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

ÍNDICE

Introducción 3

Análisis integral: gestión del riesgo y control interno 4

- Diagnóstico y establecimiento del contexto 8
- Valoración del riesgo 10
  - Identificación y análisis del riesgo 10
- Método para adelantar la gestión del riesgo 15
- Calificación del riesgo 18
- Evaluación del riesgo 20
- Tratamiento del riesgo 24
  - Comunicación y consulta 26
  - Monitoreo y seguimiento 26
- Mapa de riesgos 26
- Bibliografía 28

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.