

# GESTIÓN, ADMINISTRACIÓN DE RIESGOS Y MODELOS DE CONTROL INTERNO

Javier Castañeda

**EJE 1**

Conceptualicemos

A 3D graphic of interlocking puzzle pieces. The word 'risk' is printed in black on a yellow piece, and 'management' is printed in black on a grey piece. The background features a geometric pattern of overlapping triangles in shades of green, yellow, and grey.

**risk**  
**management**

Introducción . . . . .	3
Orígenes del riesgo y su universalidad . . . . .	5
¿Qué es el riesgo? . . . . .	8
¿Qué es la gestión del riesgo? . . . . .	9
Clasificación y caracterización de los riesgos . . . . .	10
Normatividad vigente de la gestión y administración de riesgos . . . . .	12
Proceso metodológico de gestión y administración de riesgos . . . . .	13
Etapas de la gestión del riesgo . . . . .	13
Sistema de administración de riesgo . . . . .	17
Bibliografía . . . . .	18





# 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.

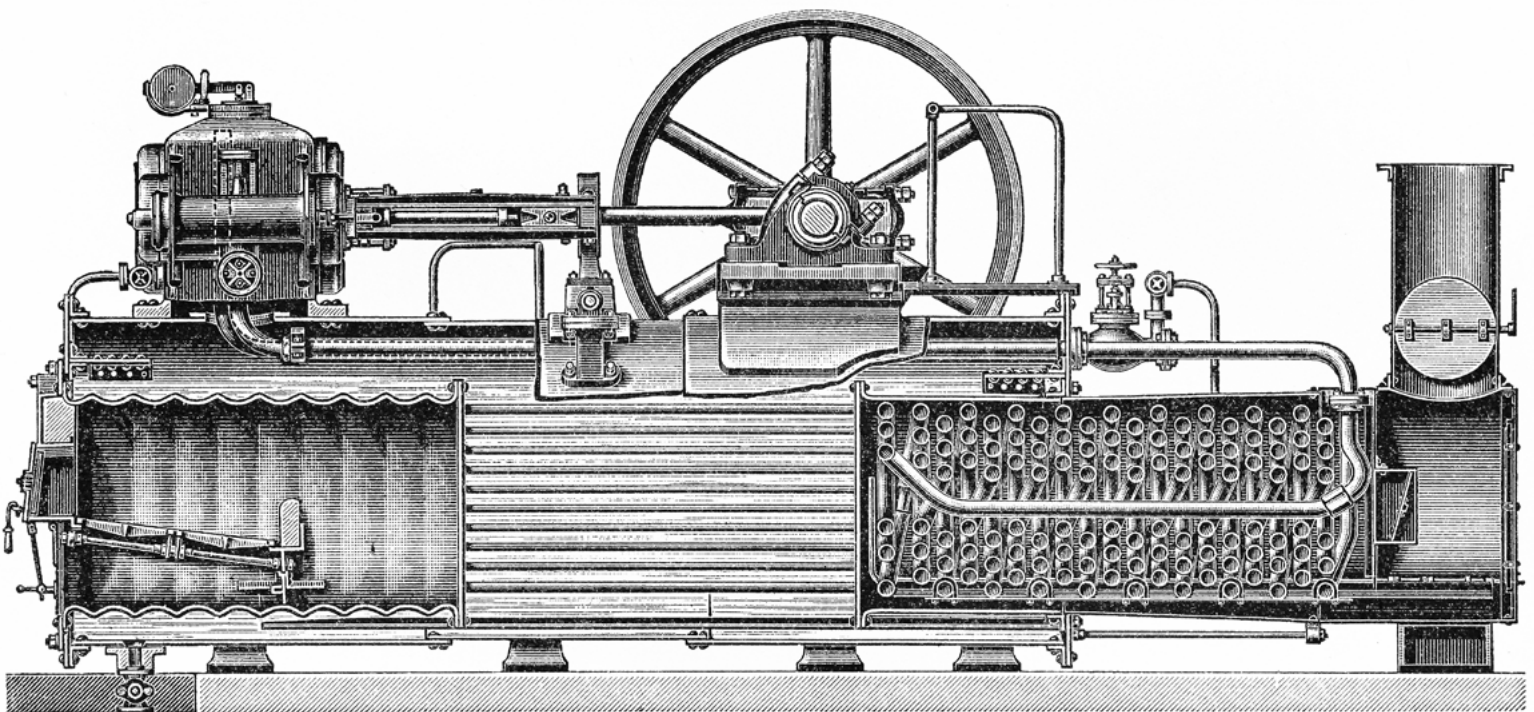


Figura 1. Máquina de vapor  
Fuente:shutterstock/93873745

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.

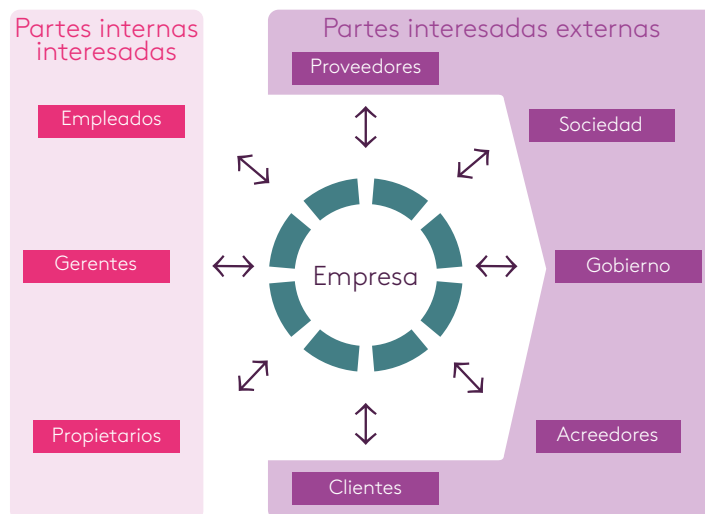


Figura 3. Mapa de *stakeholders*  
Fuente: Gallego (2012)



## 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.

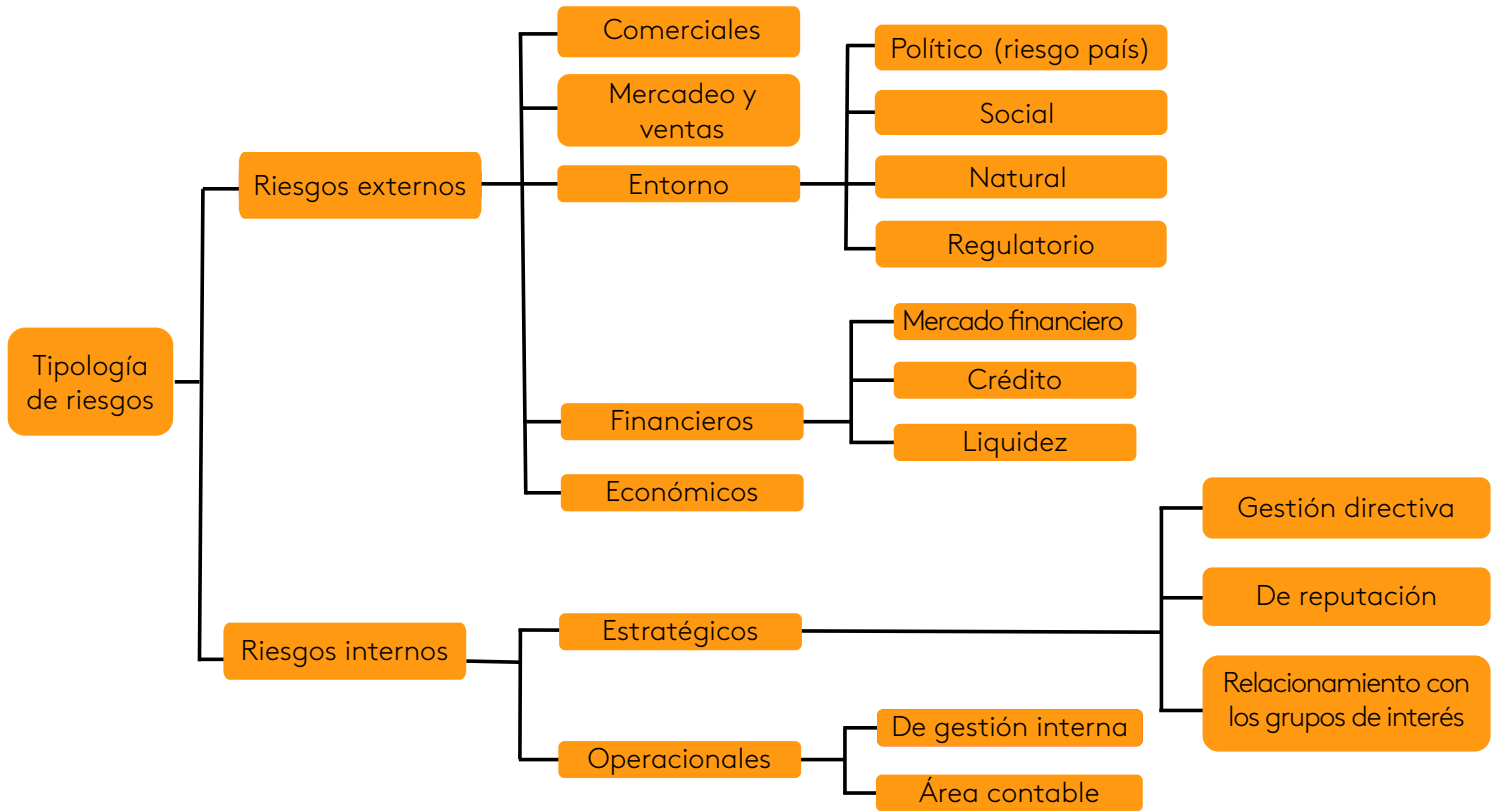


Figura 4. Clasificación de los tipos de riesgo  
Fuente: Castañeda (2016)

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.

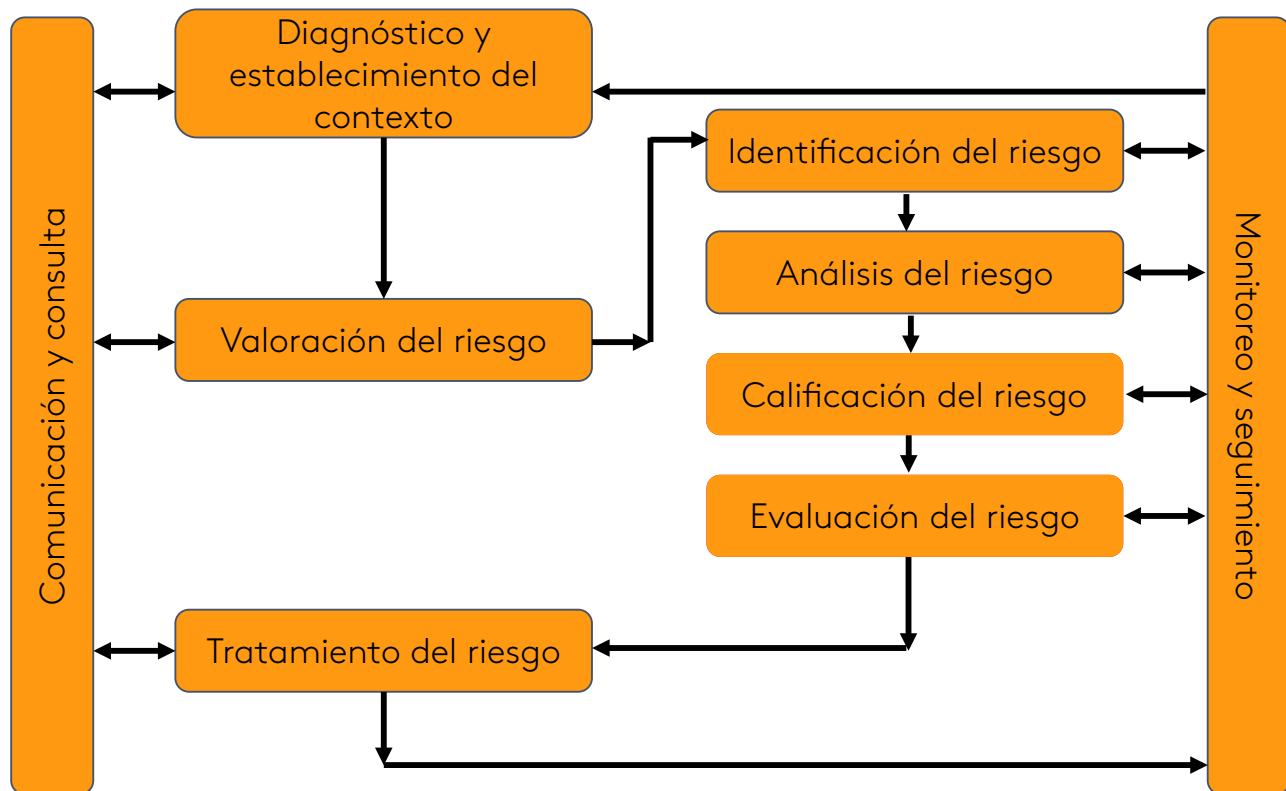


Figura 6. Etapas de la gestión del riesgo  
Fuente: Castañeda (2016)

### 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.

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. *Teoría 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>