GESTIÓN, ADMINISTRACIÓN DE RIESGOS Y MODELOS DE CONTROL INTERNO

Javier Castañeda

AREANDINA
Fundación Universitaria del Área Andina

MIEMBRO DE LA RED
ILUMNO

Gestión, Administración de Riesgos y Modelos de Control Interno
Javier Castañeda
Bogotá D.C.

Fundación Universitaria del Área Andina. 2018

Catalogación en la fuente Fundación Universitaria del Área Andina (Bogotá).

Gestión, Administración de Riesgos y Modelos de Control Interno

ISBN (impreso): 978-958-5462-78-6

Fundación Universitaria del Área Andina
Calle 70 No. 12-55, Bogotá, Colombia
Tel: +57 (1) 7424218 Ext. 1231
Correo electrónico: publicaciones@areandina.edu.co

Director editorial: Eduardo Mora Bejarano
Coordinador editorial: Camilo Andrés Cuéllar Mejía
Corrección de estilo y diagramación: Dirección Nacional de Operaciones Virtuales
Conversión de módulos virtuales: Katherine Medina

BANDERA INSTITUCIONAL

Pablo Oliveros Marmolejo †
Gustavo Eastman Vélez
Miembros Fundadores

Diego Molano Vega
Presidente del Consejo Superior y Asamblea General

José Leonardo Valencia Molano
Rector Nacional
Representante Legal

Martha Patricia Castellanos Saavedra
Vicerrectora Nacional Académica

Jorge Andrés Rubio Peña
Vicerrector Nacional de Crecimiento y Desarrollo

Tatiana Guzmán Granados
Vicerrectora Nacional de Experiencia Areandina

Edgar Orlando Cote Rojas
Rector – Seccional Pereira

Gelca Patricia Gutiérrez Barranco
Rectora – Sede Valledupar

María Angélica Pacheco Chica
Secretaria General

Eduardo Mora Bejarano
Director Nacional de Investigación

Camilo Andrés Cuéllar Mejía
Subdirector Nacional de Publicaciones

GESTIÓN, ADMINISTRACIÓN DE RIESGOS Y MODELOS DE CONTROL INTERNO

Javier Castañeda

AREANDINA
Fundación Universitaria del Área Andina

MIEMBRO DE LA RED
ILUMNO

ÍNDICE

GESTIÓN, ADMINISTRACIÓN DE RIESGOS Y MODELOS DE CONTROL INTERNO

Javier Castañeda

EJE 1

Conceptualicemos

AREANDINA
Fundación Universitaria del Área Andina
MIEMBRO DE LA RED
ILUMNO

Fuente: Shutterstock/394229008

INTRODUCCIÓN

En los escenarios nacional e internacional se repiten situaciones de **riesgo** que afectan el sector organizacional. La manifestación del riesgo es diversa y existen múltiples riesgos de carácter estratégico, táctico, operativo, geopolítico (riesgo país), legal, crediticio, tecnológico, etc. En el año 2017, el mundo se estremeció inerme ante el ataque cibernético al sector público y privado realizado por *hackers* con un virus bautizado como WannaCry, el cual afectó, según IT User (2017), a más de 100 países y millares computadoras de prestigiosas empresas como Telefónica y Renault, bloqueando el acceso a información común y sensible. Los piratas informáticos pidieron de manera extorsiva el pago de un rescate en *bitcoin*, moneda virtual que permite transacciones con mínima posibilidad de trazabilidad. Los medios de comunicación y expertos de compañías especializadas en seguridad informática calcularon que el ataque podría haber costado entre 1000 y 4000 millones de dólares estadounidenses.

El riesgo es una situación asociada a cualquier actividad que desarrolla el ser humano, de ahí que en el campo empresarial se presenten de manera permanente múltiples situaciones que pueden generar daños y pérdidas. Ante este tipo de amenazas, se han adoptado políticas de **gestión del riesgo** y modelos de control interno, entendidos como las herramientas que permiten adelantar la gestión de estos, teniendo en cuenta que no solo basta con reducirlos, sino que se deben gestionar entendiéndolos de manera sistemática para abordarlos mediante diferentes opcio nes de manejo.

En el presente eje se propone la pregunta: ¿cómo la conceptualización de gestión del riesgo y los modelos de control interno permiten identificar escenarios de riesgo de manera efectiva para ser tratados a fin de reducir su impacto en las organizaciones?, con el ánimo de abordar los conceptos de la gestión del riesgo y los modelos que se emplean en su implantación en las organizaciones. Cuando se entiende un proceso en detalle y se comprenden su terminología y sus alcances, es posible actuar y tomar decisiones acertadas, por lo cual es imperativo que quienes hacen parte de una organización conozcan los procesos, los conceptos y sus alcances, puesto que en esto reside la capacidad de una organización para responder un requerimiento

Riesgo

Según el Icontec (2009), es el efecto de la incertidumbre sobre los objetivos.

Gestión del riesgo

Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo (Icontec, 2009).

que, en este caso, es la gestión del riesgo. Para atender estos requerimientos hay muchas metodologías y enfoques que, en mayor o menor medida, son efectivos si se tiene clara su aplicación. Como menciona Moncayo (2016): "Se puede confirmar que tanto la gerencia de los riesgos como un adecuado sistema de control interno pueden contribuir al logro de objetivos empresariales", lo cual deja claro que se deben combinar estas dos acciones para obtener un buen resultado.

El presente referente de pensamiento está organizado para desarrollar una aproximación a la conceptualización de la gestión del riesgo en los **sistemas de control interno** y **auditorías**, realizando un proceso que va de lo general a lo particular, donde se trabajarán definiciones que permitan estandarizar las posturas frente a diferentes significados. Se desarrollará una taxonomía de los riesgos organizacionales y corporativos; también se abordarán de manera general las normas y los sistemas en la gestión del riesgo, los modelos de control interno actuales y la metodología de gestión del riesgo definida en la Norma Técnica Colombiana ISO 31000. En el eje 2 se tratarán con detalle los modelos de control interno y su relación con la gestión y administración del riesgo.

Sistemas de control interno

El Sistema de Control Interno (SCI) es el conjunto de políticas, principios, normas, procedimientos y mecanismos de verificación y evaluación establecidos por la junta directiva, la alta dirección y demás funcionarios de la organización para proporcionar un grado de seguridad razonable en cuanto a la consecución de los objetivos (Serfinansa, s. f.).

Auditorías

Proceso que consiste en el examen crítico, sistemático y representativo del sistema de información de una empresa o parte de ella, realizado por un experto con independencia y utilizando técnicas determinadas, con el propósito de emitir una opinión profesional sobre la misma que permita la adecuada toma de decisiones y brindar recomendaciones que mejoren el sistema examinado (Cuellar, s. f.).

Orígenes del riesgo y su universalidad

El riesgo es una situación connatural al hombre. Su origen etimológico está en el idioma árabe con la palabra *rizq*. También se origina del término italiano *rishio*, asociado a la idea de *risco*.

El hombre siempre ha estado acompañado de riesgos de origen natural y creados por él mismo. Por el nivel de tecnología y desarrollo, los materiales y los procesos, al principio los riesgos creados eran básicos, puesto que las actividades del hombre estaban centradas en el ámbito rural, con dedicación a la agricultura, la ganadería, la pesca, el comercio y otras faenas. Con los adelantos tecnológicos, como el descubrimiento de la rueda, la capacidad de construir estructuras complejas y la revolución industrial (con la cual se implantó la máquina de vapor), el hombre dio un salto tecnológico que cambió la humanidad. El concepto se volvió urbano, los procesos se volvieron complejos, puesto que se contaba con herramientas que podían transformar el entorno de manera significativa y rápida, y se pasó a la industrialización y la mecanización de los procesos. Estos adelantos representaron un punto de inflexión para los seres humanos; con ellos, aumentaron los riesgos para quienes trabajaban y operaban la tecnología y para quienes estaban a su alrededor.

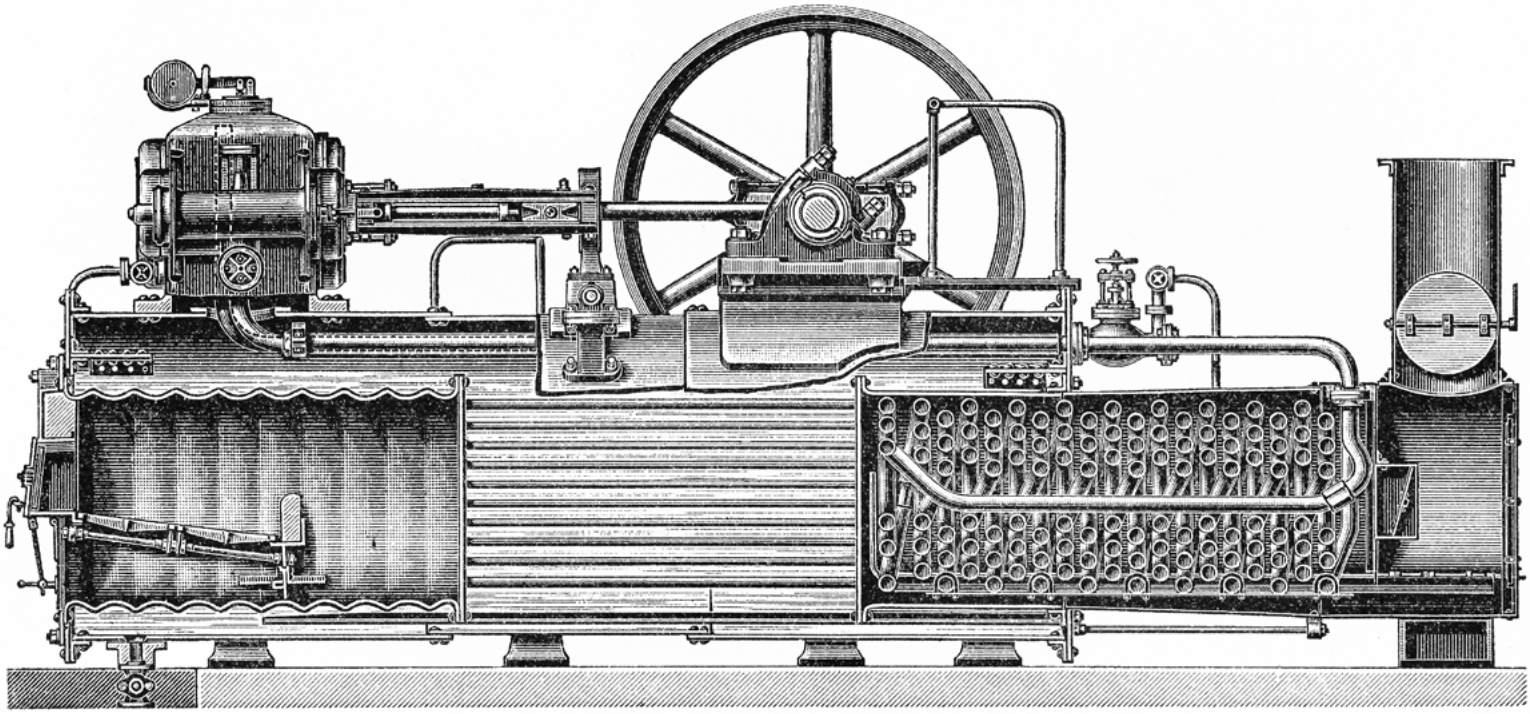

Figura 1. Máquina de vapor
Fuente:shutterstock/93873745

De la Revolución industrial derivaron beneficios para la humanidad: el transporte alcanzó niveles de desarrollo importantes, luego vendría el avión, la producción de energía por medios sofisticados, como el combustible nuclear para generar electricidad, y otras invenciones que han facilitado los procesos productivos, pero también han aumentado los niveles de riesgo en el campo tecnológico. A esto se sumarían otros modos o tipos de riesgo como el financiero, el biológico, el laboral, etc.

En el campo empresarial, las organizaciones están sujetas a riesgos. De hecho, su definición abarca acciones como esfuerzo, trabajo y dificultades (Castañeda, 2016), las cuales están ligadas al desempeño del talento humano y a errores, fallas y procedimientos producto del proceder del hombre en el contexto social.

El riesgo, entendido como una acción que se puede manifestar de múltiples maneras y en diferentes momentos, ha sido objeto de estudio con posturas y consideraciones desde el ámbito público y el privado; por ello, el concepto de gestión del riesgo ha servido para paliar sus efectos. Aunque hay escépticos ante su implementación y aplicación, las circunstancias cambiantes y los nuevos paradigmas de la actualidad nacional e internacional demandan atención al riesgo como un factor de competitividad.

Si bien es cierto que desde la posición epistemológica es clara la conceptualización de riesgos, en su aplicación no se tiene conciencia de su integralidad, la cual permite que esta permee todos los escenarios y procesos de la organización, tanto de manera endógena como exógena, con el objetivo de manejar los riesgos a partir de una visión holística que permita tomar decisiones de manera ordenada y sistemática.

Se llama a todos los miembros de la organización a interactuar en la gestión del riesgo. A pesar de que la alta dirección es la encargada de implementar y apoyar los procesos, los resultados se dan por la gestión de todos, desde su responsabilidad, desempeño y compromiso. Por esto, es imprescindible crear la cultura del riesgo, entendida como el cúmulo de políticas, normas y disposiciones de la organización para adelantar acciones que identifiquen, analicen, evalúen, traten y monitoreen el riesgo.

¡Importante!

Más allá de anular el riesgo, el objetivo de la gestión es minimizarlo, teniendo claro que, por más acciones de tratamiento que se apliquen, siempre existirá un riesgo residual, de allí que se busque que su materialización o impacto sean leves, sin causar daños o perjuicios que demanden mayor intervención y recursos para recuperar o normalizar el proceso que tuvo desviaciones.

¿Qué es el riesgo?

La palabra riesgo tiene muchas acepciones que dependen de la perspectiva desde donde se mire. En este eje, su definición se centrará en los riesgos propios del ejercicio empresarial, abarcando la conceptualización de la normatividad vigente internacional con base en las normas ISO y los modelos de control interno.

La NTC ISO 31000 define riesgo como el "efecto de la incertidumbre sobre los objetivos" (Icontec, 2009, p. 4). Se entiende efecto como el comportamiento diferente al esperado, lo cual ocasiona consecuencias para quienes son objeto del resultado. La incertidumbre es la falta de claridad e información ante efectos o eventos que se pueden producir, por ende, es difícil prevenir desenlaces nocivos sobre las metas trazadas, las cuales pueden tener diferentes consideraciones: financieras, económicas, de seguridad, de impacto ambiental y legales. Por su nivel, pueden afectar lo estratégico, táctico u operativo.

Una definición más detallada de riesgo es: "Conjunto de factores externos y/o internos que posibilitan la ocurrencia de un evento de carácter negativo que puede alterar el desarrollo de un proceso, siendo sus componentes la amenaza y la vulnerabilidad en un grado de exposición nocivo" (Castañeda, 2016, p. 4).

Figura 2. Esquema del riesgo
Fuente: Castañeda (2016)

Para definir el riesgo empresarial, el enfoque se da en términos de los factores externos e internos que convergen en el desarrollo del objeto social de la organización. Este se plantea como el conjunto de factores de carácter externo e interno que, por su interacción en el ámbito empresarial, pueden originar eventos negativos de diferentes niveles de impacto, causando alteraciones en los objetivos de manera significativa (parcial o total).

Fuente: 404762026

Las organizaciones poseen grupos de interés llamados *stakeholders*, los cuales tienen alcances desde lo interno y externo; por ello, en la gestión del riesgo es importante abarcar todos estos actores, puesto que, en buena medida, aportan a prevenir daños.

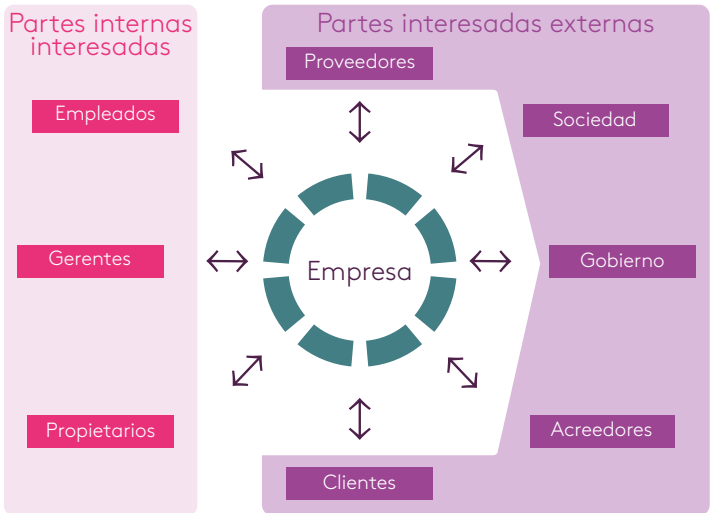

Figura 3. Mapa de *stakeholders*
Fuente: Gallego (2012)

Instrucción

Con el fin de entender y complementar de una manera práctica la interrelación de los *stakeholders* en torno a una organización y su injerencia como fuentes de riesgo, desarrolle la actividad de aprendizaje "Caso carrusel de la contratación en Bogotá", donde se deja en evidencia cómo se articulan el sector interno y externo maximizando los escenarios de riesgo.

¿Qué es la gestión del riesgo?

La NTC ISO 31000 define la gestión del riesgo como las actividades coordinadas para dirigir y controlar una organización con respecto al riesgo; sin embargo, una definición más amplia y detallada se da en la Ley 1523 de 2012:

> Es el proceso [...] de planeación, ejecución, seguimiento y evaluación de políticas y acciones permanentes para el conocimiento del riesgo y promoción de una mayor conciencia del mismo, impedir o evitar que se genere, reducirlo o controlarlo cuando ya existe y para prepararse y manejar las situaciones de [materialización del riesgo], así como para la posterior recuperación [...] En resumen, la gestión del riesgo como se ha mencionado es lograr a través de acciones conjuntas un resultado que resuelva un problema, que para el caso es la tratar el riesgo para minimizar su efecto (Congreso de la República de Colombia, 2012, p. 4).

Clasificación y caracterización de los riesgos

En el ámbito del riesgo existen varias clasificaciones. Una variable que permite realizar de manera ordenada esta estructuración son los contextos en los cuales interactúa una organización (campo externo e interno), aspectos que agrupan todas las áreas de riesgo.

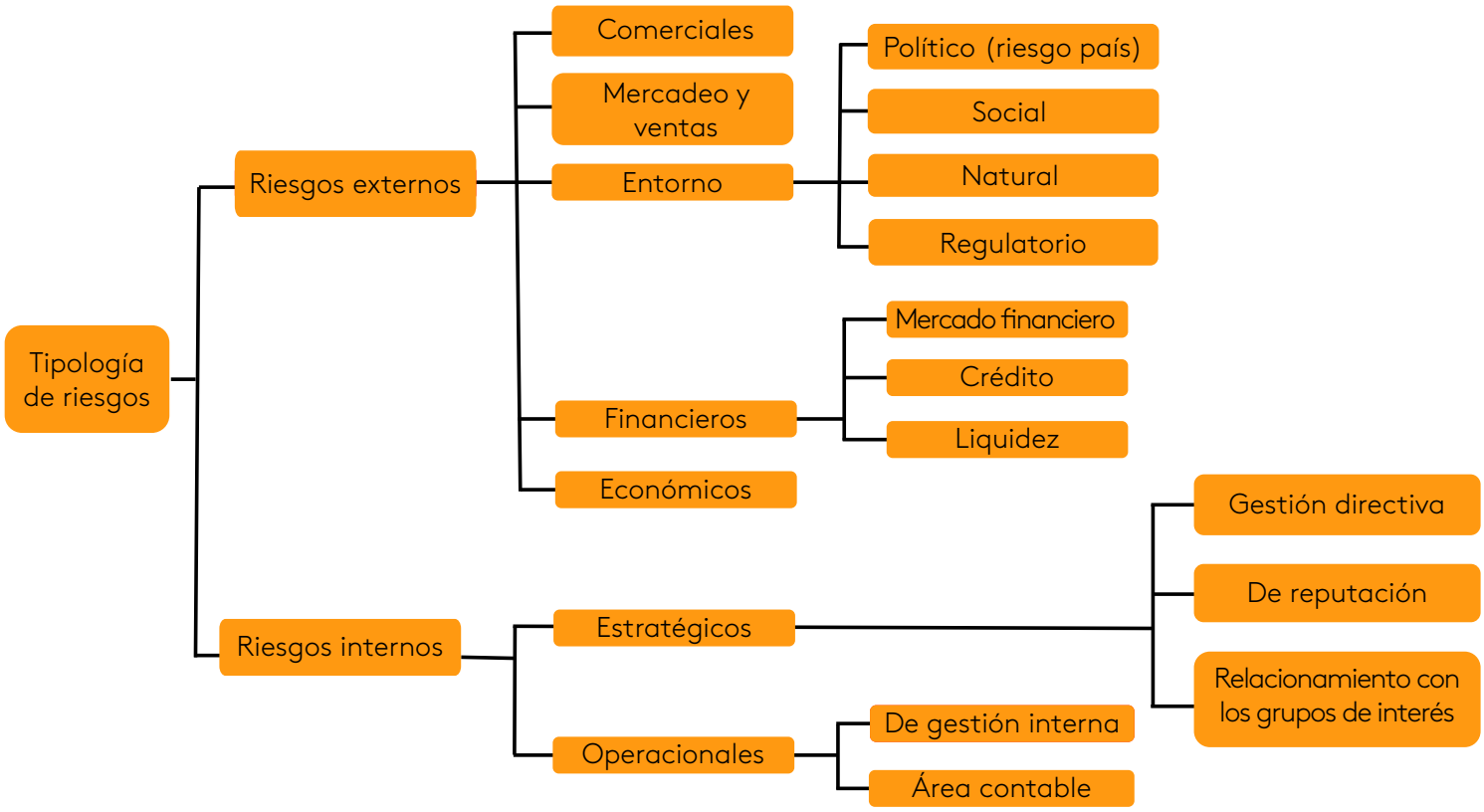

Figura 4. Clasificación de los tipos de riesgo
Fuente: Castañeda (2016)

Los riesgos en el contexto interno tienen su origen en las actividades que se desarrollan dentro de la organización. Los miembros de esta, denominados parte involucrada, son quienes generan y se convierten en fuentes de riesgos por factores relacionados con el desconocimiento, la inexperiencia o la negligencia. Con esto, se gesta la probabilidad de la materialización de los riesgos.

La presente clasificación tuvo en cuenta dos tipos de riesgo que, si bien dependen del contexto externo, pueden ser controlados e intervenidos desde la alta dirección de la organización por su manifestación interna:

- Estratégicos: abarcan aquellos que se generan en los niveles altos de decisión de la organización, como la gestión directiva, la reputación de la organización y el relacionamiento con grupos de interés.

- Operacionales: están orientados a la actividad propia adelantada por los miembros de la organización. Se consideran de gestión interna. Entre otros, está el manejo del área contable.

Los riesgos que provienen del contexto externo afectan la operación de la organización de manera importante. Para su tratamiento, se deben adoptar medidas adaptativas, de transferencia o cambios estructurales para evitar daños mayores. La clasificación se hizo en cinco tipos de riesgos que tienen una subclasificación por su campo de afectación.

- Comerciales: son todos aquellos factores que pueden afectar la cadena de suministro de una empresa desde los procesos logísticos, como el aprovisionamiento externo, la producción (que tiene aspectos internos y externos) y la distribución (que tiene parte interna y externa por parte de la organización).

- Mercadeo y ventas: están vinculados a los aspectos que adelanta la organización desde su rol, pero también del entorno externo donde se puedan aplicar los procesos planeados, los impactos esperados, la fidelización y el servicio al cliente.

- Financieros: se consideran las variables que interfieren en la tasa de retorno esperada y cuya materialización es nociva para los intereses de la organización de manera parcial o total, como el mercado financiero, el crédito y la liquidez.

- Económicos: son factores que se manejan en el campo macroeconómico. Su injerencia es desde la alta dirección del Estado y las intervenciones de organismos internacionales que regulan el comportamiento económico mundial.

- Entorno: se tienen en cuenta factores que, por su origen, se centran en los campos del poder y son propios de un país, dado que su manejo y responsabilidad están a cargo de sus habitantes: lo político, lo social y lo regulatorio. También están considerados los riesgos de origen natural producto de las manifestaciones de la naturaleza.

Instrucción

Para ampliar y complementar el conocimiento acerca de la tipología de riesgos y poner en práctica lo aprendido, le sugiero que desarrolle el caso "Foncolpuertos", identificando y analizando los riesgos allí materializados.

Normatividad vigente de la gestión y administración de riesgos

Figura 5. Representación reconocimiento ISO 39000 en manejo de riesgo
Fuente:shutterstock/549134926

En el campo de la gestión del riesgo existen numerosas directrices que orientan a las organizaciones para el tratamiento del mismo. Las normas ISO contemplan la gestión del riesgo desde diferentes perspectivas, pero la que abarca de forma específica el concepto es la ISO 31000, anteriormente denominada 5154 de Icontec. En el sector público también se tienen documentos referentes a la gestión del riesgo. Un documento que integra de manera sistemática lo relacionado con el tema es la *Guía para la administración riesgo del* Departamento Administrativo de la Función Pública.

Lectura recomendada

Para profundizar en el conocimiento de la gestión del riesgo se debe investigar sobre la temática. Lo invito a leer en la página principal del eje, el documento *Guía para la administración del riesgo* (pp. 13-14) del Departamento Administrativo de la Función Pública, en el cual hay una conceptualización básica en riesgos.

Proceso metodológico de gestión y administración de riesgos

La gestión del riesgo considera las acciones sistemáticas, cíclicas e integrales que permiten identificar, valorar y tratar eventos y riesgos de diferentes orígenes que pueden causar daño a la organización. Esta se desarrolla de manera organizada en la ISO 31000, la cual establece un proceso metodológico para su aplicación en cualquier campo del conocimiento y, específicamente, en el empresarial.

Etapas de la gestión del riesgo

Para adelantar el proceso de gestión del riesgo con base en la ISO 31000, existe una ruta lógica y sistemática que permite hacer la valoración y el tratamiento del riesgo con un alto grado de detalle, lo cual asegura que siempre exista flujo de comunicación y monitoreo para garantizar que cualquier cambio retroalimente todo el proceso. El diseño del proceso proyecta un desarrollo de lo general a lo particular, con el fin de trabajar a partir de información general la información específica.

Las etapas del proceso son:

- Diagnóstico y establecimiento del contexto:
  - Contexto estratégico o externo.
  - Contexto organizacional o interno.
  - Contexto de la gestión del riesgo.
  - Criterio para la evaluación del riesgo.
  - Definir la estructura de gestión del riesgo.
- Valoración del riesgo:
  - Identificación del riesgo.
  - Análisis del riesgo.
  - Calificación del riesgo.
  - Evaluación del riesgo.
- Tratamiento del riesgo.
- Comunicación y consulta.
- Monitoreo y seguimiento.

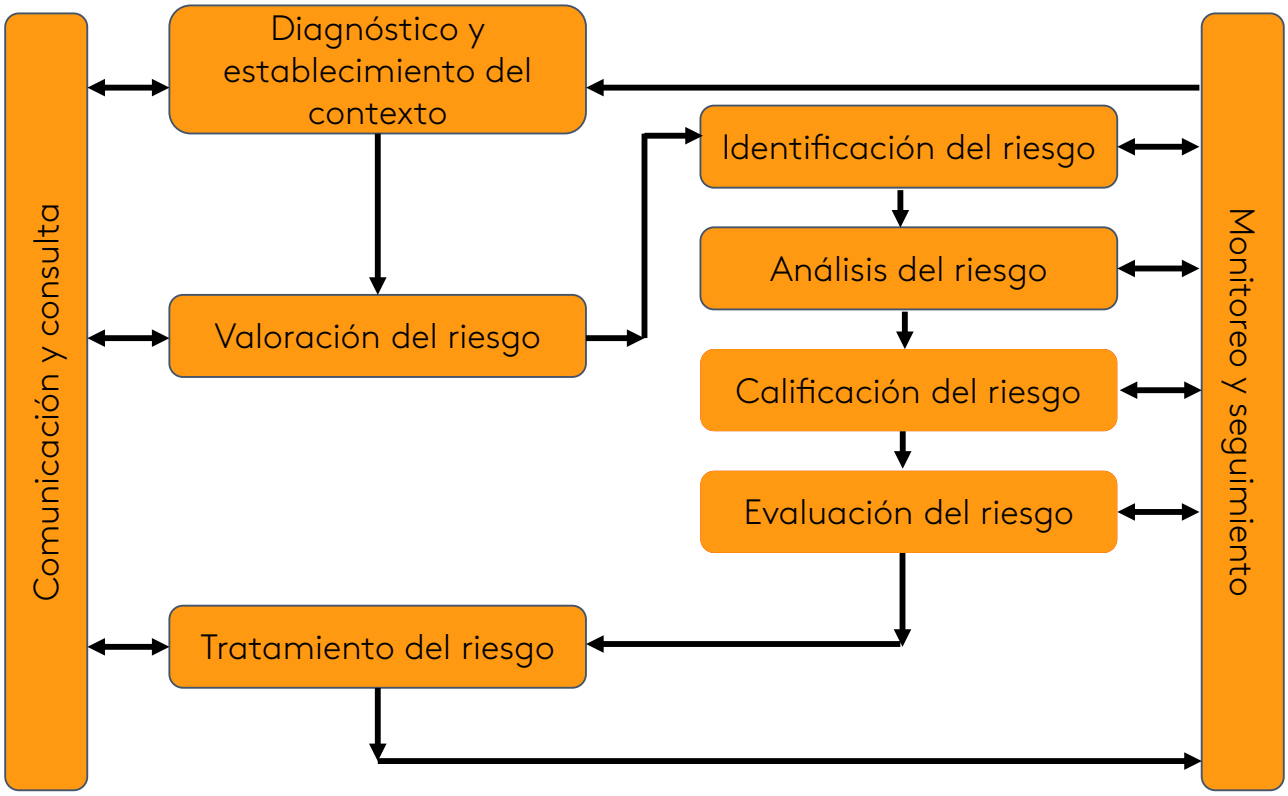

Figura 6. Etapas de la gestión del riesgo
Fuente: Castañeda (2016)

Diagnóstico y establecimiento del contexto

Esta etapa tiene como objetivo establecer de manera espacio-temporal la situación de la organización con respecto al contexto externo e interno. Aquí se fijan los alcances del proceso en materia de administración del riesgo, así como los detalles de las acciones y los eventos pasados y presentes que intervienen en el inicio del diagnóstico.

Valoración del riesgo

Por las actividades que se desarrollan, esta es una de las etapas más importantes:

- Identificación y medición del riesgo: en este punto se evidencian las situaciones que revisten riesgos para la organización. Es un momento del proceso que da la posibilidad de tomar acciones preventivas.

- Análisis del riesgo: implica abordar el evento de manera detallada con el fin de conocerlo a fondo. En este paso se establece la probabilidad de que ocurra el riesgo y, a la vez, el impacto de su materialización.

- Calificación del riesgo: tiene como objetivo determinar la magnitud del riesgo para establecer qué tan representativo sería para la organización si se llegara a materializar. La variable que se emplea en este punto es la probabilidad de ocurrencia por el impacto de las consecuencias de su materialización. Las escalas pueden ser cuantitativas, cualitativas o semicuantitativas.

- Evaluación del riesgo: establece cuál es la situación de los eventos analizados y calificados. Indica cuáles tienen mayores valores en lo cualitativo o cuantitativo, con el fin de dar prioridad a su tratamiento por el nivel de gravedad que revisten para la organización.

Tratamiento del riesgo

La norma ISO 31000 determina varias opciones que permiten el manejo y tratamiento del riesgo:

- Evitar el riesgo al decidir no iniciar o continuar la actividad que lo origina.
- Tomar o incrementar el riesgo para perseguir una oportunidad.
- Retirar la fuente de riesgo.
- Cambiar la probabilidad.
- Cambiar las consecuencias.
- Compartir el riesgo con una o varias de las partes (incluyendo los contratos y la financiación del riesgo).
- Retener el riesgo mediante una decisión informada.

Autores como Mejía (2006) plantean seis medidas para tratar el riesgo, según dos variables: el control y la financiación, esta última entendida como recursos económicos adicionales en el tratamiento del riesgo. En el siguiente cuadro se pueden evidenciar las variables mencionadas:

Medida	Control	Financiación
Evitar	X	
Aceptar, tomar o incrementar	X	
Anticipar o prevenir	X	
Proteger	X	
Transferir	X	X
Retener	X	X

Tabla 1. Medidas para tratar riesgos
Fuente: Mejía (2006) y Castañeda (2016)

Visitar página

Una herramienta importante en el proceso de aprendizaje es el mapa conceptual. Consulte el siguiente *link* sobre el tratamiento del riesgo.

Comunicación y consulta - monitoreo y seguimiento

Figura 7. Concepto de gestión de riesgo
Fuente: shutterstock/284064425

En el desarrollo de la metodología de gestión del riesgo se adelanta el proceso de comunicación y consulta, en el cual se revisan los pasos para complementar información, agregar hallazgos, actualizar datos, etc. A la vez, se trabaja con un esquema de monitoreo y seguimiento, con el fin de evidenciar la pertinencia y oportunidad de las actividades que se realizan y, con ello, detectar acciones oportunas para minimizar daños a la organización. Estos procesos son constantes, puesto que su objetivo es estar presentes en el desarrollo metodológico de la gestión del riesgo.

Sistema de administración de riesgo

El sistema de administración de riesgo se implementa a partir de las políticas de la organización para el tratamiento del riesgo. Su objetivo es administrar el riesgo, con el fin de fortalecer los sistemas de control interno. En la Ley 87 de 1993 se define el Sistema de Control Interno (SCI) como:

> Sistema integrado por el esquema de organización y el conjunto de los planes, métodos, principios, normas, procedimientos, y mecanismos de verificación y evaluación adoptados por una Entidad, con el fin de procurar que todas las actividades, operaciones y actuaciones, así como la administración de la información y los recursos, se realicen de acuerdo con las normas [...], dentro de las políticas trazadas por la dirección y en atención a las metas y objetivos previstos (Congreso de la República de Colombia, 1993, p. 1).

Si desea ampliar sus conocimientos sobre el decreto por el cual se establecen las normas para el ejercicio del control interno en las entidades y los organismos del Estado, consulte: Ley 87 de 1993.

La gestión del riesgo es parte integral de los sistemas de control interno. Su implementación se hace través de la alta dirección de las organizaciones que buscan transparencia y calidad en sus procesos, reduciendo al máximo los eventos que puedan afectar su normal desarrollo.

La metodología para la gestión del riesgo aplica para el análisis, la evaluación y el tratamiento de cualquier tipo de riesgo asociado a la empresa. Su objetivo es complementar el SCI que se estructure en la organización.

BIBLIOGRAFÍA

Castañeda, J. (2016). Módulo: *Prevención y gestión del riesgo*. Bogotá, Colombia: Fundación Universitaria del Área Andina.

Congreso de la República de Colombia. (24 de abril de 2012). Ley 1523 de 2012. DO: 48411.

Congreso de la República de Colombia. (29 de noviembre de 1993). Ley 87 de 1993. DO: 41120.

Cuellar, G. (s. f.). Concepto universal de auditoría. T*eoría general de la auditoría y revisoría fiscal*. Recuperado de ftp://ftp.unicauca.edu.co/cuentas/.cuentasbajadas29092009/gcuellar.back/docs/teoria.pdf

Departamento Administrativo de la Función Pública. (2011). *Guía para la administración del riesgo*. Recuperado de http://www.funcionpublica.gov.co/documents/418537/506911/1592.pdf/73e5a159-2d8f-41aa-8182-eb99e8c4f3ba

Gallego, M. (2012). Relación con los stakeholders. Recuperado de http://slideplayer.es/slide/1064742/

Icontec. (2009). NTC ISO 31000. *Gestión del riesgo*. Bogotá, Colombia: Icontec.

IT User. (2017). *El coste del ciberataque de WannaCry podría superar los 4.000 millones de dólares*. Recuperado de http://www.ituser.es/seguridad/2017/05/el-coste-del-ciberataque-de-wannacry-podria-superar-los-4000-millones-de-dolares

Mejía, R. (2006). Administración de riesgos. *Un enfoque empresarial*. Bogotá, Colombia: Fondo Editorial Universidad Eafit.

Moncayo, C. (21 de julio de 2016). *Importancia del control interno en las empresas*. Recuperado de http://www.incp.org.co/importancia-del-control-interno-en-las-empresas/

Moreno, T. (2012). *Historia de la gestión de riesgos en el mundo y en el Ecuador*. Recuperado de http://es.calameo.com/read/002896401c5ffd0ca7f9c

GESTIÓN, ADMINISTRACIÓN DE RIESGOS Y MODELOS DE CONTROL INTERNO

Javier Castañeda

EJE 2

Analicemos la situación

AREANDINA
Fundación Universitaria del Área Andina
MIEMBRO DE LA RED
ILUMNO

Fuente: Shutterstock/258980774

INTRODUCCIÓN

A lo largo de la historia se han presentado múltiples situaciones anormales dentro de las organizaciones producto de fallas y acciones humanas indebidas. La corrupción, la negligencia, la ineficiencia, la competencia desleal, la piratería informática, el comportamiento errático de la economía mundial y otros flagelos han generado circunstancias difíciles de dirigir para quienes están al frente de empresas e instituciones.

En la actualidad, los escenarios nacionales e internacionales están saturados de riesgos y amenazas que nacen del ejercicio empresarial. El talento humano es el principal factor para contrarrestar sus efectos, pero también el causante de muchos de ellos. Ante este panorama, diversas organizaciones han creado mecanismos y soluciones que permitan implantar metodologías sistemáticas, claras y oportunas para atenuar los efectos nocivos que pueden tener estos problemas sobre los procesos administrativos.

En muchos países se han desarrollado modelos de control interno que incluyen la gestión del riesgo como opción para minimizar los daños a las organizaciones. Existen múltiples experiencias desastrosas de empresas que fueron prósperas, pero cayeron en bancarrota por el mal manejo financiero, comercial, contable, etc.

Los modelos que se exponen en el eje tienen ventajas y alcances con matices y estructuras diferenciadas en su aplicación; sin embargo, su finalidad es implantar un esquema que logre gestionar los procesos dentro de la organización mediante el control de sus actividades, procesos, procedimientos y funciones, generando de manera natural, pero sistemática, mecanismos para materializar un SCI efectivo que permita cumplir las metas y, a la vez, garantice la integridad y salud de la organización.

Este referente de pensamiento busca hacer una revisión integral de los sistemas de control interno que se han desarrollado en el mundo con altos estándares de aplicación, con el objetivo de generar doctrina frente a la necesidad de las organizaciones de controlar los escenarios de riesgo causados por factores de orden humano que suelen materializarse ante situaciones de poco o nulo control. La pregunta que enmarca la finalidad del referente es: ¿de qué forma los sistemas de gestión y administración de riesgos permiten generar un ámbito de control donde se puedan identificar los riesgos para actuar oportunamente ante situaciones que atenten contra la sostenibilidad de una organización? De allí que se trabajen los modelos más notables y se haga un desarrollo a partir de actividades para el aprendizaje, en las cuales se evidencien y pongan en práctica acciones para mejorar la vida de las organizaciones.

Sistemas y modelos de control interno

Figura 1. Control interno
Fuente: shutterstock/432626284

Los sistemas y modelos de control interno han evolucionado de la mano con la existencia del hombre. En documentos y grabados en piedra existen evidencias del control de los recursos económicos de los pueblos, con el fin de evitar que se perdieran o fueran hurtados. Los inicios y avances en la materia se dieron con el ánimo de garantizar los recursos del Estado y de las empresas. Con el tiempo, se evolucionó en la concepción de los procesos y la figura de la auditoría se fortaleció, como expone el Ministerio de Comercio, Industria y Turismo (2005): "La auditoría como profesión fue reconocida por primera vez bajo la Ley Británica de Sociedades Anónimas de 1862. Entre 1862 y 1905, la profesión de auditor creció en Inglaterra y su principal objetivo entonces era la detección del fraude". Pronto, esta concepción llegó a otras latitudes y, con mayor o menor interpretación en su rol, se aplicó para controlar los procesos internos de las organizaciones y detectar posibles situaciones de dolo en el manejo de recursos financieros.

El desarrollo de modelos de control interno como un proceso metódico e integrado cobró fuerza en el siglo XX. Las actuaciones comerciales de las empresas después de la Segunda Guerra Mundial, la corrupción sistemática, los escándalos en gobiernos del primer mundo, el aumento de las quiebras de empresas importantes, etc., fueron la antesala para que se idearan diferentes modelos. El primero que se referencia es el Modelo de Control Interno del Committee of Sponsoring Organizations of The Treadway Commission (COSO), estructurado en Estados Unidos. Posteriormente, en otros países se constituyeron variados modelos para ejercer control sobre las organizaciones y garantizar su permanencia.

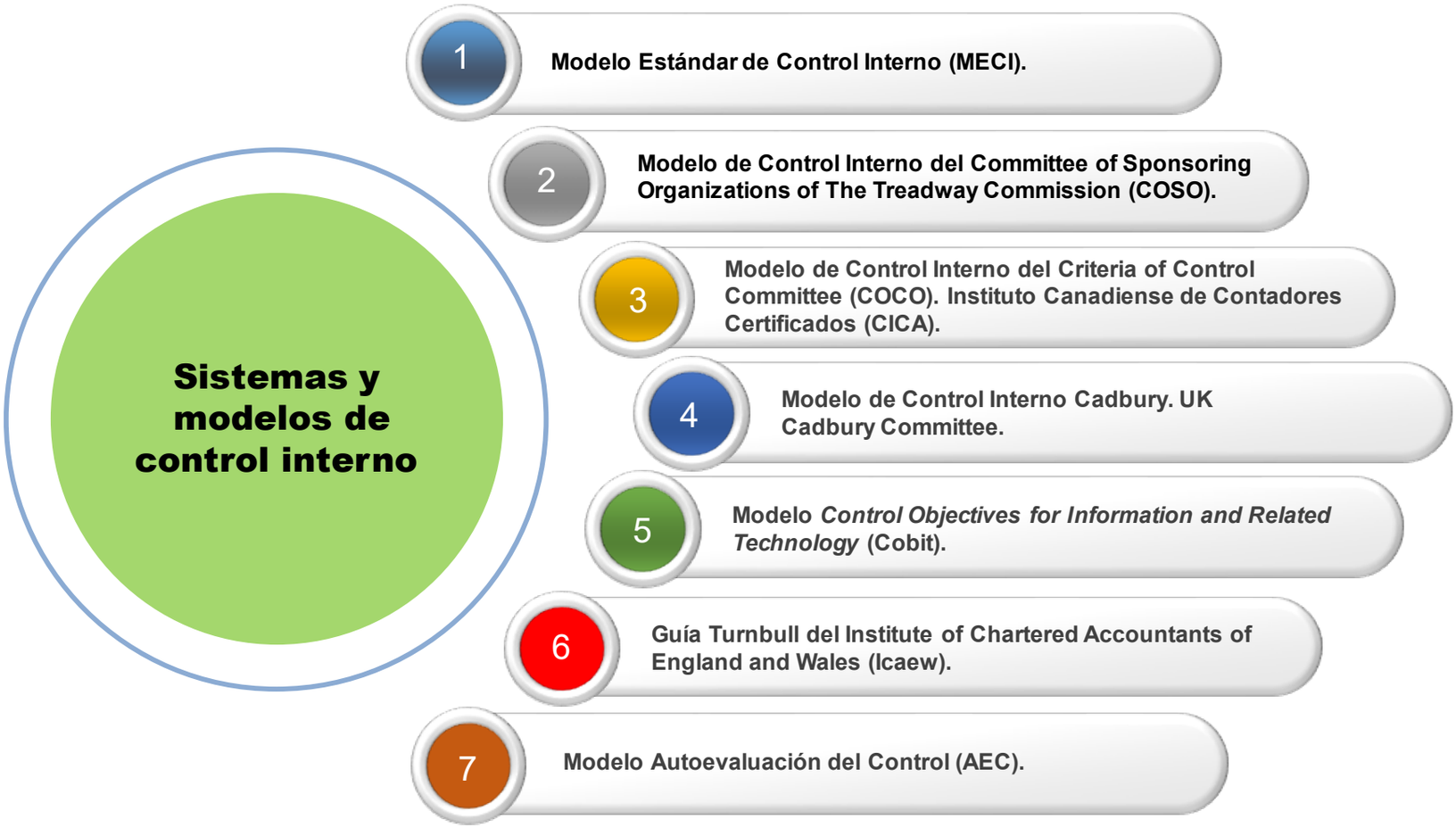

Figura 2. Sistemas y modelos de control interno
Fuente: Castañeda (2017)

Modelos de control interno y su relación con la gestión y administración de riesgos

En el desarrollo del objeto social de una organización son constantes las situaciones de riesgo. Normalmente, estos riesgos se presentan desde diferentes orillas con intensidades diversas, generando efectos nocivos y daños que pueden ser letales para la empresa. Ante la necesidad de dar respuesta a estos escenarios, los gobiernos, mediante empresas públicas, y las empresas privadas, con la presión de los accionistas y la sociedad, han ideado modelos de control interno. Según la Ley 87 de 1993, el control interno es:

> El sistema integrado por el esquema de organización y el conjunto de los planes, métodos, principios, normas, procedimientos y mecanismos de verificación y evaluación adoptados por una entidad, con el fin de procurar que todas las actividades, operaciones y actuaciones, así como la administración de la información y los recursos, se realicen de acuerdo con las normas constitucionales y legales vigentes dentro de las políticas trazadas por la dirección y en atención a las metas u objetivos previstos (artículo 1).

La definición deja clara la interdependencia de las estructuras de una organización para que esta pueda adoptar el modelo, el cual define los parámetros, estándares y controles que se deben implementar para prevenir la materialización de situaciones de riesgo y lograr condiciones estandarizadas de calidad.

En este contexto está inmerso el concepto de riesgo y, por ende, su gestión, con el fin de manejarlo y mitigarlo, a través del tratamiento de los escenarios identificados como potencialmente dañinos para la organización. Precisamente, el control interno busca detectar de manera oportuna estas situaciones para darles soluciones beneficiosas para la organización.

¡Importante!

Para la implementación de un modelo de control interno en una empresa u organización de naturaleza pública o privada se hace necesario, como ilustra Isaza (2012), organizar la empresa y estandarizar los procesos y el manejo del área de recursos humanos.

Modelo Estándar de Control Interno

En Colombia, con la Ley 87 de 1993, entró en vigor la norma para todas las instituciones del Estado en materia de control interno. En su contenido se determinaron los niveles de estandarización de responsabilidades. En primera instancia está el gerente de la entidad y, en segundo orden, el auditor. A ello se suman los niveles de gestión y control, los cuales están inmersos en los dos primeros, puesto que se desarrollan de manera simultánea.

Posteriormente, con la promulgación del Decreto 1599 de 2005, derogado por el Decreto 943 de 2014, se adoptó el Modelo Estándar de Control Interno (MECI) para el Estado Colombiano, dándose con ello alcance a lo ordenado en el artículo 5.° de la Ley 87 de 1993, en el cual se estableció el campo de aplicación que comprende todas las instituciones del Estado.

Estandarización
Proceso de búsqueda de patrones de equilibrio y unificación de las características de un producto o servicio, con el fin de establecer normas de asimilación a un modelo a seguir para la fabricación en serie (Que significado, s. f.).

El Decreto 943 de 2014 actualizó el MECI, el cual indica "los lineamientos y las metodologías necesarias para que las entidades establezcan, implementen y fortalezcan el Sistema de Control Interno" (Departamento Administrativo de la Función Pública —DAFP—, 2014), aportando una herramienta más completa para mejorar la gestión de las instituciones del Estado.

Concepto

En el artículo 1.° del Decreto 943 se expresa:

> Adóptese la actualización del Modelo Estándar de Control Interno para el Estado Colombiano (MECI), en el cual se determinan las generalidades y estructura necesaria para establecer, implementar y fortalecer un Sistema de Control Interno en las entidades y organismos obligados a su implementación, de acuerdo con lo dispuesto en el artículo 5.° de la Ley 87 de 1993 (Presidencia de la República de Colombia, 2014).

Con lo anterior, queda claro que su implementación es responsabilidad de las máximas directivas de los organismos u entidades.

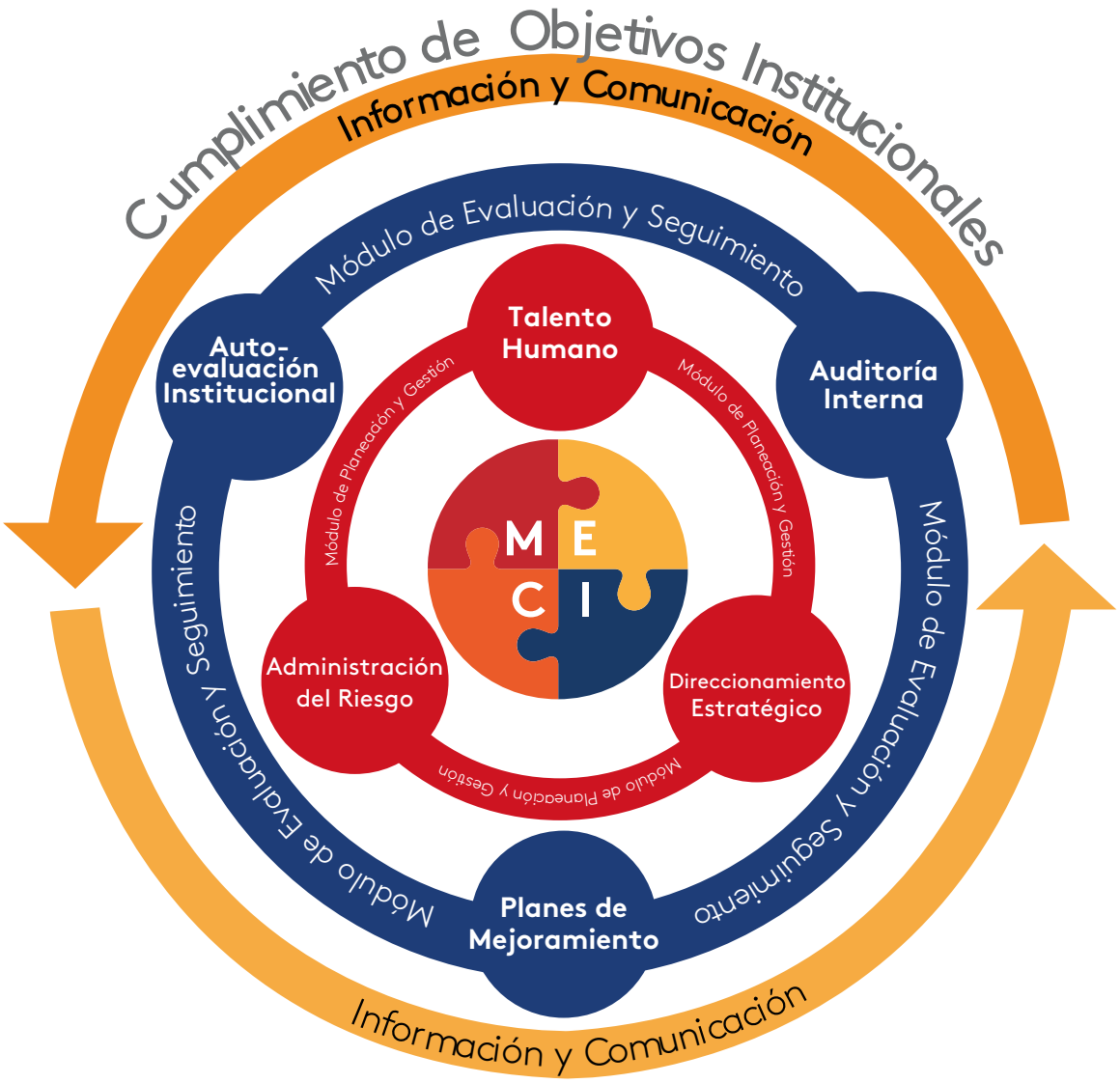

Figura 3. El Modelo estándar de Control Interno
Fuente: DAFP (2014)

Componentes

El MECI tiene como objetivo crear reglas y criterios que permitan a cualquier entidad del Estado generar controles a los procesos que revisten acciones como planear, gestionar, evaluar y hacer seguimiento en el ejercicio estatal. Por su estructura y diseño, estas pautas se pueden adaptar a cualquier entorno público al definir los roles y responsabilidades de quienes deben intervenir por su responsabilidad e investidura, liderando los procesos de control interno de manera activa y prospectiva a fin de proteger lo público de cualquier amenaza de tipo antrópico o conexos.

Antrópico
Término que proviene del griego ἄνθρωπος, cuya pronunciación es "anthropos", que significa "humano" (Concepto Definición, s. f.).

La estructura del MECI está compuesta por dos módulos, seis componentes y 13 elementos:

- Módulos

1. Módulo de control de planeación y gestión.
2. Módulo de control de evaluación y seguimiento.

- Componentes

1. Talento humano.
2. Direccionamiento estratégico.
3. Administración del riesgo.
4. Autoevaluación institucional.
5. Auditoría interna.
6. Planes de mejoramiento.

- Elementos

1. Acuerdos, compromisos o protocolos éticos.
2. Desarrollo del talento humano.
3. Planes, programas y proyectos.
4. Modelo de operación por procesos.
5. Estructura organizacional.
6. Indicadores de gestión.
7. Políticas de operación.
8. Políticas de administración del riesgo.
9. Identificación del riesgo.
10. Análisis y valoración del riesgo.

11. Autoevaluación del control y gestión.

12. Auditoría interna.

13. Plan de mejoramiento.

El módulo de control de planeación y gestión tiene como objetivo ejercer control sobre la planeación y la ejecución, evidenciando los alcances de la gestión y el desarrollo de los macroprocesos de direccionamiento estratégico, misional, de apoyo y evaluación. Este módulo cuenta con tres componentes: talento humano, direccionamiento estratégico y administración de riesgos, cuya estructura y proyección están dirigidas a generar cultura del control interno.

Por otra parte, este módulo permite revisar de manera atenta y minuciosa los procesos de planeación, con el fin de detectar desviaciones que afecten el cumplimiento de las metas de la entidad.

¡Importante!

El módulo de control de evaluación y seguimiento está diseñado para adelantar de manera continua un proceso de valoración de la efectividad en la aplicación de las directrices de control interno en la entidad, evidenciando desde la eficacia y la eficiencia la ejecución de los planes, programas y proyectos fijados, siendo objeto de observación la gestión realizada para establecer de manera temprana posibles desviaciones y, con ello, generar acciones preventivas o correctivas en aras de mejorar el desempeño de la entidad.

Todo instrumento de gestión y control requiere evaluación, a fin de seguir el cumplimiento de lo planeado contra lo ejecutado, partiendo de controlar, en primera instancia, lo que se planea. Este desarrollo se centra en la supervisión permanente y planeada con evaluaciones continuas que arrojen información cierta y oportuna para tomar decisiones. Por ello, el modelo busca que se implementen mecanismos de medición, evaluación y verificación, cuya aplicabilidad permita establecer los niveles alcanzados por el SIC en su finalidad, que es garantizar que la entidad alcance los objetivos propuestos en su misión. El módulo está estructurado en tres componentes: autoevaluación institucional, auditoría interna y planes de mejoramiento.

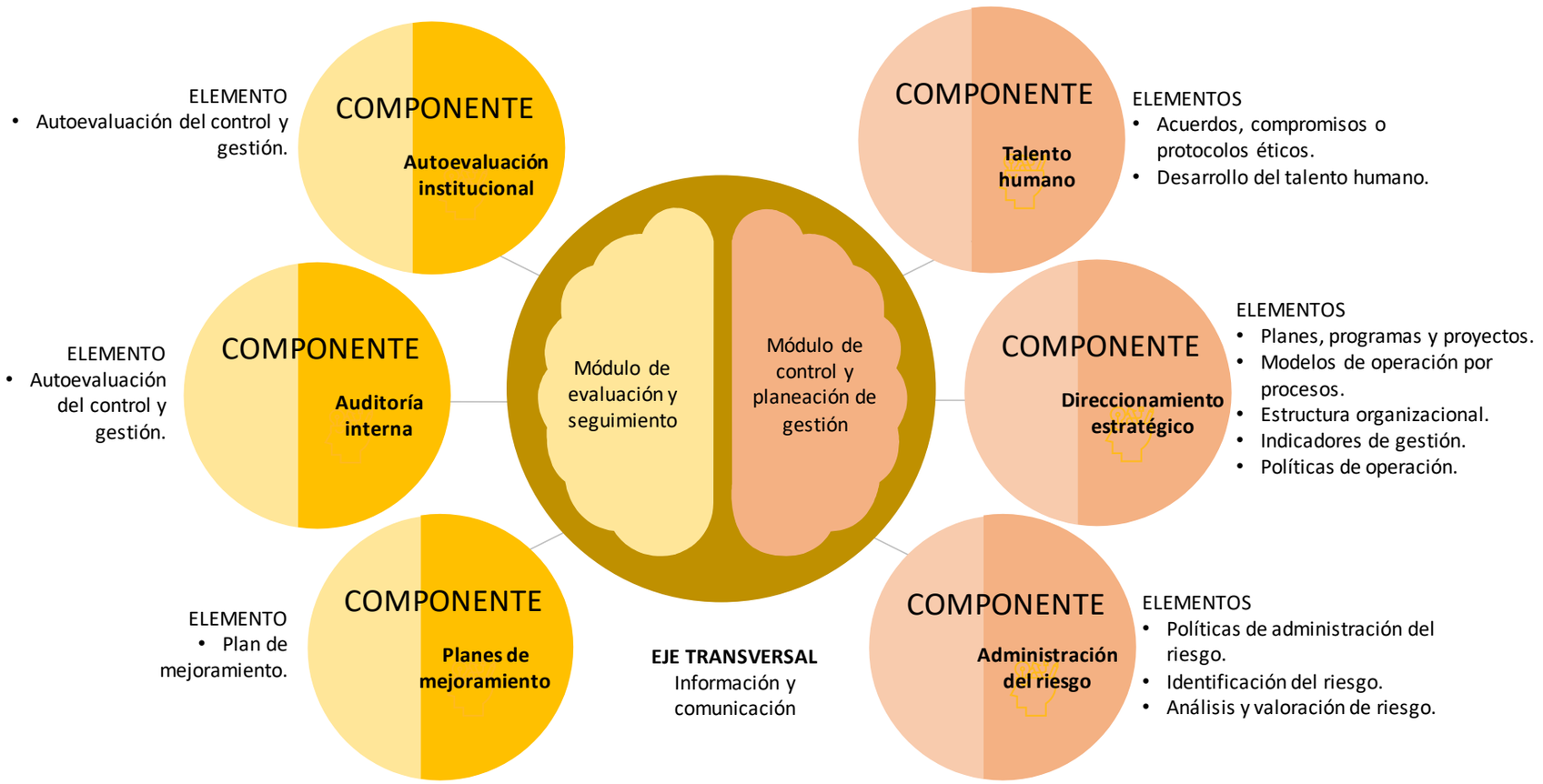

Figura 4. Módulos, componentes, elementos y eje transversal del Modelo Estándar de Control Interno
Fuente: Castañeda (2016)

Lectura recomendada

Con el ánimo de ampliar el conocimiento acerca del control interno, invito a leer en la página principal del eje el documento *Manual técnico del modelo estándar de control interno para el Estado Colombiano MECI 2014* (pp. 28-90) del Departamento Administrativo de la Función Pública.

Instrucción

Una forma de aplicar el conocimiento es a través de la casuística. Por ello, le invito a desarrollar en la página principal del eje, la actividad denominada "Caso Reficar", con la cual se podrá profundizar en el MECI, trabajando el componente de direccionamiento estratégico y el elemento de la estructura organizacional, determinantes de este penoso caso del escenario nacional.

Modelo de Control Interno COSO

El Modelo de Control Interno COSO tiene sus orígenes en Estados Unidos a partir de la situación de corrupción desbordada por la que atravesaba el país en los años posteriores a la Segunda Guerra Mundial, el desarrollo de la Guerra Fría, el conflicto armado con Vietnam, los altos niveles de inflación de países emergentes y las malas prácticas de multinacionales estadounidenses, como sobornar para posicionarse en el extranjero. A ello se sumó el escándalo Watergate, el cual develó que el presidente Richard Nixon y su administración trataron de encubrir manejos y adquisición fraudulenta de información en el seguimiento al Comité Nacional del Partido Demócrata. Posteriormente, la investigación evidenció excesos de sus funcionarios y de órganos del Estado sobre entidades y personas, con base en las políticas del Nixon (Canel y Sanders, 2005).

Figura 5. Ley de Prácticas Corruptas en el Extranjero (FCPA, por sus siglas en inglés)
Fuente: shutterstock/678428038

A raíz de esto, el Congreso de Estados Unidos promulgó la Ley de Prácticas Corruptas en el Extranjero (FCPA, por sus siglas en inglés) (Departamento de Justicia de los Estados Unidos, 2012), en la cual se determinó que la función de control interno debía estar en cabeza de las directivas empresariales y no de los departamentos de contabilidad. Así, se incrementó el control interno con la rendición de informes y memorias de movimientos contables. La alta dirección que debía manifestar su posición frente a los informes.

En los años 70 y 80, ante el auge de los fracasos financieros, muchas de las conclusiones se centraron en la falta de advertencias oportunas que se debieron originar en las auditorías y el fraude en los informes financieros.

En 1985 se crea la Comisión Treadway. Tras realizar detallados estudios de casos de múltiples empresas quebradas, en 1987 la comisión determinó que 50 % de ellas tenían algo en común: fallas y vacíos en el desarrollo de actividades de control interno (Contabilidad, 2012). En 1992 se emite el informe COSO, en el cual participaron cinco de las más prestigiosas organizaciones financieras estadounidenses. En el documento se sugiere una nueva conceptualización del control interno para entender el proceso como una acción integrada a las actividades de la empresa y no simplemente como un cúmulo de políticas y normas.

¡Impor tante!

El modelo ha tenido tres momentos clave de evolución: en 1992 se denominó Marco de Control Interno COSO I y se establecieron cinco componentes. En el año 2004 se implementó la conceptualización detallada de riesgos. La mejora se conoce como COSO II Enterprise Risk Management (ERM) y tenía ocho componentes. Por último, en el 2006 se implementó el COSO III, el cual tenía cinco componentes originales de la primera versión del COSO I y se orientó a las pymes.

Concepto

Existen múltiples definiciones a partir de los conceptos abarcados en el *Informe COSO*, Coopers & Lybrand S. A. (1997) lo definen como: "Un proceso ejecutado por el consejo de directores, la administración y el resto del personal de una entidad, diseñado para proporcionar seguridad razonable con miras a la consecución de objetivos" (p. 16). El enfoque está dirigido a tres aspectos relevantes que enmarcan la salud empresarial: la efectividad y eficiencia de las operaciones de la organización, la confiabilidad en la información financiera que se deriva de las operaciones comerciales y el cumplimiento de las leyes y regulaciones vigentes dentro de la organización.

Componentes

En la estructuración del modelo inicialmente se consideraron cinco elementos o componentes. Posteriormente, se aumentaron a ocho, como se relaciona a continuación con base en lo que menciona Rodríguez (2013):

- **COSO I:** tiene cinco componentes: ambiente o entorno de control, evaluación de riesgos, actividades de control, información y comunicación y monitoreo, los cuales están alineados a las operaciones, la información financiera y el cumplimiento de normas en las unidades de negocio de la organización.

Figura 6. Modelo de Control Interno COSO
Fuente: https://goo.gl/YR5aBd

- **COSO II ERM:** en su estructuración se implementó una mejora en la gestión del riesgo, aumentando a ocho sus componentes: ambiente interno, establecimiento de objetivos, identificación de eventos, evaluación de riesgos, respuesta al riesgo, actividades de control, información y comunicación y monitoreo.

Figura 7. Modelo de Control Interno COSO II ERM
Fuente: http://coso2.blogspot.com.co/

- **COSO III Pymes:** se simplificó a los cinco primeros componentes potenciales del COSO I. Como menciona Gómez (2012), su objetivo se amplió a visualizar información financiera y no financiera. Asimismo, tiene 17 principios que, por su pertinencia, deben ser considerados por la organización que quiera mantener un ambiente de control efectivo:

1. Ambiente de control

- Principio 1. Demuestra compromiso con la integridad y los valores éticos.
- Principio 2. Ejerce responsabilidad de supervisión.
- Principio 3. Establece estructura, autoridad y responsabilidad.
- Principio 4. Demuestra compromiso para la competencia.
- Principio 5. Hace cumplir con la responsabilidad.

2. Evaluación de riesgos

- Principio 6. Especifica objetivos relevantes.
- Principio 7. Identifica y analiza los riesgos.
- Principio 8. Evalúa el riesgo de fraude.
- Principio 9. Identifica y analiza cambios importantes.

3. Actividades de control

- Principio 10. Selecciona y desarrolla actividades de control.
- Principio 11. Selecciona y desarrolla controles generales sobre tecnología.
- Principio 12. Se implementa a través de políticas y procedimientos.
- Principio 13. Usa información relevante.

4. Sistemas de información y comunicación

- Principio 14. Comunica internamente.
- Principio 15. Comunica externamente.

5. Supervisión del sistema de control. Monitoreo

- Principio 16. Conduce evaluaciones continuas o independientes.
- Principio 17. Evalúa y comunica deficiencias.

Figura 8. Modelo de Control Interno COSO III Pymes
Fuente: https://goo.gl/4CCYxN

En la estructura de las versiones del COSO el concepto de gestión del riesgo es parte integral del control interno, dado que solo con su administración se pueden reducir los efectos dañinos sobre la organización.

Lectura recomendada

Para profundizar en el COSO III, le sugiero que ingrese al siguiente documento donde podrá apreciar de manera más detallada las generalidades, objetivos y componentes, principios, responsabilidades e implementación del modelo, en el link: https://www.ofstlaxcala.gob.mx/doc/material/27.pdf

Instrucción

El modelo COSO III es una importante herramienta que implementa 17 principios como parte de un modelo de control interno efectivo, la invitación en este espacio es a que desarrolle el caso de la DIAN y la devolución fraudulenta de IVA, situación de corrupción que sacudió el sector público por los montos manejados en el fraude, aquí se trabajará el sexto principio relacionado con los objetivos que se deben definir para poder hacer control y seguimiento.

Modelo de Control Interno del Criteria of Control Committee

El Modelo de Control Interno del Criteria of Control Committee (COCO) fue publicado por el Instituto Canadiense de Contadores Certificados (CICA) en 1995. Nació por las constantes quejas frente a la compleja implementación del COSO. Su objetivo fue simplificar los conceptos y el lenguaje del COSO para abarcar de manera integral el concepto de control en cualquier tipo de organización.

Concepto

La Secretaría de la Función Pública de México (2015) define el COCO como el control interno que incluye "aquellos elementos de una organización (recursos, sistemas, procesos, cultura, estructura y metas) que tomados en conjunto apoyan al personal en el logro de los objetivos de la institución" (p. 13). Por su alcance, estos objetivos pueden referirse a una o más de las siguientes condiciones:

- Efectividad y eficiencia en las operaciones.
- Confiabilidad en los reportes internos o para el exterior.
- Cumplimiento con las leyes, reglamentos aplicables y políticas internas.

El modelo COCO tiene un enfoque dirigido a abordar el control de una manera amplia, centrándose en el talento humano y los conceptos de autocontrol y autoevaluación, siendo lo humano el principal factor de una cultura de control (Mantilla, 2005).

Componentes

El sistema COCO tiene cuatro componentes: propósito, compromiso, aptitud y evaluación y aprendizaje, los cuales agrupan 20 criterios que permiten establecer un marco de referencia orientado a todos los miembros de la organización, con el fin de que sean empleados para "diseñar, desarrollar, modificar o evaluar el control" (Echeverri, 2006, p. 30). Esto demanda capacidad de análisis y comparación para entender los criterios con base a la particularidad de la organización.

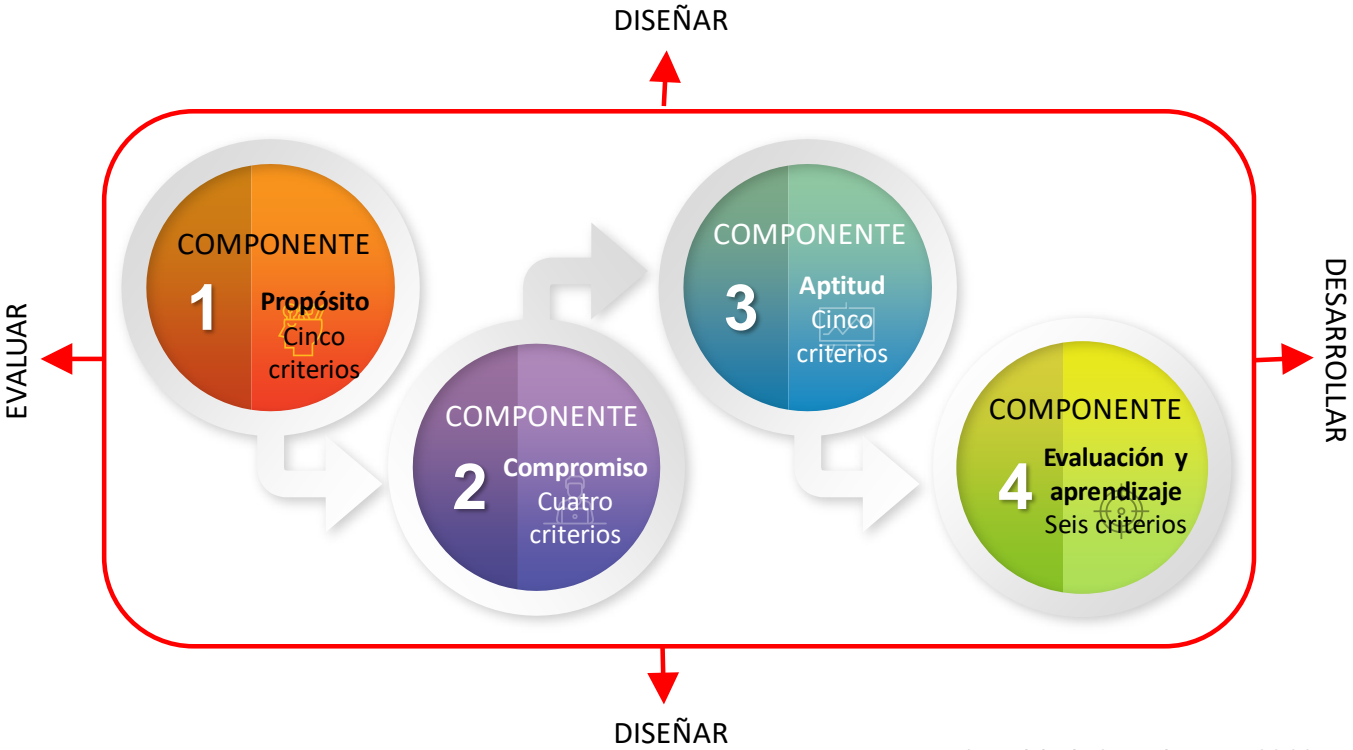

Figura 9. Modelo de Control Interno COCO
Fuente: Castañeda (2016)

1. Propósito: sentido de dirección a la organización. Tiene cinco criterios:

- Los objetivos deben ser comunicados.
- Se deben identificar los riesgos internos y externos que afecten el logro de objetivos.
- Las políticas para apoyar el logro de objetivos deben ser comunicadas y practicadas para que el personal identifique el alcance de su libertad de actuación.

- Se deben establecer planes para guiar los esfuerzos.
- Los objetivos y planes deben incluir metas, parámetros e indicadores de medición del desempeño.

2. Compromiso: sentido de identidad y valores de la organización. Tiene cuatro criterios:

- Se deben establecer y comunicar los valores éticos de la organización.
- Las políticas y prácticas sobre recursos humanos deben ser consistentes con los valores éticos de la organización y con el logro de sus objetivos.
- La autoridad y responsabilidad deben ser claramente definidos y consistentes con los objetivos de la organización para que las decisiones se tomen por el personal apropiado.
- Se debe fomentar una atmósfera de confianza para apoyar el flujo de la información.

3. Aptitud: sentido de competencia o aptitud de la organización. Tiene cinco criterios:

- El personal debe tener los conocimientos, habilidades y herramientas necesarios para el logro de objetivos.
- El proceso de comunicación debe apoyar los valores de la organización.
- Se debe identificar y comunicar información suficiente y relevante para el logro de objetivos.
- Las decisiones y acciones de las diferentes partes de una organización deben ser coordinadas.
- Las actividades de control deben ser diseñadas como una parte integral de la organización.

4. Evaluación y aprendizaje: sentido de evolución de la organización. Tiene seis criterios:

- Se debe monitorear el ambiente interno y externo para identificar información que oriente hacia la reevaluación de objetivos.
- El desempeño debe ser evaluado contra metas e indicadores.
- Las premisas consideradas para el logro de los objetivos deben ser revisadas periódicamente.
- Los sistemas de información deben ser evaluados nuevamente en la medida en que cambien los objetivos y se precisen deficiencias en la información.
- Debe comprobarse el cumplimiento de los procedimientos modificados.

– Se debe evaluar periódicamente el sistema de control e informar de los resultados.

Los aspectos expuestos son retos para quien emplee el modelo frente a otros de corte tradicional. Se requiere un esfuerzo adicional, dado que los alcances de los componentes y los criterios son amplios, lo cual demanda apertura mental en su interpretación frente a aspectos intangibles e informales desde los elementos de juicio físicos, como documentos, o desde la percepción de los mismos, como valores, identidad corporativa, etc.

Modelo de Control Interno Cadbury

Este modelo de origen inglés se desarrolló en 1991. El organismo que adelantó su construcción fue el Comité Cadbury (UK Cadbury Committee). Su finalidad fue generar un cúmulo de medidas y acciones que se debían adoptar para el manejo de la información financiera y contable, aspectos sensibles en una época de imprecisiones y ambigüedades en las normas contables, expectativa frente a las auditorías y las organizaciones, múltiples quiebras y, sobre todo, carencia de una política clara que evidenciara la responsabilidad de los miembros de la alta dirección en el control de sus empresas y organizaciones (González, 2000).

Concepto

El modelo Cadbury se centra en las políticas de gobierno. Analiza de manera detallada el código de ética sobre aspectos de carácter financiero del gobierno, las organizaciones y las sociedades.

Su temática se basa en el estudio de tres aspectos de carácter fundamental e interés de las organizaciones: "(1) las funciones del consejo de administración de las entidades, (2) el bajo nivel de confianza en la información financiera de las organizaciones y (3) la falta de capacidad de los auditores para ofrecer en sus informes la protección requerida y esperada de los dueños de la misma" (Tizoc, s. f.).

Componentes

Los componentes del modelo Cadbury son similares a los del modelo COSO. Solo difieren en el objetivo relacionado con la información, el cual está integrado en los demás componentes. También hay un enfoque más detallado en la gestión del riesgo.

Este sistema está orientado a proporcionar normas y políticas de seguridad en torno al manejo de las siguientes variables (Spira y Slinn, 2013):

- Confiabilidad de la información y los reportes del área financiera.
- Cumplimiento de leyes y reglamentos.

- Efectividad y eficiencia de las operaciones.
- Salvaguardia del patrimonio.

Modelo *Control Objectives for Information and Related Technology*

En la época de la sociedad de la información y la comunicación, el manejo de las tecnologías de la información (TI) se ha convertido en un aspecto sensible para las organizaciones. La informática y las telecomunicaciones han permitido que se intercambie información en tiempo real sin limitantes. Su manejo cobra importancia frente al incremento de la dependencia de datos y los sistemas que permiten su flujo, a la vulnerabilidad frente ataques cibernéticos y *hackers*, los costos de inversión en equipos y sistemas, y la capacidad que tienen las TI para transformar una organización. Por esto, una preocupación de la modernidad es el control de los sistemas tecnológicos de información para garantizar el alcance de los objetivos.

El Modelo *Control Objectives for Information and Related Technology* (Cobit) se constituye en un marco de control interno implementado en 1996. Fue enfocado a las TI, partiendo del principio de que estas deben generar información que permita alcanzar los objetivos. Este modelo, que fomenta el enfoque y la propiedad de los procesos, fue el resultado de una investigación realizada por la Information Systems Audit and Control Association (Isaca).

Concepto

Como lo menciona la Universidad Eafit (2007):

> Cobit se aplica a los sistemas de información de toda la empresa, incluyendo los computadores personales y las redes. Está basado en la filosofía de que los recursos TI necesitan ser administrados por un conjunto de procesos naturalmente agrupados para proveer la información pertinente y confiable que requiere una organización para lograr sus objetivos.

Componentes

El modelo Cobit, definido como un marco de referencia en el manejo y control de las TI, clasifica en cuatro dominios los procesos que se presentan en estas y ubica 34 objetivos de control de alto nivel (Comité de Dirección de COBIT e Information Systems Audit and Control Foundation, 1998).

Los cuatro dominios son: planificación y organización; adquisición e implantación; entrega y soporte; y monitoreo.

El dominio de planificación y organización tiene 11 objetivos. Su enfoque está dirigido a establecer las estrategias para lograr que las TI puedan aportar de manera importante a la consecución de los objetivos de la organización.

El dominio de adquisición e implantación tiene seis objetivos y se fundamenta en la necesidad de adquirir o desarrollar las TI necesarias, con el fin de implementarlas en la organización y fortalecer las posibilidades de alcanzar los objetivos.

El dominio de entrega y soporte tiene trece objetivos y está considerado para que permita que las TI fluyan de manera ininterrumpida y en la intensidad requerida. Va desde lo básico en soporte, aspectos de seguridad y entrenamiento de quienes intervienen en el proceso.

El dominio de monitoreo tiene cuatro objetivos y su aplicación está centrada en la necesidad de evaluar de manera constante los procesos para evidenciar su calidad, pertinencia y suficiencia, con base en lo establecido en los procesos de control.

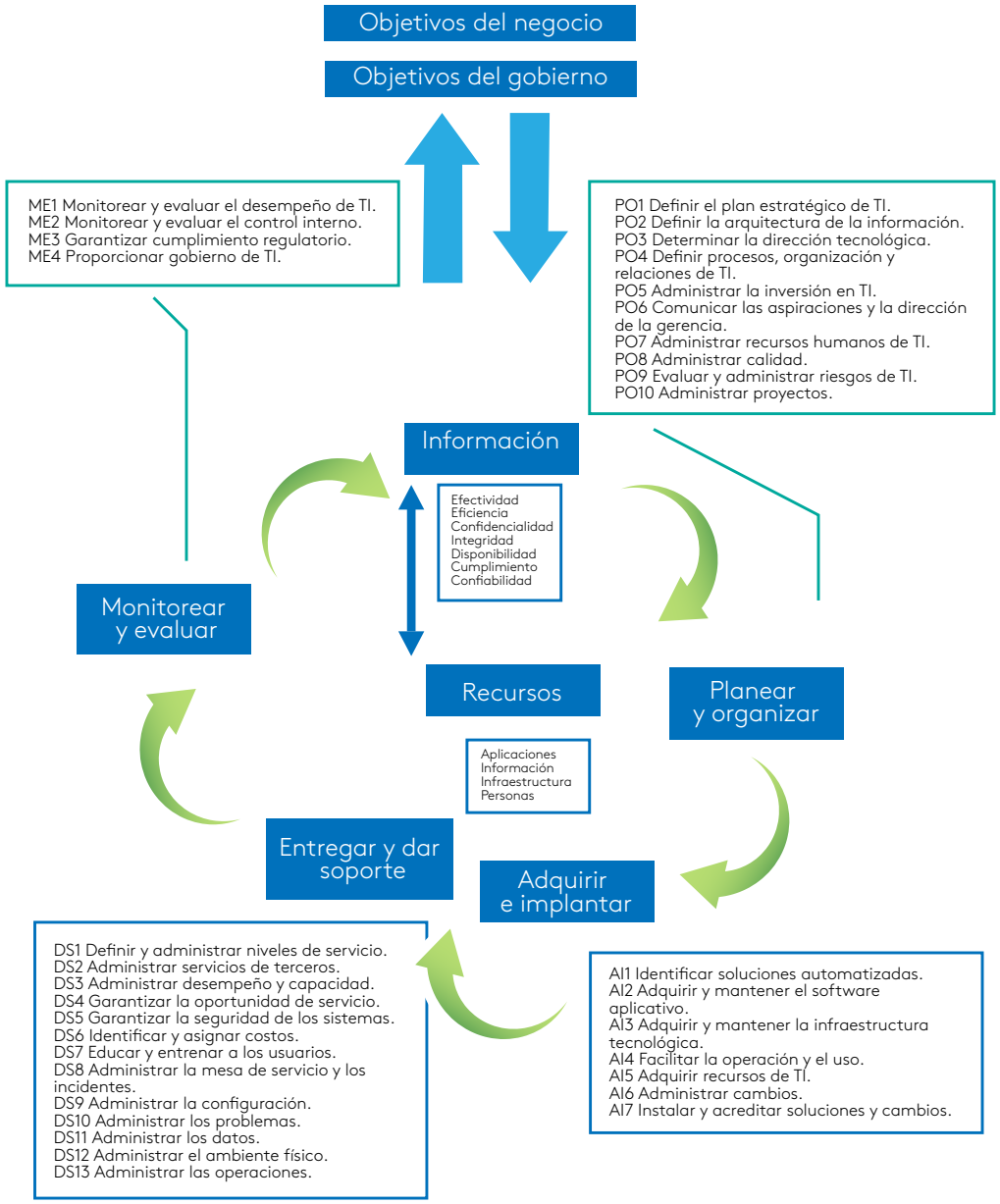

Figura 10. Procesos de TI de Cobit definidos dentro de los cuatro dominios
Fuente: Comité de Dirección de COBIT e Information Systems Audit and Control Foundation (1998)

Instrucción

El modelo Cobit está orientado a las tecnologías de la información, un factor de competitividad muy importante en la época que vivimos de la sociedad de la información y del conocimiento. Lo invito a revisar en la página principal del eje la galería de los dominios del modelo. Identifique cada uno y recuerde en qué consisten.

Guía Turnbull del Institute of Chartered Accountants of England and Wales

Originario de Inglaterra, se inició en 1998 —como lo menciona Gaspar (2004)— con el informe *The Combined Code of the Committee on Corporate Governance,* desarrollado por el Comité sobre Dirección Corporativa, liderado por Sir Ronald Hampel. En su contenido se establecieron 14 principios y 44 provisiones orientados a aspectos de gran relevancia en la dirección corporativa en varias temáticas, entre ellas el control interno, como determinan el principio D2: "El Consejo de Administración deberá mantener un sistema solvente de control interno para salvaguardar las inversiones de los accionistas y los activos de la compañía" y el D2.1:

> Los directores deberán, como mínimo una vez al año, realizar una revisión de la efectividad de los sistemas de control interno y deben informar a los accionistas de que dicha revisión se ha realizado. La revisión debe cubrir todos los controles, financieros, operacionales y de control de riesgos (Gaspar, 2004).

Posteriormente, con base en *The Combined Code* y con el ánimo de aplicar los principios y provisiones, la Bolsa de Londres encargó al Institute of Chartered Accountants in England and Wales (Icaew) elaborar una cartilla de aplicación. Este documento fue lo que se conoció como el Informe *Turnbull*, publicado en 1999, llamado así en referencia al director de Grupo Nigel Turnbull. Su enfoque está en la implementación de un sistema de control interno basado en la administración y gestión del riesgo en cualquier campo inherente a la organización y el monitoreo de su efectividad.

Modelo Autoevaluación del Control

Este modelo está centrado en la realización de la evaluación a través de talleres con los implicados en el proceso. El liderazgo del ejercicio debe estar en cabeza de una persona con preparación académica y experiencia en el área. Además de ello, con una conceptualización lo suficientemente amplia y clara en el campo del control interno. La recomendación es un auditor interno o auditor líder, quien por su trabajo y dedicación tiene la suficiente idoneidad.

El Modelo Autoevaluación del Control (AEC) es un proceso documentado donde los integrantes de la organización trabajan en una función, juzgando la efectividad del proceso de control que adelanta la organización y, con ello, se determina si es seguro alcanzar los objetivos propuestos o algunos de ellos.

Componentes

Los componentes AEC están enfocados a realizar el proceso de autoevaluación en cinco fases o etapas: preparación, control interno, planificación, autoevaluación de controles y optimización del sistema de control interno.

Según Espinoza (2006), las etapas mencionadas tienen la siguiente definición:

> Etapa I. Preparación: comprende la evaluación del recurso humano y financiero, razones para llevar a cabo el modelo diagnóstico.
>
> Etapa II. Control Interno: atiende la evaluación del sistema de control interno, evaluación de procesos y análisis de los resultados de las evaluaciones.
>
> Etapa III. Planificación: abarca la formación del comité de autoevaluación de controles y la unidad técnica de calidad, identificación de los métodos de recolección de datos, evaluación de la dirección de la autoevaluación de controles.
>
> Etapa IV. Autoevaluación de controles: en esta etapa se elabora la matriz de autoevaluación de controles, análisis de la información, elaboración del informe de autoevaluación de controles, comunicación de los resultados.
>
> Etapa V. Optimización del Sistema de Control Interno: es el momento de la obtención de información oportuna, fiable, razonable y eficiente, obtención de seguridad razonable sobre los procesos de control aplicados en la empresa, obtención de la integración, motivación y comprensión en el recurso humano respecto del desarrollo del proceso de control (p.1).

BIBLIOGRAFÍA

Canel, M. y Sanders, K. (2005). El poder de los medios en los escándalos políticos: la fuerza simbólica de la noticia icono. *Anàlisi, 32*, 163-178.

Castañeda, J. (2016). *Módulo: Prevención y gestión del riesgo*. Bogotá, Colombia: Fundación Universitaria del Área Andina.

Comité de Dirección de COBIT e Information Systems Audit and Control Foundation. (1998). *COBITTM. Gobernabilidad, control y auditoría de información y tecnologías relacionadas*. Buenos Aires, Argentina: Sindicatura General de la Nación.

Concepto Definición. (s. f.). *Antrópico*. Recuperado de http://conceptodefinicion.de/antropico/

Congreso de la República de Colombia. (29 de noviembre de 1993). Ley 87 de 1993. DO: 41120.

Contabilidad. (2012). *Informe COSO: historia*. Recuperado de http://www.contabilidad.com.py/articulos_75_informe-coso-historia.html

Coopers & Lybrand S. A. (1997). *Los nuevos conceptos de control interno*. Informe COSO. Madrid, España: Ediciones Díaz de Santos.

Departamento Administrativo de la Función Pública. (2014). *Manual técnico del Modelo Estándar de Control Interno para el Estado Colombiano MECI 2014*. Recuperado de http://www.funcionpublica.gov.co/documents/418537/506911/Manual+T%C3%A9cnico+del+Modelo+Est%C3%A1ndar+de+Control+Interno+para+el+Estado+Colombiano+MECI+2014/065a3838-cc9f-4eeb-a308-21b2a7a040bd

Departamento de Justicia de los Estados Unidos. (2012). *A resource guide to the United States Corrupt Practices Act*. Recuperado de https://www.sec.gov/spotlight/fcpa/fcpa-resource-guide.pdf

Echeverri, O. (2006). *Análisis comparativo del sistema del control interno en las entidades de la administración pública colombiana* (tesis de especialización). Escuela Superior de Administración Pública, Bogotá, Colombia.

Espinoza, N., González, R. y Reyes, K. (2006). *Modelo de autoevaluación de controles para optimizar el sistema de control interno en las grandes empresas del sector servicios, ubicadas en la Ciudad de Santa Tecla, Departamento de La Libertad* (tesis de pregrado). Universidad Francisco Gavidia, San Salvador, El Salvador.

BIBLIOGRAFÍA

Gaspar, J. (2004). *Planes de contingencia, la continuidad del negocio en las organizaciones*. Madrid, España: Ediciones Díaz de Santos.

Gómez, J. (2012). *Diseño de un sistema de control interno basado en COSO III (pymes), elaborado por un contador público y auditor independiente para un restaurante de comida rápida* (tesis de licenciatura). Universidad de San Carlos de Guatemala, Guatemala, Guatemala.

González, E. (2000). Análisis ético del informe Cadbury: aspectos financieros del gobierno de las sociedades. *Papeles de Ética, Economía y Dirección*, (5), 1-8.

González, R. (s. f.). *Marco integrado de control interno. Modelo COSO III. Manual del participante*. Recuperado de https://www.ofstlaxcala.gob.mx/doc/material/27.pdf

Isaza, A. (2012). *Control interno y sistema de gestión de la calidad*. Bogotá, Colombia: Ediciones de la U.

Mantilla, S. (2005). *Auditoría del control interno*. Bogotá, Colombia: Ecoe Ediciones.

Ministerio de Comercio, Industria y Turismo. (2005). Historia del control interno. Recuperado de http://www.mincit.gov.co/publicaciones/14015/historia_del_control_interno

Presidencia de la República de Colombia. (21 de mayo de 2014). Decreto 943 de 2014. DO: 49158.

Que Significado. (s. f.). *Estandarización*. Recuperado de http://quesignificado.com/estandarizacion/

Rodríguez, E. (2013). *Control interno basado en el sistema COSO*. Recuperado de http://www.nunezdubonyasociados.com/sitio/index.php/noticias/350-control-interno-basado-en-sistema-coso

Secretaría de la Función Pública de México. (2015). *Asesoría en control interno en la administración pública estatal*. Recuperado de http://www.aguascalientes.gob.mx/SEGOB/PDF/Asesor%C3%ADa%20en%20Control%20Interno.pdf

Spira, L. y Slinn, J. (2013). *The Cadbury committee: a history. Oxford*, Reino Unido: Oxford University Press.

Tizoc, F. (s. f.). *Modelo Cadbury*. Recuperado de https://www.academia.edu/24930911/MODELO_CADBURY

Universidad Eafit. (2007). *Cobit: modelo para auditoría y control de sistemas de información*. Recuperado de http://www.eafit.edu.co/escuelas/administracion/consultorio-contable/Documents/boletines/auditoría-control/b13.pdf

GESTIÓN, ADMINISTRACIÓN DE RIESGOS Y MODELOS DE CONTROL INTERNO

Javier Castañeda

EJE 3

Pongamos en práctica

AREANDINA
Fundación Universitaria del Área Andina
MIEMBRO DE LA RED ILUMNO

Fuente: Shutterstock/128500544

INTRODUCCIÓN

Diariamente, en Colombia y en el mundo se publican noticias sobre el comportamiento económico y empresarial de los países, en las cuales se evidencian situaciones anómalas en empresas que, por mal manejo interno, fraudes o errores, entran en procesos de renegociación o liquidación, o son afectadas por eventos externos generados por diferentes tipos de riesgos, desde circunstancias de carácter natural hasta acontecimientos políticos o el denominado riesgo país. Ante estos escenarios cotidianos, cabe el cuestionamiento sobre si se hubieran podido evitar estos descalabros y cómo.

La sociedad, en su afán por evitar estas situaciones de desastre económico o financiero, ha afinado el concepto de gestión del riesgo, alineando al control interno y la auditoría para los contextos endógenos y exógenos de las organizaciones, lo cual es una herramienta de vital importancia para detectar los riesgos y tratarlos, con el fin de evitar o minimizar su impacto.

En el campo del control interno y la auditoría se busca generar normas y procesos de control y, a la vez, la posibilidad de evidenciar su cumplimiento mediante la investigación, revisión y evidencia de lo proyectado con lo ejecutado. En estos procesos, la gestión del riesgo está presente ante la necesidad de identificar y tratar los riesgos para aportar a la integridad de la organización.

Para este referente de pensamiento se proyectó la pregunta: ¿cómo se pueden estructurar en un diagnóstico los aspectos preventivos y propositivos de una auditoría para gestionar el riesgo, incluyendo el contexto normativo? Se busca que el contenido del documento ayude al estudiante a orientar un proceso de auditoría en un contexto de control interno donde haya una convergencia conceptual y procedimental de la gestión del riesgo, siempre desde los criterios de auditoría y las normas nacionales e internacionales.

El eje está estructurado de manera secuencial haciendo un recorrido por el proceso de auditoría, el control interno y la administración del riesgo, en el cual, de manera breve y concisa, se abordan los conceptos para su aplicación, dejando claros los pasos y etapas para lograr un buen resultado de auditoría. En esencia, el objetivo central del curso es integrar los conceptos tomando como hilo conductor la administración del riesgo, puesto que esta es el determinante que permite evitar escenarios de daños y detrimento para las organizaciones. Por ello, al finalizar el eje se grafica cómo se aborda un modelo de control interno en una pyme. Se incluye el resultado de una auditoría y las políticas de manejo del riesgo, con el fin de generar en el futuro especialista interés por aplicar lo trabajado en los ejes anteriores y proponer modelos de control interno con nuevas o mejores herramientas para optimizar y garantizar la permanencia de las organizaciones.

Auditoría, control interno y gestión y administración de riesgos

Una de las premisas del directivo de una organización es garantizar la prevalencia y sostenibilidad en el tiempo de la empresa. Para ello, debe garantizar un efectivo control de las áreas, a través del control interno, el cual permite determinar los posibles escenarios de riesgo. Por lo tanto, se debe hacer una correcta gestión y administración del riesgo.

En este campo, la auditoría es muy importante. Esta se entiende como la revisión de carácter investigativo, analítico, crítico y sistemático que una persona o entidad realiza a una organización siendo independiente a la misma, con el objetivo de emitir un concepto técnico y profundo de la gestión efectuada, frente al ente u órgano auditado.

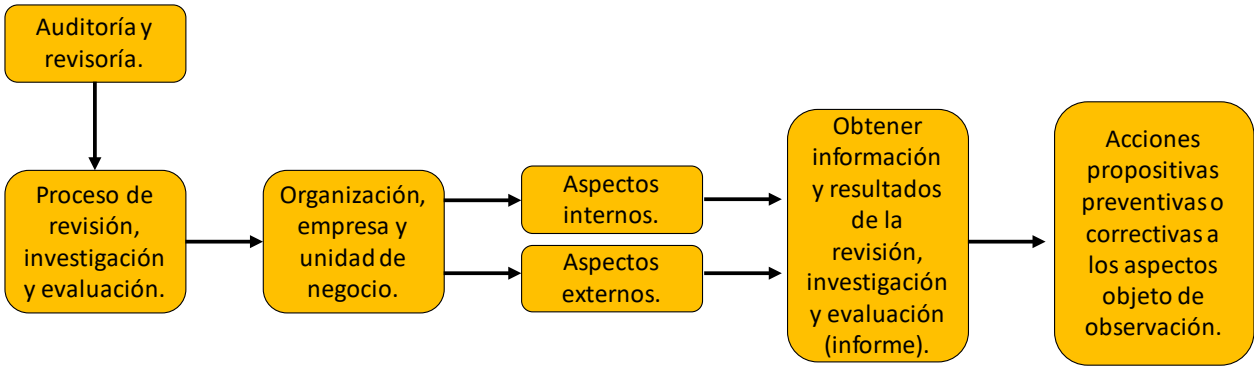

Figura 1. La auditoría y su ciclo
Fuente: Castañeda (2016)

Existen múltiples tipos de auditoría, según las áreas que sean objeto de verificación; sin embargo, la auditoría ha sido asociada a la revisión de los estados financieros o contables de una empresa. Esta especialidad es una rama de la contabilidad y se define como:

> Aquella confrontación de lo escrito con las pruebas de lo acontecido y las respectivas referencias de los registros. Esto quiere decir que el auditor observa la exactitud, integridad y autenticidad de tales demostraciones, registros y documentos que fueron elaborados durante un periodo determinado llevados a cabo por una empresa (Guzmán, s. f., párr. 2).

Video

Lo invitamos a apreciar el video La auditoría del futuro y el futuro de la auditoría con el ánimo de ampliar el concepto prospectivo de lo que se espera de la auditoría y la necesidades de ser más efectivos en los controles.

En la siguiente tabla se relacionan algunos de los escenarios que pueden encontrarse en el ejercicio de una auditoría, partiendo de las consideraciones que los generan como son el fraude o el error humano.

Fraude	Error
Con conocimiento	Equivocaciones
Intención	Con desconocimiento
Necesidad	Ignorancia
Condición	No cumplimiento de procedimientos
Contra la empresa	Sin intención
Contra terceros	Desconocimiento
Presión	torpeza
Amenaza	Negligencia

Tabla 1. Situaciones de fraude y error
Fuente: Andrés Riportella (Carvajal y Escobar, 2012)

Tipos de auditoría

A continuación, se presentan algunos tipos de auditoría que tienen relación directa con el desarrollo y la operación empresarial:

Auditoría integral

Como su nombre lo indica, sus alcances son totales en la empresa. Evalúa la estructura organizacional, las políticas, los sistemas de control interno, la información financiera, el manejo financiero y las metas, con el fin de obtener una visión holística del desempeño de la empresa.

Auditoría externa

Se adelanta por parte de un auditor externo o grupo de auditores, con la condición de que no tengan ningún tipo de vínculo con la entidad, a fin de evitar resultados parcializados.

Auditoría interna

Se origina en las políticas de la empresa u organización. Su finalidad es realizar el seguimiento de los objetivos y procesos que se adelantan internamente para validar su

coherencia y validez. La revisión debe generar informes que permitan evaluar la situación y tomar decisiones preventivas o correctivas.

Auditoría financiera

También llamada auditoría contable, tiene su esencia en el examen y la revisión detallada de los estados financieros y contables:

> Consiste en el examen y evaluación de los documentos, operaciones, registros y estados financieros de la entidad, para determinar si estos reflejan razonablemente su situación financiera y los resultados de sus operaciones, así como el cumplimiento de las disposiciones financieras, con el objetivo de mejorar los procedimientos relativos a la gestión financiera y el control interno (Grupo Consultor Internacional, s. f., párr. 1).

La desarrolla el auditor a partir del elemento llamado "evidencia de auditoría", es decir, sobre las operaciones realizadas por la organización.

Auditoría operacional

Tiene como finalidad mejorar la eficacia y la eficiencia de una empresa. La adelanta un profesional con experticia en el área o una especialidad empresarial para proponer ideas sobre la gestión de la organización.

Auditoría fiscal

Se enmarca en la revisión detallada del cumplimiento de las obligaciones de pagar impuestos y acatar leyes tributarias (Gerencie, s. f.).

Auditoría forense

Recurso de carácter jurídico para determinar acciones criminales y posibles hechos delictivos. Con base en la Normativa Internacional de Auditoría (NIA), las siguientes normas tienen, por sus consideraciones, mayor injerencia en el campo del control interno (AOB Auditores, s. f., párr. 3):

- NIA 240: responsabilidades del auditor en la auditoría de estados financieros con respecto al fraude.
- NIA 265: comunicación de las deficiencias en el control interno a los responsables de gobierno y a la dirección de la entidad.
- NIA 300: planificación de la auditoría de estados financieros.
- NIA 315: identificación y valoración de los riesgos de incorrección material, mediante el conocimiento de la entidad y su entorno.
- NIA 330: respuestas del auditor a los riesgos valorados.

En la actualidad, las normas y políticas internacionales sobre la estandarización de procesos son referentes de calidad. Por ello, lo invito a ampliar el conocimiento de la Normativa Internacional de Auditoría (NIA) que proyecta AOB Auditores.

Considerando que el rol del auditor es decisivo en el proceso de auditoría, la NIA 315 define el control interno como:

> El proceso diseñado, implementado y mantenido por los responsables del gobierno de la entidad, la dirección y otro personal, con la finalidad de proporcionar una seguridad razonable sobre la consecución de los objetivos de la entidad, a la fiabilidad de la información financiera, la eficacia y eficiencia de las operaciones, así como sobre el cumplimiento de las disposiciones legales y reglamentarias aplicables (Instituto de Contabilidad y Auditoría de Cuentas, 2013, p. 2).

A partir de esta delimitación, también es pertinente considerar, como indica la NIA 315, que el objetivo del auditor es "identificar y valorar los riesgos de incorrección material, debida a fraude o error, tanto en los estados financieros como en las afirmaciones, mediante el conocimiento de la entidad y de su entorno" (Instituto de Contabilidad y Auditoría de Cuentas, 2013, p. 2). Este concepto comprende la evaluación, la revisión y el control de procesos, garantizando el seguimiento al cumplimiento de las normas y políticas internas de la organización.

Proceso de auditoría

Muchos autores han estructurado el proceso de auditoría en diferentes etapas. En este eje se consideran tres etapas y seis pasos que pueden ser aplicados a cualquier tipo de auditoría:

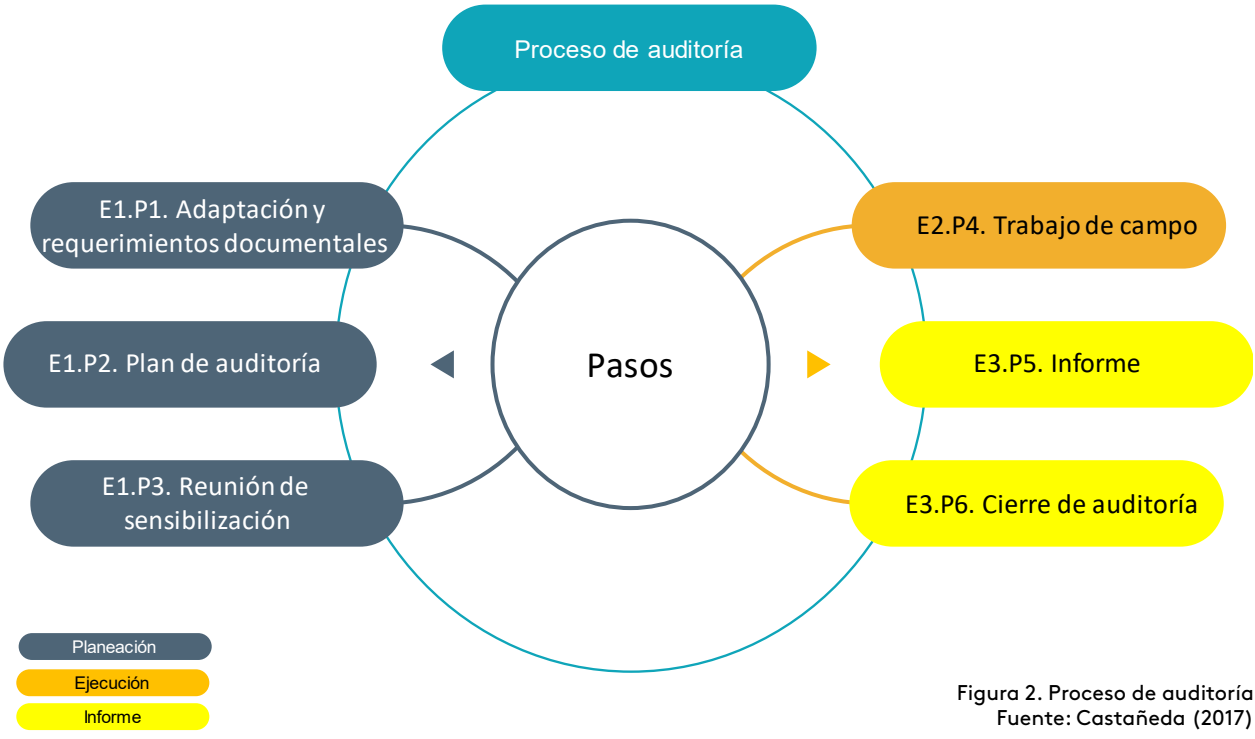

Figura 2. Proceso de auditoría
Fuente: Castañeda (2017)

Etapa de planeación

Consiste en realizar las actividades previas a la auditoría. La organización integra el equipo auditor a su estructura y se inicia el proceso de conocimiento de la situación de la empresa, sus sistemas de información, su estructura organizacional, sus planes y objetivos, sus normas y políticas, en fin, de todos los aspectos que le permitan al auditor tener un conocimiento integral de la organización.

Esta etapa demanda, entre otras, las siguientes consideraciones:

- Estructura organizacional y operativa de la empresa.
- Objetivos, metas y alcances de la auditoría.
- Revisión y análisis de los procesos y normas de control interno.
- Análisis de escenarios de riesgos y su materialización en la organización.
- Realización del plan y del programa de auditoría.

En esta etapa se adelantan los tres primeros pasos.

El proceso se retroalimenta y complementa continuamente:

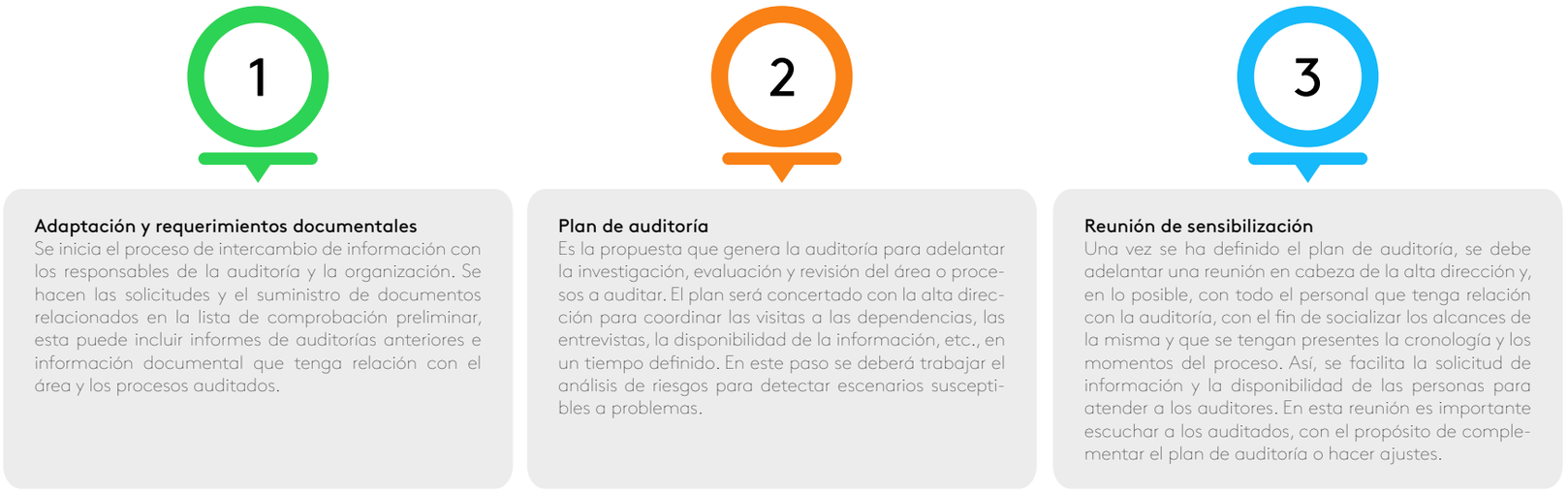

Figura 3. Pasos en la etapa de planeación
Fuente: propia

Etapa de ejecución

Se adelanta el proceso aplicando pruebas, técnicas, procedimientos y análisis de auditoría a los estados auditados. Se detectan errores y hallazgos, se coteja información y se hacen conjeturas y conclusiones a partir de la realidad de lo revisado.

Es la etapa central y más importante del proceso de auditoría, puesto que es donde se aplican técnicas de muestreo, se recolectan evidencias de auditoría, evidencia documental, etc.

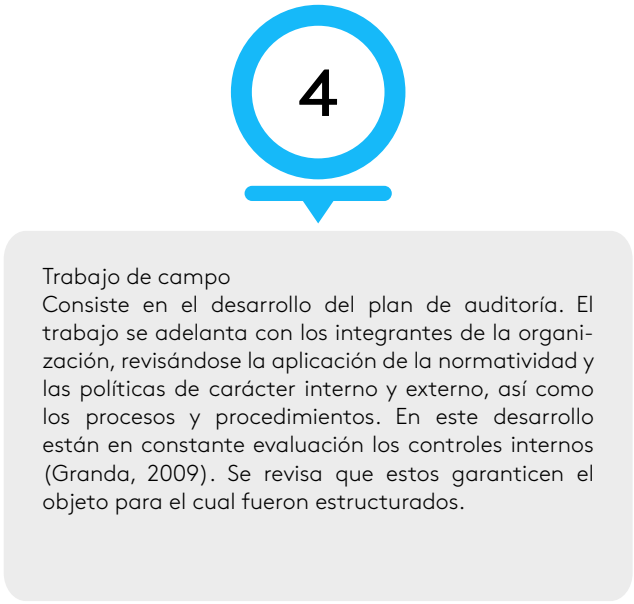

Figura 4. Paso en la etapa de ejecución
Fuente: propia

Se aplicarán las diferentes técnicas de auditoría para la obtención de evidencia, como la inspección visual, las declaraciones, los contenidos verbales, los documentos (físicos y virtuales) y, en general, la inspección física (Gerencie, s. f.).

Si surgen hallazgos, inconformidades y problemas, la auditoría hace requerimientos de ampliación en aspectos documentales y procesales, a fin de dar respuestas y definir si se tienen en cuenta como actividades que serán objeto del informe final o, por el contrario, se solucionan en su momento.

Etapa de informe

Se consolida lo hallado en la auditoría. Como mínimo, debe incluir un dictamen del área o proceso auditado, un informe sobre el cumplimiento del control interno en la organización, conclusiones y recomendaciones, y una descripción detallada de las inconsistencias y los hallazgos.

5

Informe
Finalizado el plan de auditoría, se deberá elaborar un informe del resultado de la misma, donde se consignen los hallazgos que representan un valor importante para la organización. Deberán estar relacionados los aspectos preocupantes, la postura frente a ellos y las recomendaciones para mitigar o corregirlos.

6

Reunión de cierre
Una vez entregado el informe, la auditoría solicitará a la alta dirección una reunión de cierre con las partes auditadas, con el fin de revisar los hallazgos, el plan de mejoramiento y el tiempo definido para su cumplimiento. La reunión permite resolver incongruencias con los interesados y dejar claro el objetivo del informe de la auditoría.

Figura 5. Pasos en la etapa de informe
Fuente: propia

Un método recomendado para realizar la auditoría de un área o proceso es el propuesto por Puerres (2013). Propone, de manera sistemática, ocho actividades que metodológicamente permiten el desarrollo de los pasos dos, cuatro, cinco y seis.

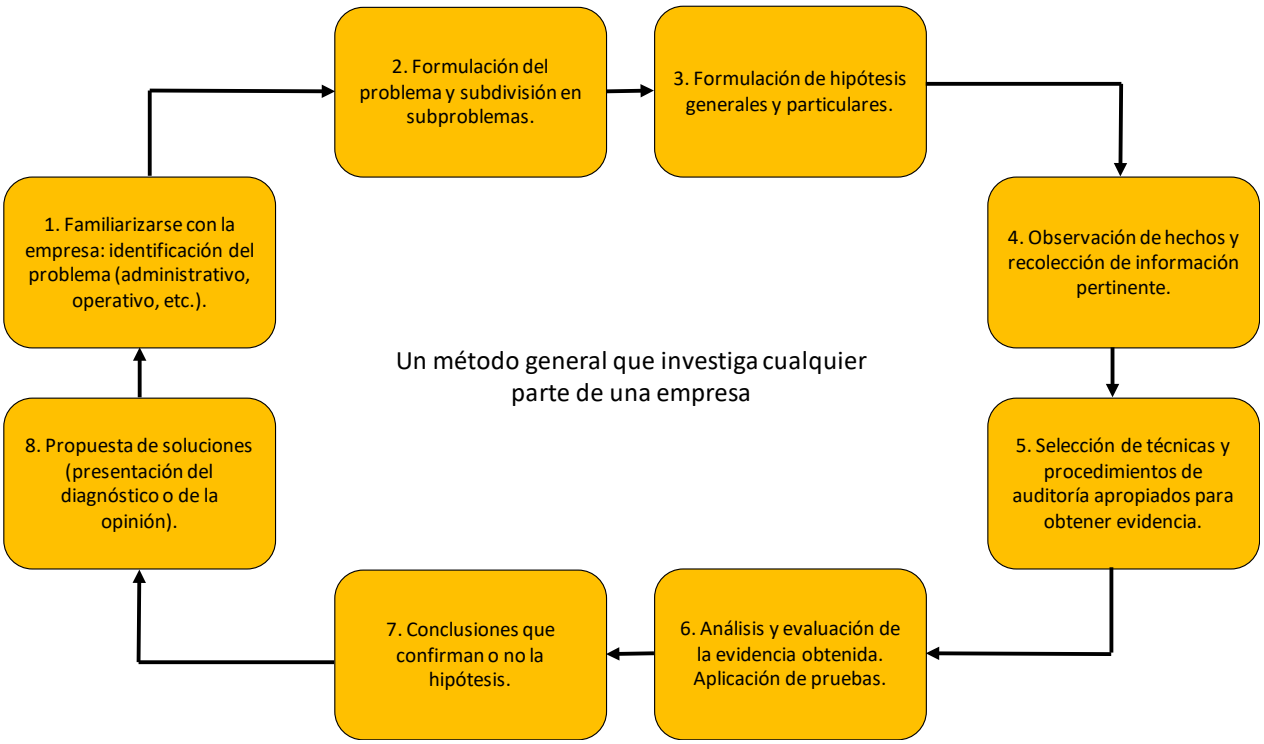

Figura 6. Metodología para realizar auditorías
Fuente: Puerres (2013)

Instrucción

Conocer y dominar las etapas y los pasos de un proceso de auditoría es crucial para un gerente o un auditor, dado que estos momentos marcan de manera sistemática el resultado. Lo invito a navegar en la galería de las etapas y los pasos del proceso de auditoría que encuentra en la página principal del eje.

Informe de auditoría

Figura 7. Informe de auditoría
Fuente:shutterstock/294489512

El informe de auditoría es el documento final de la investigación, evaluación y verificación del área o proceso auditado. En él, el auditor expone los resultados de las técnicas y los procedimientos aplicados para recolectar pruebas, realizar cotejos y evidenciar hallazgos, a fin de sustentar su postura sobre la razonabilidad de la información y las actividades adelantadas en la organización, con base en las normas y los aspectos planteados por la misma.

El informe debe contener información que permita determinar el periodo de tiempo auditado, los objetivos y alcances que se proyectaron para la auditoría y la postura u opinión de quien o quienes adelantaron la auditoría. Este documento sustentará decisiones posteriores por parte de la alta dirección. Es una poderosa herramienta para la dirección de una organización, dado que ayuda a mejorar los procesos.

Video

Lo invito a ampliar la información revisando un caso importante en la historia de la auditoría, la caída del gigante norteamericano WorldCom: ¿Qué falló en WorldCom? de la Universidad Alas Peruanas.

Estructura del informe

Para estructurar un informe de auditoría es necesario tener en cuenta aspectos que generen credibilidad en su contenido. Debe haber suficiencia en lo expresado. Además, lo expuesto debe ser coherente y comprensible. La postura y la opinión del auditor deben ser oportunas para que el informe cumpla con la normatividad.

La estructura puede variar, pero, en esencia, debe contener los apartados citados anteriormente. El informe se desarrolla de forma secuencial e informativa. Chambi (2010) recomienda algunos puntos que se deben tener en cuenta:

- Receptor: una vez finalizada la auditoría y entregados los resultados en el informe borrador, se deberá hacer una reunión previa al informe final con los auditados, con el ánimo de escuchar a la otra parte y colocar en el informe sus posturas frente a los hallazgos. De allí, el informe se dirigirá al representante de la alta dirección de la organización.

- Lugar y fecha: este dato determina la fecha de emisión del informe y el alcance de la auditoría. Deja claro hasta dónde va la responsabilidad del auditor por hechos posteriores que puedan afectar el resultado de la auditoría de manera significativa.

- Orden de trabajo: hace referencia al enfoque y la naturaleza de la investigación, análisis y revisión que se va adelantar, mencionando los motivos que originaron la necesidad de aplicar la auditoría.

- Objetivos general y específicos: de manera detallada y sistemática se deberán mencionar las razones del ejercicio y los fines que se buscan, dejando claro de manera taxativa el tema que ocupa la auditoría. La redacción de los objetivos debe estar en estricta concordancia con el enfoque, la naturaleza y el plan de auditoría.

- Alcance: permite relacionar los niveles de profundidad de la auditoría que se puede adelantar, así como la cobertura permitida, determinando las áreas de consideradas.

- Normatividad aplicada: relacionar las normas y directrices aplicadas en el desarrollo de la auditoría, explicando los alcances de cada una y dejando salvedades en caso de no observarse algún precepto o apartado de las mismas.

- Magnitud, profundidad y cobertura de la auditoría: aquí se debe colocar información espacio-temporal relacionada con la ubicación de los sitios de auditoría, la ventana de observación de tiempo, áreas o procesos objeto de la auditoría, los tipos de muestra que se tomaron y su cotejo con el universo considerado, tipos y fuentes de origen de la información y evidencia, relación de problemas en la adquisición y tratamiento de la información.

- Metodología: mencionar las técnicas y los métodos que se emplearon para la obtención de información orientada a dar respuesta a los objetivos de la auditoría.

- Resultados de la auditoría: se deben colocar de manera clara y expresa los hallazgos producto del examen en cumplimento de los objetivos de la auditoría. Los hallazgos deberán estar relacionados con base en su relevancia para la organización, a partir de los efectos reales o potenciales de su manifestación.

- Opinión del auditor y conclusiones: el auditor debe desarrollar deducciones lógicas sobre los hallazgos encontrados y no simplemente repetir en qué consisten. La opinión favorable, limpia o sin salvedades hace referencia a que el auditor está totalmente de acuerdo; es decir, que la presentación y el contenido motivo del examen es correcto y está alineado con lo proyectado. La opinión con salvedades quiere decir que el auditor ha encontrado una o varias circunstancias significativas que no afectan la fidelidad del resultado o permiten que el auditor pueda tener un juicio cierto a pesar de estar presentes. La opinión desfavorable, negativa o adversa está enmarcada en la manifestación del auditor acerca del resultado. Lo encontrado dista significativamente de lo proyectado. Por otra parte, la opinión denegada o abstención de opinión se da cuando el auditor no ha tenido suficiente evidencia para generar un juicio.

Definir los tipos de opinión de la auditoría permite tener exactitud en el proceso.

- Recomendaciones: en este ítem deben desarrollarse, a partir de la experticia del o los auditores, los posibles cursos de acción para tratar los hallazgos. Las recomendaciones deben estar alineadas con las conclusiones; asimismo, deben ser acciones específicas, factibles y conducentes.

- Opiniones de los funcionarios auditados: la auditoría deberá solicitar que los miembros de la organización responsable presenten de manera escrita sus comentarios frente a los resultados y hallazgos de la auditoría.

- Firma: los informes y documentos de los resultados de la auditoría deben estar firmados con el número de la matrícula profesional.

Para la interpretación de un informe de auditoría se debe centrar la atención en las opiniones del auditor, a fin de establecer cuáles fueron las consideraciones del mismo y, a partir de las recomendaciones realizadas en el informe, tomar acciones para tratar los hallazgos.

Instrucción

Los procesos de auditoría son herramientas poderosas para mantener y mejorar la integridad de una organización, si son bien empleadas y ejecutadas. Lo invito a revisar la página principal del eje y desarrollar la actividad de lectura relacionada con "Los escándalos financieros y la auditoría: pérdida y recuperación de la confianza en una profesión en crisis". Conteste las preguntas y los requerimientos.

Aplicación de un modelo de control interno

La implantación de un sistema de control interno surge de la necesidad de proteger los recursos de una organización y prevenir o detectar errores y fraudes. Para ello, se establecen políticas y métodos que, integrados de manera armónica, generan efectos positivos en las operaciones empresariales.

¡Importante!

En este escenario, las motivaciones de un sistema de control interno nacen de la estructura organizacional como gestión de la alta gerencia, o como producto de un informe de auditoría donde se evidencian errores o fraudes en las operaciones.

En la aplicación de la gestión del riesgo en un sistema de control interno este apartado se incluye, generalmente, en la etapa de planeación del sistema. En las auditorías, también se plantea la necesidad de la gestión del riesgo en la etapa de planeación de la misma, con el fin de identificar los escenarios de riesgo.

¡Recordemos que!

En la práctica, un sistema de control interno debe ser fácil de implementar. Para nuestro desarrollo, el enfoque lo colocamos en las pequeñas y medianas empresas con el modelo COSO III pymes, visto en el anterior eje.
Este modelo propone un esquema compacto que permite adelantar el control interno, obviando algunos pasos que, por su profundidad, no aplican en una empresa mediana o pequeña.

La presentación del modelo se puede estructurar a partir de una secuencia lógica. En primera instancia, se evalúa la situación de la organización, con el fin de entender el entorno interno y externo. Posteriormente, la gerencia determina una visión del control interno. Después, se examinan los 17 principios del COSO III y se define cuáles aplican a la empresa. Luego, se dan los elementos de evaluación, con los cuales se fijan las políticas y los lineamientos para el seguimiento y la evaluación del control interno. Una vez definida esta base conceptual, se debe establecer el plan de implementación del modelo y cómo se comunicará a la organización, sensibilizando de manera eficaz a todos los integrantes de la misma para lograr su adhesión al modelo.

Los cinco componentes del control interno del COSO III se deben adaptar a la condición propia de la organización con base en sus alcances y tamaño:

1. Ambiente de control

Es necesario que la empresa implemente actividades de control como normas, políticas, códigos de conducta y procedimientos, entre otros, con el fin de generar conceptos frente al control y, con ellos, permear la conciencia de los miembros de la misma. En el caso de las pymes, estos escenarios son informales y trascienden a la tradición de la organización de una manera orientada al proceder el empleado por su formación ética.

Algunos factores de control interno que se deben tener en cuenta son:

- Código de valores y ética empresarial.
- Consejo de administración u órgano de dirección.
- Modelo de gestión y organización de la empresa.
- Organización y estructura administrativa.
- Manual de procesos y procedimientos.
- Gestión del talento humano.

2. Evaluación de riesgos

Este proceso permite identificar amenazas potenciales. El ciclo para realizar la gestión del riesgo tiene los siguientes momentos:

- Identificar riesgos.
- Reconocer las áreas de posible riesgo.
- Realizar la valoración de riesgos.
- Documentarse sobre dichos riesgos.
- Planificar posibles soluciones.
- Realizar la carta de recomendaciones.

La implementación de la gestión del riesgo en las pequeñas empresas es mucho más expedita, debido a que los canales de comunicación son menos extensos y los niveles de autoridad son menores, así, se conocen de primera mano los problemas y las posibles soluciones; es decir, el ambiente organizacional y empresarial favorece la comunicación y la toma de decisiones.

3. Actividades de control

Por las dimensiones e interacción de una empresa mediana o pequeña, las actividades de control son mucho más efectivas, así, su acción está dada a corto plazo. En ellas intervienen normalmente los dueños de las mismas y los encargados de la dirección, por ello, se puede ejercer un mayor y mejor seguimiento al cumplimiento de los objetivos y los procesos de la organización.

Algunas actividades de control pertinentes en estos casos son (Carvajal y Escobar, 2012):

- Normas y políticas de la alta dirección de la organización en el control.
- Evaluación, prevención y tratamiento de riesgos.
- Selección y ejecución de actividades de control con base a costos y pertinencia de los procesos.
- Sistemas de información para el manejo y captura de datos sensibles de la organización.

4. Información y comunicación

Los canales de información en las pymes son más cortos y efectivos. La interacción entre directivos y trabajadores es prácticamente directa, se da sin formalismos. Aspectos importantes son el flujo de información de áreas sensibles, la información disponible sobre normas de control interno y la facilidad de acceso a información interna y externa en los niveles de pertinencia correspondientes con base en su rol en la organización.

5. Monitoreo

En las pymes, esta actividad está en cabeza de la administración por tener niveles jerárquicos estrechos. Este ejercicio permite tener contacto directo con las áreas y los procesos sensibles de la organización y conocer de primera mano los problemas y alcances que no se realizaron o se salieron de los parámetros esperados. Los resultados del monitoreo se pueden conocer rápidamente, lo que genera opciones de tratamiento oportuno para mejorar los procesos y las acciones.

Tener claros la estructura y los componentes del COSO III permite aplicar de manera puntual la metodología y el modelo a cualquier escenario donde el control interno puede ser un factor de competitividad y garantía de integralidad de la organización. Lo invito a consultar el mapa conceptual sobre el COSO III, con el fin de que revise e interiorice su mecánica.

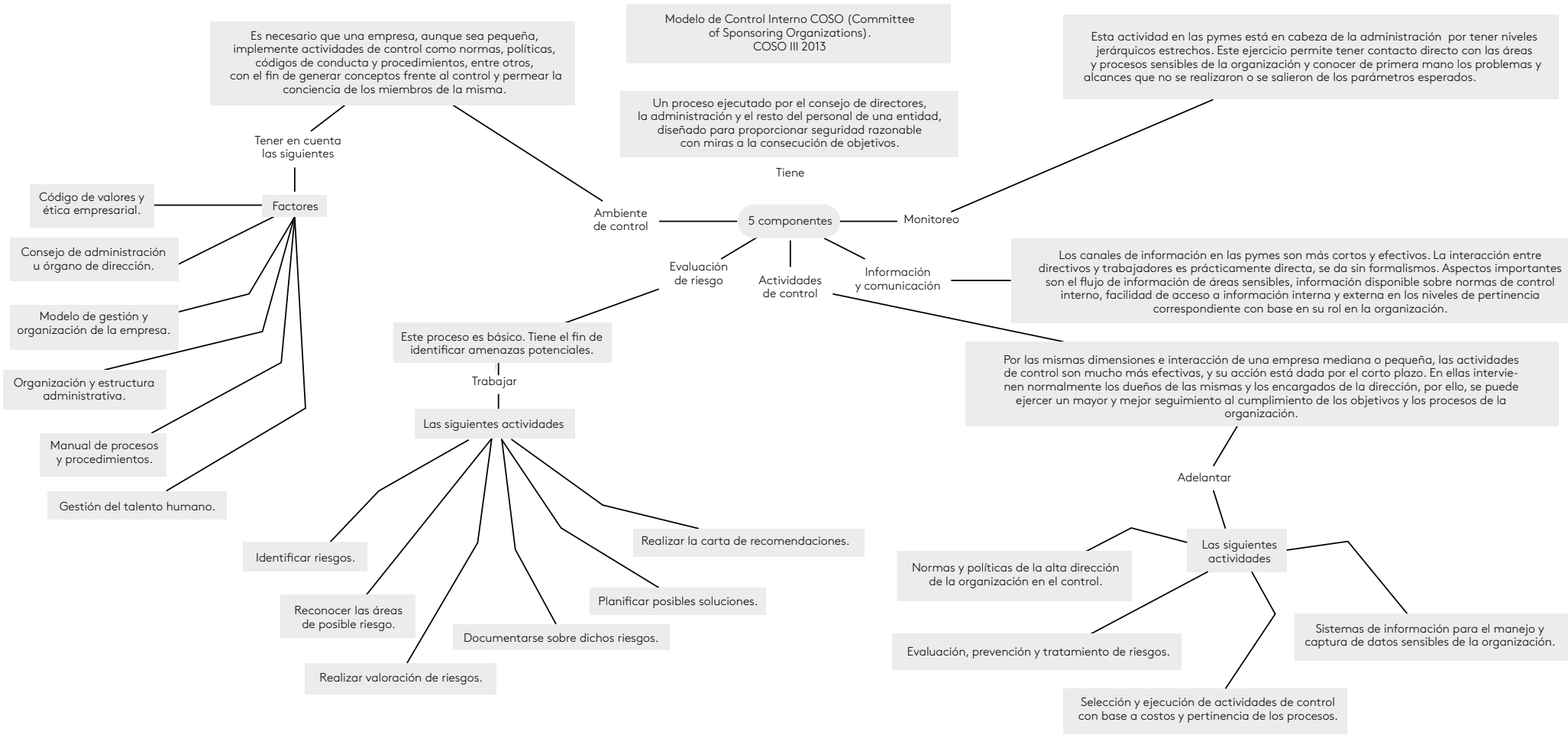

Figura 8. Informe de auditoría
Fuente: propia

Aplicación del modelo de control interno basado en el COSO III a una empresa en el área de impuestos

Contexto

La empresa no pagó oportunamente los impuestos (impuesto de renta, impuesto al valor agregado (IVA), ICA, retención en la fuente, impuesto al patrimonio, gravamen a los movimientos financieros, y aportes parafiscales).

Entorno de control

Una de las responsabilidades de la alta dirección de una organización es velar por el cumplimiento de las obligaciones tributarias ante los organismos del Estado en materia impositiva, impuestos que son de obligatorio cumplimiento en los plazos y términos establecidos.

Evaluación de riesgos

En las etapas de la gestión del riesgo un escenario que representa riesgo para la organización es el incumplimiento de obligaciones tributarias, por los altos costos que representan las sanciones y multas posteriores a su incumplimiento, afectando de manera significativa las utilidades de los propietarios.

Actividades de control

Diseño de un mecanismo para garantizar el cumplimiento de los pagos oportunos de las obligaciones tributarias, mediante un sistema de alarmas tempranas para hacer la gestión con base en los cronogramas de los organismos de recaudación de impuestos y gravámenes.

Información y comunicación

La alta dirección debe pedir al encargado del área de contabilidad un informe detallado del incumplimiento del pago y la forma como la empresa tiene dispuesto pagar el valor del impuesto y la multa correspondiente.

Monitoreo o supervisión

Verificación de la implementación del mecanismo de alerta temprana en el pago de impuestos y la realización del mismo en las fechas previstas.

Instrucción

Para mayor comprensión de la implementación de este modelo, vamos a resolver en la página principal del eje la actividad de refuerzo y a desarrollar el caso Parmalat y Deloitte, con el cual podrá aplicar la metodología para realizar auditorías expuestas en este eje, y a desarrollar el caso Banesto, con el cual podrá desplegar el modelo de informe de auditoría.

BIBLIOGRAFÍA

AOB Auditores. (s. f.). *Normas Internacionales de Auditoría*. Recuperado de http://aobauditores.com/nias/

Carvajal, A. y Escobar, M. (2012). *Herramienta integrada de control interno y administración del riesgo*. Bogotá, Colombia: Universidad Externado de Colombia.

Castañeda, J. (2016). *Módulo: Prevención y gestión del riesgo*. Bogotá, Colombia: Fundación Universitaria del Área Andina.

Chambi, G. (2010). *Estructura de los informes de auditoría*. Recuperado de http://www.mailxmail.com/estructura-informes-auditoría_h

Emprendepyme. (s. f.). *Tipos de auditoría*. Recuperado de https://www.emprendepyme.net/tipos-de-auditoría.html

Gerencie. (s. f.). *Auditoría financiera*. Recuperado de https://www.gerencie.com/auditoría-financiera.html

Granda, R. (2009). *Manual de control interno, sectores público, privado y solidario. Un modelo simplificado y práctico*. Bogotá, Colombia. Grupo Editorial Nueva Legislación LTDA.

Grupo Consultor Internacional (s. f.). *Confianza y control empresarial*. Recuperado de https://grupoconsultorefe.com/servicio/auditoría/estados-financieros

Grupo Consultor Internacional. (s. f.). *Auditoría de estados financieros*. Recuperado de https://grupoconsultorefe.com/servicio/auditoría/estados-financieros

Guzmán, L. (s. f.). *Tipos de auditoría*. Recuperado de https://www.ccpm.org.mx/servicios/gaceta_universitaria/junio_julio_2012/espacio_universitario.html

Instituto de Contabilidad y Auditoría de Cuentas. (2013). *NIA 315. Identificación y valorización de los riesgos de incorreción material mediante el conocimiento de la entidad y de su entorno*. Recuperado de http://www.icac.meh.es/NIAS/NIA%20315%20p%20def.pdf

Instituto Mexicano de Contadores Públicos. (2013). *Modelos de dictámenes y otras opiniones e informes del auditor. Guía para la preparación de dictámenes y otros informes*. Ciudad de México, México: Comisión de Normas de Auditoría y Aseguramiento.

Puerres, I. (2013). *Una mirada práctica de la auditoría*. Bogotá, Colombia: Pontificia Universidad Javeriana.

GESTIÓN, ADMINISTRACIÓN DE RIESGOS Y MODELOS DE CONTROL INTERNO

Javier Castañeda

EJE 4

Propongamos

Fuente: Shutterstock/258980774

AREANDINA
Fundación Universitaria del Área Andina
MIEMBRO DE LA RED ILUMNO

INTRODUCCIÓN

En la actualidad, la aplicación de la gestión del riesgo es un proceso permanente en las organizaciones responsables. El lenguaje del control interno y el de la auditoría han permeado la alta dirección, puesto que hoy más que nunca los avances tecnológicos, la gestión del conocimiento, la investigación, los factores producto de la evolución del hombre y la necesidad de implementar nuevas estrategias y soluciones a las demandas de la humanidad han generado escenarios complejos con mayores riesgos. Por consiguiente, adelantarse a su impacto y posibles daños es una de las misiones del gerente del siglo XXI, cuyo objetivo es velar por la integridad de la organización.

La gestión del riesgo es un proceso que, a partir de etapas lógicas, se inicia de lo general a lo particular, empleando el método deductivo. Se ejecuta en los sistemas de control interno como una de las partes que permiten identificar escenarios de riesgos para ejercer control y evitar su materialización. En las auditorías también está presente, puesto que en las etapas iniciales del proceso el auditor debe identificar los riesgos del área o los procesos y aplicar su trabajo investigativo y evaluativo.

El proceso de gestión del riesgo es una actividad que debe ser desarrollada por profesionales preparados, con experiencia en su aplicación y con conocimiento de la organización, el área o los procesos a auditar o intervenir para la aplicación del control interno. Esta premisa es crucial porque cuando se está implementando el modelo de gestión del riesgo los criterios de aplicación y alcances son diseñados de manera particular para la organización, lo que quiere decir que no existe un modelo estándar. Hay un componente de subjetividad en su construcción, por ello, se busca que quienes intervengan tengan experiencia. Solo así, desde un trabajo en equipo y un proceso de intersubjetividad, se modelan políticas, normas y procedimientos ajustados a las necesidades de la organización.

Para el presente referente de pensamiento se planteó la pregunta: ¿cuál podría ser la propuesta de un sistema de gestión y administración del riesgo que dé respuesta a las necesidades de las organizaciones actuales? A partir de ella y con el desarrollo de la metodología de la matriz de vulnerabilidad, el estudiante podrá, mediante un proceso reflexivo y crítico, generar ideas y modelaciones de propuestas para aplicarlos a situaciones específicas en organizaciones de cualquier índole.

Teniendo en cuenta los temas tratados en los anteriores ejes: el riesgo y su gestión, los sistemas de control interno y la conceptualización de auditoría y el desarrollo de un caso desde la gestión del riesgo, en este eje trataremos a detalle la gestión del riesgo, la cual se aplica como una actividad dentro de los sistemas de control interno, pero también como insumo en una auditoría.

Análisis integral: gestión del riesgo y control interno

El presente desarrollo esbozará la aplicación de la gestión del riesgo con un esquema general aplicable a cualquier entorno. Los parámetros establecidos pueden ser ajustados a las particularidades de cada organización o empresa, de hecho, existen muchas propuestas de aplicación y variación en los conceptos y estimativos, teniendo en cuenta que la gestión del riesgo es un proceso con un alto nivel de subjetividad, producto de la incertidumbre. Por consiguiente, la finalidad es reducir y controlar, a través de un proceso sistemático, los aspectos que pueden generar daños y perjuicios a la organización.

Las instancias de la gestión del riesgo tienen alcances en el sector público y en el privado, como se ha mencionado. Los riesgos y la incertidumbre en los procesos están presentes al tomar cualquier decisión, sea desde el Estado o el campo empresarial.

Lo invito a consultar un portal importante para evidenciar el marco normativo en el sector público: el Normograma publicado por la Presidencia de la República.

Figura 1. Fachada del edificio de Odebrecht en Sao Paulo
Fuente:shutterstock/550164199

Otro campo en el cual el Estado ha implementado herramientas importantes para su manejo específico es la gestión del riesgo de corrupción, ello ante los constantes casos en el sector público, donde ha habido graves daños al erario público, producto de las acciones de funcionarios corruptos que han causado detrimento patrimonial a través de argucias y colusión para cometer desfalcos millonarios. En la historia reciente del país se han visto comprometidos los tres poderes del Estado. En el caso del poder ejecutivo, se ha evidenciado cómo con dinero de se financiaron campañas a la presidencia. Por otro lado, en el poder legislativo, muchos senadores y congresistas se han visto envueltos en actos de corrupción por tráfico de influencias en la contratación estatal, sobornos, etc. Además, recientemente, en el poder judicial se destapó el denominado "Cartel de la toga". Tres expresidentes de la Corte Suprema de Justicia han sido señalados de haber recibido dinero por desviar sus decisiones, afectando la integridad de la administración de la justicia. Tampoco se puede olvidar el escándalo del fiscal anticorrupción corrupto.

Instrucción

La corrupción es un fenómeno que se presenta en el sector público y en el privado. La ***Guía para la gestión del riesgo de corrupción 2015*** es una herramienta que puede ser adaptada a cualquier entorno en el que se quiera trabajar la corrupción y atacar sus orígenes y causas. Lo invito a consultar el documento que guarda similitudes con la metodología aquí propuesta en la página principal del eje.

Establecer el impacto de un riesgo es una de las tareas importantes de la gestión del riesgo, definir si es moderado, mayor o catastrófico permite establecer las acciones que se deben adoptar para tratarlo, lo invito a adelantar la actividad denominada "El cartel de la toga", teniendo en cuenta el formato para determinar el impacto de estas acciones corruptas, empleé la *Guía para la Gestión del Riesgo de Corrupción*.

En el campo de la auditoría, las Normas Internacionales de Auditoría (NIA) son un referente obligatorio. Se suman a ellas la Norma ISO 19011 del año 2002, la cual establece directrices para la auditoría de los sistemas de gestión de la calidad y/o ambiental; la Norma ISO 19011 del año 2011, que establece las directrices para la auditoría de sistemas de gestión, siendo una herramienta importante para adelantar auditorías en cualquier sistema de gestión; la ISO 9001; ISO 14001; OHSAS 18001; ISO 22000, entre otras.

¡Importante!

La norma ISO 19011 tiene lo atinente a las directrices para la auditoría de sistemas de gestión. Es una herramienta de consulta importante para el profesional que desee trabajar en campo de la gestión del riesgo.

Por otra parte, recordemos las etapas de la gestión del riesgo, las cuales están definidas en la Norma ISO 31000 (Icontec, 2011) y cuyos alcances tienen aplicabilidad a cualquier entorno organizacional, dado que su estructura ha sido desarrollada de manera secuencial, lógica e integral considerándose un sistema que tiene flujo hacia adelante y hacia atrás, mediante constante comunicación y monitoreo. Así, la precisión, que no es un concepto lineal, sino holístico, se desarrolla de forma simultánea en sus etapas con constante retroalimentación.

1. Diagnóstico y establecimiento del contexto:

- El contexto estratégico o externo.
- El contexto organizacional o interno.
- El contexto de la gestión del riesgo.
- Criterio para la evaluación del riesgo.
- Definir la estructura de gestión del riesgo.

2. Valoración del riesgo:

- Identificación del riesgo.
- Análisis del riesgo.
- Calificación del riesgo.
- Evaluación del riesgo.

3. Tratamiento del riesgo.

4. Comunicación y consulta.

5. Monitoreo y seguimiento.

¡Importante!

A continuación, con el ánimo de generar una propuesta de gestión del riesgo con base en el modelo de la matriz de análisis de vulnerabilidades, se desarrollarán de manera detallada las etapas y, posteriormente, se hará un ejercicio dirigido.

Diagnóstico y establecimiento del contexto

Para iniciar un proceso de gestión del riesgo la primera actividad que se debe adelantar es la contextualización del entorno, con el fin de definir un marco situacional que incluya el contexto externo e interno y, a la vez, las políticas y la postura de la organización frente a la gestión del riesgo, estableciendo los criterios y la estructura de la misma.

Figura 2. Diagnóstico y establecimiento del contexto de la gestión del riesgo
Fuente: Castañeda (2016)

El contexto estratégico o externo permite establecer las oportunidades y amenazas del entorno. La Norma ISO 31000 lo define como:

> El ambiente social y cultural, político, legal, reglamentario, financiero, tecnológico, económico, natural y competitivo, bien sea internacional, nacional, regional o local, los impulsores clave y las tendencias que tienen impacto en los objetivos de la organización y las relaciones con las partes involucradas externas y sus percepciones y valores (Icontec, 2011, pp. 12-13).

La forma de establecerlo es a partir de estudios de los factores mencionados. Una de las muchas herramientas puede ser la matriz DOFA (debilidades, oportunidades, fortalezas y amenazas), la cual facilita la determinación de los parámetros que se tendrán en cuenta en la gestión del riesgo.

El contexto interno permite establecer la situación de la organización: sus debilidades, fortalezas, capacidades y limitaciones. Es definido por la Norma ISO 31000, la cual incluye, entre otros, los siguientes factores de la organización:

> Gobierno, estructura organizacional, funciones y responsabilidades, políticas, objetivos y estrategias implementadas para lograrlos, las capacidades, entendidas en términos de recursos y conocimiento (por ejemplo capital, tiempo, personas, procesos, sistemas y tecnologías), sistemas de información, flujos de información y procesos para la toma de decisiones (tanto formales como informales), relaciones con las partes involucradas internas y sus percepciones y valores, la cultura de la organización, normas, directrices y modelos adoptados por la organización, y forma y extensión de las relaciones contractuales (Icontec, 2011, p. 6).

El contexto de la gestión del riesgo determina los alcances, estrategias y objetivos que la alta dirección y la organización establecieron para gestionar el riesgo en la entidad. Allí, se definen responsabilidades, profundidad, relaciones interorganizacionales, metodologías, evaluación, especificaciones y los aspectos referentes a atender el riesgo de manera sistemática y organizada. En este contexto es necesario establecer de manera explícita cuáles serán los criterios de evaluación del riesgo.

La Norma ISO 31000 determina algunos factores que se deben considerar al momento de definir estos criterios:

> La naturaleza y los tipos de causas y consecuencias que se pueden presentar y la forma en que se van a medir; cómo se va a definir la probabilidad; los marcos temporales de la probabilidad, las consecuencias, o ambas; cómo se va a determinar el nivel de riesgo; los puntos de vista de las partes involucradas; el nivel en el cual el riesgo se torna aceptable o tolerable; y si se debería o no tener en cuenta combinaciones de riesgos múltiples y, si es así, cómo y cuáles combinaciones se deberían considerar (Icontec, 2011, p. 20).

Por otra parte, también se deberá definir la estructura de la gestión del riesgo, estableciendo cómo se desarrollará la identificación, la evaluación y el tratamiento del riesgo, buscándose con ello incluir todo tipo de riesgos que puedan ser dañinos para la organización.

Valoración del riesgo

En esta etapa del proceso se busca establecer una visión total del riesgo, con el fin de desarrollar acciones de tratamiento que generen resultados apreciables para la organización, minimizando el impacto o su materialización.

Identificación y análisis del riesgo

Para realizar el proceso de caracterización del riesgo existen numerosas herramientas que, en esencia, contribuyen a la identificación, el análisis y la evaluación del riesgo. La Asociación Española de Gerencia de Riesgos y Seguros (2011) realizó una recopilación de la mayoría de herramientas que permiten gestionar el riesgo.

Proceso de evaluación del riesgo						
Herramientas y técnicas	Identificación del riesgo	Análisis del riesgo			Evaluación del riesgo	
		Consecuencia	Probabilidad	Nivel del riesgo		
Tormenta de ideas *(brainstorming)*	FA	NA				B01
Entrevistas estructuradas o semiestructuradas	FA	NA	NA	NA	NA	B02
Delphi	FA	NA	NA	NA	NA	B03
Lista de verificación *(check-lists)*	FA	NA	NA	NA	NA	B04
Análisis preliminar de riesgos	FA	NA	NA	NA	NA	B05
Estudios de riesgos operacionales (Hazop)	FA	FA	A	A	A	B06
Análisis de riesgos y puntos de control críticos (Haccp)	FA	FA	NA	NA	FA	B07

Valoración del riesgo medioambiental	FA	FA	FA	FA	FA	B08
Qué pasaría si *(what if)*	FA	FA	FA	FA	FA	B09
Análisis de escenario	FA	FA	A	A	A	B10
Análisis del impacto del negocio	A	FA	A	A	A	B11
Análisis de causa	NA	FA	FA	FA	FA	B12
Análisis modal de fallos potenciales y sus efectos (ANFE-FMEA)	FA	FA	FA	FA	FA	B13
Análisis de árbol del fallos	A	NA	FA	A	A	B14
Análisis de árbol de sucesos	A	FA	A	A	NA	B15
Análisis de causa consecuencia	A	FA	FA	A	A	B16
Análisis de causa efecto	FA	FA	NA	NA	NA	B17
Análisis de niveles de protección	A	FA	A	A	NA	B18
Árbol de decisión	NA	FA	FA	A	A	B19
Análisis de fiabilidad humana	FA	FA	FA	FA	A	B20
Análisis de la pajarita	NA	A	FA	FA	A	B21
Mantenimiento centrado en la confiabilidad	FA	FA	FA	FA	FA	B22
Análisis de errores de diseño *(Sneak)*	A	NA	NA	NA	NA	B23
Análisis de Markov	A	FA	NA	NA	NA	B24
Simulación de Monte Carlo	NA	NA	NA	NA	FA	B25

Estadísticas y redes Bayesianas	NA	FA	NA	NA	FA	B26
Curvas FN	A	FA	FA	A	FA	B27
Índices de riesgos	A	FA	FA	A	FA	B28
Matriz de consecuencia/ probabilidad	FA	FA	FA	FA	A	B29
Análisis de coste/ beneficio	A	FA	A	A	A	B30
Análisis de decisión multicriterio	A	FA	A	FA	A	B31

FA: fuertemente aplicable. A: aplicable. NA: no aplicable.

Tabla 1. Herramientas y técnicas para la valoración del riesgo: aplicación de la Norma ISO 31010
Fuente: Asociación Española de Gerencia de Riesgos y Seguros (2011)

Instrucción

Las técnicas y los métodos para la valoración de riesgos permiten al profesional identificar, analizar y evaluar el riesgo. La herramienta análisis de causa y efecto para este caso puede ser el diagrama de Ishikawa o espina de pescado, el cual está disponible en la ISO 31010 o también en el *link*: Esta ayuda de manera sistemática a establecer las causas de un efecto. Lo invito a desarrollar la actividad y responder las preguntas del artículo de la *Revista Dinero* "Revisores fiscales al banquillo: ¿ciegos o con exceso de funciones?" en la página principal del eje.

Las herramientas de identificación de riesgos que pueden ser de gran ayuda y se emplean regularmente son:

- **Cuestionario de identificación y análisis de riesgos:** consiste en realizar un listado de preguntas frente a las diferentes áreas de la organización en las cuales se quiere gestionar el riesgo.

- **Lista de chequeo para la identificación y análisis del riesgo:** herramienta empleada por las empresas aseguradoras con el fin de considerar de manera general las situaciones que puedan afectar una empresa u organización. Su limitación es el enfoque a riesgos que pueden tener cobertura, por ello, es un punto de partida, pero en la empresa se deben incluir todos los riesgos, inclusive aquellos que no son susceptibles de asegurar por alto nivel de impacto y pocas posibilidades de tratamiento.

Lista de chequeo de las pólizas de seguros	
Grupo	**Riesgo**
Riesgos de la naturaleza	Terremoto, maremoto, tsunami, erupción volcánica, emanación natural de gas o vapor, lluvia torrencial, nieve, granizado, caída de rayo, desbordamiento de ríos, lagos, inundación, alud, avalancha, ola de calor o de frío, sequía, alimañas, roedores, moho, hongos, etc.
Riesgos tecnológicos	Incendio, explosión, humo, polvo, derrame de productos químicos, escape de gases y vapores, contaminación súbita, avería mecánica o eléctrica de maquinaria, corte súbito de energía eléctrica, desmoronamiento de material apilado, etc.
Riesgos marítimos de aviación y transporte	Avería de medio de transporte aéreo, marítimo o terrestre, colapso de artefacto espacial, naufragio, colisión de automóvil matriculado, pérdida o deterioro de mercancía, error de conducción de automóvil, de vehículo de transporte terrestre o en operación de transporte aéreo.
Riesgos político-sociales	Guerra civil o internacional, acto bélico, levantamiento militar, civil revolución, asonada, motín, huelga legal, confiscación, etc.
Riesgos antisociales	Terrorismo, sabotaje, huelga ilegal, acto vandálico, piromanía, asesinato, atentado, secuestro, robo, hurto, desaparición misteriosa, mermas, infidelidad de empleados, falsificación, desfalco, fraude, intrusión y espionaje industrial.
Riesgos indirectos	Daños a bienes arrendados a terceros, o bajo dominio de terceros, o bajo su responsabilidad civil.
Riesgos consecuenciales	Demolición necesaria de partes ilesas, pérdida de uso, desempleo temporal de mano de obra, pérdida de persona clave, gastos financieros extraordinarios, etc.
Responsabilidad civil empresarial	Daño a edificio o local arrendado, daño a bien de terceros en: depósito, proceso de transformación, mezcla o ensamble, incumplimiento de contrato, difamación, calumnia, piratería industrial o comercial, competencia desleal, etc.
Responsabilidad civil patronal	Incumplimiento de normas de higiene, de seguridad, de convenio colectivo, de contrato individual, daños a bienes de empleados, etc.
Responsabilidad automóviles	Daños materiales a ocupantes o a terceros, daños corporales a ocupantes o a terceros.

Responsabilidad civil profesional	Error técnico, de diseño o cálculo, error administrativo, error médico, abandono de funciones profesionales, negligencia, dolo de personal directivo, etc.
Responsabilidad civil ecológica	Contaminación gradual del ambiente, contaminación súbita o accidental, delito ecológico, contaminación radioactiva, lluvia ácida.
Riesgos personales	Muerte por accidente laboral, muerte por accidente no laboral, invalidez permanente, incapacidad profesional, incapacidad laboral transitoria, secuestro, asesinato, atentado, desempleo, etc.
Riesgos financieros	Riesgos de créditos, riesgo de inversión en el exterior, riesgo de caución, riesgo de cambio.

Tabla 2. Lista de chequeo de pólizas de seguro
Fuente: Business Alliance for Secure Commerce (s. f.)

- **Diagramas de flujo:** manera gráfica de entender un proceso. Es una herramienta importante para analizar la secuencia y, con ello, determinar los momentos en los cuales se generan actividades que pueden revestir riegos en el proceso.

- **Análisis de los estados financieros de la empresa:** proceso mediante el cual la alta dirección hace seguimiento a la integridad en el campo de las finanzas y los estados contables, revisando aspectos como rentabilidad, liquidez, nivel de endeudamiento, rotación de inventarios, balances, análisis de activos, pasivos, pérdidas y ganancias, cantera, entre otros.

- **Análisis de registros documentales, políticas, informes, etc.:** esta herramienta es una fuente efectiva de información acerca de riesgos en la organización, reflejada en resultados y conclusiones, como informes de auditoría, oficina y reportes de quejas y reclamos, siniestralidad en procesos contractuales, etc.

- **Inspección física e identificación en análisis de riesgos:** todo proceso es susceptible de ser complementado y, en este caso, los encargados de la gestión del riesgo deben adelantar acciones que amplíen, corroboren o desvirtúen la información en documentos sobre situaciones de riesgo.

¡Importante!

Se recomienda combinar las anteriores herramientas y todas las que permitan realizar procesos más completos y obtener resultados más exactos. Lo importante es que al integrarlas no afecten ni vuelvan complejo y lento el proceso.

Método para adelantar la gestión del riesgo

Existen varias alternativas de métodos para la gestión del riesgo. La mayoría de ellas conduce al mismo resultado: cómo tratar el riesgo y hacerle seguimiento. La matriz de análisis de vulnerabilidad se emplea en empresas tanto del sector público como del privado. Fue estructurada por Duque (1999) bajo el Modelo del Sistema Gestión Integral del Riesgo en las Organizaciones (GIRO). Esta metodología considera todas las actividades que se deben realizar para tener una visión completa del riesgo y su administración y gestión en la organización. Es una de las más se ajusta a este proceso.

Para adelantar el análisis de vulnerabilidad se debe tener en cuenta lo siguiente:

1. Definición del equipo evaluador.
2. Determinación del sistema de referencia y ámbito de aplicación.
3. Determinación de factores de vulnerabilidad.
4. Definición de nivel de riesgo aceptable.
5. Identificación de los recursos, procesos o actividades amenazadas.
6. Identificación y selección de amenazas.
7. Determinación de consecuencias reales del sistema.
8. Cálculo de porcentaje de vulnerabilidad.
9. Evaluación.

El equipo evaluador debe estar integrado por personas que, por su experiencia y preparación profesional, puedan gestionar el riesgo desde una posición soportada en procesos técnicos que garanticen los resultados.

El sistema de referencia corresponde a la estructura (empresa, departamento, unidad de negocio, sección, etc.) en la cual se va adelantar el proceso de gestión del riesgo, con el fin de identificar las vulnerabilidades.

El ámbito de aplicación se refiere a aspectos que pueden ser afectados en el sistema de referencia, tales como recursos, procesos, instalaciones, etc. Mediante una herramienta de diagnóstico se identifican las amenazas que se puedan materializar dentro de los ámbitos de aplicación. En este momento del proceso, la organización encargada de la gestión del riesgo debe establecer la forma de dar un peso representativo a la amenaza, este concepto se denomina significancia, que es la ponderación de la amenaza por su tamaño relativo y su potencial de daño. Normalmente, para todo el proceso de análisis de riesgos se emplean escalas cualitativas y cuantitativas, las cuales pueden ser ajustadas a las situaciones particulares de cada organización.

Una vez identificada la significancia de la amenaza, se establece el tamaño relativo (T), que hace referencia a lo representativa que puede llegar a ser para la organización. Allí interviene la experticia del profesional del riesgo para evaluarla en una escala cualitativa de bajo, medio y alto, y cuantitativa de 1, 2 y 3. Por otra parte, el potencial de daño (P) es el grado de daño que puede ocurrir si se materializa el riesgo. Al igual que el tamaño relativo, esta apreciación es trabajo del profesional en riesgos. Su gradación es igual a la anterior: de bajo a alto y de 1 a 3.

El grado de significancia es producto de multiplicar el tamaño relativo (T) por el potencial de daño (P). En la siguiente matriz se puede establecer el grado de significancia.

Grado de significacia de la amenaza				Potencial de daño de la amenaza (P)		
				Bajo	Medio	Alto
				Escala		
				1	2	3
Tamaño relativo de la amenaza (T)	Bajo	Escala	1	1	2	3
	Medio		2	2	4	6
	Alto		3	3	6	9
				Grado de significancia de la amenaza (S)		

Tabla 3. Grado de significancia de la amenaza
Fuente: Castañeda (2016)

El criterio para tener en cuenta una amenaza por su grado de significancia es que esté por encima de 1, es decir, en el grado bajo-bajo. De ahí en adelante, la amenaza tiene un valor representativo y debe ser gestionada a partir de las consideraciones de la administración y gestión del riesgo.

Cuando se establecen las amenazas, se procede a identificarlas con una nomenclatura o código que facilite su reconocimiento y clasificación.

Amenaza	Código
Amenaza 1	A
Amenaza 2	B
Amenaza 3	C
Amenaza 4	D
Amenaza 5	E

Tabla 4. Nomenclatura o código amenazas
Fuente: Castañeda (2016)

Luego de establecer los parámetros para el grado de significancia y el código o nomenclatura de la amenaza, se aplican los conceptos para verificar si se considera o no la amenaza. Se puede emplear la siguiente tabla:

Amenaza	Código	Significancia			Selección	
		Tamaño relativo de la amenaza (T)	Potencial de daño (P)	Significancia (S)	Sí	No
Amenaza	A					
Amenaza	B					
Amenaza	C					
Amenaza	D					
Amenaza	E					

Tabla 5. Selección de amenazas por su significancia
Fuente: Castañeda (2016)

Después de establecer el ámbito de aplicación en que se va trabajar, se deben identificar los recursos o actividades amenazadas, las cuales también se deben nombrar con un código para su clasificación e indización. Este código debe ser diferente al de las amenazas.

Recurso	Código
Recurso	1
Recurso	2
Recurso	3
Recurso	4
Recurso	5

Tabla 6. Nomenclatura o código del recurso o actividad
Fuente: Castañeda (2016)

Una vez se determinan las posibles amenazas y los recursos que pueden ser afectados si estas se materializan, se procede a realizar lo que Duque (1999) denominó "escenario de riesgos", que es la representación gráfica del recurso contra las amenazas a las que pueda estar sometido, entendiendo que las amenazas no afectan todos los recursos; allí, se configura la codificación del escenario sumando el código del recurso al de la amenaza. A continuación, se proyecta una matriz de escenario de riesgos.

Sistema de referencia	Empresa de consultoria		
Ámbito de aplicación	Contabilidad		
	Amenaza		
Recurso	Desconocimiento (A)	Desorganización (B)	Hurto (C)
Informes financieros (1)	A-1 (errores humanos)		
Entrada de dinero (2)			C-2 (hurto de recursos)
Controles financieros (3)		B-3 (fallas en el control)	

Tabla 7. Escenario de riesgos codificado
Fuente: Castañeda (2016)

Con la codificación de los posibles escenarios de riesgo se puede desarrollar un catálogo que la empresa emplee de manera regular para trabajar la gestión del riesgo. Así, cada vez que se vaya a intervenir un ámbito de aplicación no se tiene que empezar de nuevo.

Calificación del riesgo

Para calificar el riesgo se debe establecer un proceso de valoración del mismo. En las diferentes herramientas que se emplean normalmente se trabaja la frecuencia o probabilidad y la consecuencia o impacto, las cuales tienen escala valorativa cualitativa y cuantitativa.

Figura 3. Calificación del riesgo
Fuente:shutterstock/608549384

La frecuencia o probabilidad determina las veces que se puede llegar a materializar un evento crítico en una ventana de tiempo establecida sobre un recurso de la organización. Por su parte, la consecuencia o impacto determina la intensidad de la manifestación del evento crítico sobre el recurso considerado de la organización. La gradación de la frecuencia o el impacto es propia de cada organización y depende las particularidades de la misma. Duque (1999) plantea las siguientes gradaciones a partir de la observación de varias empresas, estableciendo un parámetro estándar.

Para la calificación de la frecuencia o probabilidad la siguiente tabla establece una escala numérica lineal, unos niveles y un número de eventos por año. Esta información puede ser trabajada desde los registros estadísticos de la organización y de allí inferir lapsos de frecuencia o probabilidad, con base en el histórico, o proyectarla teniendo en cuenta estudios de otras organizaciones.

Calificación de frecuencias		
Valor	Nivel	Casos por año
1	Improbable	Menos de un caso cada 50 años
2	Remoto	Un caso entre 21 y 50 años
3	Ocasional	Un caso entre 6 y 20 años
4	Moderado	Un caso entre 1 y cinco años
5	Frecuente	Entre 1 y 10 casos al año
6	Constante	Más de 10 casos al año

Tabla 8. Calificación de la frecuencia o probabilidad
Fuente: Castañeda (2016)

En la calificación del impacto o consecuencia se establece una escala numérica incremental para dar mayores cifras de diferencia, una gradación cualitativa y un alcance de la consecuencia.

Calificación de frecuencias		
Valor	Nivel	Montos considerados
1	Insignificante	Menor a USD 10.000
2	Marginal	Entre USD 10.000 y USD 100.000
5	Grave	Entre USD 100.000 y USD 500.000
10	Crítico	Entre USD 500.000 y USD 2.000.000
20	Desastroso	Entre USD 2.000.000 y USD 5.000.000
50	Catastrófico	Más de USD 5.000.000

Tabla 9. Calificación de la consecuencia o impacto
Fuente: Castañeda, J. (2016)

Se pueden plantear diferentes calificaciones para el impacto o consecuencia de diferentes recursos. Según los intereses de la organización, pueden ser recursos como el talento humano, el medioambiente, la operación de la empresa, la imagen corporativa, el comportamiento en el mercado, etc.

¡Importante!

La calificación del riesgo se da cuando se hace un cruce entre los valores de la frecuencia o probabilidad y la consecuencia o impacto.

La calificación del riesgo se da desde dos variables, las cuales se combinan para poder determinar la calificación del riesgo, normalmente se expresan de manera cualitativa y cuantitativa asignándole valores y niveles con base a las particularidades de la organización en el tratamiento del riesgo, lo invito a consultar el mapa conceptual sobre la calificación de los riesgos.

Evaluación del riesgo

En la evaluación del riesgo y con base en el modelo de la matriz de análisis de riesgo, se deben estructurar las matrices para determinar riesgo, vulnerabilidad, criterios y aceptabilidad.

Para la construcción de la matriz de riesgos se tiene en cuenta la conceptualización cualitativa y cuantitativa que se realizó en el título anterior, así como la frecuencia e impacto, ubicando estos valores a partir de un plano cartesiano. En el eje Y se coloca la frecuencia y en el eje X el impacto.

La disposición de las escalas cuantitativas y cualitativas inician de cero, de menor a mayor valor. Los valores sugeridos son de Duque (1999), pero pueden ser modificados según la necesidad o las particularidades del proceso. Estos están estructurados para la frecuencia de 1 a 6 en un aumento lineal y para el impacto de 1 a 50 en un aumento incremental. El valor máximo es de 300. Los valores de las demás casillas se determinan multiplicando el valor de la frecuencia por el valor del impacto.

Frecuencia	Constante	6	12	30	60	120	300
	Frecuente	5	10	25	50	100	250
	Moderado	4	8	20	40	80	200
	Ocasional	3	6	15	30	60	150
	Remoto	2	4	10	20	40	100
	Improbable	1	2	5	10	20	50
Matriz de riesgo		Insignificante	Marginal	Grave	Crítico	Desastroso	Catastrófico
		Impacto					

Tabla 10. Matriz de riesgos
Fuente: Castañeda (2016)

Después de establecer la matriz de riesgos, se debe estructurar la matriz de vulnerabilidad, la cual se expresa en porcentaje. Mediante una regla de tres simple se hace la equivalencia del mayor valor de la matriz al 100 %. En el caso anterior, el máximo valor es 300, lo que quiere decir que este equivale al 100 %. Los valores de las demás casillas se calculan a partir de multiplicar el número en la misma por 100 y dividirlo entre 300. Ejemplo: el valor de la casilla 1 se calcula multiplicando 1 por 100 y dividiéndolo entre 300 (1*100/300 = 0,3 %).

Los valores en términos porcentuales permiten tener una visión de la magnitud del riesgo evaluado. A continuación, se desarrolla la matriz en términos porcentuales.

Frecuencia	Constante	2,0%	4,0%	10,0%	20,0%	40,0%	100,0%
	Frecuente	1,7%	3,3%	8,3%	16,7%	33,3%	83,3%
	Moderado	1,3%	2,7%	6,7%	13,3%	26,7%	66,7%
	Ocasional	1,0%	2,0%	5,0%	10,0%	20,0%	50,0%
	Remoto	0,7%	1,3%	3,3%	6,7%	13,3%	33,3%
	Improbable	0,3%	0,7%	1,7%	3,3%	6,7%	16,7%
Matriz de vulnerabilidad		Insignificante	Marginal	Grave	Crítico	Desastroso	Catastrófico
		Impacto					

Tabla 11. Matriz de vulnerabilidad
Fuente: Castañeda (2016)

Al tener esta matriz, es necesario definir los niveles de aceptación del riesgo que la empresa está dispuesta a asumir. Este cálculo se hace con base en las fortalezas que tiene la organización.

Para el presente desarrollo se plantean cuatro zonas de aceptabilidad del riesgo:

1. **Zona aceptable:** por su frecuencia e impacto, los riesgos no requieren ser intervenidos ni tratados.

2. **Zona tolerable:** los riesgos requieren intervención y tratamiento, pero en una escala secundaria, adoptando medidas que se pueden proyectar a mediano plazo.

3. **Zona inaceptable:** en este nivel, la intervención y el tratamiento demandan una escala primaria con medidas para su manejo a corto plazo.

4. **Zona inadmisible:** el riesgo reviste una alta importancia y por ello debe ser intervenido y tratado de manera urgente y prioritaria, dado que representa un peligro inminente.

En la siguiente tabla se representan los conceptos frente a la aceptabilidad del riesgo y los rangos y porcentajes en términos de vulnerabilidad, sugeridos por Duque.

Criterios o niveles de aceptabilidad del riesgo	
Criterio o nivel	Rango
Aceptable	Vulnerabilidad hasta el 3%
Tolerable	Vulnerabilidad del 3,1% al 5%
Inaceptable	Vulnerabilidad del 5,1% al 30%
Inadmisible	Vulnerabilidad mayor al 30%

Tabla 12. Rangos porcentajes de vulnerabilidad
Fuente: Duque (1999)

Posterior a esto, se trabaja la matriz de aceptabilidad para representar de manera total el escenario de aceptación con base en los porcentajes establecidos.

Frecuencia	Constante	2,0%	4,0%	10,0%	20,0%	40,0%	100,0%
	Frecuente	1,7%	3,3%	8,3%	16,7%	33,3%	83,3%
	Moderado	1,3%	2,7%	6,7%	13,3%	26,7%	66,7%
	Ocasional	1,0%	2,0%	5,0%	10,0%	20,0%	50,0%
	Remoto	0,7%	1,3%	3,3%	6,7%	13,3%	33,3%
	Improbable	0,3%	0,7%	1,7%	3,3%	6,7%	16,7%
Matriz de vulnerabilidad		Insignificante	Marginal	Grave	Crítico	Desastroso	Catastrófico
		Impacto					

Tabla 13. Matriz de vulnerabilidad graficada por colores en rangos de vulnerabilidad
Fuente: Castañeda (2016)

Con esta matriz se grafican los alcances de aceptación del riesgo, ocupando las casillas con su descripción cualitativa.

Frecuencia	Constante	Aceptable	Tolerable	Inaceptable	Inaceptable	Inadmisible	Inadmisible
	Frecuente	Aceptable	Tolerable	Inaceptable	Inaceptable	Inadmisible	Inadmisible
	Moderado	Aceptable	Aceptable	Inaceptable	Inaceptable	Inaceptable	Inadmisible
	Ocasional	Aceptable	Aceptable	Tolerable	Inaceptable	Inaceptable	Inadmisible
	Remoto	Aceptable	Aceptable	Tolerable	Inaceptable	Inaceptable	Inadmisible
	Improbable	Aceptable	Aceptable	Aceptable	Tolerable	Inaceptable	Inaceptable
Matriz de vulnerabilidad		Insignificante	Marginal	Grave	Crítico	Desastroso	Catastrófico
		Impacto					

Tabla 14. Matriz de aceptabilidad
Fuente: Castañeda (2016)

Por su disposición y estructura, la matriz de aceptabilidad permite visualizar los riesgos calificados, partiendo de allí para realizar su tratamiento, estableciendo un perfil de riesgos.

Posteriormente y definido el nivel de aceptabilidad, se procede a graficar los escenarios de riesgo con base en la frecuencia y el impacto estimado. A continuación, se proponen tres escenarios de riesgo A1, B1 y C1, los cuales salen de la codificación entre el recurso y la amenaza. Para graficarlos se propone la siguiente definición: A1: escenario de riesgo frecuente con impacto insignificante. B1: su frecuencia es moderada y su impacto es crítico. C1: su frecuencia es constante y su impacto es desastroso.

Frecuencia	Constante					C1	
	Frecuente	A1					
	Moderado				B1		
	Ocasional						
	Remoto						
	Improbable						
		Insignificante	Marginal	Grave	Crítico	Desastroso	Catastrófico
		Consecuencia					

Aceptable
Tolerable
Inaceptable
Inadmisible

Tabla 15. Gráfica de escenarios de riesgo
Fuente: Castañeda (2016)

Ubicar los escenarios de riesgo en la matriz permite visualizar el estado del recurso, su afectación y las prioridades de atención de riesgos en su tratamiento.

Tratamiento del riesgo

Cuando se identifican los escenarios de riesgos y se establece el nivel de aceptabilidad, se debe trabajar en el tratamiento de los mismos. La ISO 31000 considera todas las medidas de tratamiento del riesgo. Estas medidas se pueden clasificar como un control o como una actividad de financiamiento del impacto en la materialización del riesgo.

Una condición de las medidas de tratamiento del riesgo es que pueden ser complementarias y no necesariamente excluyentes. Su implementación se ajusta de manera particular a cada situación, existiendo la posibilidad de que no se ajuste a todo caso.

Las medidas son:

- Evitar (EV): que desde la frecuencia no ocurra.
- Aceptar (AC): cuando en la frecuencia o impacto su consideración es que no afectará la organización y no se tienen recursos para afrontarlo.
- Anticipar (AN): adelantar las acciones necesarias para limitar la ocurrencia o minimizar su impacto.
- Proteger (PR): son las acciones para enfrentar el riesgo.
- Transferir (TR): tercerizar la responsabilidad frente al riesgo. Se cuenta con recursos financieros para tal erogación.
- Retener (RE): se diferencia de "Aceptar" porque en este se tienen recursos para afrontar el daño o pérdida.

Una vez se han definido los tipos de tratamiento se puede diseñar una matriz de actividades de respuesta ante un riesgo. A continuación, se sugiere una, la cual puede ser modificada y ajustada según las particularidades de la organización y los rangos de aceptabilidad del riesgo.

Figura 4. Medidas de tratamiento del riesgo
Fuente: Norma ISO 31000 (Icontec, 2011)

Frecuencia o probabilidad	Constante	Aceptable (2,0%) (AC)	Tolerable (4,0%) (AN, RE)	Inaceptable (10,0%) (AN, PR, TR)	Inaceptable (20,0%) (AN, PR, TR)	Inadmisible (40%) (AN, PR, TR)	Inadmisible (100,0%) (EV, AN, PR)
	Frecuente	Aceptable (1,7%) (AC)	Tolerable (3,3%) (AN, RE)	Inaceptable (8,3%) (AN, PR, TR)	Inaceptable (16,7%) (AN, PR, TR)	Inadmisible (33,3%) (AN, PR, TR)	Inadmisible (83,3%) (EV, AN, PR)
	Moderado	Aceptable (1,3%) (AC)	Aceptable (2,7%) (AC)	Inaceptable (6,7%) (AN, PR, TR)	Inaceptable (13,3%) (AN, PR, TR)	Inaceptable (26,7%) (AN, PR, TR)	Inadmisible (66,7%) (EV, AN, PR)
	Ocasional	Aceptable (1,0%) (AC)	Aceptable (2,0%) (AC)	Tolerable (5,0%) (AN, PR, RE)	Inaceptable (10,0%) (AN, PR, TR)	Inaceptable (20,0%) (PR, TR)	Inadmisible (50,0%) (AN, PR, TR)
	Remoto	Aceptable (0,7%) (AC)	Aceptable (1,3%) (AC)	Tolerable (3,3%) (AN, PR, RE)	Inaceptable (6,7%) (AN, PR, TR)	Inaceptable (13,3%) (PR, TR)	Inadmisible (33,3%) (AN, PR, TR)
	Improbable	Aceptable (0,3%) (AC)	Aceptable 0,7%) (AC)	Aceptable (1,7%) (AC)	Tolerable (3,3%) (PR, TR)	Inaceptable (6,7%) (PR, TR)	Inaceptable (16,7%) (PR, TR)
Matriz de aceptabilidad		Insignificante	Marginal	Grave	Crítico	Desastroso	Catastrófico
		Consecuancia o impacto					

Tabla 16. Actividades de respuesta ante un riesgo
Fuente: Castañeda (2016)

Cuando se trata el riesgo, nuevamente se debe someter a una calificación con el fin de determinar en qué nivel de aceptabilidad quedó y si es aceptable o tolerable. Si no, se debe revisar el tratamiento para aumentar su cobertura y permitir que el riesgo baje.

Toda medida de tratamiento para riesgo debe tener un límite tiempo, el cual podrá ser prolongado de acuerdo a la necesidad. Un ejemplo es la compra de una póliza para cubrimiento de riesgos de un vehículo, la cual se compra anualmente. Al final del lapso, el dueño del vehículo determina si la renueva o no.

Lectura recomendada

En el artículo ¿Por qué es importante la gestión de riesgos para tu empresa? se evidencian razones para adelantar la gestión del riesgo en su empresa, como empleado o propietario.

Comunicación y consulta

En desarrollo del proceso de gestión del riesgo se deben cumplir actividades de retroalimentación e intercambio de información, con el fin de complementar los procesos, ajustar y mejorar la información, y aplicar medidas preventivas o correctivas a tiempo. No se debe esperar que se entregue un informe u ocurra un daño a la organización.

Monitoreo y seguimiento

Es una de las tareas más importantes, puesto que indica si lo que se previó se cumplió o se está cumpliendo. Si no, expresa cómo mejorar el proceso, dejando claro que la inversión de trabajo y recursos fue efectiva. Esta etapa de la gestión del riesgo debe responder a lo que se está haciendo para minimizar los escenarios de riesgo.

El monitoreo se define como: "El seguimiento rutinario de la información prioritaria de un programa, su progreso, sus actividades y sus resultados" (Unicef, 2007, p. 11). Llevada esta acepción a la gestión del riesgo significa el rastreo de las acciones proyectadas para gestionar el riesgo y revisar si se está cumpliendo con la misión de reducir las posibilidades de su materialización o impacto. Se puede adelantar a través de revisión de informes y reportes, observación y aplicación de instrumentos de medición. Normalmente, se emplean indicadores de riesgo, lo cuales se estructuran con base en la experiencia y las necesidades de la organización.

Fuente: goo.gl/Hr5Mct

Mapa de riesgos

Como insumo de todo el proceso de gestión del riesgo está el mapa de riesgo: gráfica que integra toda la información del proceso y permite hacer seguimiento. Su estructura lleva la misma línea de las etapas de la gestión del riesgo y se trabaja a partir de términos cuantitativos y cualitativos.

ESTABLECIMIENTO DEL CONTEXTO			
Aspectos empresariales objeto de la gestión del riesgo			
Sistema de referencia	Ámbito de aplicación (recurso, proceso, instalación, etc.)	Código actividad	Actividad amenazada

IDENTIFICACIÓN DEL RIESGO					
Amenaza o peligro		Escenario de riesgo (descripción)		Características del riesgo	
Código amenaza	Amenaza	Código	Escenario de riesgo	Tipo de riesgo (factor de vulnerabilidad)	Consecuencias

ANÁLISIS DEL RIESGO		EVALUACIÓN DE ESCENARIOS DE RIESGO		
Riesgo inherente				
Calificación antes del tratamiento				
Matriz de riesgos			Matriz de aceptabilidad	
Frecuencia o probabilidad	Impacto o consecuencias	Calificación del riesgo	Criterio de aceptabilidad o nivel de riesgo	Zona de aceptabilidad (matriz de vulnerabilidad)

TRATAMIENTO DEL RIESGO						
Tratamiento del riesgo						
Medida						Control
Anticipar (AN)	Proteger (PR)	Evitar (EV)	Aceptar (AC)	Transferir (TR)	Retener (RE)	Tipo de control

TRATAMIENTO DEL RIESGO												
Riesgo residual						Desarrollo del tratamiento						
Calificación después del tratamiento						Fecha						
Matriz de riesgos			Matriz de aceptabilidad		Control	Inicio			Término			
Frecuencia o probabilidad	Impacto o consecuencias	Calificación del riesgo	Criterio de aceptabilidad o nivel de riesgo	Zona de aceptabilidad (matriz de vulnerabilidad)	Efectividad del control	D	M	A	D	M	A

MONITOREO DEL RIESGO				
Monitoreo, revisión y evaluación de riesgos				
Fecha de monitoreo	Indicador	Los controles son efectivos (si o no)	% de avance de las acciones	Obs.

Tabla 17. Formato mapa de riesgos
Fuente: Castañeda (2016)

BIBLIOGRAFÍA

Asociación Española de Gerencia de Riesgos y Seguros. (2011). *Herramientas y técnicas para la valoración del riesgo: aplicación de la Norma ISO 31010*. Madrid, España: Asociación Española de Gerencia de Riesgos y Seguros.

Business Alliance for Secure Commerce. (s. f.). *Lista de chequeo de pólizas de seguros*. Recuperado de http://www.bascbogota.com/es/material_curso/CHEQUEO%20POLIZA%20DE%20SEGUROS.xls

Castañeda. J. (2016). *Módulo: Prevención y gestión del riesgo*. Bogotá, Colombia: Fundación Universitaria del Área Andina.

Departamento Administrativo de la Función Pública (DAFP). (2015). *Guía para la gestión del riesgo de corrupción 2015*. Recuperado de http://www.funcionpublica.gov.co/eva/admon/files/empresas/ZW1wcmVzYV83Ng==/archivos/1461159134_5808c334fdf5c054b27c28ada33880f8.pdf

Duque, C. & Asociados. (1999). *Seminario taller gestión integral de riesgos organizacionales*. Bogotá, Colombia: Duque, C. & Asociados.

Instituto Colombiano de Normas Técnicas y Certificación. (2002). *NTC-ISO **19011***. Recuperado de http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO19011.pdf

Instituto Colombiano de Normas Técnicas y Certificación. (2011). *NTC-ISO 19011*. Recuperado de http://www.umc.edu.ve/pdf/calidad/normasISO/Norma_ISO_19011-2011_Espanol.pdf

Instituto Colombiano de Normas Técnicas y Certificación. (2011). ***NTC-ISO 31000***. Recuperado de https://sitios.ces.edu.co/Documentos/NTC-ISO31000_Gestion_del_riesgo.pdf

Mejía, R. (2006). Administración de riesgos. *Un enfoque empresarial*. Medellín, Colombia: Fondo Editorial Universidad Eafit.

Unicef. (2007). *IMAS de educación en el riesgo de las minas. Guía de mejores prácticas 7*. Bogotá, Colombia: Editorial Gente Nueva.

Esta obra se terminó de editar en el mes de Septiembre 2018
Tipografá BrownStd Light, 12 puntos
Bogotá D.C,-Colombia.

AREANDINA

Fundación Universitaria del Área Andina

MIEMBRO DE LA RED

ILUMNO