

# GESTIÓN DE RIESGOS EN ENTORNOS EMPRESARIALES ALINEADOS A LA NORMA ISO 31000

Díaz Gómez Diego Andrés  
Universidad Piloto de Colombia  
Bogotá D.C., Colombia

**Resumen**— El presente trabajo describe los principales aspectos que se deben contemplar para llevar a cabo la gestión y análisis de riesgos en entornos organizacionales teniendo en cuenta los principios establecidos por la Norma ISO 31000.

El análisis de riesgos es básicamente un proceso estructurado para estimar la magnitud de los riesgos a los que se encuentra expuesta una organización. Este proceso está compuesto por diferentes tareas de monitoreo y vigilancia que se deben realizar internamente en las organizaciones, con el fin de prevenir la materialización de algún evento inesperado que afecte el cumplimiento de los objetivos de la entidad o la satisfacción de sus clientes. Es precisamente en este momento del proceso donde se recomienda el uso de diferentes tipos de herramientas que facilitan la identificación. La gestión de riesgos, en este caso la norma de referencia ISO 31000, creada para que las organizaciones apoyen las tareas de análisis y gestión de riesgos.

El gestionar dichos riesgos es un tema de mucho interés para las organizaciones, pues al contemplar aspectos que involucran la ejecución y cumplimiento de los objetivos estratégicos del negocio, se requiere de un alto grado de análisis. Para llevar a cabo este meticuloso análisis, el proceso planteado en la norma ISO 31000, está estructurado por etapas. En una de ellas, la de evaluación del riesgo, se establece el impacto que los mencionados riesgos pueden causar sobre los objetivos del negocio en caso de su materialización; para posteriormente continuar con la fase de análisis, momento en el cual se plantean las consecuencias resultantes y las probabilidades de ocurrencia.

En esta norma igualmente se instauran los principios, directrices y marco de trabajo, en los cuales las organizaciones se deben apoyar para poder identificar, tratar y dar seguimiento a los riesgos, con el objetivo de tener un control sobre los mismos, asegurando así el cumplimiento de sus objetivos estratégicos.

Las organizaciones de todo tipo y tamaño, siempre estarán enfrentadas a factores internos y externos que le restan certeza a la posibilidad de alcanzar sus objetivos. Este comportamiento es definido como riesgo y será una constante en el desarrollo de los diferentes procesos de la organización.

Es por lo anteriormente expuesto que las organizaciones modernas han optado por implementar estrategias para mitigar o disminuir los riesgos; estrategias que son esenciales, ya que su función es garantizar y respaldar la operación, dar continuidad a los negocios, identificar continuamente los riesgos y poder gestionarlos de manera eficaz.

**Índice de Términos**— Riesgo, ISO 31000, gestión de riesgos, análisis de riesgo, monitoreo.

**Abstract**— The present work describes the main aspects that must be contemplated to carry out the management and analysis of risks in organizational environments taking into account the principles established by ISO 31000.

Risk analysis is basically a structured process for estimating the magnitude of the risks to which an organization is exposed. This process is composed of different monitoring and surveillance tasks that must be carried out internally in the organizations, in order to prevent the materialization of some unexpected event that affects the fulfillment of the objectives of the entity or the satisfaction of its clients. It is precisely at this point in the process that the use of different types of tools that facilitate identification is recommended. Risk management, in this case the ISO 31000 reference standard, created for organizations to support the analysis and risk management tasks.

Managing these risks is an issue of great interest to organizations, because when contemplating aspects that involve the execution and fulfillment of the strategic objectives of the business, a high degree of analysis is required. In order to carry out this meticulous analysis, the process proposed in ISO 31000 is structured in stages. In one of them, the risk assessment, establishes the impact that the aforementioned risks can cause on the business objectives in case of materialization; and then continue with the analysis phase, at which point the resulting consequences and the probabilities of occurrence are raised.

This standard also establishes the principles, guidelines and framework, in which organizations must be supported in order to be able to identify, treat and monitor the risks, with the aim of having control over them, thus ensuring compliance of its strategic objectives.

Organizations of all types and sizes will always be confronted with internal and external factors that detract from the possibility of reaching their objectives. This behavior is defined as risk and will be a constant in the development of the different processes of the organization.

It is for the foregoing that modern organizations have opted to implement strategies to mitigate or reduce risks; strategies that are essential, since their function is to guarantee and to support the operation, to give continuity to the businesses, to continuously identify the risks and to be able to manage them effectively.

**Index of Terms** — Risk, ISO 31000, risk management, risk analysis, monitoring.

## I. INTRODUCCIÓN

Las organizaciones actualmente se encuentran en constante evolución, adaptándose a nuevas necesidades y formas de operación de sus procesos. Es por este motivo que se requiere la creación y adaptación de estándares y buenas prácticas respaldadas por normativas, en este caso la norma de referencia, la ISO 31000. Esta norma es integral y puede ser aplicada a las industrias en general y a todos los tipos de riesgo; brindando apoyo de una manera más eficiente a las organizaciones en la gestión de los riesgos a los cuales están permanentemente expuestas.

Al adoptar los lineamientos y principios que la norma establece, se tiene claridad en la ruta para alcanzar un objetivo. Durante la operación normal de cualquier proceso, es conocido que los imprevistos que desvían el plan inicial son una constante. Debido a esto, se dispone de una herramienta de gestión que posibilita la medición y la frecuencia del riesgo, al igual que la probabilidad de ocurrencia y sus niveles de impacto. Una vez implementada y aplicada correctamente, dicha herramienta brinda la posibilidad de reducir la incertidumbre y gestionar los riesgos efectivamente.

Al estar expuestas a todo tipo de riesgos e incertidumbre, las organizaciones cada vez le otorgan una mayor importancia a gestionarlos de una manera estructurada. Si no lo hacen, estos riesgos pueden impactar de manera significativa las metas y objetivos de la organización, al punto de interrumpir su operación habitual. Este impacto puede generar pérdidas económicas, penalizaciones y afectación de la imagen, causando inconvenientes en los niveles estratégicos y operativos de la organización.

La norma ISO 31000 plantea que las organizaciones actuales llevan a cabo sus procesos en una situación de incertidumbre, lo que en ocasiones los lleva a gestionarlos de manera preventiva. Para hacerlo, se requiere la implementación de un sistema de gestión que asegure que los riesgos sean correctamente manejados, mejorando así la capacidad de la organización en la identificación de amenazas y oportunidades. Es de esta manera como aumenta significativamente la probabilidad de que se logren los objetivos establecidos en la organización.

Aunque la práctica de la gestión del riesgo se ha desarrollado con el paso del tiempo y en muchos sectores para satisfacer diversas necesidades, la

adopción de procesos consistentes dentro de un marco de referencia exhaustivo, puede ayudar a garantizar que el riesgo se gestione de forma eficaz y eficiente en toda la organización. El enfoque genérico que se describe en la norma ISO 31000, suministra los principios y las directrices para la gestión de cualquier forma de riesgo de una manera sistemática, transparente y creíble, en cualquier alcance y contexto [1].

## II. GENERALIDADES SOBRE EL RIESGO

A continuación se especifican los términos más comunes de la gestión de riesgos, la comprensión de estos conceptos es importante para el entendimiento de la temática del presente documento:

*Riesgo:* Efecto de la incertidumbre sobre los objetivos.

Un efecto es una desviación de aquello que se espera, sea positivo, negativo o ambos.

Los objetivos pueden tener aspectos diferentes (por ejemplo: financiero, salud, seguridad, y metas ambientales) y se pueden aplicar en niveles distintos (a nivel estratégico, en la totalidad de la organización, en proyectos, productos y procesos). Definición según la norma NTC-ISO 31000 [2].

*Impacto:* consecuencias que la materialización del riesgo puede ocasionarle a la organización.

*Acciones:* aplicación concreta de las opciones de gestión del riesgo que entrarán a prevenir o a reducir el riesgo y están contempladas en el plan de manejo del riesgo.

*Responsables:* las dependencias o áreas encargadas de adelantar las acciones propuestas.

*Indicadores:* se consignan los resultados y datos diseñados para evaluar el desarrollo de las acciones implementadas.

## III. ISO 31000 EN LAS ORGANIZACIONES

La norma ISO 31000 brinda a las organizaciones elementos de apoyo para la gestión de riesgos. Esta norma expone las directrices para que el proceso de gestión pueda ser definido de acuerdo con las necesidades particulares de la organización que lo aplica. Esto se logra realizando la identificación de riesgos mediante una metodología sistemática que facilita el análisis, la evaluación y posteriormente la definición de estrategias para dar respuesta a los riesgos. De esta manera, el posible impacto puede tornarse positivo o evitar que no genere pérdidas significativas para la organización, en caso de que

estos riesgos se concreten. Identificar los riesgos en la organización es anticiparse a las consecuencias que impactarían los objetivos, estrategias y operaciones de la organización, si estos riesgos se ven materializados. Es importante que la identificación de riesgos contemple la clasificación de los eventos.

La gestión de los riesgos en las organizaciones es fundamental, ya que por medio de este proceso se establecen medidas preventivas y planes de acción para poder responder a los riesgos, sin que los impactos sean negativos. El tener un control de los riesgos en la organización, contribuye al cumplimiento de los objetivos estratégicos.

El concepto de riesgo definido en la visión integral de la norma, indica que es el efecto de la incertidumbre sobre los objetivos, toda desviación de los resultados esperados que son positivos o negativos y que tienen un impacto en el cumplimiento de los objetivos.

Las organizaciones actuales cuentan con planes estratégicos que contemplan los aspectos financieros, clientela, servicios, productos, procesos internos y actividades, en los cuales se tienen identificados los riesgos y planes de acción en caso de que los riesgos se concreten. Adicionalmente se contemplan aspectos de innovación y aprendizaje conformados por el recurso humano que gestiona los procesos donde también se presentan riesgos que deben ser identificados. Por ejemplo, cuando una persona que conoce los procesos tiene cierta experiencia y antigüedad en la organización, decide retirarse, es fundamental tener control sobre las consecuencias que genera esta situación, ya que puede impactar significativamente el servicio o producto que se distribuye.

El escenario presentado anteriormente alcanza a detallar un poco la importancia de tener controlados todos los riesgos y conocer perfectamente los procesos de la organización.

Durante la implementación de un sistema de gestión de riesgos, es recomendable la participación de la totalidad de personal que interactúa en los procesos. Este proceso no puede ser aislado, sino que tiene que integrar a todos los miembros de la organización, ya que al ser ellos los que conocen en detalle su funcionamiento, son una fuente confiable de información para tomar las decisiones adecuadas durante el proceso de la gestión de riesgos.

Las estrategias de respuesta al riesgo dependen directamente de la realidad de cada organización, sus necesidades y la capacidad de asumir, mitigar, transferir y en algunos casos aceptar el riesgo.

La visión integral del riesgo contempla la existencia de riesgos tanto negativos como positivos. Los positivos se convierten en oportunidades para que las organizaciones puedan evolucionar y crecer, mientras que los negativos tarde o temprano se constituyen como amenazas. Las buenas prácticas recomiendan tener implementado un sistema de análisis con matrices en las cuales se identifiquen con precisión los riesgos significativos y los que no lo son. Para el primer tipo de riesgos se deben definir controles operacionales, planes de acción con actividades concretas con responsables y tiempos que permitan un monitoreo detallado de las tareas.

#### IV. ESTRUCTURA DE LA NORMA ISO 31000

La norma ISO 31000 está estructurada en tres elementos claves para llevar a cabo una gestión de riesgo efectiva, transparente, sistemática y creíble, dichos elementos son:

*A. Principios de la Gestión del Riesgo*

*B. Marco de trabajo para la Gestión de Riesgos*

*C. Proceso de Gestión de Riesgos.*

Esta norma establece varios principios que se deben cumplir para hacer que la gestión sea eficaz, adicionalmente la norma recomienda que las organizaciones desarrollen, implementen y mejoren un marco de referencia o marco de trabajo, cuyo propósito sea integrar el proceso.

**A. Principios de la Gestión de Riesgos:**

- a) Crear valor**
  - b) Es parte integral de los procesos de la organización**
  - c) Es parte de la toma de decisiones**
  - d) Aborda explícitamente la incertidumbre**
  - e) Es sistemática, estructurada y oportuna**
  - f) Se basa en la mejor información disponible**
  - g) Está adaptado**
  - h) Toma en consideración a los factores humanos y culturales**
  - i) Es transparente e inclusiva**
  - j) Es dinámica, reiterativa y receptiva al cambio**
  - k) Facilita la mejora y realiza a la organización**
- Principios  
(numeral 3)**

*Es parte de la toma de decisiones:* se analiza el impacto de los riesgos, tanto positivos como negativos para la organización y de acuerdo con este análisis se toman decisiones.

*Aborda explícitamente la incertidumbre:* ayuda a las organizaciones a gestionar la incertidumbre, su naturaleza y la forma de tratarla.

*Es sistemática, estructurada y oportuna:* se debe definir un mecanismo para identificar los riesgos (evaluación, talleres, entrevistas, dinámicas grupales, etc.). Es importante contar con información confiable para el beneficio de las organizaciones.

*Se basa en la mejor información disponible:* la información debe ser facilitada por los gestores de riesgo en tiempo real, siendo un insumo confiable para el proceso que apoye la toma de decisiones.

*Está adaptado:* no impone una estructura o no está establecido un formato para su aplicación. Cada organización puede implementar los riesgos de acuerdo a sus necesidades o cultura organizacional.

*Toma en consideración a los factores humanos y culturales:* es lo más importante ya que es el recurso que mueve todo el proceso y la gestión de riesgos, teniendo en cuenta los factores culturales que afectan a la organización.

*Es transparente e inclusiva:* dentro del alcance de la gestión de riesgos debería participar toda la organización o la totalidad de los procesos.

*Es dinámica, reiterativa y receptiva al cambio:* la gestión del riesgo reacciona a los cambios en la medida en que los acontecimientos externos e internos se producen, teniendo en cuenta el contexto y el conocimiento, el análisis crítico de los riesgos, el surgimiento de nuevos riesgos o su desaparición.

*Facilita la mejora y realiza a la organización:* aumenta la probabilidad de alcanzar los objetivos, fomenta la gestión proactiva, cumple con las exigencias legales. Si la organización es previsible, controla e identifica los riesgos, va a cumplir con la normatividad internacional.

**B. Marco de trabajo para la Gestión de Riesgos:** es uno de los elementos fundamentales en la gestión, ya que integra el proceso de gestión de riesgos al gobierno corporativo de la organización. El marco de trabajo debe ser sencillo y flexible, pues debe permitir ajustes y adaptaciones durante el proceso, en continua búsqueda de una mejora, los componentes que lo conforman son los siguientes:

Fig. 1. Estructura de la Norma ISO 31000: Principios de la Gestión del Riesgo

Fuente: Icontec, I. (2011) Principios de la Gestión de Riesgos de la NTC-ISO 31000, Gestión del riesgo. Principios y directrices (p. 3). Bogotá: Instituto Colombiano de Normas Técnicas y Certificación.

*Crea Valor:* al manejar óptimamente los riesgos, la organización está preparada y es capaz de cumplir con la legislación y normativas y de tener controlado el cumplimiento de los objetivos estratégicos.

*Es parte integral de los procesos de la organización:* el proceso de gestión del riesgo debe ser integrador de todos los procesos. Por cada actividad crítica se deben identificar los riesgos, estableciendo mecanismos de evaluación y de análisis con planes de acción para su tratamiento.

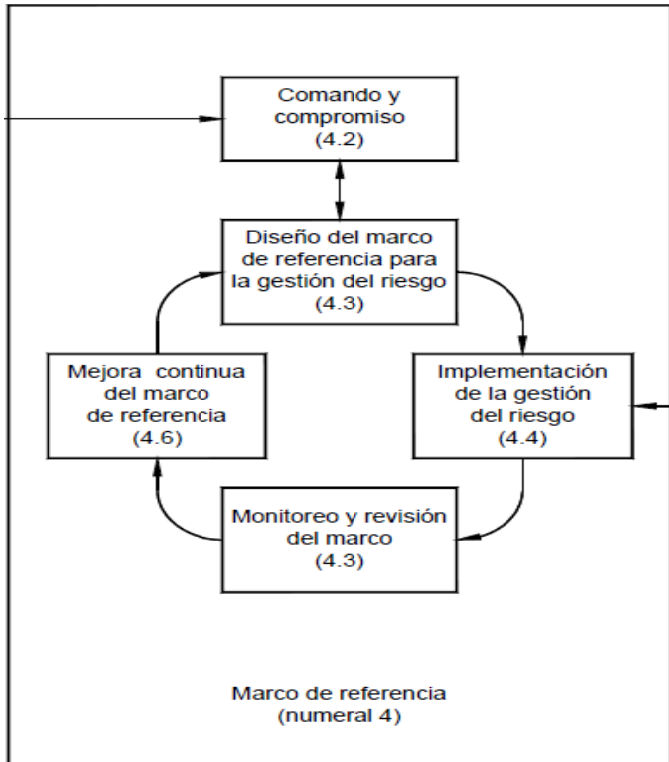


Fig. 2. Estructura de la Norma ISO 31000: Marco de Referencia

Fuente: Icontec, I. (2011) Marco de Referencia de la NTC-ISO 31000, Gestión del riesgo. Principios y directrices (p. 3). Bogotá: Instituto Colombiano de Normas Técnicas y Certificación.

*Compromiso de la Dirección:* cuando se implementa un sistema de gestión de riesgos es de vital importancia contar con el compromiso y el apoyo de la alta dirección. Si durante la implementación del sistema de gestión de riesgos no se cuenta con esta aprobación, se van a presentar muchos inconvenientes porque probablemente el personal que gestiona los procesos no va a tener compromiso con la metodología del sistema, para lo cual el compromiso de la alta dirección es de vital importancia.

*Diseño del marco de Referencia para la gestión del riesgo:* brinda las bases y disposiciones necesarias para ayudar a la gestión del riesgo de manera eficaz. Establecer un marco de referencia adecuado permite extraer la información necesaria del proceso de gestión para la toma de decisiones.

*Implementación de la Gestión del Riesgo:* la gestión del riesgo se debería aplicar garantizando que el proceso descrito en la Fig. 3, se lleve a cabo, contemplando todos los niveles y las funciones pertinentes de la organización como parte de sus prácticas y procesos [5].

*Monitoreo y Revisión del Marco:* con el fin de garantizar que la gestión del riesgo sea eficaz y continua, sustentando el desarrollo de la organización, esta etapa debe medir el desempeño de la gestión frente a los indicadores, estas métricas deben ser revisadas periódicamente para determinar su idoneidad. Adicionalmente se requiere la medición periódica del progreso que se ha tenido frente al plan para la gestión del riesgo y las desviaciones con respecto a éste. De la misma manera, se deben realizar revisiones de adaptación al marco de referencia, la política y el plan para la gestión del riesgo, ya que con el paso del tiempo estos aspectos tienden a cambiar teniendo en cuenta el contexto interno y externo de la organización.

Es importante la presentación de informes sobre el riesgo y el progreso que ha tenido frente al plan definido, exponiendo el nivel o porcentaje de cumplimiento de la política que permita validar la eficacia del marco de referencia para la gestión del riesgo en la organización.

*Mejora continua del Marco de Referencia:* esta gestión es dinámica y está en continuo cambio, cada vez se debe ir mejorando a medida que se va adquiriendo experiencia en la gestión. Pueden presentarse cambios en las políticas, formatos, métodos de evaluación, con el fin de establecer una metodología más ágil y práctica que sea de total comprensión para todos los colaboradores de la organización, permitiendo una adecuada toma de decisiones.

c. *Proceso de Gestión de Riesgos:*

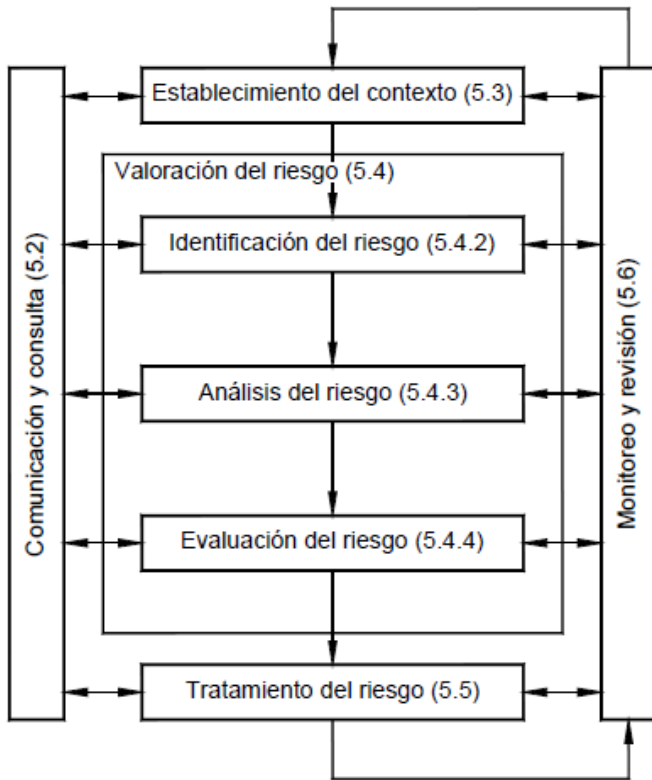


Fig. 3. Estructura de la Norma ISO 31000: Proceso de Gestión de Riesgos

Fuente: Icontec, I. (2011) Marco de Referencia de la NTC-ISO 31000, Gestión del riesgo. Principios y directrices (p. 3). Bogotá: Instituto Colombiano de Normas Técnicas y Certificación.

*Establecimiento del contexto:* son los parámetros internos y externos que deben tenerse en cuenta. Cuando se habla del contexto externo se hace referencia a temas culturales, sociales y políticos, pues los cambios en los modelos económicos afectan directamente a las organizaciones. Por otra parte, el contexto interno se refiere a temas estructurales de las organizaciones como lo son las funciones, responsabilidades, políticas, objetivos, estrategias y demás recursos que se tienen en cuenta para alcanzar los objetivos.

*Valoración del riesgo:* se deben desarrollar mecanismos para lograr identificar los riesgos de la organización. Para hacerlo deben tenerse en cuenta los eventos pasados y las lecciones aprendidas, llevar a cabo entrevistas o reuniones con los dueños de los procesos, ya que son ellos los que conocen en detalle las actividades e identifican los riesgos inherentes en cada una de ellas. Igualmente conocen cuál es su impacto en el proceso y la organización.

*Tratamiento del Riesgo:* el tratamiento del riesgo involucra la selección e implementación de una o más opciones para modificar estos riesgos. Una vez implementado, el tratamiento suministra controles o los modifica. Dicho tratamiento del riesgo implica un proceso cíclico de su valoración, se decide sobre si los niveles de riesgo residual son tolerables o no, se genera un nuevo tratamiento para el riesgo y se ajusta la valoración de su eficacia.

*Monitoreo y Revisión:* se lleva a cabo un monitoreo constante de los riesgos identificados, en conjunto con la revisión de la metodología. Este es un ciclo continuo, por tal razón el proceso vuelve a iniciar al regresar a la etapa de establecimiento del contexto, evaluación del riesgo y análisis.

*Comunicación y Consulta:* esta etapa del proceso interactúa y está presente en todos los ciclos. Este es el momento donde se establece el contexto adecuado, todas las partes interesadas son entendidas y se tienen en cuenta, ayudan a asegurar que todos los riesgos estén identificados, brindando respaldo y apoyo para el plan de tratamiento de riesgos. Igualmente soporta la gestión del cambio durante el proceso de gestión de riesgos.

**V. BENEFICIOS DE IMPLEMENTAR LA NORMA ISO 31000 EN LAS ORGANIZACIONES**

Con la implementación de la norma ISO 31000 para la gestión de los riesgos en las organizaciones, se busca *fomentar una gestión proactiva libre de riesgos*, aumentando en la organización la probabilidad de lograr los objetivos identificando previamente lo que puede suceder y de esta forma tener la posibilidad de definir un plan de acción en el caso que se materialice el riesgo. Se obtiene una *alta probabilidad de poder cumplir con los objetivos estratégicos*, si se cumplen con los objetivos estratégicos de la organización se obtienen beneficios como mayor rentabilidad, crecimiento y sostenibilidad. Se facilita la *identificación de las oportunidades y amenazas*, aspecto conformado por los riesgos positivos y riesgos negativos, los negativos se convierten en amenazas para la organización y los riesgos positivos se convierten en oportunidades para la organización previniendo eventos y sorpresas desagradables que la puedan afectar negativamente evitándole sanciones por el incumplimiento de normas.

## VI. IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE RIESGOS BASADO EN LA NORMA ISO 31000

En la implementación de un sistema de gestión de riesgos basado en la norma ISO 31000, se deben tener en cuenta los recursos humanos, los procesos que van a intervenir y la tecnología a utilizar. Lo anterior teniendo en cuenta que los niveles de información que se manejan deben ser de conocimiento público en todos los niveles de la organización. En la implementación del sistema de gestión de riesgos, todos los principios de la norma ISO 31000 deben estar direccionados hacia la cúspide de la jerarquía de la organización.

## VII. EVALUACIÓN DE RIESGOS Y TRATAMIENTO BASADO EN LA NORMA ISO 31000

En el proceso de medición del riesgo se deben contemplar cuatro aspectos principales detallados a continuación:

*Identificar el Riesgo:* es en este punto donde se determina el origen del riesgo y sus posibles consecuencias.

La norma ISO 31000 define la identificación de riesgos como el “proceso para encontrar, reconocer y describir los riesgos” [8].

*Analizar el Riesgo:* se determina el nivel de probabilidad y consecuencia del riesgo identificado.

*Evaluar el Riesgo:* implica determinar a nivel de probabilidad y consecuencia cual es el nivel de riesgo asociado al evento identificado. Por ejemplo, si se define una probabilidad baja y una severidad alta, el nivel de riesgo es medio, sin embargo, si se define una probabilidad baja y severidad baja el nivel de riesgo es riesgo medio. Dependiendo del nivel de riesgo la necesidad de su tratamiento es distinta, para un riesgo alto o no aceptable se debe definir un tratamiento que permita controlar el evento. El proceso de evaluación de riesgos establece controles y acciones que disminuyen su nivel, de tal forma que este riesgo sea controlado y aceptado por la organización.

La evaluación del riesgo consiste en realizar un análisis de la probabilidad de ocurrencia de un incidente y su impacto en los resultados. Este análisis puede efectuarse en términos cualitativos o cuantitativos, dependiendo de la importancia o disponibilidad de información. Teniendo en cuenta

los factores de costos y complejidad, realizar una evaluación cualitativa es más sencillo y económico.

Para realizar el proceso de evaluación de riesgos, las entidades se pueden apoyar en la norma ISO 31010, la cual brinda soporte a la norma ISO 31000. Esta norma establece directrices para la selección y aplicación de herramientas y técnicas sistemáticas para la evaluación del riesgo. Además, la mencionada norma presenta una serie de técnicas, y hace referencia a otras normas donde se describe con mayor detalle el concepto y la aplicación de algunas de ellas.

*Tratamiento del Riesgo:* en esta parte se aplican los controles para mitigar o modificar el riesgo, tomando controles que reduzcan el nivel de riesgo.

*Eliminar el riesgo:* se consigue eliminando los diferentes activos a los cuales pueda estar asociado el riesgo, normalmente es una elección bastante costosa y drástica por lo que normalmente se buscan otras medidas de control. *Transferir el riesgo* en el cual normalmente se considera la contratación de servicios externos o la contratación de pólizas que cubran los gastos en caso de que se presente un incidente. En muchos casos los valores de los activos y el tipo de riesgo asociado no hacen viable la subcontratación, como puede ser el caso de activos altamente confidenciales para la organización.

La tercera forma de tratamiento de los riesgos es *asumirlos*, lo cual implica que no se van a tomar medidas de protección contra ese riesgo y la decisión de manejarlo de esta forma debe ser tomada y firmada por la dirección de la organización. Ésta sólo es viable en el caso en el que la organización implemente controles para el riesgo. Este riesgo debe mantenerse en constante monitoreo para que no aumente o se propague.

La última forma de tratamiento es *mitigar el riesgo* en el cual la organización debe implementar medidas que salvaguarden los activos, todas las medidas aplicadas deben ser documentadas y gestionadas por la entidad.

Se debe tener claridad que un evento es catastrófico cuando de llegar a presentarse tiene un estado del cual la organización no puede recuperarse y no hay posibilidad de otra oportunidad. Por tal motivo es muy importante identificar los eventos importantes y someterlos a estudio, hallando su probabilidad. Posteriormente se debe calcular la consecuencia y el punto donde se crucen puede ser un riesgo alto, medio o bajo.

**VIII. TÉCNICAS DE EVALUACIÓN DE RIESGOS DE ACUERDO A LA NORMA ISO 31010**

Los tipos de técnicas de evaluación de riesgos contempladas por la Norma ISO 31010 son clasificadas de la siguiente manera:

En la Tabla 1 se presenta la primera clasificación, detallando cómo se aplican las técnicas y herramientas en cada etapa del proceso de evaluación del riesgo, teniendo en cuenta diferentes aspectos tales como:

Identificación del riesgo, análisis del riesgo, análisis de las consecuencias, análisis del riesgo, estimación de la probabilidad cualitativa, semicuantitativa o cuantitativa, análisis del riesgo, evaluación de la eficacia de todos los controles existentes, análisis del riesgo, estimación del nivel de riesgo, valoración. Para cada etapa del proceso de evaluación del riesgo, la aplicación del método se describe como muy aplicable, aplicable o no aplicable [9]. Ver Tabla 1.

En las herramientas y técnicas contempladas en la identificación del riesgo definidas en la Tabla 1, se pueden identificar de acuerdo a su aplicabilidad cuáles herramientas y técnicas son Muy aplicables, Aplicables o No Aplicables. Igualmente, el aspecto de análisis de riesgo, consecuencia, probabilidad, nivel de riesgo y evaluación del riesgo, de tal forma que se puedan clasificar y asignar una de las valoraciones (MA, NA y A) con los anexos correspondientes de la norma especificados en la última columna denominada con el título (Ver anexo).

**TABLA I**  
**APLICABILIDAD DE LAS HERRAMIENTAS UTILIZADAS PARA LA EVALUACIÓN DEL RIESGO**

Herramientas y técnicas	Identificación del riesgo	Análisis del riesgo			Valoración del riesgo	Ver anexo
		Consecuencia	Probabilidad	Nivel de riesgo		
Tormenta de ideas	MA	NA	NA	NA	NA	B.1
Entrevistas estructuradas o semiestructuradas	MA	NA	NA	NA	NA	B.2
Delphi	MA	NA	NA	NA	NA	B.3
Listas de verificación	MA	NA	NA	NA	NA	B.4
Análisis preliminar de peligros	MA	NA	NA	NA	NA	B.5
Estudios de peligros y de operatividad (HAZOP)	MA	MA	A	A	A	B.6
Análisis de peligros y de puntos críticos de control (HACCP)	MA	MA	NA	NA	MA	B.7
Evaluación de riesgos ambientales	MA	MA	MA	MA	MA	B.8
Estructura "¿Y si...?" (SWIFT)	MA	MA	MA	MA	MA	B.9
Análisis de escenario	MA	MA	A	A	A	B.10
Análisis de impacto en el negocio	A	MA	A	A	A	B.11
Análisis de la causa raíz	NA	MA	MA	MA	MA	B.12
Análisis de modos y efectos de fallas	MA	MA	MA	MA	MA	B.13
Análisis del árbol de fallas	A	NA	MA	A	A	B.14
Análisis del árbol de eventos	A	MA	A	A	NA	B.15
Análisis de causa-consecuencia	A	MA	MA	A	A	B.16
Análisis de causa y efecto	MA	MA	NA	NA	NA	B.17
Análisis de capas de protección (LOPA)	A	MA	A	A	NA	B.18
Árbol de decisiones	NA	MA	MA	A	A	B.19
Análisis de fiabilidad humana	MA	MA	MA	MA	A	B.20
Análisis bow tie	NA	A	MA	MA	A	B.21
Mantenimiento centrado en la fiabilidad	MA	MA	MA	MA	MA	B.22
Análisis del circuito de fuga	A	NA	NA	NA	NA	B.23
Análisis Markov	A	MA	NA	NA	NA	B.24
Simulación Monte-Carlo	NA	NA	NA	NA	MA	B.25
Estadísticas Bayesian y redes Bayes	NA	MA	NA	NA	MA	B.26
Curvas FN	A	MA	MA	A	MA	B.27
Índices de riesgo	A	MA	MA	A	MA	B.28
Matriz de consecuencia/probabilidad	MA	MA	MA	MA	A	B.29
Análisis de costo/beneficio	A	MA	A	A	A	B.30
Análisis de decisión multi-criterios (MCDA)	A	MA	A	MA	A	B.31

1) Muy aplicable.  
 2) No aplicable.  
 3) Aplicable.

Fuente: Recuperado de “Norma Técnica Colombiana NTC-ISO 31010”, de Icontec, I., 2013 Técnicas de Evaluación del Riesgo, pp. 19 – 20.

Como se puede apreciar en la Tabla 2 presentada a continuación, se detallan los atributos de las herramientas que tienen la funcionalidad de reducir riesgos. Algunas tienen una complejidad alta y otras bajas, algunas proveen resultados cuantitativos en estadísticas y otras no.



**TABLA II**  
**ATRIBUTOS DE UNA SELECCIÓN DE HERRAMIENTAS**  
**PARA LA EVALUACIÓN DEL RIESGO**

Tipo de técnica de evaluación del riesgo	Descripción	Importancia de los factores que influyen			¿Puede proporcionar resultados cuantitativos?
		Recursos y capacidad	Naturaleza y grado de la incertidumbre	Complejidad	
<b>MÉTODOS DE BÚSQUEDA</b>					
Listas de verificación	Una forma sencilla de evaluación del riesgo. Una técnica que proporciona una lista de incertidumbres típicas que es necesario tener en consideración. Los usuarios pueden consultar listas, códigos o normas previamente desarrolladas.	Bajo	Bajo	Baja	No
Análisis preliminar de riesgos	Un método inductivo sencillo de análisis cuyo objetivo es identificar los riesgos y situaciones de riesgo y los eventos que pueden causar daños en una determinada actividad, instalación o sistema.	Bajo	Alto	Media	No
<b>MÉTODOS DE APOYO</b>					
Entrevista estructurada y tormenta de ideas	Un medio de recopilación de un amplio conjunto de ideas y evaluación, que luego es clasificado por un equipo. La tormenta de ideas se puede estimular mediante proposiciones o técnicas de entrevistas uno a uno o uno con varios.	Bajo	Bajo	Baja	No
Entrevista estructurada y tormenta de ideas	Un medio de recopilación de un amplio conjunto de ideas y evaluación, que luego es clasificado por un equipo. La tormenta de ideas se puede estimular mediante proposiciones o técnicas de entrevistas uno a uno o uno con varios.	Bajo	Bajo	Baja	No
Técnica Delphi	Un medio de combinar las opiniones de expertos que puede apoyar la identificación del origen y de la influencia, la estimación de la probabilidad y de la consecuencia, y la valoración del riesgo. Es una técnica de colaboración para crear el consenso entre expertos. Implica el análisis independiente y la votación de los expertos.	Medio	Medio	Media	No
SWIFT estructurado ("¿y si...?")	Un sistema para ayudar a un equipo en la identificación de riesgos. Normalmente se utiliza dentro de un taller de trabajo dirigido. Por lo general está relacionado con una técnica de análisis y valoración del riesgo.	Medio	Medio	Alguna	No
Análisis del árbol de fallas	Una técnica que comienza con un evento no deseado (evento superior) y determina todos los caminos por los que puede ocurrir. Estos se representan gráficamente en un árbol de diagrama lógico. Una vez desarrollado el árbol de fallas, se deben tener en consideración los caminos para reducir o eliminar las posibles causas/orígenes.	Alto	Alto	Media	Si

(CONTINÚA)

Tipo de técnica de evaluación del riesgo	Descripción	Importancia de los factores que influyen			¿Puede proporcionar resultados cuantitativos?
		Recursos y capacidad	Naturaleza y grado de la incertidumbre	Complejidad	
Análisis del árbol de eventos	Se aplican razonamientos inductivos para determinar las probabilidades de que se inicien diferentes eventos con sus posibles efectos.	Medio	Medio	Media	Si
Análisis de causa y consecuencia	Una combinación de los análisis del árbol de fallas y del árbol de eventos que permite la inclusión de demoras de tiempo. Se consideran las causas y las consecuencias de la iniciación de un evento.	Alto	Medio	Alta	Si
Análisis de causa y efecto	Los diversos factores que contribuyen a que se produzca un efecto se pueden agrupar en diferentes categorías. Con frecuencia, estos factores contributivos se identifican a través de la tormenta de ideas y se representa mediante una estructura en árbol o de espina de pescado "Fishbone".	Bajo	Bajo	Media	No
<b>ANÁLISIS FUNCIONAL</b>					
FMEA y FMECA	Análisis de modos y efectos de fallas (FMEA) es una técnica que identifica los modos y mecanismos de falla y sus efectos. Existen varios tipos de análisis FMEA: FMEA del Diseño (o del producto), que se aplica a componentes y a productos; FMEA del Sistema, que se aplica a sistemas; FMEA del Proceso, que se aplica a procesos de fabricación y de montaje; FMEA del Servicio y FMEA del Software. El FMEA puede ir seguido por un análisis de criticidad que defina la importancia de cada modo de falla de forma cualitativa, semicuantitativa o cuantitativa (FMECA2). El análisis de criticidad se puede basar en la probabilidad de que el modo de falla provocará la falla del sistema, o en el nivel de riesgo asociado al modo de falla, o en un número de prioridad del riesgo.	Medio	Medio	Media	Si
Mantenimiento centrado en la fiabilidad	Un método para identificar las políticas que se deben implementar para gestionar las fallas, a fin de conseguir eficaz y acertadamente la seguridad, la disponibilidad y la economía de funcionamiento requeridas en todos los tipos de equipos.	Medio	Medio	Media	Si
Análisis de fugas (Análisis del circuito de fugas)	Una metodología para identificar errores de diseño. Una condición de fuga es una condición latente en el hardware o en el software o una condición integrada que puede originar un evento no deseado o que puede inhibir un evento deseado que no es causado por falla de un componente. Estas condiciones se caracterizan por su naturaleza aleatoria y por la facilidad de evadir la detección durante los ensayos más rigurosos de sistemas normalizados. Las condiciones de fuga pueden causar un funcionamiento inadecuado, la pérdida de disponibilidad del sistema, demoras en el programa, o incluso lesiones o la muerte de personas.	Medio	Medio	Media	No

(CONTINÚA)

Tipo de técnica de evaluación del riesgo	Descripción	Importancia de los factores que influyen			¿Puede proporcionar resultados cuantitativos?
		Recursos y capacidad	Naturaleza y grado de la incertidumbre	Complejidad	
HAZOP Análisis de riesgos y de operatividad	Un proceso general de identificación del riesgo para definir posibles desviaciones con respecto al rendimiento esperado o previsto. Este proceso utiliza una palabra guía basada en el sistema. Se evalúan las criticidades de las desviaciones.	Medio	Alto	Alta	No
HACCP Análisis de peligros y de puntos críticos de control	Un sistema metódico, proactivo y preventivo para asegurar la calidad del producto, la fiabilidad y seguridad de los procesos, mediante la medición y monitoreo de las características específicas que se requiere que estén dentro de unos límites definidos.	Medio	Medio	Media	No
<b>APRECIACION DE LOS CONTROLES</b>					
LOPA (Análisis de niveles de protección)	(También se puede denominar análisis de barrera). Permite evaluar los controles y la eficacia de éstos.	Medio	Medio	Media	Si
Análisis bow tie	Un medio diagramático sencillo para describir y analizar los caminos de un riesgo, desde los peligros hasta los efectos, incluyendo la revisión de los controles. Se puede considerar que es una combinación de la lógica de un árbol de fallas que analiza las causas de un evento (representado por el mudo de un corbatín) y de un árbol de eventos que analiza las consecuencias.	Medio	Alto	Media	Si
<b>METODOS ESTADISTICOS</b>					
Análisis Markov	El análisis Markov, a veces llamado análisis estado-espacio, se utiliza comúnmente para analizar sistemas complejos reparables que pueden existir en múltiples estados, incluidos distintos estados degradados.	Alto	Bajo	Alta	Si
Simulación Monte-Carlo	La simulación Monte-Carlo se utiliza para establecer la variación agregada en un sistema, resultante de diversas variaciones del sistema, para un determinado número de entradas de datos, donde cada entrada tiene una distribución definida y las entradas están relacionadas con las salidas de datos a través de relaciones definidas. La simulación se puede aplicar para un modelo específico donde las interacciones de las diversas entradas se pueden definir matemáticamente. Las entradas se pueden basar en una variedad de tipos de distribución de acuerdo con la naturaleza de la incertidumbre que tales entradas están destinadas a representar. Para la evaluación del riesgo, se utilizan normalmente distribuciones triangulares o distribuciones beta.	Alto	Bajo	Alta	Si
Análisis Bayesian	Un procedimiento estadístico que utiliza datos de la distribución previa para determinar la probabilidad del resultado. El análisis Bayesian depende de la precisión de la distribución previa para deducir un resultado exacto. El modelo causa y efecto de las redes Bayesian establece una variedad de dominios mediante la captura de relaciones probabilísticas de entradas de datos variables para obtener un resultado.	Alto	Bajo	Alta	Si

Fuente: Recuperado de “Norma Técnica Colombiana NTC-ISO 31010”, de Icontec, I., 2013, Atributos de una selección de herramientas para la evaluación del riesgo, pp. 21 – 25.

La norma 31010 contempla una variedad de herramientas que tienen un propósito en común, la elección de cualquiera de estas herramientas depende del tipo de riesgo a evaluar, ya que cada una presenta diferente funcionalidad. El uso o la elección de cada herramienta depende de las necesidades y expectativas de cada organización.

Para realizar un análisis de riesgo adecuado, se deben tener identificados varios aspectos, primero tener claridad de cuál es el proceso misional de la organización, identificando los servicios o productos que se provean. Posteriormente se realiza la identificación de riesgos, es decir, de los aspectos que pueden fallar en la organización y que pueden impactar a los clientes y partes interesadas. Luego se selecciona la herramienta a utilizar (árbol de decisiones, AMEF, HAZOP LOPA, etc.), siempre y cuando ayude a reducir los riesgos. Seguido a esto se deben determinar las acciones para minimizar el riesgo y finalmente se recomienda realizar un monitoreo y revisión constante para determinar si están cumpliendo con la funcionalidad sobre los riesgos asociados.

Cada una de las herramientas que se implementen deben tener la función de informar si el riesgo es tolerable, si está reduciéndose y cuáles son las acciones que se deben tomar para poder reducirlo o eliminarlo.

Un aspecto muy importante para el análisis de riesgos es determinar si los riesgos residuales son aceptables o no.

La organización debe tener identificado cuál es el nivel permitido de quejas y cuáles son las consecuencias de las mismas, si es aceptable tener un determinado número de rechazos y cuáles son sus consecuencias. En la técnica que se seleccione se deben contemplar estos elementos, teniendo en cuenta que lo que se quiere lograr es el cumplimiento de los objetivos.

Es importante que en la definición de los riesgos se valoren adecuadamente las consecuencias de no lograr los resultados esperados, las consecuencias de tener una queja, reclamo o rechazo y el tratamiento que se le debe dar.

*Riesgo Residual* es el nivel de riesgo existente después de implementar un control que debe ser medido. Son soluciones de sentido común o temporales las cuales están compuestas por dos aspectos principales, fuente de riesgo y los controles que se establecen para reducir el impacto.

La norma ISO 31000 define el riesgo residual como el “Riesgo remanente después del tratamiento del riesgo”.

El riesgo residual puede contener un riesgo no identificado.

El riesgo residual también se conoce como "riesgo retenido" [12].

### IX. IDENTIFICACIÓN DE LOS RIESGOS EN LA ORGANIZACIÓN

Para llevar a cabo exitosamente esta actividad es necesario tener claridad acerca de los tipos de riesgos que están adheridos en los diferentes procesos de la organización, con el objetivo de llevar a cabo una administración de riesgos integral.

La diversidad de riesgos puede ser alta, igual que las formas de clasificarlos y abordarlos, por lo tanto, no es posible establecer una única clasificación de tipos de riesgos en la organización.

La siguiente clasificación de riesgos fue definida en el libro de *Administración de riesgos. Un enfoque empresarial*<sup>1</sup> del autor Mejía Quijano, presentado en dos tablas, la primera corresponde a la Tabla 3 en la cual se exponen los riesgos generados por el entorno organizacional, presentando la esquematización de las categorías de los riesgos derivados del medio empresarial:

TABLA III  
RIESGOS GENERADOS POR EL ENTORNO ORGANIZACIONAL

Riesgos del Entorno		
Origen del riesgo	Tipo de Riesgo	Explicación
Naturaleza	Provenientes de la naturaleza	Riesgos generados por el medio ambiente natural, tales como: huracanes, vientos fuertes, lluvias, inundaciones, maremoto, sequías, terremotos, movimientos sísmicos, erupción volcánica, deslizamiento de tierras, plagas, bacterias, virus, epidemias, etc.
	Generados a la naturaleza por parte de la empresa	Uso inadecuado de recursos naturales que pueden afectar la naturaleza.

(CONTINÚA)

Riesgos del Entorno		
Origen del riesgo	Tipo de Riesgo	Explicación
Naturaleza	Generados a la naturaleza por parte de la empresa	Consecuencia: efecto invernadero; disminución de la capa de ozono; contaminación acumulativa del aire, agua, suelos; generación de residuos de alta peligrosidad.
Riesgos asociados al país, la región y la ciudad de ubicación	Riesgo geopolítico	Debido a dificultades políticas entre naciones se pueden alterar las condiciones comerciales, que pueden implicar pérdidas de negocios, demoras o conflictos con proveedores o clientes.
	Riesgo social	Tiene que ver con la cultura de la región, las condiciones de seguridad, empleo, desarrollo de las comunidades, vivienda y bienestar, etc. Riesgos que pueden originarse en la sociedad son: hurto, sabotaje, chantajes y extorsiones, terrorismo, migraciones masivas, hambre, enfermedades, epidemias, colapso de servicios públicos indispensables, conflictos de baja intensidad, explotación de grupos sociales, cambios en los hábitos de consumo, demandas colectivas, conflictos comerciales.
	Riesgo económico	Relacionado con el crecimiento económico nacional y local, debido a las fluctuaciones de variables macroeconómicas: pib, inflación, desempleo, balanza de pagos. El decrecimiento de la economía puede generar riesgos que conlleven detrimento patrimonial a las empresas, al disminuir la capacidad de compra de sus clientes y la demanda de sus productos.
	Riesgo político	El manejo político del país, y las implicaciones que tiene sobre la economía nacional, afecta las organizaciones según sus condiciones particulares.

<sup>1</sup> R. C. Mejía Quijano, *Administración de riesgos. Un enfoque empresarial*.

(CONTINÚA)

Riesgos del Entorno		
Origen del riesgo	Tipo de Riesgo	Explicación
Sector económico e industrial	Riesgo sistemático	Riesgo que se origina por el hecho de competir en un sector determinado, ejemplo: campañas de desprestigio de la competencia comercial, corrupción institucional y privada, operaciones ilícitas, daños por productos, accidentes y enfermedades profesionales; accidentes industriales.

Fuente: Recuperado de “Administración de riesgos. Un enfoque empresarial”, de Mejía-Quijano, R., 2006, Identificación de Riesgos, II serie, pp. 35-36. Copyright 2006 de Fondo Editorial Universidad EAFIT.

Como se puede apreciar en la Tabla 4 se detallan los riesgos generados en la organización y se relacionan las categorías de riesgos que puede propiciar la organización en la ejecución de sus operaciones.

TABLA IV  
RIESGOS GENERADOS EN LA ORGANIZACIÓN

Riesgos generados en la Organización	
Tipo de Riesgo	Explicación
No sistemáticos	Riesgos propios y específicos de cada empresa que pueden afectar procesos, recursos, clientes o imagen.
Riesgo de reputación	Desprestigio de la organización, que acarrea pérdida de credibilidad y confianza del público, por fraude, insolvencia, conducta irregular de empleados, rumores o errores cometidos en la ejecución de alguna operación.
Riesgo puro	Origina pérdidas, como incendio, accidente, inundación
No sistemáticos	Riesgos propios y específicos de cada empresa que pueden afectar procesos, recursos, clientes o imagen.
Riesgo de reputación	Desprestigio de la organización, que acarrea pérdida de credibilidad y confianza del público, por fraude, conducta irregular de empleados, rumores o errores cometidos en la ejecución de alguna operación.
Riesgo puro	Al materializarse origina pérdidas, como incendio, accidente, inundación.
Riesgo especulativo	Al materializarse presenta la posibilidad de generar indistintamente beneficio o pérdida, como una aventura comercial, inversión en divisas ante expectativas de devaluación o revaluación, lanzamiento de nuevos productos.

(CONTINÚA)

Riesgos generados en la Organización	
Tipo de Riesgo	Explicación
Riesgo estratégico	Tiene que ver con pérdidas ocasionadas por definiciones estratégicas inadecuadas o errores en el diseño de planes, estructura, integración del modelo de operación con el direccionamiento estratégico, asignación de recursos; además de ineficiencia en la adaptación a los cambios constantes del entorno empresarial.
Riesgo operativo	Consiste en la posibilidad de pérdidas ocasionadas en la ejecución de procesos y funciones de la empresa, por fallas en procesos, sistemas, procedimientos o personas.
Riesgos financieros	Los riesgos financieros impactan la rentabilidad, ingresos y nivel de inversión, pueden provenir no sólo por decisiones de la empresa, sino por condiciones del mercado, ellos son: Riesgo de mercado, tiene que ver con fluctuaciones de las inversiones en bolsa de valores; también hacen parte de éste las fluctuaciones de precios de insumos, la tasa de cambio y las tasas de interés. Riesgo de liquidez, se relaciona con la imposibilidad de transformar en efectivo un activo o portafolio o tener que pagar tasas de descuento inusuales y diferentes a las del mercado para cumplir con obligaciones contractuales Riesgo de crédito, consiste en que los clientes y las partes a las cuales se les ha prestado dinero y fallen en el pago.
Riesgos legales	Se refieren a pérdidas en caso de incumplimiento de la contraparte en un negocio, sumado a la imposibilidad de exigir jurídicamente la satisfacción de los compromisos adquiridos. También se puede presentar al cometer algún error de interpretación jurídica u omisión en la documentación.
Riesgos tecnológicos	Son generados por el uso de tecnología, como virus informáticos, vandalismo puro, fraudes, intrusiones de hackers, colapso de las telecomunicaciones que puede generar daño de información o interrupción del servicio. También incluyen la actualización y dependencia de un proveedor, o de tecnología específica, bien sea en el campo informático, médico, de transporte u otras áreas.
Riesgos laborales	Los riesgos laborales, como accidentes de trabajo y enfermedades profesionales, pueden ocasionar daños a las personas y a la misma organización. Un accidente de trabajo puede producir lesiones orgánicas, invalidez, muerte o una perturbación funcional. La enfermedad profesional, por su parte, puede ser permanente o temporal, consecuencia del trabajo desempeñado o del medio en el cual se realizan las funciones. Existen otros riesgos laborales que surgen de la relación de la empresa con sus empleados, asociaciones o sindicatos, como huelgas, sabotajes, etc.

(CONTINÚA)

Riesgos generados en la Organización	
Tipo de Riesgo	Explicación
Riesgos físicos	Afectan los recursos materiales, como cortocircuitos, explosiones, daños en maquinaria o equipos (por su operación, diseño, fabricación, montaje o mantenimiento), deterioro de productos y daño en vehículos.

Fuente: Recuperado de “Administración de riesgos. Un enfoque empresarial”, de Mejía–Quijano, R., 2006, Identificación de Riesgos, II serie, pp. 37-39. Copyright 2006 de Fondo Editorial Universidad EAFIT.

### X. CONCLUSIONES

En el presente artículo se ha realizado una descripción de la Norma ISO 31000:2009 y su aplicación en entornos organizacionales, permitiendo entender sus importantes avances para ayudar a las organizaciones de todo tipo a gestionar el riesgo óptimamente.

La norma ISO 31000 es aplicable a cualquier tipo de organización ya sea pública o privada, grande o pequeña, es una herramienta muy práctica y concreta en la búsqueda de la gestión de riesgos.

Los aspectos contemplados por la norma ISO 31000 pueden ser aplicados durante toda la vida útil de una organización, ya que la norma se adapta perfectamente a los cambios, apoyando continuamente el alcance de los objetivos de las organizaciones.

La implementación de la gestión de riesgos con la norma ISO 31000 permite a las organizaciones establecer planes de acción para poder darles tratamiento a los riesgos para que en el momento que se concreten el impacto sea mínimo para la organización.

Establecer un método para identificar y gestionar los riesgos es de vital importancia para las organizaciones, ya que se pueden tener métricas del impacto que puedes causar los riesgos en caso de materializarse. De esta forma la organización puede estar preparada para actuar y establecer medidas preventivas y planes de contingencia previamente definidos, para realizar el respectivo tratamiento de riesgos. Adoptar estas prácticas le permitirán a la organización optimizar la operación en varios aspectos, impactando positivamente la eficiencia y rentabilidad de la organización.

Finalmente, es importante destacar que no importa el campo en el cual se encuentre operando una organización, se sugiere siempre llevar a cabo los diferentes procesos, teniendo en cuenta los principios y lineamientos de la gestión de riesgos.

SIA-Seminario de Investigación Aplicada. Artículo Gestión de Riesgos

### REFERENCIAS

- [1] Enfoque Genérico de la Norma ISO 31000. [Online] Available: [https://sitios.ces.edu.co/Documentos/NTC-ISO31000\\_Gestion\\_del\\_riesgo.pdf](https://sitios.ces.edu.co/Documentos/NTC-ISO31000_Gestion_del_riesgo.pdf)
- [2] Términos y Definiciones de la Norma ISO 31000. [Online] Available: [https://sitios.ces.edu.co/Documentos/NTC-ISO31000\\_Gestion\\_del\\_riesgo.pdf](https://sitios.ces.edu.co/Documentos/NTC-ISO31000_Gestion_del_riesgo.pdf)
- [3] Icontec, I., (16 de febrero, 2011). Fig. 1. Norma Técnica Colombiana NTC-ISO 31000 Recuperado de [https://sitios.ces.edu.co/Documentos/NTC-ISO31000\\_Gestion\\_del\\_riesgo.pdf](https://sitios.ces.edu.co/Documentos/NTC-ISO31000_Gestion_del_riesgo.pdf)
- [4] Icontec, I., (16 de febrero, 2011). Fig. 2. Norma Técnica Colombiana NTC-ISO 31000 Recuperado de [https://sitios.ces.edu.co/Documentos/NTC-ISO31000\\_Gestion\\_del\\_riesgo.pdf](https://sitios.ces.edu.co/Documentos/NTC-ISO31000_Gestion_del_riesgo.pdf)
- [5] Implementar La Gestión Del Riesgo de la Norma ISO 31000. [Online] Available: [https://sitios.ces.edu.co/Documentos/NTC-ISO31000\\_Gestion\\_del\\_riesgo.pdf](https://sitios.ces.edu.co/Documentos/NTC-ISO31000_Gestion_del_riesgo.pdf)
- [6] Monitoreo y Revisión del Riesgo de la Norma ISO 31000. [Online] Available: [https://sitios.ces.edu.co/Documentos/NTC-ISO31000\\_Gestion\\_del\\_riesgo.pdf](https://sitios.ces.edu.co/Documentos/NTC-ISO31000_Gestion_del_riesgo.pdf)
- [7] Icontec, I., (16 de febrero, 2011). Fig. 3. Norma Técnica Colombiana NTC-ISO 31000 Recuperado de [https://sitios.ces.edu.co/Documentos/NTC-ISO31000\\_Gestion\\_del\\_riesgo.pdf](https://sitios.ces.edu.co/Documentos/NTC-ISO31000_Gestion_del_riesgo.pdf)
- [8] Términos y Definiciones de la Norma ISO 31000. [Online] Available: [https://sitios.ces.edu.co/Documentos/NTC-ISO31000\\_Gestion\\_del\\_riesgo.pdf](https://sitios.ces.edu.co/Documentos/NTC-ISO31000_Gestion_del_riesgo.pdf)
- [9] Icontec, I. (2013). Norma Técnica Colombiana NTC-ISO 31010. , Tipos de técnicas de evaluación del riesgo, P.18.
- [10] Icontec, I., (2013). Norma Técnica Colombiana NTC-ISO 31010. *Técnicas de evaluación del riesgo*, pp. 19 – 20. TABLA I.
- [11] Icontec, I., (2013). Norma Técnica Colombiana NTC-ISO 31010. *Atributos de una selección de herramientas para la evaluación del riesgo*, pp. 21 – 25. TABLA II.
- [12] Riesgo Residual de la Norma ISO 31000. [Online] Available: [https://sitios.ces.edu.co/Documentos/NTC-ISO31000\\_Gestion\\_del\\_riesgo.pdf](https://sitios.ces.edu.co/Documentos/NTC-ISO31000_Gestion_del_riesgo.pdf)
- [13] Mejía, R.C. (2006). Administración de riesgos: Riesgos Generados por el Entorno Organizacional. Medellín, Colombia: Fondo Editorial Universidad EAFIT. TABLA III.
- [14] Mejía, R.C. (2006). Administración de riesgos: Riesgos Generados en la Organización. Medellín, Colombia: Fondo Editorial Universidad EAFIT. TABLA IV.