el despacho hacia la mesa.

Una vez despachado el pedido hacia la mesa del cliente se termina el proceso.

Envío a domicilio:

Este proceso comienza cuando el cliente genera un pedido telefónico a Don Pizza, el cual es atendido por el área de punto de venta, que brinda información acerca de las opciones que tiene la pizzería. El área de punto de venta recibe y registra la orden de pedido a través de una boleta, que luego envía al área de cocina, que recibe recibe el pedido y empieza su preparación. Para ello, previamente hace la consulta sobre la disponibilidad de insumos al almacén y en caso esté abastecido procede a preparar, si no, el área de compras hace el envío de los insumos para empezar la preparación. Una vez hecha la preparación por el área de cocina, se envía la orden terminada al área de punto de venta, la cual recibe y registra la orden terminada. Luego se envía al área de domicilios la orden terminada y la boleta del pedido, para que se encargue de llevar el pedido al domicilio registrado. El cliente recibe el pedido y la boleta en su domicilio y le cancela al encargado de domicilios el pago de su pedido, quien finalmente se retira.

Por otro lado, la pizzería actualmente está recolectando datos sobre las quejas de algunos clientes sobre los siguientes inconvenientes:

- La pizza no llega a tiempo o jamás llega.
- Los pedidos de delivery llegan errados.
- La pizza se pega contra la tapa de la caja.
- Algunos de los meseros no tratan bien al cliente.
- No reciben en el pedido el tipo de masa de la pizza que solicita el cliente.
- Los lavanderos no lavan rápido los servicios.
- El horno no llega a su punto de cocción.
- Algunos cocineros se retrasan en la preparación.

Por otro lado, el gerente de planificación estratégica tiene pensado vender sus pizzas clásicas a s/. 25.00 nuevos soles. Según sus procesos operacionales requerirán de costos fijos de s/. 8,000.00 nuevos soles y los materiales y la mano de obra tendrán un costo de s/. 10.5 por cada unidad.

Preguntas a resolver:

- Elabore el mapa de procesos de la empresa Don Pizza.
- Elabore el *swimline* del envío a domicilio.
- Elabore el diagrama causa – efecto que enfrenta la empresa.
- Determine el volumen de unidades que les permite llegar a su punto de equilibrio

Caso II: Gestión de procesos – Conazul S.A

CONAZUL es una organización que trabaja de manera conjunta con SEDAPAL, empresa que brinda servicios de agua y alcantarillado en Lima, brindándole servicios de saneamiento domiciliario. Por otro lado, fue conformada por Aguazul (Colombia), y el grupo Arcaya & Cabrera (Perú), unificados solo para cubrir la demanda de SEDAPAL; en otras palabras, CONAZUL opera solo para un gran cliente.

Los objetivos estratégicos de la empresa, se centran en la calidad, tanto para el usuario del servicio de SEDAPAL, como para la misma SEDAPAL. CONAZUL posee diversos objetivos estratégicos que le guían en el camino de la calidad:

- Satisfacer eficazmente los requisitos de SEDAPAL y de los usuarios atendidos.
- Aplicar y mejorar los desarrollos tecnológicos en cada uno de los procesos contratados
- Promover el desarrollo y bienestar del equipo humano.
- Garantizar y mantener la infraestructura y recursos necesarios para nuestra gestión.
- Buscar Rentabilidad para el Consorcio AZB – HCI – CONAZUL.
- Mejorar continuamente la eficacia, y eficiencia de los procesos orientando el sistema hacia la excelencia.

Por otro lado CONAZUL S.A. cuenta con los siguientes procesos:

- A nivel estratégico: gestión estratégica, gestión de proceso de negocio
- A nivel operativo: acciones persuasivas, gestión social, catastro, gestión comercial, instalación, inspección comercial, ventas, distribución, facturación.
- A nivel soporte: gestión financiera, gestión administrativa, gestión legal, gestión de sistemas y tecnología y gestión de recursos humanos.

Procesos en un catastro: [39]

- Verificar documentos: actividad realizada por la secretaria del área de operaciones de CONAZUL para revisar si la solicitud recibida cumple con los requisitos necesarios para avalar el inicio de un nuevo catastro.
- Registrar solicitud: esta actividad es realizada por el oficinista y consta de archivar en la base de datos de CONAZUL la solicitud previamente aprobada.
- Inspeccionar inmueble: realizado por el asistente del valuador. Esta actividad se realiza antes del avalúo y comprende la verificación de la propiedad y sus conexiones de agua y desagüe.
- Registrar ficha de inspección en el expediente: esta actividad es realizada por el asistente del valuador y consiste en archivar el documento resultante de la observación realizada. Este proceso genera un documento.
- Realizar avalúo: consiste en la tasación de las conexiones de agua y desagüe del inmueble que han sido registradas por el valuador.
- Registrar avalúo: consiste en la documentación de la ficha resultante de la realización del avalúo. Esta actividad es realizada por el valuador. Este proceso genera un documento.
- Revisar y firmar avalúo: esta actividad es realizada por el director del área de operaciones de CONAZUL y consiste en otorgar la aprobación al avalúo realizado previamente.
- Archivar expediente: la documentación del avalúo aprobada por el director es registrada en el sistema por el archivista.
- Entregar constancia al solicitante: proporcionar el comprobante que justifica el avalúo realizado en el inmueble al solicitante, que en este caso es el jefe de operaciones de SEDAPAL. Esta actividad es realizada por el archivista.

Gráfico 71: Conclusiones: Cambios y actividades afectadas

Procesos	Actualmente	
	Tiempo minutos	Operarios
Verificar documentos	86	1
Inspección inmueble	100	1
Registrar ficha de inspección	25	1
Registrar avalúo	25	1
Realizar avalúo	60	1
Revisar y firmar avaluó	40	1

[39] Catastro: registro o inventariado de un inmueble con fines administrativos

Por otro lado, también se identificó algunos problemas en las áreas de trabajo, y los más frecuentes son:

- Monotonía y dolor cervical de los trabajadores en el área administrativa (65~~).~~
- Caídas a distinto nivel en los almacenes de tuberías y materiales (55~~).~~
- Cortes en las manos debido a las herramientas mal empleadas (40~~).~~
- Fracturas por golpes de objetos en movimiento porque no hay un layout definido (30~~).~~

Preguntas a resolver
En relación al caso y la teoría señalada, se pide elaborar lo siguiente:

- Elabore el mapa de procesos de la empresa.
- Elabore el flujo-grama del proceso: Realizar pedido.
- Elabore el mapa de riesgos.
- Elabore el diagrama de Pareto con los tiempos indicados.

Caso III : Creación de una aplicación para iPhone y su venta en la App Store de Apple

ALCANCE DEL PROYECTO

Dar a conocer a través de una aplicación de pago para celular los destinos turísticos y principales atracciones de la ciudad de Trujillo, Arequipa o Cuzco.

La empresa encargada de realizar la aplicación es Trujillo Tech e incluye todos los procesos de desarrollo, desde la implementación hasta su ingreso a la tienda de Apple. Esta empresa se encargará además de la publicidad a través de la web.

La aplicación será publicada en la App Store de Perú y posteriormente lanzada a la App Store de USA.

OBJETIVO DEL PROYECTO

- Desarrollar una aplicación para iPhone que permita conocer las costumbres, gastronomía, historia y cultura de la ciudad de Trujillo-Perú en diferentes idiomas y de forma intuitiva.
- Posicionar a la aplicación creada dentro del top five de descargas pagadas para crear una imagen de marca en el lanzamiento de futuras aplicaciones.

- Ganar experiencia en el mercado de las aplicaciones para celulares con el objetivo de ampliar el mercado futuro a otros smartphones y a tablets.

JUSTIFICACIÓN DEL PROYECTO

- IPhone es uno de los smartphones de mayor venta en el mundo y la tienda App Store la que tiene mayores descargas y programas de todo tipo y en todos los idiomas.
- El crecimiento logarítmico de los smartphones y los planes de internet asequibles a los usuarios abren un mercado importante a las aplicaciones de celulares.
- Afianzar la imagen de destino turístico y gastronómico que tiene el Perú y complementar la imagen histórica del país con una aplicación moderna.

CLIENTES

- Usuarios de iPod, iPod Touch, iPhone, iPhone 6, iPhone 6 Plus, Iphone 5 e iPhone 5S

DESCRIPCIÓN DEL PROYECTO

- La aplicación cuenta con una fuerte interacción entre usuario y smartphone, aprovechando el giroscopio, GPS y retina display del celular. Tiene configuración para visualizarla en cinco idiomas: español, inglés, chino, francés y portugués, con proyección a desplegarse en otros idiomas.

- La aplicación se llamará iloveTrujillo y en ella podemos encontrar la información siguiente en módulos.

- La aplicación aparecerá primero como versión trial o libre en la cual funcionarán algunos de los módulos (30 %); cuando llegue a posicionarse en el top de descargas se procederá a lanzar la aplicación de pago.

INFORMACIÓN HISTÓRICA

Steve Jobs, CEO de Apple marcó una etapa, una nueva era de la tecnología móvil y las tablets, que bien podríamos resumir en un antes del iPhone (AI) y un después del iPhone (DI). El iPhone, el más famoso de los smartphones hizo su aparición en el mercado en el año 2010 y junto a su sistema operativo iOS y sobre todo a la aparición de su tienda virtual iTunes ha logrado apoderarse del corazón de los amantes de la tecnología. Aún ahora con la fuerte competencia de Samsung y sus modelos Galaxy, una de las ventajas competitivas del teléfono de la manzanita es la cantidad de aplicaciones que hay y se siguen subiendo a la nube.

La segunda versión del smartphone, el iPhone 5s vio la luz el año 2014 y ya contaba con GPS y acelerómetro. El iPhone 6 se lanza en junio del año 2015, es más rápido que su versión anterior y cuenta con 500MB de RAM además de traer cristal antihuellas. En junio del 2015 se lanza el iPhone 6 Plus que incluye grabación en HD y una cámara de 10 megapixeles; la versión final del smartphone por excelencia.

La pantalla del iPhone tiene un tamaño de 5.5 pulgadas y tiene 16 millones de colores, las aplicaciones se muestran nítidas y el sistema touch screen es uno de los mejores del mercado. Uno de los puntos en contra es la duración de la batería, la cual dura menos de un día, pero esto no ha sido motivo suficiente para que los amantes del iPhone lo cambien por algún otro celular de la competencia. El iPhone tiene un teclado con opción a 21 idiomas diferentes. La App Store de Apple llegó en marzo del 2012 a 25 billones de descargas y tiene 600,000 aplicaciones hasta mayo del éste mismo año. Uno de los casos de éxito más sonados de una aplicación vendida en la App Store es el juego Angry Birds el cual ya se ha convertido en una leyenda y un referente de lo exitoso que puede ser una aplicación de calidad, divertida, original y de buen gusto.

SUPUESTAS RESTRICCIONES

- Se requiere conocer el software Objetive-C para crear la aplicación.
- Adquirir una licencia de creador de aplicaciones con Apple (USD $ 100.00).
- Una vez subida la aplicación se debe esperar la aprobación de Apple y su puesta en venta.
- Apple se queda con el 30% del total de las ventas, el usuario percibe el restante 70%.

Se pide:

- Determine los riesgos del proyecto
- Prepare la matriz de severidad.

Caso IV: Diversos casos de ISO 31000[40]

CASO IV. PARTE 1

Javier Urrutia es el presidente de la Empresa Fidelac S.A. dedicada a la producción y comercialización de leche y derivados de la misma como quesos, kumis, yogurts, mantequillas entre otros.

Actualmente la compañía está buscando un nuevo terreno en la sabana de Bogotá para ampliar su producción donde ubicará ganado y una planta de pasteurización.

El pasado fin de semana Daniel Vergara, el mejor amigo de Javier lo invitó a un juego de golf en el Country Club de Bogotá, donde conoció a una hermosa y adinerada mujer llamada Alicia Pasqueletti de nacionalidad Suizo–Italiana.

Javier como buen galán la invitó a tomarse un trago y le contó sobre su vida, profesión y expectativas. Incluso le mencionó sobre el proyecto de la nueva planta de Fidulac.
Alicia le comentó que ella tenía una finca con un terreno de 1.000 hectáreas en la sabana de Bogotá, la cual había heredado de su marido y que como se sentía tan sola la estaba vendiendo, ya que no quería ocuparse de ella porque le traía muchos recuerdos de aquel hombre "su adorado esposo".

Javier como todo un caballero, le dijo "la entiendo muy bien", "y es más podríamos hacer negocios, claro dependiendo del precio, el terreno, etcétera."

Alicia seguida se mostró bastante contenta y le dijo: "por el precio no se preocupe que lo podemos arreglar. Lo único que si le pido es que de hacer negocios, éstos sean cuanto antes ya que con la venta de esta propiedad voy a realizar una obra benéfica con niños y ancianos".

Javier quedó sorprendido ante la nobleza de esta mujer y acordó una cita dentro de un par de días.

Ella le dio su número telefónico y se despidió con un gran beso en la mejilla, diciéndole: "fue un placer y espero que hagamos más que negocios".

Javier quedó atónito y pensó: "perfecto una ganancia por partida doble, las tierras y la mujer".

Preguntas caso IV / parte 1:

a. Realice un análisis del contexto interno y externo.
b. Teniendo en cuenta que se va a realizar una compra, ¿qué riesgos considera que puedan ser parte de este proceso?

[40] Fuente: ISO 31000 Bureau Veritas, seminario Perú

c. ¿Qué controles asociados a estos riesgos considera que deban existir?
d. Con base en la información mencionada, ¿con qué controles cuenta la compañía para mitigar estos riesgos?
e. ¿Qué acciones le recomendaría al vicepresidente de producción?
f. ¿En su concepto cómo evalúa el componente de comunicación, que aspectos considera que deban ser mejorados?

CASO IV. PARTE 2

1. Javier muy interesado en el negocio y en Alicia, decidió programar una cita para continuar con la negociación. Alicia en seguida aceptó citándolo en su finca el domingo.

2. Cuando Javier llegó a dicha finca, esta era una hacienda con bastos terrenos, ganado y caballos. El quedó sorprendido al ver la majestuosidad de este lugar.

3. Javier, un hombre de negocios con bastante experiencia y con bastantes títulos académicos pensó por un momento en el valor de esta propiedad, calculando más de USD 5,000.000. Se sentía en problemas, ya que el terreno era demasiado extenso y estaba seguro que la junta directiva no iba a aprobar dicha compra. Sin embargo, no podía echarse atrás ¿Cómo quedaría ante Alicia?

4. Alicia lo esperaba en la sala de su casa, con un par de copas y una botella de champagne. Javier pensó en seguida en algo más que en negocios, pero sabía que primero debía hablar de la compra.

5. Alicia le dio un recorrido por la casa y después en su camioneta de alta gama le dio un recorrido por las tierras. Alicia conocía del negocio ganadero, ya que tenía varias vacas en este lugar. Además le dijo que su padre había tenido una industria de quesos en Suiza, pero que la había vendido para dedicarse a pasar su vejez en un hermoso chalet en los Alpes.

6. Javier estaba maravillado con las tierras y con las historias de Alicia, así que decidió tomar la palabra y negociar el precio. Cuándo Javier le preguntó por el valor, Alicia le dijo que la totalidad del lugar costaba US D 8.000.000 los cuales podía negociar

7. Javier leyó por encima el contrato, no se percató ni siquiera que los datos de Fidelac como el NIT y su documento de identidad ya estaban inscritos en el contrato. Lo único que revisó fue el espacio para firmar. Alicia mientras que el leía le decía que se sentía muy feliz de hacer negocios con él y que este era solo el inicio de negocios y demás cosas que iban a hacer juntos.

8. Javier firmó el documento, miró a los ojos a Alicia, alzaron las copas y brindaron. Por los negocios

y por todo lo que vendrá, ¡salud!.

9. Mientras tanto el abogado sacó un pequeño dispositivo conectado a su computador portátil, pidiéndole el favor a Javier de firmar y poner la huella de su índice derecho. A Javier le pareció extraño, pero Alicia en seguida le dijo "es más seguro así, tú sabes, ya estamos migrando del físico a lo digital".

10. Una vez realizado lo referente a la firma y huella, el abogado se despidió dejando a la pareja. Javier no sabía en lo que se había metido, tantos años de estudio, trabajo y sacrificio no habían servido para nada. Lo que aprendió en la Universidad de Stanford sobre gestión del riesgo se desvaneció en su mente ante los encantos de una hermosa mujer.

11. Alicia después de brindar, le dijo "bueno Javier, ¡ay discúlpame!, olvidaba que tengo que atender un asunto familiar urgente y me tengo que ir. Pero llámame esta semana para almorzar juntos y seguir celebrando".

12. Javier quedó pasmado, y ella fríamente salió de la casa sin casi despedirse pensó por un momento "será que cometí un error". Pero regresaba a su mente la idea de "yo soy el presidente, yo no cometo errores".

13. Llegó el lunes y al poco tiempo llamó el abogado de Alicia manifestando que necesitaba algunos documentos para formalizar el trato, una información sencilla de la empresa y de Javier ya que el aparte de ser epresidente, era el representante legal. A Javier le pareció sospechoso, pero en el transcurso de su reflexión mientras hablaba con el abogado, llamó Alicia a su celular preguntándole como estaba y solicitándole el favor tener listos los papeles antes del mediodía.

14. Javier solicitó al área legal y financiera la información requerida dentro de las que se incluía el detalle de las cuentas bancarias de Fidulac tanto en el país como en el exterior.

15. Para el medio día un delegado por Alicia fue a recoger los documentos.

16. Después de haber realizado la entrega, Javier llamó a Alicia quien no contesto. En la tarde y noche insistió pero tampoco le contestó.

17. Javier dentro de sí pensaba que algo estaba mal, pero en seguida se repetía: "yo he hecho muchísimos negocios y mucho más grandes, así que no hay de qué preocuparse".

18. Javier fue víctima de un caso de lavado de activos, vinculando a la empresa en todo esto.

19. Después de unos días, la fiscalía encontró que se habían abierto cuentas a nombre de Javier Urrutia y realizado grandes movimientos. Un delito más que lo incriminaba.

20. Javier, cuando supo de esto, exclamó "yo no tengo nada que ver", pero en seguida se acordó del momento de la firma y huella en el documento y en el dispositivo del abogado. Así mismo, el no revisó página a página, letra a letra y recordó a uno de sus grandes maestros de Stanford, quien le dijo "cuando firmes algún documento, tómate todo el tiempo que necesites para leerlo. Asegúrate de lo que firmas es el objeto del documento y no un anexo al mismo. Deja tu firma o visto bueno en todos los papeles para asegurarte de que lo que estás firmando es correcto y conserva una copia para ti".

21. Javier fue condenado a 10 años de cárcel por lavado de activos, la empresa investigada por varios meses y liquidada, ya que ninguna de las partes interesadas como clientes y proveedores querían saber de la misma.

Información adicional

a. Según el último informe de Fidulac las importaciones de leche en el último año se han incrementado en un 25—y las exportaciones han disminuido en un 5—.
b. Los otros productos derivados de la leche han mantenido un crecimiento de ventas constante de un 1.5—desde el 2009 hasta el 2012.
c. Fidulac S.A. tiene el 40—de participación del mercado colombiano y el 10—del total de las exportaciones de productos lácteos.
d. Uno de los objetivos en el mediano plazo que tiene Fidulac es aumentar la participación en el mercado colombiano y las exportaciones, alcanzando el 55—del mercado nacional y un 15—del mercado extranjero, a través de aumento de la producción y organización de "ferias lácteas en Colombia y en el exterior".
e. Actualmente Fidulac opera al 95—de su capacidad instalada.
f. Fidulac exporta actualmente leche y derivados de la misma a USA, Canadá, Ecuador y República Dominicana.
g. El vicepresidente de auditoria quien reporta al presidente, evaluó con su equipo de trabajo el proceso de compras del año pasado identificando debilidades en la contratación, ya que se estaban vinculando proveedores sin la documentación soporte requerida en la política. Como plan de acción se definió la revisión y aprobación de la creación de proveedores por parte del gerente de compras.
h. La policía de compras detalla que previo a la creación de proveedores en el sistema se debe validar la siguiente información:
   - NIT o RUC o documento de identidad.

- Revisar certificado de la Cámara de Comercio validando los nombres de las personas quienes figuran como accionistas, representante legal, junta directiva y revisor fiscal en la lista OFAC.
- Validar las referencias comerciales anexas por el proveedor.
- Realizar análisis de los estados financieros dictaminados al último corte.
- Documento soporte de autorización de creador del proveedor de acuerdo al monto de atribuciones.

i. De acuerdo a un informe de la fiscalía, el delito por lavado de activos se ha disparado en los últimos años. Dichas declaraciones indican que el 70—del lavado se realiza a través de empresas del sector industrial y de alimentos.
j. Se anexa organigrama

Preguntas caso IV / parte 2:

- ¿Qué riesgos se materializaron?
- De acuerdo a las opciones de tratamiento del riesgo, ¿qué opción tomó Javier?
- ¿Qué debilidades de control identificó?
- ¿Qué pasó con el componente de supervisión y monitoreo?

Gráfico 72: Conclusiones: Cambios y actividades afectadas

Reputacional	Legal , accionistas
Sobrecostos por falencias en la evaluación de proveedores (precios, calidad entre otros) generando pérdidas económicas.	Realizar evaluación a los proveedores por parte del comité de compras asegurando que las decisiones se toman en base a; precio, calidad, requerimientos, tiempos de entrega, reputación del proveedor entre otras, dejando registro de la decisión en acta de comité,

4. Controles que posee la compañía

La compañía cuenta con los siguientes controles relacionados con la vinculación de proveedores:

- Revisión del certificado de de la Cámara de Comercio validando los nombres y documento de identidad de las personas quienes figuran como accionistas, representante legal, junta directiva y revisor fiscal en la lista OFAC, al igual que el nombre y NIT de la empresa dejando evidencia

. de la validación realizada.

- Validar las referencias comerciales anexas por el proveedor revisando: quien emite la referencia, , entre otros, dejando un visto bueno en la carpeta del proveedor.
- Realizar análisis de los estados financieros dictaminados al último corte, evaluando el capital de trabajo, rotación de inventarios, deuda, entre otros, dejando evidencia del visto bueno en la carpeta del proveedor.
- Revisar el documento soporte de autorización de creador del proveedor de acuerdo al monto de atribuciones dejando evidencia del visto bueno en la carpeta del proveedor.

Pese a que existen montos de autorización para las compras, la base de la cultura en gestión de riesgos es muy débil, por lo tanto, el proceso resultará con falencia. No se cuenta con controles sólidos orientados a la denuncia de situaciones sospechosas.

5. Recomendaciones al vicepresidente de producción

- Evaluar la inversión a realizar en la ampliación de las plantas dadas las condiciones del mercado.
- Presentar formalmente al presidente las razones por las cuales:
  - Razones por las cuales se debe revisar la evaluación de la inversión.
  - Los riesgos a los que está expuesta la compañía.
  - Los controles y las debilidades en los mismos.
  - Las transgresiones a las normas de la empresa al no aplicar los debidos procedimientos en compras[41]"

[41] Bureau Veritas, cursos ISO 31000

Gráfico 73: Organigrama

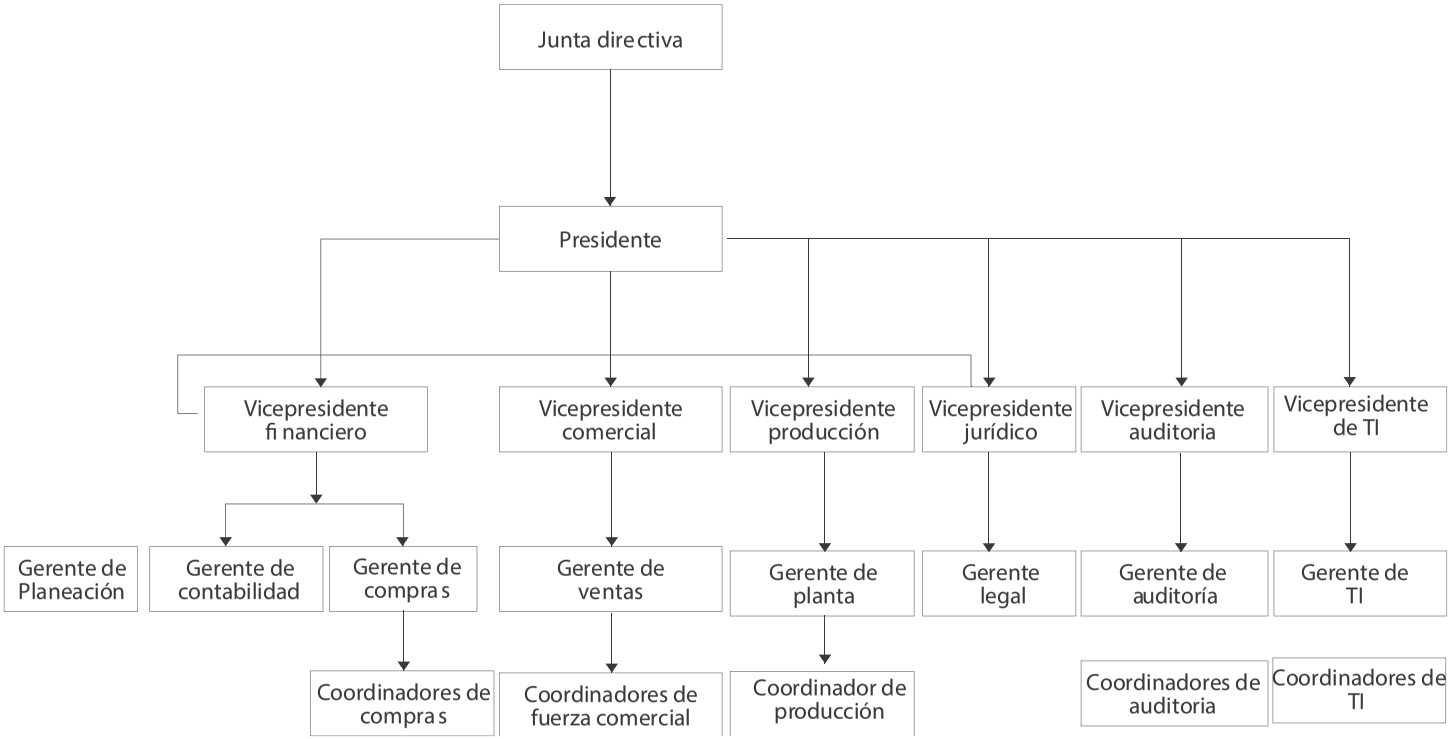


Gráfico 74: Escala de impacto y probabilidad

ESCALA DE IMPACTO

Raro	Económico	Repuntual	Personas	Ambiente
Insignificante	Hasta USD 50.00	Conocimiento de dueños de proceso	Lesión leve, no afecta rendimiento laboral.	Afectación ambiental leve, no genera contaminación, acciones de remediación inmediata.
Menor	Entre USD 50.001 y 100.000 USD	Conocimiento interno de la alta gerencia		Afectación ambiental sin efectos duraderos, requiere reparación en el corto plazo.
Moderado	Entre USD 100.001 y 500.000 USD	Conocimiento de la Junta Directiva, apertura de investigación por parte de entes de control	Limitación en ciertas activ. mientras se recupera, genera incapacidad, afecta rendimiento laboral.	Afectación ambiental a predios vecinos, requiere reparación en el mediano plazo.
Mayor	Entre USD 50.001 y 1.0000.000 USD	Conocimiento por parte de los medios nacionales, afectación del nombre y marca a largo plazo	Incapacidad permanente, daños irreversibles de salud.	Afectación ambiental grave, requiere reparación a largo plazo, quejas de la comunidad ante organismos ambientales.
Catastrófico	Más de USD 1.000.000	Conocimiento por parte de los medios, internacionales, daño irreparable del nombre y de la marca de la empresa	Muerte de un trabajador a	Afectación ambiental irreparable, requiere medidas de compensación.

ESCALA DE PROBABILIDAD

Raro	Económico	Reputacional	Personas	Ambiente
Ha ocurrido en la industria/puede ocurrir en circunstancias.	Ha ocurrido en los últimos 5	Ha ocurrido en los últimos 3 años/	Ha ocurrido en el último año/ Probablemente ocurra	Ha ocurrido más de una vez en el último año/ Existe un alto nivel de certeza que ocurrirá
Error cada 10.000 operaciones	Error cada 1.000	Error cada 100 operaciones	Error cada 100 operaciones	Error cada dos operaciones

Referencias Bibliográficas Empleadas

ABIDIN, S. y M. N. MOHAMAD-NOR
2016 "Competition in Malaysian Audit Industry: What the Market is Telling Us?".En: *Mediterranean Journal of Social Sciences*, 7(1), p. 306.

AENOR PERÚ,
2011 *Interpretación de la Norma* UNE-ISO/IEC 27001:2007. Lima: AENOR Perú formación.

AMORRAZARAIN, M.
1999 *La gestión por procesos.* País Vasco: Editorial Mondragón Corporación

ASBANC
Materiales Académicos – Programas Corporativos Instituto de Formación Bancaria – ASBANC.

ELIZONDO, Alan (coord.)
2012 *Medición Integral del Riesgo de Crédito.* México , D. F.: Limusa. Visitado el 25 de abril de 2016 en: http://www.worldcat.org/title/medicion-integral-del-riesgo-de credito/oclc/777894773/viewport

ARIS, Y. B. W. y N.A.A. JALIL
2016 "Antecedents in Developing a Risk Culture in Public Listed Companies (PLCs): Introduction to Enterprise Risk Management (ERM)". En: PEYEMAN, J., W.E.W. RASHID, A. HANIF, et al. (editores). *Proceedings of the 1st AAGBS International Conference on Business Management 2014* (AiCoBM 2014). Singapur: Springer, pp. 201-208.

SALAMANCA, Gehiner
2009 Basilea II, *la pérdida esperada e inesperada, su diseño, cálculo, uso e impacto sobre el riesgo, la cultura corporativa y la rentabilidad.* Ponencia en ppt en Trujillo. Visitado el 25 de abril de 2016 en: http://www.sbs.gob.pe/repositorioaps/0/0/jer/pres_doc_basilea/Curso~~-20~~Trujillo-P~~-C3-A9~~rdida~~-20~~Esperada-Basilea~~-20~~II.pdf

BELTRÁN, J., M. CARMONA, R. CARRASCO, M.A. RIVAS Y F. TEJEDOR
2009 *Guía para una gestión basada en procesos.* Sevilla: Instituto Andaluz de Tecnología. Visitado el 25 de abril de 2016 en: http://excelencia.iat.es/files/2012/08/2009.Gestion-basada-procesos-completa.pdf

BERGGRUN. L. y J. C. ALONSO
2015 *Introducción al análisis de riesgo financiero.* Cali: Universidad Icesi.

BOWLING D. y L. RIEGER
2005 "Making sense of COSO's New Framework for Enterprise Risk Management". En: *Bank accounting* & Finance, 18:2, pp.29–34.

BUREAU VERITAS
2013 Documentos del curso "Gestión del Riesgo ISO 31000:2009".

BRENNER, J.
2007 "Risk Management and Compliance". En: *Risk Management*, vol. 54, n.° 1, Risk and Insurance Management Society Publishing, Inc. http://www.rmmagazine.com

CABALLERO SAMAMÉ, César
2011 Curso de Riesgo Operativo-Basilea II (ppt), Lima: Intelectum Consultores SAC. http://www.intelectumconsultores.com/plataforma/archivos/GEIRI01OO/documentos/d_699_GESTION-20DE-20RIESGOS-20NOV2011-20(77ppt).ppt

CACPECO-COOPERATIVA DE AHORRO Y CREDITO DE LA PEQUEÑA EMPRESA DE COTOPAXI
2008 *Manual de administración integral de riesgos.* Latacunga, Ecuador: CACPECO LTDA. Recuperado de: http://idbdocs.iadb.org/wsdocs/getdocument.aspx?docnum=35811973

CALDER, A.
2009 Information *Security base on ISO27001/27002: A Management Guide.* Amsterdam: Van Harem Publishing.

CAÑAS, L.
2009 *Gestión de riesgos de negocio. Desarrollo e implementación de sistemas de gestión de riesgos.* Documentos Ocasionales N.° 2009-1. El Salvador: Departamento de Investigación Económica y Financiera del Banco Central de Reserva de El Salvador. Visitado el 26 de abril de 2016 en: http://www.bcr.gob.sv/bcrsite/uploaded/content/category/790395247.pdf

CASARES, I.
2013 Proceso de gestión de riesgos y seguros en las empresas. Madrid: CASARES, Asesoría Actuarial y de Riesgos, S.L.
2014 *Implementación de la Gestión Integral de Riesgos en el Sector Asegurador bajo la Norma ISO 31000.* Madrid: CASARES, Asesoría Actuarial y de Riesgos, S.L.

CASARES, I. y M. I. MARTÍNEZ T.-E.
2011 "El proceso de gestión de riesgos como componente integral de la gestión empresarial". En: *Boletín de Estudios Económicos*, vol. LXVI, n.° 202, abril 2011, pp.73-93. Bilbao. Visitado el 26 de abril de

2016 en: http://www.mcasares.es/Docs/Biblio/GestRiesgos/GESTION-20DE-20RIESGOS-20COMO-20COMPONENTE-20INTEGRAL-20EMPRESARIAL.pdf

CELAYA F., Roberto y María Elvira LÓPEZ PARRA
2004 "¿Cómo determinar su riesgo empresarial?". En: *Revista Escuela de Administración de Negocios,* n.°52, setiembre-diciembre Universidad EAN. Bogotá, Colombia www.bis.org/publ/bcbs128_es.pdf Visitado el 26 de abril de 2016 en: http:// journal.ean.edu.co/index.php/Revista/article/viewFile/309/296

COMITÉ DE SUPERVISIÓN BANCARIA DE BASILEA
2006 *Convergencia internacional de medidas y normas de capital. Marco revisado. Versión integral.* (Normas de Basilea II). Visitado el 26 de abril de 2016 en: www.bis.org/publ/bcbs128_es.pdf

COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION (COSO),
2004 *Enterprise Risk Management Integrated Framework.* Executive Summary. Visitado el 26 de abril de 2016 en: http://www.coso.org/documents/coso_erm_executivesummary.pdf

CONTRERAS, J. R.
2016 "Estimación de métricas de riesgo de mercado usando mixturas gaussianas". En: *Contaduría y Administración*, 61(1), pp. 202-219. Visitado el 26 de abril de 2016 en: http://www.scielo.org.mx/pdf/cya/v61n1/0186-1042-cya-61-01-00202.pdf

COOPER, Dale, Stephen GREY, Geoffrey RAYMOND y Phil WALKER
2005 Project Risk Management Guidelines – Managing Risk in Large Projects and Complex Procurements. Nueva Jersey: John Wiley & Sons.

Club de Gestión de Riesgos [en línea]. Recuperado el <25 de junio de 2010>, de http://www.clubgestionriesgos.org/es/secciones/riesgo_de_credito/introduccion/Perú, 19, 42-56.

DE LARA, A.
2005 *Medición y Control de Riesgos Financieros.* México D.F.: Limusa. Visitado el 26 de abril de 2016 en: *http://books.google.com.pe/books?id=PrQ-vTEWLqoC&printsec=frontcover&hl=es&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false*

DE LOS RÍOS M., Mariana
2009 *Plan de Gestión de Riesgos para la construcción del túnel de conducción superior en el proyecto hidroeléctrico el Diquís del Instituto Costarricense de Electricidad.* Proyecto final de graduación presentado como requisito parcial para optar por el título de master en administración de proyectos. Costa Rica: Universidad para la Cooperación Internacional. Visitado el 26 de abril de 2016 en: http://www.uci.ac.cr/Biblioteca/Tesis/PFGMAP647.pdf

DIONNE, G.
2013 "Risk management: history, definition, and critique". En: *Risk Management and Insurance Review,* 16(2), pp.147-166.

CARDONE, C. y A. TRUJILLO P.
2007 "Efectos del aval de las SGR en la financiación de las PYME y los requerimientos de capital de Basilea II". En: *Revista Española de Financiación y Contabilidad,* vol. XXXVII, n.° 136, octubre-diciembre, pp. 757-789. Visitado el 26 de abril de 2016 en: file:///D:/En-20Proceso/Esan/Libro-20Riesgos-20(CE)/Dialnet-EfectosDelAvalDeLasSGREnLaFinanciacionDeLasPYMEYLo-2525030.pdf

CRUZ, Marcelo G.
2002 *Modeling, Measuring and Hedging Operational Risk.* Nueva York: John Wiley & Sons.

DEL CARPIO, C. y M. ZEVALLOS
2010 "Estimación de capital por riesgo de precio: Evaluando metodologías para el caso peruano". En: *Revista Estudios Económicos,* n.° 19. Lima: Banco Central de Reserva del Perú. Visitado el 26 de abril de 2016 en: http://www.bcrp.gob.pe/docs/Publicaciones/Revista-Estudios-Economicos/19/Estudios-Economicos-19-3.pdf

ESTUPIÑÁN GAITÁN, R.
2006 *Administración o gestión de riesgos E.R.M. y la auditoría interna: Gobierno corporativo, mapa de riesgos, comités de auditoría, listas y cuestionarios de control, normas internacionales de auditoría interna.* Bogotá D.C: Ecoe Ediciones. Visitado el 26 de abril de 2016 en: https://www.academia.edu/10269763/Administraci-C3-B3n_de_riesgos_E.R.M._y_la_auditor-C3-ADa_interna?auto=download

ESPIÑEIRA, SHELDON Y ASOCIADOS
2008 *Boletín de Asesoría Gerencial - Gestión Integral de riesgo (GIR): Alternativas de organización*, n.° 5. Visitado el 26 de abril de 2016 en:
https://www.pwc.com/ve/es/asesoria-gerencial/boletin/assets/boletin-advisory-edicion-05-2008.pdf

DOPAZO, M. del P. y M. I. CANDELARIO
2011 *Gerencia de riesgos sostenibles y responsabilidad social empresarial en la entidad aseguradora.* II Premio Internacional Julio Sáez sobre Investigación de Gerencia de Riesgos. Madrid: Fundación Mapfre.

GALICIA ROMERO, M.
2003 *Nuevos enfoques de riesgo de crédito. México D. F.: Instituto del riesgo financiero.*

GARCÍA, M. y C. SÁNCHEZ,
2004 *Riesgo de crédito en México aplicación del modelo CreditMetrics*. Tesis de Licenciatura. Puebla: Departamento de Contaduría y Finanzas, Escuela
de Negocios, Universidad de las Américas.

GÓMEZ, D y J.M. LÓPEZ
2002 *Riesgos financieros y operaciones internacionales. Madrid: ESIC Editorial.*

GORZEN-MITKA, I.
"Evolution of Corporate risk Management approach". Polonia: Czestochowa University of Technology. Visitado el 26 de abril de 2016 en: file:///D:/En-20Proceso/Esan/Libro-20Riesgos-20(CE)/Gorzen.pdf

MARTÍNEZ CASTILLO, C.A.
2007 "Basiléa II, retos y oportunidades. Hacia una mayor regulación y supervisión financiera en el siglo XXI". En: Gestión y Política Pública, vol. XVI, n.° 2. Visitado el 26 de abril de 2016 en: *http://www.gestionypoliticapublica.cide.edu/num_anteriores/Vol.XVI_No.II_2dosem/Martinez_Castillo.pdf*

HORCHER, K.
2005 Essentials of Financial Risk Management. Nueva York: John Wiley & Sons. Puede visitarse con usuario y clave en la biblioteca de la Universidad La Gran Colombia en: *http://biblioteca.ugca.edu.co/cgi-bin/koha/opac-detail.pl?biblionumber=29079)*

HRBACKOVA, L.
2016 "Risk-based thinking in the production process using the methods of Quality Assurance Matrix and the FMEA Process". En: *Journal of Systems Integration*, 7(1), 21-28. Visitado el 26 de abril de 2016 en: http://www.si-journal.org/index.php/JSI/article/viewFile/247/199

JORION, Philippe
1997 *Value at Risk: The New Benchmark for Controlling Derivatives Risk.* Nueva York: Mc Graw Hill.

KNIGHT, K. W.
2010 "AS/NZS ISO 31000: 2009-The New Standard for Managing Risk". En: *Keeping Good Companies,* 62(2), pp. 68-69.

GASTINEAU, Gary L.
1999 *Dictionary of Financial Risk Management*. Nueva York: Wiley.

GJERDRUM, D., y M. PETER
2011 "The new international standard on the practice of risk management–A comparison of ISO 31000: 2009 and the COSO ERM framework". En: *Risk Management*, n.° 21, pp. 8–12. Vistado el 26 de abril de 2016 en: https://www.soa.org/library/newsletters/risk-management-newsletter/2011/march/jrm-2011-iss21-gjerdrum.pdf

LIZARZABURU, Edmundo
2011 "Risk Management, an Initial Guide: Literature Review, Statistics Use, Theory and Actual Information" (April 26, 2011). Available at SSRN: http://ssrn.com/abstract=1823845
2014 "La Gestión de Riesgos, un pilar en las organizaciones: Guía – ISO 31000". Recuperado de http://www.researchgate.net/publication/273777272_La_Gestin_de_Riesgos_un_pilar_en_las_organizaciones_Gua__ISO_31000

LALONDE, C. y O. BOIRAL
2012 "Managing risks through ISO 31000: A critical analysis". En: *Risk Management*, 14(4), pp. 272–300.

LENIN, Vladimir
S/f "Administración de riesgos financieros". México D.F.: Instituto Tecnológico Autónomo de México, 22 abril, (paper inédito).

LEITCH, M.
2010 "ISO 31000: 2009—The new international standard on risk management". En: Risk Analysis, 30(6), pp. 887–892.

Lizarzaburu, E. . 2013
2013 "Guía Revisión ISO 31000". 50° Asamblea Anual de Cladea 2015. En *Revista Oficial de Cladea*. Edición N° 33.

LIZARZABURU, E, L. BERGGRUN y J. QUISPE
2012 "Gestión de riesgos financieros. Experiencia en un banco latinoamericano". En: *Estudios Gerenciales* 12/2012; 28(125), pp. 87–95.

LIZARZABURU, E., L. BERGGRUN, H. GALINDO Y K. BURNEO
2015 Emerging Markets Integration in Latin America (MILA) Stock Market indicators: Chile, Colombia, and Peru (2008 – 2013). En: *Journal of Economics, Finance and Administrative Science*, 12/2015, 20(39).

LIZARZABURU, E. y L. BERGGRUN
2013 L. Gestión del riesgo cambiario: aplicación a una empresa exportadora peruana. En: Estudios

Gerenciales, 07/2013, 29(128), pp. 379-384.

LOPATINA, E.
2016 "Prospects of Risk Management on Small Trade Enterprises". En: BILGIN, M.H., H. DANIS, E.DEMIR y U. CAN (eds.). *Business Challenges in the Changing Economic Landscape*-Vol. 2, pp. 401-410). Springer International Publishing.

MARTÍNEZ TORRE-ENCISO, M. I. Y M. I. CASARES SAN JOSÉ-MARTÍ
2011 "El proceso de gestión de riesgos como componente integral de la gestión Empresarial". En: *Boletín de Estudios Económicos,* vol. LXVI, n.° 202, abril, pp. 73-93. Visitado el 26 de abril de 2016 en: https://www.fundacionmapfre.org/documentacion/publico/es/catalogo_imagenes/grupo.cmd?path=1068214

MARTÍNEZ FERREIRA, M.
2005 *Diagramas causa-efecto, Pareto y flujogramas. Gestión de la calidad.* Visitado el 26 de abril de 2016 en: http://www.gestiopolis.com/diagramas-causa-efecto-pareto-y-de-flujo-elementos-clave/

MARCELINO SÁDABA, S., A. PÉREZ-EZCURDIA, A. M. ECHEVERRÍA-LAZCANO Y M. BENITO AMURRIO
2016 "Definition of innovation projects in small firms: A Spanish study". En: *R&D Management*, vol. 46, n.° 1, pp. 36-48.

MASCAREÑAS, J.
2008 "El riesgo país". Visitado el 26 de abril de 2016 en: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2315675

MOELLER, R.
2007 *COSO Enterprise Risk Management: Understanding the new integrated ERM framework.* Nueva York: John Wiley and Sons.

ORGANIZACIÓN PARA LA COOPERACIÓN Y EL DESARROLLO ECONÓMICOS (OECD)
2004 *Principios de Gobierno Corporativo.* Visitado el 26 de abril de 2016 en: https://www.oecd.org/daf/ca/corporategovernanceprinciples/37191543.pdf

PATEL, N.
2016 "International trade finance and the cost channel of monetary policy in open economies. Bank For International Settelments-BIS, working papers n.° 539. Visitado el 26 de abril de 2016 en: http://www.bis.org/publ/work539.pdf.

SUPERINTENDENCIA DE BANCA Y SEGUROS DE LA REPÚBLICA DEL ECUADOR
2004 *Normas generales para las instituciones del sistema financiero.* Visitado el 26 de abril de 2016 en: http://www.sbs.gob.ec/medios/PORTALDOCS/downloads/normativa/nueva_codificacion/todos/L1_X_cap_I.pdf

PÉREZ FERNÁNDEZ DE VELAZCO, J.
2009 *Gestión por procesos. Reingeniería y mejora de los procesos de empresa.* México D.F.: ESIC Editorial.

Pérez, R.
1982 Punto de equilibrio. El análisis económico financiero.

PHILIPPE, J.
2003 *Value Financial Risk Manager Handbook.* Nueva York: Riley.
2010 *Valor en riesgo : el nuevo paradigma para el control de riesgos con derivados.* México D.F.: Limusa.

PINTO, J. y G. WINCH
2016 "The unsettling of "settled science:" The past and future of the management of projects". En: *International Journal of Project Management,* vol. 34, n.°2, pp. 237–245. Visitado el 26 de abril de 2016 en: http://www.sciencedirect.com/science/article/pii/S0263786315001325

PROJECT MANAGEMENT INSTITUTE (PMI)
2004 *Project Management Body of Knowledge.* Pensylvania: PMI.

PURDY, G.
2010 "ISO 31000: 2009—setting a new standard for risk management". En: *Risk analysis,* 30(6), pp. 881–886.

RAMÍREZ, A. y Z. ORTIZ
2011 "Gestión de riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios". En: *Ingeniería,* vol. 16, n.° 2, pág. 56–66.

ROISENZVIT, A. y M. ZÁRATE
2006 "Hacia una cultura de Risk Management: El próximo desafío para la región y cómo esto afecta los procesos de evaluación FSAP". Buenos Aires: Superintendencia de Entidades Financieras y Cambiarias (SEFC)–Banco Central de la República Argentina. Visitado el 26 de abril de 2016 en: http://www.riesgooperacional.com/docs/paper_alfredo.pdf

SAMANIEGO, R y J. MARTÍN
2008 *El Riesgo de Crédito en el Marco de Basilea II. Sevilla:* Universidad Pablo Olavide. Publicaciones universitarias.

SCHROEDER, R., S. MEYER, M. RUNGTUSANATHAM
2011 *Administración de operaciones.* México D. F.: McGraw-Hill.

SRIVANNABOON, S.
2006 "Linking Project Management with Business Strategy". PMI Global Congress Proceedings. Visitado el 26 de abril de 2016 en: http://depts.washington.edu/pmgroup/GlobalCongress2006/BNS05_wp.pdf

Shimiko, D ; Went, P. Market Risk Management, 2010.

Universidad de Vigo (2000). *Diagrama causa-efecto. Gestión de la calidad, la seguridad y el medio ambiente.*

WILLIAMSON, D.
2007 "The COSO ERM Framework: A critique from systems theory of management control". En: *International Journal of Risk Assessment and Management*, vol.7, n.° 8.

ZASK, Ezra
"The Derivatives Risk Management Audit. En: KLEIN, R. A. y J. LEDERMAN. *Derivatives Risk and Responsibility.* Chicago: Irwin.

Páginas web:

www.bcrp.gob.pe
www.sbs.gob.pe
www.smw.gob.pe
www.asbanc.com.pe

INTRODUCCIÓN A LA GESTIÓN INTEGRAL DE RIESGOS EMPRESARIALES
ENFOQUE: ISO 31000

Isabel Casares San José-Martí
Edmundo R. Lizarzaburu Bolaños

Los autores proponen un trabajo de aplicación sobre los principales marcos teóricos y de implementación de la gestión de los riesgos tomando como eje principal la norma ISO 31000, la cual permite contar con una aproximación a la gestión sistemática, ordenada y auditable de los riesgos de cualquier compañía.

Se desarrollan los principios del estándar ISO 31000 como marco general para la gestión de los riesgos y control interno, pero también la implementación de la actualización del marco de trabajo de COSO en su versión 2013, dando énfasis en la gestión de la seguridad de la información y el desarrollo del riesgo de fraude como entidad separada de los otros riesgos. Esta actualización de principios permite una visión sistemática e integral de la gestión de riesgos y su evolución en los últimos veinte años.

En tal sentido, este libro busca ayudar a entender la necesidad de gestionar los riesgos de una empresa, no solo reducirlos, y así generalizar un criterio para todo tipo de riesgos, incluidos los riesgos estratégicos, legales, operacionales, financieros, tecnológicos, reputacionales, etcétera.

La principal ventaja del camino escogido por los autores es la escalabilidad de las recomendaciones propuestas para distintos tamaños de empresa y niveles de complejidad del negocio, y casos prácticos para el desarrollo del lector.

Platinum Editorial