

RESUMEN ANALÍTICO DE INVESTIGACIÓN -RAI-

GUIA PARA LA IMPLEMENTACION DE LA NORMA ISO-31000 EN COLOMBIA 2018*

*BUITRAGO, Adriana; MONTOYA, Jorge Alonso; PALENCIA, Deymer Jesus ***

PALABRAS CLAVE

Gestion:(); Riesgos (); Estandar (); Control ()

DESCRIPCIÓN

La investigación tuvo como objetivo describir el proceso aplicado para acceder a la realización de una gestión de riesgos al interior de las organizaciones en nuestro país, la identificación, la medición y control de las posibles afectaciones, las técnicas o prácticas para abordarlas, la aplicación de políticas y de procesos a la hora de presentarse una posible pérdida. Se toma como punto de partida la información contenida en la norma NTC-ISO31000 Gestión del Riesgo del Icontec, todos sus puntos relevantes, las condiciones de medición, la tabulación de la matriz de riesgos y las respuestas definidas para cada posible ocurrencia de riesgo, la forma de clasificar los tipos de pérdida y como evitar o mitigar su impacto, finalmente contar con un plan de continuidad del negocio que permita mantener la operación en funcionamiento aminorando al máximo las consecuencias producidas al momento de presentarse un evento que redunde en una situación negativa a las diferentes actividades de la industria.

FUENTES

Se consultaron un total de 6 referencias bibliográficas distribuidas así: sobre el tema de la Norma NTC-ISO31000 sobre gestión del Riesgo de Icontec, Información sobre la estructura de la norma en www.isotools.com, Norma ISO 31000 versión 2009: Gestión de Riesgos – Principios y Guías, Análisis de riesgos por procesos basado en la norma ISO 31000:2011 para el centro comercial premier el limonar Cali Colombia, Diseño, implementación, seguimiento y mejoramiento del sistema de gestión de riesgos.

CONTENIDO

La norma ISO 31000 es un estándar internacional para la gestión de riesgos. Proporciona principios y guías exhaustivas, la norma facilita a las empresas el análisis y la evaluación de riesgos.

Es independiente a si se trabaja en una empresa pública o privada, ya que puede beneficiarse de la norma ISO 31000, se aplica a la mayoría de las actividades de la empresa, incluyendo la planificación, la operación de gestión y procesos de comunicación.

Aunque todas las empresas gestionan riesgos de algún modo, las recomendaciones de mejorar las prácticas según la ISO 31000 desarrollan la mejora de las técnicas de gestión y garantizan la seguridad en el lugar de trabajo en todo momento.

Mediante la implantación de los principios y la guía de la norma ISO 31000 en su empresa, puede mejorar su eficiencia operativa, su gobernabilidad y la confianza de las partes interesadas, al mismo tiempo que se minimiza cualquier posible pérdida. La norma ISO 31000 ayuda a fomentar el desempeño de seguridad y salud, se establece una base sólida para tomar decisiones y fomentar una gestión proactiva en todas las áreas.

La norma ISO 31000 convierte la planificación en una buena gestión de riesgos. La norma y el Risk Management deben considerarse una parte estratégica de la organización, no se encuentra aislada del resto. La finalidad es generar valor mediante el cumplimiento de los objetivos estratégicos estipulados con antelación.

METODOLOGÍA

La investigación es de tipo descriptivo, ya que recopila y ofrece el orden adecuado para hacer una Gestión de Riesgos Eficiente y practica para cualquier tipo de organización. Sus elementos esenciales, sus características y las técnicas para enfrentar cualquier adversidad que pretenda afectar la operación normal o el patrimonio que

constituye la mayor responsabilidad de la administración. Se toman como ejemplo diferentes empresas que han implementado la norma con el ánimo de ver casos reales y a partir de esa experiencia llegar de manera más sencilla a un proceso práctico y aplicado.

CONCLUSIONES

Nuestro interés hacia la investigación de la implementación de la norma NTC-ISO 31000 de la Gestión del Riesgo en una empresa Colombiana, es llegar a la vanguardia entendiendo su contexto y su forma de organización, disminuyendo la Brecha que actualmente existe sobre la implementación de la norma en las empresas, rompiendo los paradigmas que se han creado para lograr implementarla y lograr una certificación de esta índole a satisfacción.

Nuestro principal interés es conocer paso a paso de la implementación de la norma, desde el momento en el que se diseña el marco de referencia, pasando por la integración de los procesos de la organización, hasta llegar a la implementación, seguimiento y control de la norma implementada dentro de la organización con el fin de mejorar la eficacia operativa de las empresas en las que se implemente, fomentar el desempeño de seguridad y salud, estableciendo bases sólidas para la toma de decisiones y lograr una gestión proactiva en todas las áreas de una empresa.

¿Qué ventajas tiene?

- Mejorar de forma proactiva la eficacia operativa y la gobernanza
- Generar confianza entre las partes interesadas con el uso de técnicas de riesgos.
- Aplicar controles de sistemas de gestión para analizar riesgos y minimizar posibles pérdidas.
- Mejorar el desempeño y resiliencia de los sistemas de gestión.
- Implementar los presupuestos de las organizaciones estableciendo un paso a paso basado en la gestión y mitigación del riesgo.
- Generar conciencia empresarial en que implementar las mejores prácticas a

través de la aplicación de esta norma podemos implementar en la organización empresarial la mitigación y la gestión de los riesgos no solo a nivel económico y si no a su vez en todos los procesos de la organización.

- Responder a los cambios de forma eficaz y proteger su empresa mientras crece.¹

Beneficios y expectativas para la Organización

- Esta norma está destinada a personas que crean y protegen el valor en las organizaciones mediante la gestión de riesgos, la toma de decisiones, el logro de objetivos y la mejora del desempeño.
- Organizaciones de todos los tipos y tamaños se enfrentan a factores externos e internos e influencias que hacen que sea incierto si lograrán sus objetivos.
- La gestión del riesgo es dinámica y ayuda a las organizaciones a establecer estrategias, alcanzar objetivos y tomar decisiones informadas.
- La gestión del riesgo es parte de la gobernanza y el liderazgo, y es fundamental para la organización en todos los niveles. Contribuye a la mejora de los sistemas de gestión.
- La gestión del riesgo es parte de todas las actividades asociadas a una organización e incluye la interacción con las partes interesadas.
- La gestión del riesgo considera el contexto externo e interno de la organización, incluyendo el comportamiento humano y los factores culturales.
- La gestión del riesgo está basada en principios, marco de trabajo y procesos delineados, como se ilustra en la siguiente figura. Es posible que estos componentes ya existan en su totalidad o en parte dentro de la organización, sin

¹ <https://www.bsigroup.com/es-ES/ISO-31000-Gestion-de-Riesgos/>



embargo, pueden necesitar ser adaptados o mejorados para que la gestión del riesgo sea eficiente, efectiva y consistente.²

ANEXOS

La investigación realizada no incluye anexos, todos los temas referentes a la investigación está contenido en el documento.

² <https://www.globalstd.com/posada-2017/la-nueva-iso-31000-2018>

IMPLEMENTACIÓN DE LA NORMA ISO 31000

ADRIANA BUITRAGO ESPEJO

DEYMER JESÚS PALENCIA GÓMEZ

JORGE ALONSO MONTOYA OSPINA

CORPORACIÓN UNIVERSITARIA UNITEC

ESPECIALIZACIÓN EN GERENCIA DE PROYECTOS

SEMINARIO DE INVESTIGACIÓN II

BOGOTÁ

16 Diciembre de 2018

IMPLEMENTACIÓN DE LA NORMA ISO 31000

ADRIANA BUITRAGO ESPEJO

DEYMER JESÚS PALENCIA GÓMEZ

JORGE ALONSO MONTOYA OSPINA

SEMINARIO DE INVESTIGACIÓN II

TUTOR: RONALD ROJAS ALVARADO

CORPORACIÓN UNIVERSITARIA UNITEC

ESPECIALIZACIÓN EN GERENCIA DE PROYECTOS

SEMINARIO DE INVESTIGACIÓN II

BOGOTÁ

16 Diciembre de 2018

Tabla de contenido

INTRODUCCIÓN	4
1. DESCRIPCIÓN DEL PROBLEMA	5
1.1.Pregunta de investigación	6
2. Objetivo	6
2.1. Objetivo General.....	6
2.2. Objetivos Específicos.....	6
3. JUSTIFICACIÓN DE LA INVESTIGACIÓN	7
4. MARCO DE REFERENCIA	7
4.1 Antecedentes (Gestión de Riesgos)	7
4.2. Gestión de riesgos	12
4.3. Establecer el contexto	14
4.4. El tratamiento del riesgo	16
4.5. Diseño de marco para la gestión del riesgo.....	20
4.6. La aplicación de la gestión de riesgos.....	25
5. MARCO CONCEPTUAL	42
5.1. Definiciones	42
6. MARCO TEÓRICO (Ámbito de aplicación)	43
7. REFLEXIÓN	43
8. HIPÓTESIS DE TIPO CORRELACIONAL	45
9. DISEÑO METODOLÓGICO	46
10. ANÁLISIS DE RESULTADOS	57
11. CONCLUSIONES	59
12. REFERENCIAS	62

INTRODUCCIÓN

El propósito de esta investigación es la de recolectar información referente a la implementación de la norma ISO31000 sobre la gestión del riesgo en cualquier empresa u organización, muchas empresas en el mundo se han esforzado por implementarla y por contar con un modelo de gestión de riesgos.

El caso de estudio de la norma está asociado con la operación normal de las empresas y de sus operaciones, la importancia para contener o controlar los riesgos a los que se está expuesto, el propósito contempla identificar todo aquello que pueda significar una amenaza en la operación o sostenibilidad de las organizaciones.

El porqué de la aplicación de esta norma es obtener una certificación con el fin de ganar a nivel comparativo frente a otras organizaciones.

Al conocer en detalle los pasos y la forma en la que se aplica a cualquier actividad y los mecanismos por los que se puede hacer una correcta gestión de riesgos.

1. DESCRIPCIÓN DEL PROBLEMA

En el entorno actual de la economía mundial se hace necesario proteger el patrimonio y la operación de las industrias sin importar su actividad económica, para ello se ha desarrollado la Norma Internacional para la Gestión de Riesgos ISO 31000.

Los riesgos que se pueden presentar son de tipo ambiental (afectación al medio ambiente en sus procesos productivos) Naturales asociados a la fuerza de la naturaleza, económicos (Competencia de mercado), daños y afectaciones a terceros (afectaciones con las sociedades que las rodean) y de factor humano (Incidentes o accidentes laborales), todos estos riesgos de no ser considerados pueden ocasionar a la organización grandes pérdidas económicas y afectación en la imagen de la organización.

Contar con un plan que les ayude a tener un control de riesgo el cual permitirá minimizar las probabilidades de que ocurran accidentes o incidentes generados por no tener implementado la gestión integral de los riesgos.

Esta norma es un estándar de alcance internacional, la información se encuentra disponible y siempre está la posibilidad de acceder a cursos o programas que están orientados a que las organizaciones desarrollen esfuerzos para buscar obtener esta certificación.

1.1.Pregunta de investigación

¿Cómo se realiza la implementación de la norma ISO 31000?

2. OBJETIVOS

2.1 Objetivo General

Conocer los pasos para la implementación de la norma ISO31000, sobre la gestión del Riesgo, sus diferentes condiciones y requisitos.

2.2 Objetivos Específicos

- ✓ Recolectar información relacionada de la norma ISO 31000 para su implementación, utilizando los diferentes canales de investigación.
- ✓ Analizar cada uno de los procesos, actividades y tareas relacionados con la norma ISO31000 y su aplicación en las organizaciones para la implementación de la Gestión del Riesgo.
- ✓ Identificar y clasificar los riesgos a los que está expuesta una compañía y sobre los cuáles se puede aplicar la Norma ISO 31000.
- ✓ Aprender a través de la presente investigación cada uno de los pasos que nos llevan a la implementación de un modelo de Gestión de Riesgos con el fin de mitigar los peligros actuales y prevenir los futuros.

3. JUSTIFICACIÓN DE LA INVESTIGACIÓN

El propósito de este documento es identificar y orientar acerca de los pasos que se deben tener en cuenta a la hora de realizar una implementación de la Norma NTC ISO 31000 sobre la Gestión de Riesgos; por tal motivo la elaboración de este proyecto se realiza con el propósito de dar a conocer cómo se puede implementar en cualquier tipo de área, proceso y riesgos presentes; de igual forma permitir la disminución del gasto económico, mejorar la calidad de vida de los trabajadores e implementación de estrategias para la mejora continua en cualquier aspecto de la organización, evitando desviar las metas y objetivos.

4. MARCO DE REFERENCIA

4.1 Antecedentes de la norma (ISO 31000 Gestión de Riesgos)

La norma ISO 31000:2008, Gestión de Riesgos, es una norma de gestión creada para colaborar a todos los tipos y tamaños de organizaciones con el fin de gestionar los riesgos a los cuales se encuentran expuestos.

Figura 1. Historia de la Norma ISO 31000

Historia de la Norma ISO 31000	
Junio 2004:	Recuperación de Aplicaciones <<rápido - al tacto>> AS/NZS43360 en ISO - negado (negó)
Junio 2005:	Inicio del procedimiento de ISO
Sept. 2005:	ISO = Directriz = Certificación
Febrero 2006:	Sept, 2006, Mayo 2007 , Diciembre 2007
Abril 2008:	Investigación y Redacción del DIS
Dic. 2008:	Proyecto Final - va a votación en la comisión
Début 2009:	Votación de los miembros
Dic. 2009:	Publicación

Fuente: <https://es.slideshare.net/Uro26/iso-31000>

Principios Básicos para la Gestión de Riesgos

Se deben tener en cuenta los siguientes principios para que exista una mayor eficacia en la gestión del riesgo:

- Crea Valor
- Está integrada con los procesos de una organización
- Forma parte de la toma de decisiones
- Trata explícitamente la incertidumbre
- Es sistemática, estructurada y adecuada
- Está basada en la mejor información disponible
- Está hecha a la medida
- Tiene en cuenta factores humanos y culturales
- Es transparente e inclusiva
- Es dinámica, interactiva y sensible al cambio
- Facilita la mejora continua de la organización

La norma ISO 31000 ayuda a responder a la interrogante fundamental en la gestión del riesgo: Cómo llegar a todo el mundo para hablar sobre el riesgo de la misma manera.

La norma ISO 31000 es un estándar internacional para la gestión de riesgos. Proporciona principios y guías exhaustivas, la norma facilita a las empresas el análisis y la evaluación de riesgos.

Es independiente a, si se trabaja en una empresa pública o privada, ya que puede beneficiarse de la norma ISO 31000, se aplica a la mayoría de las actividades de la empresa, incluyendo la planificación, la operación de gestión y procesos de comunicación.

Aunque todas las empresas gestionan riesgos de algún modo, las recomendaciones de mejorar las prácticas según la ISO 31000 desarrollan la mejora de las técnicas de gestión y garantizan la seguridad en el lugar de trabajo en todo momento.

Mediante la implantación de los principios y la guía de la norma ISO 31000 en su empresa, puede mejorar su eficiencia operativa, su gobernabilidad y la confianza de las partes interesadas, al mismo tiempo que se minimiza cualquier posible pérdida.

La norma ISO 31000 ayuda a fomentar el desempeño de seguridad y salud, se establece una base sólida para tomar decisiones y fomentar una gestión proactiva en todas las áreas. (Fuente: <https://es.slideshare.net/Uro26/iso-31000>)

La norma ISO 31000 convierte la planificación en una buena gestión de riesgos. La norma y el Risk Management deben considerarse una parte estratégica de la organización, no se encuentra aislada del resto. La finalidad es generar valor mediante el cumplimiento de los objetivos estratégicos estipulados con antelación.

Identificación en Gestión de Riesgos

Es necesario hacer énfasis en la definición de objetivos:

- Línea de negocio, procesos y subprocesos
- Procesos críticos
- Aspectos metodológicos
- Riesgo inherente
- Asignación de responsabilidad

La identificación del riesgo se ha de realizar mediante un grupo multidisciplinar de expertos en la materia. En ella se ha de reconocer todas las amenazas posibles, dentro de cada uno de los procesos o ítems.

Análisis en Risk Management

El análisis se mide en función a la probabilidad del impacto que pueda ocasionar cualquier tipo de riesgo inherente a un proceso:

- Metodología acorde al grado de madurez.
- Cualitativa o cuantifica.
- Registro de eventos o incidentes.
- Controles y su grado de efectividad.

Evaluación en Gestión de Riesgos

Una vez que se han establecido los objetivos de priorización, se procede a la evaluación:

- Criterios de riesgo
- Apetito de riesgo
- Priorización de riesgos

Tratamiento en Risk Management

- Es necesario tener en cuenta el riesgo y la cobertura que se establece según el apetito de riesgo establecido por la organización.
- Planes de acción
- Seguimiento de cumplimiento de plan de acción
- Razonabilidad del control y medidas de tratamiento
- Asignación de presupuesto
- Indicadores de efectividad

Comunicación y consulta en Gestión de Riesgos

Los planes de comunicación pueden ser internos o externos:

- Reportes internos o externos.
- Informar y consultar.
- Nivel y evolución indicadores de riesgo.
- Seguimiento al perfil de riesgo.
- Mantener eficiencia.

Revisión y monitoreo

Se lleva a cabo según los indicadores establecidos previamente:

- Cumplimiento de políticas y procedimientos
- Efectividad del sistema
- Seguimiento al perfil de riesgo
- Periodicidad
- Responsabilidad

La gestión del riesgo no hay que verla como algo aislado, sino como un modelo que debe involucrar todos los procesos de la empresa. La norma ISO 31000 contribuye a la toma de decisiones.

En los últimos años las empresas se han esforzado en implantar sistemas de gestión de riesgos, apoyados en diferentes metodologías, entre las que se destaca la norma ISO 31000, siendo esta última la más aceptada. Para realizar esta tarea se han realizado inversiones que van desde la creación de áreas especializadas hasta la compra de herramientas de software, pasando por el pago a consultores

y tipos para establecer un modelo de gestión de riesgos sobre las necesidades de la organización.

A veces, todos los elementos no son suficientes para ser exitosos en la misión, muchas veces se dejan de lado o no se realizan los esfuerzos suficientes para involucrar a todo el personal que se encuentra realizando la operación, quien es el responsable de ejecutar los controles definidos y de reportar posibles materializaciones de riesgos. No siempre somos conscientes de la importancia de generar una cultura real del riesgo en las empresas, cada persona debe reflexionar sobre su papel dentro del sistema, deberá ser consciente de la necesidad de realizar seguimiento a los riesgos de los procesos, según la oportunidad en el registro de los eventos, la revisión permanente de la efectividad de los controles, identificando las claves y mitigando los riesgos. Se deja claro que la articulación con diferentes áreas que propinan insumos de importancia para establecer dinamismo y sostenibilidad.

Los aspectos se convierten en factores críticos para establecer el éxito al implantar un sistema de gestión de riesgos en las empresas. En ese momento encontramos un desafío que va a permitir a una empresa para conseguir beneficios que se consigan en diferentes frentes, incluyendo el estratégico, el táctico y el operativo.

(Fuente:<https://www.isotools.org/2018/03/19/que-necesita-saber-a-la-hora-de-implementar-la-norma-iso-31000/>)

4.2 Gestión de riesgos

Conjunto de componentes que proporcionan las bases y modalidades de organización para diseñar, implementar, control (2,28), la revisión y mejora continua de la gestión del riesgo (2,2) en toda la organización.

Norma ISO 31000 versión 2009: Gestión de Riesgos – Principios y Guías

NOTA 1 Las bases incluyen la política, objetivos, mandato y compromiso con la gestión del riesgo (2,1).

NOTA 2 Los acuerdos incluyen planes de organización, relaciones, responsabilidades, recursos, procesos y actividades.

Nota 3: El marco de gestión de riesgo está incrustado dentro de la organización global estratégica y operativa las políticas y prácticas.

Actitud ante el riesgo

Enfoque de la organización para evaluar y, eventualmente, seguir, mantener, adoptar o alejarse de riesgo (2,1)

Plan de gestión de riesgos

Régimen en el marco de la gestión del riesgo (2,3) especificando el planteamiento, la gestión de componentes y los recursos que se aplicarán a la gestión del riesgo (2,1)

NOTA 1: Los componentes de gestión suelen incluir los procedimientos, prácticas, la asignación de responsabilidades, la secuencia de y el calendario de actividades.

NOTA 2 El plan de gestión de riesgo se puede aplicar a un determinado producto, proceso y proyecto, y parte o la totalidad de la organización.

Proceso de gestión de riesgos

La aplicación sistemática de políticas de gestión, procedimientos y prácticas para las actividades de comunicación, consultoría, se establece el contexto, y la identificación, análisis, evaluación, tratamiento, seguimiento (2,28) y la revisión de riesgo (2,1)

4.3. Establecer el contexto

La definición de los parámetros internos y externos que deben tenerse en cuenta en la gestión de riesgos, y el establecimiento del ámbito de aplicación y criterios de riesgo (2,22) para la política de gestión del riesgo (2,4).

Contexto externo

Entorno externo en el que la organización busca alcanzar sus objetivos

NOTA contexto externo puede incluir:

La cultural, social, político, jurídico, reglamentario, financiero, tecnológico, económico, natural y competitivo, ya sea internacional, nacional, regional o local; Factores clave y las tendencias con repercusiones en los objetivos de la organización, y las relaciones con, y las percepciones.

Contexto interno

Ambiente interno en el que la organización busca alcanzar sus objetivos

NOTA contexto interno puede incluir:

- ✓ Gobernanza, la estructura organizativa, las funciones y responsabilidades;
- ✓ Las políticas, los objetivos y las estrategias que están en marcha para alcanzarlos;

- ✓ La capacidad, entendida en términos de recursos y conocimientos (capital, por ejemplo, tiempo, Personas, procesos, sistemas y tecnologías);
- ✓ Los sistemas de información, flujos de información y la toma de decisiones (tanto formales como informales);
- ✓ Relaciones con, y las percepciones y los valores de, grupos de interés internos;
- ✓ Cultura de la organización;
- ✓ Normas, directrices y modelos adoptados por la organización, y
- ✓ La forma y el alcance de las relaciones contractuales.

(Fuente: NORMA INTERNACIONAL ISO 31000 Primera edición - Noviembre 15 de 2009)

Fuente de riesgo

Elemento que por sí sola o en combinación tiene el potencial intrínseco para dar lugar a riesgo (2,1)

NOTA Una fuente de riesgo puede ser tangible o intangible.

Evento

La aparición o cambio de un conjunto particular de circunstancias

NOTA 1 Un evento puede ser uno o más casos, y puede tener varias causas.

Nota 2: Un evento puede consistir en algo que no sucede.

Nota 3: Un evento a veces puede ser contemplado como un "incidente" o "accidente".

NOTA 4 Un evento sin consecuencias (2,18) también puede ser contemplado como una "cerca de la señorita", "incidente", "cerca de Hit" o "cerca de llamada".

Probabilidad

Posibilidad de que suceda algo

NOTA 1 En la terminología de la gestión de riesgos, la palabra "riesgo" se utiliza para referirse a la posibilidad de que ocurra algo, si se define, mide, o determinar de forma objetiva o subjetiva, cualitativa o cuantitativamente, y se describen utilizando términos generales o las matemáticas (como una probabilidad o frecuencia durante un período de tiempo determinado).

NOTA 2 El término inglés "riesgo" no tiene un equivalente directo en algunas lenguas, en cambio, el equivalente del término "probabilidad" se utiliza a menudo. Sin embargo, en inglés, "probabilidad" es a menudo de una interpretación restrictiva como un término matemático. Por lo tanto, en la terminología de la gestión de riesgos, "probabilidad" se utiliza con la intención de que deben tener la misma amplia interpretación del término "probabilidad" tiene en muchos idiomas distintos.

4.4 El tratamiento del riesgo

El proceso para modificar el riesgo (2,1)

Nota 1: el tratamiento del riesgo puede incluir:

- ✓ evitar el riesgo al decidir no iniciar o continuar con la actividad que da lugar al riesgo;
- ✓ Tomando o aumentar el riesgo con el fin de perseguir una oportunidad;
- ✓ La eliminación de la fuente de riesgo (2,16);
- ✓ Cambiar la probabilidad (2,19);
- ✓ Cambiando las consecuencias (2,18);

- ✓ Compartir el riesgo con la otra parte o partes (incluidos los contratos y la financiación de riesgo), y
- ✓ Mantener el riesgo de decisiones informada.

NOTA 2: Tratamientos de riesgo que lidiar con las consecuencias negativas se refieren a veces como "reducción del riesgo", "riesgo de eliminación ", "prevención de riesgos "y" reducción de riesgos ».

NOTA 3: Tratamiento de los riesgos puede crear nuevos riesgos o modificar los riesgos existentes.

Seguimiento

Control continuo, supervisar, observar críticamente o de determinar el estado a fin de determinar el cambio del nivel de rendimiento requerido o esperado
Seguimiento NOTA puede ser aplicado a un marco de gestión del riesgo (2,3), el proceso de gestión del riesgo (2,8), el riesgo de (2,1) o el control (2,26).

Revisar

Actividad emprendida para determinar la conveniencia, la idoneidad y la eficacia de la materia objeto de lograr objetivos establecidos

NOTA revisión puede ser aplicada a un marco de gestión del riesgo (2,3), el proceso de gestión del riesgo (2,8), el riesgo (2,1) o el control (2,26). (Fuente: NORMA INTERNACIONAL ISO 31000 Primera edición - Noviembre 15 de 2009)

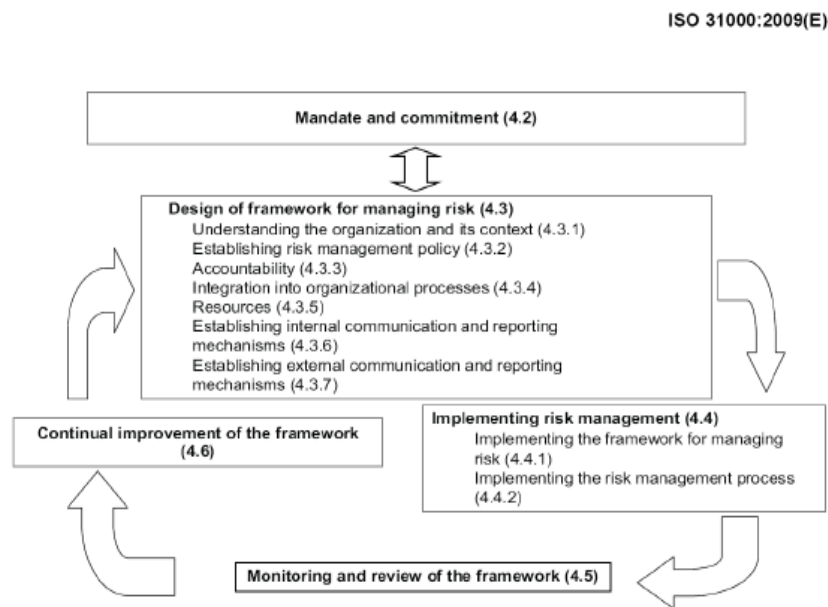
Estructura de la Guía.

General

El éxito de la gestión del riesgo dependerá de la eficacia del marco de gestión que proporciona las bases y disposiciones que incrustarlo en toda la organización en

todos los niveles. El marco ayuda en la gestión de los riesgos de manera efectiva a través de la aplicación del proceso de gestión del riesgo (ver punto 5) en la diferentes niveles y dentro de contextos específicos de la organización. El marco garantiza que la información sobre los riesgos derivados del proceso de gestión de riesgo está adecuadamente informada y se utiliza como base para la decisión de toma de decisiones y la rendición de cuentas en todos los niveles pertinentes de organización. Esta cláusula se describen los componentes necesarios del marco para la gestión del riesgo y la manera en que se interrelacionan de manera iterativa, como se muestra en la Figura 2.

Figura 2. Proceso Norma ISO 31000:209(E)



**Fuente: NORMA INTERNACIONAL ISO 31000 Primera edición -
 Noviembre 15 de 2009**

Este marco no tiene por objeto establecer un sistema de gestión, sino más bien para ayudar a la organización a la integrar la gestión de riesgos en su sistema de

gestión global. Por lo tanto, las organizaciones deben adaptar las componentes del marco de sus necesidades específicas.

Si las prácticas de gestión existentes en la organización y procesos incluyen componentes de la gestión de riesgos o si la organización ya ha adoptado un proceso formal de gestión de riesgo para determinados tipos de riesgo o de situaciones, entonces estos deben ser revisados y evaluados críticamente en contra de esta norma internacional, incluida los atributos que figuran en el anexo A, a fin de determinar su adecuación y eficacia.

Mandato y el compromiso

La introducción de la gestión del riesgo y asegurar su eficacia permanente, requiere fuerte y sostenido compromiso por parte de la gestión de la organización, así como la planificación estratégica y rigurosa para alcanzar Compromiso en todos los niveles. La dirección debería:

- ✓ definir y aprobar la política de gestión de riesgos;
- ✓ garantizar que están alineados la cultura de la organización y la política de gestión de riesgos;
- ✓ determinar los indicadores de gestión de riesgo de incumplimiento que se alinean con los indicadores de rendimiento de la organización;
- ✓ alinear los objetivos de gestión del riesgo con los objetivos y estrategias de la organización;
- ✓ garantizar el cumplimiento legal y reglamentario;
- ✓ asignar responsabilidades y las responsabilidades en los niveles apropiados dentro de la organización;
- ✓ garantizar que los recursos necesarios destinados a la gestión de riesgos;

- ✓ comunicar los beneficios de la gestión de riesgos a todos los interesados,
- ✓ garantizar que el marco para la gestión del riesgo sigue siendo apropiado.

4.5 Diseño de marco para la gestión del riesgo

Comprensión de la organización y su contexto

Antes de iniciar el diseño y la aplicación del marco para la gestión de riesgos, es importante evaluar y entender tanto el contexto externo e interno de la organización, ya que estos pueden reducir significativamente los influir en el diseño del marco.

Evaluación de contexto externo de la organización puede incluir, pero no se limita a:

- a) la física social y cultural, política, jurídica, reglamentaria, financiera, tecnológica, económica, y entorno competitivo, ya sea internacional, nacional, regional o local;
- b) factores clave y las tendencias con repercusiones en los objetivos de la organización
- c) las relaciones con los y las percepciones y los valores de, los interesados externos.

Evaluación de contexto interno de la organización puede incluir, pero no se limita a:

- ✓ Gobernanza, la estructura organizativa, las funciones y responsabilidades;
- ✓ Las políticas, los objetivos y las estrategias que están en marcha para alcanzarlos;
- ✓ Capacidades, entendida en términos de recursos y conocimientos (capital, por ejemplo, tiempo, personas, procesos, sistemas y tecnologías);

- ✓ Los sistemas de información, flujos de información y la toma de decisiones (tanto formales como informales);
- ✓ relaciones con, y las percepciones y los valores de, grupos de interés internos;
- ✓ Cultura de la organización;
- ✓ Normas, directrices y modelos adoptados por la organización, y
- ✓ La forma y el alcance de las relaciones contractuales.

El establecimiento de la política de gestión de riesgos

La política de gestión de riesgos debe exponer claramente los objetivos de la organización y su compromiso, el riesgo de la gestión y, normalmente, aborda los siguientes temas:

- ✓ Fundamento de la organización para la gestión de riesgos;
- ✓ Vínculos entre los objetivos de la organización y las políticas y la política de gestión de riesgos;
- ✓ La rendición de cuentas y responsabilidades de la gestión de riesgos;
- ✓ La forma en que los intereses en conflicto son tratados
- ✓ Compromiso de hacer de los recursos necesarios para ayudar a los responsables y los responsables de la gestión del riesgo;
- ✓ La forma en que los resultados de la gestión de riesgo serán medidos y reportado,
- ✓ El compromiso de revisar y mejorar la política de gestión del riesgo y el marco periódicamente y en respuesta a un suceso o cambio en las circunstancias.
- ✓ La política de gestión de riesgos debe ser comunicada apropiadamente.

Rendición de cuentas

La organización debe garantizar que haya rendición de cuentas, la autoridad y las competencias adecuadas para la gestión del riesgo, incluyendo la implementación y el mantenimiento del proceso de gestión del riesgo y garantizar la adecuación, eficacia y eficiencia de los controles. Esto puede ser facilitado por:

- ✓ La identificación de los propietarios de los riesgos que tienen la responsabilidad y la autoridad para gestionar los riesgos;
- ✓ Identificar quién es responsable de la elaboración, aplicación y mantenimiento del marco de para la gestión del riesgo;
- ✓ Otras responsabilidades de identificación de las personas en todos los niveles en la organización para la gestión del riesgo proceso;
- ✓ La medición del desempeño que se establece y externos y / o presentación de informes internos y los procesos de escalada; y
- ✓ Garantizar niveles adecuados de reconocimiento.

Integración en los procesos de organización

Gestión de riesgos debe estar integrada en todas las prácticas de la organización y los procesos de una manera que es pertinente, eficaz y eficiente. El proceso de gestión de riesgos debe formar parte de, y no separada de, los procesos de organización.

En particular, la gestión del riesgo debe ser incorporada a la política desarrollo empresarial y planificación estratégica y revisión, y los procesos de gestión del cambio.

No debería ser una organización en todo el plan de gestión de riesgos para garantizar que la política de gestión de riesgos es en práctica y que la gestión del riesgo está integrada en todas las prácticas de la organización y los procesos.

El plan de gestión de riesgo puede ser integrado en otros planes de organización, tales como un plan estratégico.

Recursos

La organización debe asignar los recursos adecuados para la gestión de riesgos.

Se debe considerar lo siguiente:

- ✓ Las personas, habilidades, experiencia y competencia;
- ✓ Los recursos necesarios para cada paso del proceso de gestión de riesgos;
- ✓ Procesos de la organización, métodos y herramientas que se utilizarán para la gestión de riesgos;
- ✓ Los procesos y procedimientos documentados;
- ✓ La información y los sistemas de gestión del conocimiento, y los programas de formación.

El establecimiento de mecanismos de comunicación interna y la presentación de informes

La organización debe establecer la comunicación interna y mecanismos de información a fin de apoyar y de fomentar la rendición de cuentas y la titularidad de riesgo. Estos mecanismos deberían garantizar que:

- ✓ Componentes clave del marco de gestión de riesgos, y cualquier modificación posterior, se comunicada apropiadamente;

- ✓ hay informes internos adecuados sobre el marco, su eficacia y los resultados;
- ✓ La información pertinente derivada de la aplicación de la gestión de riesgo es en los niveles adecuados y los tiempos,
- ✓ Hay procesos de consulta con las partes internas.

Estos mecanismos deberían, en su caso, incluir los procesos para consolidar la información de riesgo de una variedad de fuentes, y puede tener en cuenta la sensibilidad de la información.

Establecimiento de mecanismos para la comunicación externa y la presentación de informes

La organización debe desarrollar e implementar un plan de cómo va a comunicarse con los externos las partes interesadas. Esto implica:

- ✓ Involucrar a los interesados externos adecuados y garantizar un intercambio eficaz de información;
- ✓ Presentación de informes externos para cumplir con los requisitos legales, reglamentarios y de gobierno;
- ✓ Proporcionar retroalimentación y presentación de informes sobre la comunicación y de consulta;
- ✓ Comunicación utilizando para construir la confianza en la organización.
- ✓ La comunicación con las partes interesadas en el caso de una crisis o de emergencia.

Estos mecanismos deberían, en su caso, incluir los procesos para consolidar la información de riesgo de una variedad de fuentes, y puede tener en cuenta la sensibilidad de la información.

4.6. La aplicación de la gestión de riesgos

Aplicación del marco para la gestión del riesgo

En el marco de la aplicación de la organización para la gestión de riesgos, la organización debería:

- ✓ Definir el momento oportuno y la estrategia para la aplicación del marco.
- ✓ Aplicar la política de gestión de riesgos y el proceso de los procesos de organización.
- ✓ Cumplir con los requisitos legales y reglamentarios.
- ✓ Garantizar que la toma de decisiones, incluyendo el desarrollo y establecimiento de objetivos, está alineado con los resultados de los procesos de gestión de riesgos.
- ✓ Celebrar sesiones de información y formación.
- ✓ Comunicación y consulta con las partes interesadas para asegurarse de que su marco de gestión del riesgo sigue siendo adecuado.

La implementación del proceso de gestión de riesgos

La gestión del riesgo, debe aplicarse a garantizar que el proceso de gestión del riesgo descrito en la cláusula 5, se aplica a través de un plan de gestión de riesgos en todos los niveles y funciones pertinentes de la organización como parte de sus prácticas y procesos.

Seguimiento y revisión del marco

Con el fin de garantizar que la gestión de riesgos es eficaz y sigue apoyando el desempeño organizacional, la organización debe:

- ✓ Riesgo de medir el rendimiento con indicadores de gestión, que son periódicamente revisados para pertinencia;

- ✓ Periódicamente medir los progresos realizados en contra, y la desviación del plan, la gestión de riesgos;
- ✓ Revisar periódicamente si el marco de la gestión de riesgos, la política y el plan que siguen siendo pertinentes, teniendo en cuenta contexto externo e interno de las organizaciones;
- ✓ Informe sobre el riesgo, el progreso con el plan de gestión de riesgos y lo bien que la política de gestión de riesgo se está seguido,
- ✓ Revisar la eficacia del marco de gestión de riesgos.

La mejora continua del marco

Basándose en los resultados de la vigilancia y opiniones, las decisiones deben tomarse sobre la forma en la gestión del riesgo marco, la política y el plan puede ser mejorado. Estas decisiones deben conducir a mejoras en la organización de gestión del riesgo y su cultura de gestión del riesgo.

Proceso General

El proceso de gestión del riesgo debe ser:

- ✓ Una parte integral de la gestión,
- ✓ Arraigados en la cultura y las prácticas,
- ✓ Adaptados a los procesos de negocio de la organización.

Comprende las actividades descritas en 5,2 a 5,6. El proceso de gestión de riesgos se muestra en la Figura 3.

Figura 3. Proceso de gestión de riesgos

ISO 31000:2009(E)

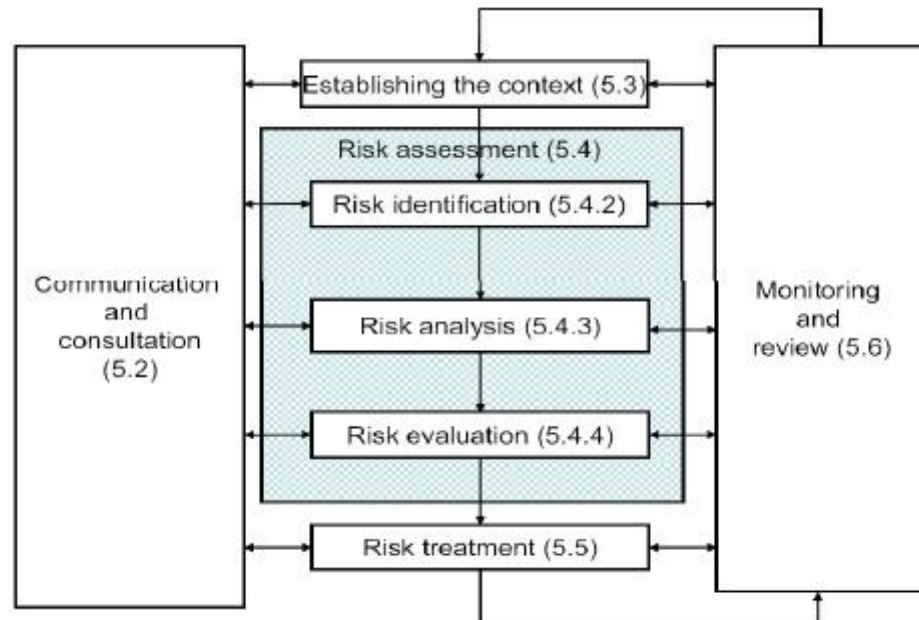


Figure 3 — Risk management process

**Fuente: NORMA INTERNACIONAL ISO 31000 Primera edición -
 Noviembre 15 de 2009**

Comunicación y Consulta

La comunicación y consulta con las partes interesadas externas e internas debería tener lugar durante todas las etapas del proceso de gestión de riesgos.

Por lo tanto, los planes de comunicación y consulta deben desarrollarse en una etapa temprana. Estos deben abordar las cuestiones relacionadas con el riesgo en sí mismo, sus causas, sus consecuencias (si se conoce), y las medidas que se adoptadas para tratarla. La comunicación interna y externa efectiva y la consulta debe llevarse a cabo para garantizar la que los responsables de la aplicación del proceso de gestión del riesgo y las partes interesadas a entender la base en la que

se toman las decisiones, y las razones por las medidas son necesarias en particular.

Un enfoque de equipo de consulta podrá:

- ✓ ayudar a establecer el contexto adecuado;
- ✓ garantizar que los intereses de las partes interesadas sean entendidas y consideradas;
- ✓ ayudar a garantizar que los riesgos están adecuadamente identificados;
- ✓ traer diferentes áreas de conocimiento para analizar juntos los riesgos;
- ✓ garantizar que los diferentes puntos de vista están debidamente considerados en la definición de criterios de riesgo y en la evaluación de riesgos;
- ✓ respaldo seguro y el apoyo a un plan de tratamiento;
- ✓ mejorar la gestión del cambio apropiados durante el proceso de gestión de riesgos,
- ✓ desarrollar una comunicación externa e interna y un plan de consulta.

La comunicación y consulta con los interesados es importante, ya que emitir juicios sobre el riesgo sobre la base de sus percepciones de riesgo. Estas percepciones pueden variar debido a diferencias en los valores, necesidades, suposiciones, conceptos y preocupaciones de los interesados. En sus puntos de vista puede tener un impacto significativo sobre las decisiones adoptadas, las percepciones de las partes interesadas deben ser identificados, registrados, y tener en cuenta en la toma de decisiones proceso.

Comunicación y consulta debería facilitar veraz, relevante, precisa y comprensible intercambios de la información, teniendo en cuenta aspectos de

confidencialidad y la integridad personal. (Fuente: NORMA INTERNACIONAL ISO 31000 Primera edición - Noviembre 15 de 2009).

Establecer el contexto del proceso de gestión de riesgos

Los objetivos, estrategias, alcance y los parámetros de las actividades de la organización, o las partes de la organización en el proceso de gestión de riesgo se están aplicando, debe ser establecido. La gestión de riesgo debe llevarse a cabo con plena consideración de la necesidad de justificar los recursos utilizados en la realización de gestión de riesgos. Los recursos necesarios, las responsabilidades y autoridades, y los registros que deben mantenerse también ser especificado.

El contexto del proceso de gestión del riesgo puede variar de acuerdo a las necesidades de una organización.

Puede implicar, pero no se limita a:

- ✓ La definición de las metas y objetivos de las actividades de gestión de riesgos;
- ✓ Para la definición de responsabilidades y en el proceso de gestión de riesgos;
- ✓ La definición del alcance, así como la profundidad y amplitud de las actividades de gestión de riesgos que deben llevarse a cabo, incluyendo las inclusiones y exclusiones específicas;
- ✓ La definición de la actividad, proceso, función, proyecto, producto, servicio o activo en términos de tiempo y lugar;
- ✓ La definición de las relaciones entre un determinado proyecto, proceso o actividad y otros proyectos, procesos o las actividades de la organización;
- ✓ La definición de las metodologías de evaluación de riesgos;

- ✓ Definir la forma y el rendimiento se evalúa la eficacia en la gestión de riesgo;
- ✓ Identificar y especificar las decisiones que tienen que ser hechas, y
- ✓ La identificación, la especificación o la elaboración de los estudios necesarios, su alcance y objetivos, y Los recursos necesarios para tales estudios.

La atención a estos y otros factores pertinentes deberían ayudar a asegurar que el enfoque de gestión de riesgos adoptados es adecuado a las circunstancias, a la organización y los riesgos que afectan a la consecución de sus objetivos.

Criterios de riesgo

La organización debe definir los criterios que se utilizarán para evaluar la importancia del riesgo. Los criterios deben reflejan los valores de la organización, objetivos y recursos. Algunos criterios pueden ser impuestas por, o deriva de, los requisitos legales y reglamentarios y otros requisitos que la organización suscriba. Los criterios de riesgo deben ser coherentes con la política de gestión de la organización de riesgo (ver 4.3.2), se definió al principio de cualquier proceso de gestión del riesgo y revisarse continuamente.

Al definir los criterios de riesgo, factores a considerar deben incluir los siguientes:

- ✓ La naturaleza y los tipos de causas y consecuencias que pueden ocurrir y cómo se mide;
- ✓ Cómo probabilidad será definida;
- ✓ El plazo (s) de la probabilidad y / o consecuencia (s);
- ✓ Cómo el nivel de riesgo es que se determine;
- ✓ Las opiniones de los interesados;

- ✓ El nivel en que se convierte en riesgo aceptable o tolerable, y
- ✓ Si las combinaciones de los múltiples riesgos que deben tenerse en cuenta y, en caso afirmativo, cómo y qué combinaciones deben ser consideradas.

La evaluación de riesgos General

Evaluación de riesgos es el proceso general de identificación de riesgos, análisis de riesgos y evaluación de riesgos. NOTA ISO / IEC 31010 proporciona orientación sobre las técnicas de evaluación de riesgos.

Identificación de riesgos

La organización debe identificar las fuentes de riesgo, zonas de impactos, los acontecimientos (incluyendo los cambios en las circunstancias) y sus causas y sus posibles consecuencias.

El objetivo de este paso es generar una lista completa de los riesgos basados en los acontecimientos que puedan crear, mejorar, prevenir, degradar, acelerar o retrasar la consecución de los objetivos. Es importante identificar los riesgos asociados a que no ejercen una oportunidad. La identificación completa es fundamental, porque el riesgo de que no se identifica en esta etapa no se incluyes en el análisis posterior.

La identificación debe incluir los riesgos o no su fuente se encuentra bajo el control de la organización, incluso aunque la fuente de riesgo o causa no puede ser evidente. De identificación de riesgos debe incluir el examen de los efectos en cadena de consecuencias particulares, incluidos los de cascada y los efectos acumulativos.

También debe considerar una amplia gama de consecuencias, incluso si la fuente de riesgo o causa no puede ser evidente.

Así como la identificación de lo que podría suceder, es necesario considerar las posibles causas y situaciones que muestran lo que consecuencias pueden ocurrir. Todas las causas y consecuencias importantes deben ser consideradas.

La organización debe aplicar herramientas de identificación de riesgos y técnicas que se adaptan a sus objetivos y capacidades, y de los riesgos que enfrentan. Pertinente y la información actualizada es importante en la identificación de riesgos. Esto debe incluir información de antecedentes adecuada que sea posible. Las personas con los conocimientos adecuados deberían de participar en la identificación de riesgos.

El análisis de riesgos

El análisis de riesgos implica el desarrollo de la comprensión de los riesgos. El análisis de riesgos proporciona una entrada a los riesgos la evaluación y las decisiones sobre si los riesgos necesitan ser tratados, y en el tratamiento del riesgo más adecuadas estrategias y métodos. El análisis de riesgos también puede aportar su contribución en la toma de decisiones en las elecciones deben ser realizados y las opciones de participación de los diferentes tipos y niveles de riesgo.

El análisis de riesgos implica la consideración de las causas y las fuentes de riesgo, sus positivos y negativos de consecuencias y la probabilidad de que esas consecuencias pueden ocurrir. Factores que afectan a las consecuencias y los riesgos debe ser identificado.

El riesgo es analizado mediante la determinación de las consecuencias y la probabilidad, y otros los atributos de los riesgos.

Un evento puede tener múltiples consecuencias y puede afectar a múltiples objetivos. Existentes los controles y su eficacia y eficiencia también deben tenerse en cuenta.

La forma en que las consecuencias y la probabilidad se expresan y la forma en que se combinan para determinar un nivel de riesgo debe reflejar el tipo de riesgo, la información disponible y de la finalidad para la que la salida de la evaluación de riesgos se va a utilizar. Todo ello debe ser coherente con los criterios de riesgo. También es importante a considerar la interdependencia de los diferentes riesgos y sus fuentes.

La confianza en la determinación del nivel de riesgo y su sensibilidad a las condiciones previas y las hipótesis deben ser considerados en el análisis, y comunicarse eficazmente a los tomadores de decisiones y, en su caso, de otros las partes interesadas.

Factores tales como la divergencia de opinión entre los expertos, la incertidumbre, la disponibilidad, calidad, cantidad y la continuidad de la relevancia de la información, o limitaciones sobre la modelización debería ser declarada, y se pueden resaltar.

El análisis de riesgos puede llevarse a cabo con diferentes grados de detalle, dependiendo del riesgo, el objetivo de la el análisis y la información, datos y recursos disponibles. Análisis pueden ser cualitativos, cuantitativos o semi - cuantitativos, o una combinación de estos, dependiendo de las circunstancias.

Consecuencias y la probabilidad puede ser determinada por la modelización de los resultados de un evento o serie de eventos, o por extrapolación de los estudios experimentales o de los datos disponibles. Las consecuencias pueden ser expresadas en términos de efectos tangibles e intangibles.

En algunos casos, más de un valor numérico o descriptor es para especificar las consecuencias y la probabilidad para distintos momentos, lugares, grupos o situaciones.

Evaluación de riesgos

El propósito de la evaluación de riesgos es ayudar en la toma de decisiones, basada en los resultados de análisis de riesgos, sobre riesgos que necesitan tratamiento y la prioridad para la aplicación del tratamiento.

Evaluación de los riesgos que supone la comparación del nivel de riesgo identificado durante el proceso de análisis con criterios de riesgo establecida cuando se considera el contexto. Basándose en esta comparación, la necesidad de que el tratamiento puede ser considerado.

Las decisiones deben tener en cuenta el contexto más amplio del riesgo y de incluir la consideración de la tolerancia de los riesgos asumidos por otras partes de la organización que se beneficia de los riesgos. Las decisiones deben tomarse en de conformidad con los requisitos legales, reglamentarios y otros.

En algunas circunstancias, la evaluación del riesgo puede llevar a una decisión de proceder a su posterior análisis. El riesgo de evaluación también puede dar lugar no a una decisión de tratar el riesgo de cualquier otra forma de mantener los controles existentes. Esta decisión se verá influida por la actitud de riesgo de la organización y los criterios de riesgo que han sido:

El tratamiento del riesgo

General

El tratamiento del riesgo consiste en seleccionar una o más opciones de modificación de los riesgos, y la aplicación de esas opciones.

Una vez en marcha, los tratamientos de proporcionar o modificar los controles.

El tratamiento del riesgo implica un proceso cíclico de:

- ✓ La evaluación de un tratamiento del riesgo;
- ✓ Decidir si los niveles de riesgo residual son tolerables;
- ✓ Si no tolerables, generando un nuevo tratamiento del riesgo,
- ✓ La evaluación de la eficacia de ese tratamiento.

Las opciones de tratamiento de los riesgos no son necesariamente excluyentes o apropiadas en todas las circunstancias.

Las opciones pueden incluir los siguientes:

- a) evitar el riesgo al decidir no iniciar o continuar con la actividad que da lugar al riesgo;
- b) tomar o aumentar el riesgo con el fin de perseguir una oportunidad
- c) eliminar la fuente de riesgo
- d) los cambios en la probabilidad
- e) cambiar las consecuencias
- f) la distribución del riesgo con la otra parte o partes (incluidos los contratos y la financiación de riesgo)
- g) mantener el riesgo por decisión informada.

Selección de opciones de tratamiento del riesgo

Selección de la opción de tratamiento más adecuado de riesgos consiste en equilibrar los costes y los esfuerzos de la aplicación contra los beneficios obtenidos, con respecto a los requisitos legales, reglamentarios y otros, tales como la responsabilidad social y la protección del medio ambiente natural. Decisiones, también debería tener en cuenta riesgos que pueden justificar el tratamiento de riesgo que no se justifica por motivos económicos, por ejemplo, grave (alta negativo consecuencia), pero raras (riesgo bajo) los riesgos.

Un número de opciones de tratamiento pueden ser consideradas y aplicadas de forma individual o en combinación. La organización que normalmente se pueden beneficiar de la adopción de una combinación de opciones de tratamiento.

Cuando la selección de las opciones de tratamiento de riesgos, la organización debe considerar los valores y percepciones de los las partes interesadas y los medios más adecuados para comunicarse con ellos. Cuando las opciones de tratamiento del riesgo tienen impacto sobre el riesgo en otras partes de la organización o con los interesados, estos deben participar en la decisión.

Aunque igual de eficaces, algunos tratamientos de riesgo pueden ser más aceptables para algunos grupos de interés que a otros. El plan de tratamiento debe identificar claramente el orden de prioridad en que los tratamientos individuales de riesgo deben ser práctica.

El tratamiento del riesgo en sí misma puede presentar riesgos. Un riesgo significativo puede ser el fracaso o la ineficacia de los riesgos medidas de tratamiento.

La vigilancia debe ser una parte integral del plan de tratamiento del riesgo de dar garantías de que las medidas siguen siendo eficaces.

El tratamiento del riesgo también puede introducir riesgos secundarios que deben ser evaluados, tratados, controlados y revisados.

Estos riesgos secundarios deben ser incorporados en el plan de tratamiento igual que el riesgo original y no se trata como un nuevo riesgo. Los vínculos entre los dos riesgos deben ser identificados y mantenidos.

Preparación y ejecución de planes de tratamiento del riesgo

El objetivo de los planes de tratamiento del riesgo es documentar cómo las opciones de tratamiento elegido se llevarán a cabo.

La información proporcionada en los planes de tratamiento debe incluir:

- ✓ Las razones para la selección de opciones de tratamiento, incluyendo los beneficios esperados que se pueden obtener;
- ✓ Los que son responsables de aprobar el plan y los responsables de la ejecución del plan;
- ✓ Acciones propuestas;
- ✓ Las necesidades de recursos
- ✓ incluidas las contingencias;
- ✓ Medidas de rendimiento y limitaciones;
- ✓ Presentación de informes y los requisitos de control, y
- ✓ Calendario y horario.

Los planes de tratamiento deben ser integrados con los procesos de gestión de la organización y discutido con partes interesadas pertinentes.

Los tomadores de decisiones y otras partes interesadas deben ser conscientes de la naturaleza y el alcance del riesgo residual después del tratamiento del riesgo. El riesgo residual debe ser documentado y sometidos a la supervisión, revisión y, cuando su caso, el tratamiento adicional.

Seguimiento y revisión

El seguimiento y la revisión debería ser una parte planificada del proceso de gestión del riesgo y la participación regular control o vigilancia. Puede ser periódica o ad hoc.

Responsabilidades de supervisión y revisión debe estar claramente definida.

Control de la organización y los procesos de revisión debe abarcar todos los aspectos de la gestión del riesgo proceso a los fines de:

- ✓ Asegurar que los controles son eficaces y eficientes tanto en el diseño y funcionamiento;
- ✓ La obtención de más información para mejorar la evaluación de riesgos;
- ✓ Analizar y aprender las lecciones de los acontecimientos (incluyendo conatos de accidentes), los cambios, las tendencias, éxitos y los fracasos;
- ✓ La detección de los cambios en el contexto externo e interno, incluidos los cambios en los criterios de riesgo y el riesgo en sí mismo que puede requerir una revisión de los tratamientos de riesgos y prioridades, y
- ✓ La identificación de riesgos emergentes.

El progreso en la aplicación de los planes de tratamiento del riesgo proporciona una medida de rendimiento. Los resultados pueden ser incorporados en la gestión del rendimiento global de la organización, la medición interna y externa y las actividades de presentación de informes.

Los resultados del monitoreo y la revisión deben ser registrados y externamente e internamente informados en su caso, y también debe ser utilizado como insumo para la revisión del marco de gestión del riesgo (ver 4.5).

Registro del proceso de gestión de riesgos

Las actividades de gestión de riesgos deben ser rastreables. En el proceso de gestión de riesgos, proporcionar los registros de Fundación para la Mejora de los métodos y herramientas, así como en el proceso global.

Las decisiones relativas a la creación de registros deben tener en cuenta:

- ✓ Necesidades de la organización para el aprendizaje continuo;
- ✓ Los beneficios de la reutilización de la información a efectos de gestión;
- ✓ Costes y esfuerzos involucrados en la creación y el mantenimiento de registros;
- ✓ Necesidades legales, reglamentarias y operativas de los registros;
- ✓ Método de acceso, la facilidad de recuperabilidad y medios de almacenamiento;
- ✓ Período de retención, y
- ✓ La sensibilidad de la información.

Atributos de la mejor gestión del riesgo

General

Todas las organizaciones deberían tratar en el nivel adecuado de rendimiento de su marco de gestión del riesgo en de acuerdo con la criticidad de las decisiones que se deben hacer. La lista de atributos a continuación representa un alto nivel de actuación en la gestión de riesgos. Para ayudar a las organizaciones para medir

su propio desempeño en contra de estos criterios, algunos indicadores tangibles se dan para cada atributo.

Entre los principales resultados

A.2.1 La organización tiene un conocimiento actual, correcto y completo de sus riesgos.

A.2.2 La organización de los riesgos están dentro de sus criterios de riesgo.

Atributos

Mejora continúa

Se hace hincapié en la mejora continua en la gestión del riesgo mediante el establecimiento de la organización metas de desempeño, la medición, la revisión y la posterior modificación de procesos, sistemas, recursos, capacidad y habilidades.

Esto puede ser indicado por la existencia de objetivos de rendimiento explícito contra el que la organización y Performance Manager individuo se mide. El desempeño de la organización puede ser publicado y comunicado. Normalmente, habrá al menos una revisión anual de rendimiento y a continuación, una revisión de procesos, y la fijación de objetivos de rendimiento revisadas para el período siguiente.

Esta evaluación de riesgos de gestión del rendimiento es una parte integral del desempeño de la organización general de evaluación y medición del sistema para los departamentos y los individuos.

Plena responsabilidad por los riesgos

La gestión del riesgo mejorada incluye amplia, totalmente definido y aceptado plenamente la responsabilidad de los riesgos, los controles y las tareas de

tratamiento de riesgos. Las personas designadas aceptan plenamente la responsabilidad, estén debidamente calificados y disponer de recursos suficientes para verificar los controles, los riesgos de vigilar, mejorar los controles y comunicarse de manera efectiva sobre los riesgos y su gestión a las partes interesadas externas e internas.

Esto puede ser indicado por todos los miembros de una organización está plenamente consciente de los riesgos, los controles y tareas para que son responsables. Normalmente, esto se hará constar en el trabajo / descripciones de puestos, bases de datos o de sistemas de información. La definición de las funciones de gestión de riesgos, responsabilidades y obligaciones debe ser parte de los programas de inducción de toda la organización.

La organización garantiza que quienes sean responsables están equipados para cumplir esa función, proporcionándoles con la autoridad, el tiempo, formación, recursos y competencias suficientes para asumir sus responsabilidades.

Aplicación de la gestión de riesgos en todas las decisiones

Toda toma de decisiones dentro de la organización, cualquiera que sea el nivel de importancia y trascendencia, implica la consideración explícita de los riesgos y la aplicación de la gestión de riesgos en cierta medida adecuada.

Esto puede ser indicada por los registros de las reuniones y decisiones para mostrar que las discusiones explícitas sobre los riesgos se lugar. Además, debería ser posible para ver que todos los componentes de la gestión de riesgos están representados dentro de procesos clave para la toma de decisiones en la organización, por ejemplo, para las decisiones sobre la asignación de capital, en las principales los proyectos y en la reestructuración y los cambios

organizacionales. Por estas razones, el riesgo de una base sólida es visto dentro de la organización como proporcionar la base para una gobernanza eficaz. (Fuente: NORMA INTERNACIONAL ISO 31000 Primera edición - Noviembre 15 de 2009)

5. MARCO CONCEPTUAL

5.1 Definiciones

Auto aseguramiento: Retener el riesgo dentro de la empresa.

Mapa de riesgos: Herramienta visual utilizada para considerar las alternativas a la serie de herramientas de gestión del riesgo.

Perfil del riesgo: Un proceso que evalúa todos los riesgos de las organizaciones y mide la frecuencia y gravedad de cada riesgo.

Riesgo: Efecto de la incertidumbre sobre los objetivos de:

NOTA 1 Un efecto es una desviación de lo esperado - positivos y / o negativos. En los Objetivos.

NOTA 2 puede tener diferentes aspectos (como la salud financiera, y la seguridad, y los objetivos medioambientales) y puede aplicar en diferentes niveles (como estratégica, en toda la organización, proyecto, producto y proceso).

NOTA 3: El riesgo se caracteriza a menudo por referencia a los eventos potenciales (2,17) y Consecuencias (2,18), o una combinación de estos.

NOTA 4 El riesgo se expresa a menudo en términos de una combinación de las consecuencias de un evento (incluidos los cambios en las circunstancias) y la probabilidad asociada (2,19) de ocurrencia.

NOTA 5 La incertidumbre es el estado, incluso parcial, de la deficiencia de la información relacionada con la comprensión o conocimiento de un caso, su consecuencia, o la probabilidad. (Fuente: NORMA TECNICA COLOMBIANA NTC-ISO 31000 Paginas 4 a la 28)

6. MARCO TEÓRICO

Esta norma internacional proporciona principios y directrices de carácter genérico sobre la gestión de riesgos.

La norma ISO 31000 puede ser utilizada por cualquier organización. Por lo tanto, no es específica de cualquier industria o sector. Esta norma le proporcionara un paso a paso a las diferentes instituciones en las cuales se desea aplicar para mitigar la exposición al riesgo a los cuales se ven expuestas en el desarrollo de sus actividades y la cual involucra en su implementación a todo el equipo de trabajo de cada una de las organizaciones que dese implementarla.

7. REFLEXIÓN

Nuestro interés hacia la investigación de la implementación de la norma NTC-ISO 31000 de la Gestión del Riesgo en una empresa Colombiana, es llegar a la vanguardia entendiendo su contexto y su forma de organización, disminuyendo la brecha que actualmente existe sobre la implementación de la norma en las empresas, rompiendo los paradigmas que se han creado para lograr implementarla y lograr una certificación de esta índole a satisfacción.

Nuestro principal interés es conocer paso a paso de la implementación de la norma, desde el momento en el que se diseña el marco de referencia, pasando por la integración de los procesos de la organización, hasta llegar a la implementación, seguimiento y control de

la norma implementada dentro de la organización con el fin de mejorar la eficacia operativa de las empresas en las que se implemente, fomentar el desempeño de seguridad y salud, estableciendo bases sólidas para la toma de decisiones y lograr una gestión proactiva en todas las áreas de una empresa.

¿Qué ventajas tiene?

- ✓ Mejora de forma proactiva la eficacia operativa y la gobernanza
- ✓ Genera confianza entre las partes interesadas con el uso de técnicas de riesgos.
- ✓ Aplica controles de sistemas de gestión para analizar riesgos y minimizar posibles pérdidas.
- ✓ Mejora el desempeño y resiliencia de los sistemas de gestión.
- ✓ Implementa los presupuestos de las organizaciones estableciendo un paso a paso basado en la gestión y mitigación del riesgo.
- ✓ Genera conciencia empresarial en que implementar las mejores prácticas a través de la aplicación de esta norma podemos implementar en la organización empresarial la mitigación y la gestión de los riesgos no solo a nivel económico y si no a su vez en todos los procesos de la organización.
- ✓ Responde a los cambios de forma eficaz y proteger su empresa mientras crece.

(Fuente: <https://www.bsigroup.com/es-ES/ISO-31000-Gestion-de-Riesgos>)

Beneficios y expectativas para la Organización

- La gestión del riesgo está basada en principios, marco de trabajo y procesos delineados, como se ilustra en la siguiente figura. Es posible que estos componentes ya existan en su totalidad o en parte dentro de la organización, sin embargo, pueden necesitar ser adaptados o mejorados para que la gestión del riesgo sea eficiente, efectiva y consistente.

8. HIPÓTESIS DE TIPO CORRELACIONAL

Para nuestro caso de investigación en el que desarrollamos la implementación de la norma ISO 31000 en una compañía podemos abarcar variedad de alternativas que nos lleven a alguna hipótesis de acuerdo al tipo de industria en la que se implemente; teniendo en cuenta que el planteamiento de la presente investigación es de carácter descriptivo se direcciona una hipótesis de carácter correlacional en la que se puede relacionar varios factores de asociación.

De acuerdo a lo anterior se puede generar el siguiente planteamiento hipotético y de carácter general:

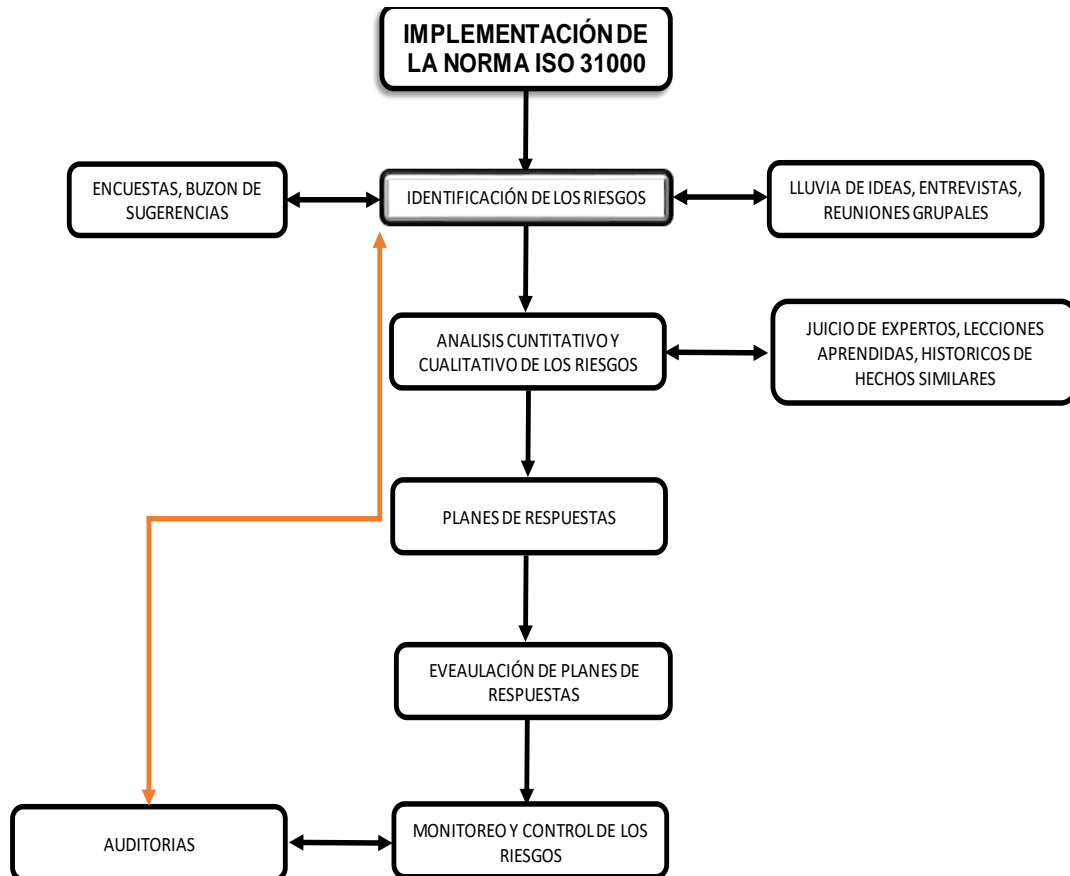
“Si se realiza la implementación de la norma ISO 31000 dentro de los procesos de una compañía se dará inicio a la mitigación de los riesgos y se asegura el éxito de sus objetivos”.

Lo anterior nos lleva directamente a relacionar y asociar que si se implementa la norma ISO 31000 en una compañía se mejoran procesos de carácter desde financiero, ambiental hasta el comercial, previniendo riesgos y generando soluciones a los riesgos que se encuentran presentes en una compañía y generando el mejor desempeño en cada proceso y cada dueño del mismo.

(Fuente: <https://www.globalstd.com/posada-2017/la-nueva-iso-31000-2018>)

9. DISEÑO METODOLÓGICO

Figura 4. Paso a paso implementación NORMA ISO 31000



Fuente: elaboración propia

9.1. Tipo y método de estudio

La metodología a implementar se relaciona con el método descriptivo y documental, donde mediante la observación se permitirá hacer un análisis de los principales riesgos que pueden ocasionar un impacto positivo y negativo a la empresa en temas relevantes como:

- ✓ Riesgos naturales y artificiales.

- ✓ Riesgos financieros
- ✓ Riesgos empresariales
- ✓ Riesgos operativos
- ✓ Riesgos sociales
- ✓ Riesgos de mercado
- ✓ Riesgos por hurtos y ataques terroristas

Por lo que la investigación se realizara por medio de diferentes métodos, los cuales se van a realizar en diferentes fases, las cuales no crearan un panorama de los principales riesgos a los cuales se encuentra expuesta la empresa en los temas mencionados anteriormente, por los cuales se realizaran las siguientes actividades:

- ✓ Tormenta de ideas; las cuales se realizarán en cada una de las ramas de la organización para que los empleados participen activamente en la ejecución de la actividad y que planten los riesgos a los que ellos consideren que se encuentren expuestos.
- ✓ Encuestas; éstas se realizarán a un grupo seleccionado de personas en cada una de las ramas involucradas a las actividades mencionadas.
- ✓ Entrevistas; éstas se realizarán a personas seleccionadas al azar en cada una de las áreas involucradas en la organización.
- ✓ Conocimiento de experiencia o documental; éstas se basarán en los hechos históricos presentado en la organización y las cuales han sido registradas.

9.2. Población y muestra

La población con la cual se realizará las muestras serán los empleados de las diferentes áreas que se encuentran involucradas con la organización y las cuales son materias de estudio, las muestras se registran en cada uno de los procesos mencionados en la

metodología de estudio, información la cual nos permitirá realizar un panorama de riesgo de la empresa con el fin de mitigar los riesgos asociados.

También se realizarán encuestas a clientes y sectores sociales de influencia de la organización, esto con el fin de tener un panorama de la percepción de las poblaciones en las cuales las organizaciones tienen su operación, con el fin de realizar ajustes en caso tal no se vea con buenos ojos la operación de la organización por parte de los sectores sociales de influencia en la operación de la empresa y prevenir un posible paro social.

9.3. Técnicas e instrumentos de recolección de información

La información para el desarrollo de la investigación se basa en la observación en sitio y la documentación se realizará mediante encuestas, entrevistas, tormentas de ideas grupales e información empírica documentada en experiencias ya vividas en la organización, por lo que se realizarán en conjunto con empleados de la empresa para que la información sea basada en las áreas de operación de la empresa.

Los riesgos de tipo financieros y de mercado a los que se ven expuestos las organizaciones se analizarán con estudios de comportamiento de mercados y se realizarán por medio de reuniones técnicas en conjunto con el área financiera y de marketing de las organizaciones, en los cuales se verán expuestos los principales riesgos que afrontaría la organización en su actividad económica.

9.4. Tratamiento de la información

Después de realizar el proceso de recopilación de información se realizará la documentación de la información relevante en la cual se analizará y se extraerán los riesgos asociados a la organización empresarial en los temas mencionados anteriormente.

Se realizará un tratamiento de los riesgos asociados, actividad que se realizará mediante un análisis detallado de los riesgos encontrados y las posibles maneras de mitigar el

riesgo, esto con el fin de crear métodos que se implementaran en las empresas para mitigar los impactos a los que se vería la organización a los posibles riesgos a los que se ve expuesta en su diario vivir.

9.5. Instrumentos de medida y procedimiento

Para realizar un análisis de los riesgos identificados se deberá realizar un análisis cualitativo de los riesgos, en el cual se definirán los riesgos de mayo magnitud de impacto.

9.5.1. Análisis Cualitativo

Para el análisis cualitativo de los Riesgos se sugiere utiliza una Matriz de Probabilidad sugerida en la Guía PMBOK, en la cual es necesario realizar una estimación de la probabilidad del riesgo valorados en un rango de 0 a 1 y el impacto estimado por valores de 4, 8, 12, 16 y 20 donde 4 es el menor impacto que puede tener. Los resultados de P x I se ubican en la Matriz de Evaluación de Riesgos (Figura 5):¹

Figura 5. Matriz de Probabilidad e Impacto

PROBABILIDAD DE OCURRENCIA		MAGNITUD DEL IMPACTO								
		MENOR	MODERADO	MAYOR	CRÍTICO	CATASTRÓFICO				
		4	8	12	16	20				
Muy Alta	1.0	I	8,0	I	12,0	C	16,0	C	20,0	C
Alta	0,8	D	6,4	I	9,6	I	12,8	C	16,0	C
Media	0,6	D	4,8	D	7,2	I	9,6	I	12,0	C
Baja	0,4	M	3,2	D	4,8	D	6,4	I	8,0	I
Muy Baja	0,2	M	1,6	M	2,4	D	3,2	D	4,0	I

Fuente: (Ureña & Beltrán, 2008)

¹ GESTIÓN DE RIESGOS EN LA FASE DE DISEÑO PARA PROYECTOS DE CONSTRUCCIÓN UTILIZANDO LA GUIA PMBOK / María del Pilar, Narváez Rosero

Los resultados valoran al riesgo como Riesgo de Menor Importancia, de Importancia Media o Moderado, Importante y de Mayor Importancia, Crítico o Catastrófico de acuerdo al color, donde el Riesgo de menor importancia es el color más claro como se muestra en la Figura 5.

De acuerdo a la metodología propuesta, en la figura 6 se presenta la Identificación y Clasificación, se muestra la codificación y la lista de riesgos identificados; y además la valoración de Probabilidad e Impacto del Análisis Cualitativo de Riesgos.

Los riesgos serán identificados mediante lluvia de ideas entre todos los interesados en el proyecto, por lo que se realizarán entrevistas y encuestas, esto se realizará a través de los interesados que tienen experiencia en el tema, para realizar el análisis de cualitativo, se tendrá en consideración la probabilidad de que el riesgo identificado se presente, multiplicado por el impacto que podría tener este riesgo en la organización, de esta forma se podrá identificar la valoración del riesgo de acuerdo a su importancia (Menor, Moderado, Mayor, Crítico y Catastrófico).

Figura 6. Matriz de evaluación de riesgos

MATRIZ DE EVALUACIÓN DE RIESGO				
TIPO DE RIESGOS	RIESGOS	PROBABILIDAD E IMPACTO		
		PROBABILIDAD (0 a 1)	IMPACTO (4, 8, 12, 16, 20)	PXL

(Fuente: Elaboración propia)

Luego de estimar la magnitud del impacto se debe definir qué hacer con los riesgos por medio de planes de respuestas.

9.5.2. Planes de Respuestas.

Luego de realizar la estimación de la magnitud del impacto de los diferentes riesgos identificados se deberán generar los planes de respuestas a los riesgos identificados para ello se deberá definir qué hacer con el riesgo y que acción tomara al respecto, posteriormente se deberán generar los planes de respuestas a cada uno de los riesgos las diferentes acciones que se pueden realizar con cada uno de los riesgos son:

- **Aceptar:** Esta acción significa asumir el riesgo y las consecuencias que este traiga consigo a l momento de presentarse, este tipo de acción se realiza cuando probabilidad de ocurrencia es baja y el impacto es bajo.
- **Transferir:** Esta acción se realiza cuando el riesgo es pasado a un tercero ya sea a un proveedor o un subcontratistas, o una póliza de seguro, este tipo de riesgos es sencillo de aplicar y de acuerdo al riesgo seguramente será la acción más económica de realizar, pero generalmente esta acción ocurre cuando ya se ha producido el daño y solo se podrá obtener una remuneración económica, pero a

su vez es causante de un impacto negativo a la imagen de la organización, siendo así una desventaja en su aplicación.

- **Mitigar:** Esta acción significa que se minimizar el impacto del riesgo, como por ejemplo los accidentes laborales los cuales se pueden mitigar atreves de acciones de seguridad y salud en el trabajo en cada una de las organizaciones.
- **Evitar:** Esta acción significa que se deben optar prácticas que eviten el riesgo identificado, es recomendable para este caso riesgos ambientales que puedan generar daño al medio ambiente o a la sociedad

9.6. Control de los riesgos

El control de los riesgos cuenta con una selección de técnicas de apreciación del riesgo, la cual se puede realizar con diferentes grados de profundidad y de detalle, y utilizando uno o varios de los métodos o técnicas y que varían desde simples a complejos. La forma de la apreciación y de sus resultados debería ser consecuente con los criterios de riesgo desarrollados como parte del establecimiento del contexto.

En términos generales, las técnicas adecuadas deberían tener las siguientes características:

- Deberían ser justificables y apropiadas a la situación u organización que se está considerando;
- Deberían proporcionar resultados de una forma que mejoren la comprensión de la naturaleza del riesgo y de cómo se puede tratar;
- Deberían poderse utilizar de una manera que sea trazable, reproducible y verificable.
- Se deberían dar las razones para la elección de técnicas, en cuanto a la importancia y a la idoneidad. Cuando se integran los resultados procedentes de

estudios diferentes, las técnicas utilizadas y los resultados deberían ser comparables.

Las técnicas descritas en la norma ISO 31010:2009 son las siguientes:

- Tormenta de ideas
- Entrevistas estructuradas o semiestructuradas
- Delphi
- Listas de ejemplo
- Análisis de riesgos preliminar (PHA)
- Estudio de Peligros y Operabilidad – HAZOP
- Análisis de peligros y puntos críticos de control (HACCP)
- Evaluación del riesgo ambiental
- Análisis de causas y consecuencias
- Análisis de causa y efecto
- Análisis de Capas de Protección (LOPA)
- Árboles de decisión
- Análisis de la fiabilidad humana
- Árbol de fallos y sucesos iniciadores (bow tie)
- Mantenimiento Centrado en la Fiabilidad (RCM)
- Análisis de circuitos de fugas
- Análisis de cadenas de Markov
- Análisis Qué pasa si
- Análisis de escenarios
- Análisis de Impacto de negocio (BIA)

- Análisis de Causa Raíz (RCA)
 - Análisis de modo y efecto de la falla (FMEA)
 - Análisis de árbol de fallos
 - Análisis de árbol de eventos
 - Simulación de Monte Carlo
 - Análisis Bayesiano
 - Curvas FN
 - Índices de riesgo
 - Matrices de probabilidad y consecuencia
 - Análisis costo beneficio
- Análisis de decisión multicriterio (MCDA)

(Fuente: <https://calidadgestion.wordpress.com/2016/10/28/gestion-del-riesgo-iso-31000/>)

Como parte del control de los riesgos se encuentra el monitoreo de los mismos, ya que se trata de un proceso continuo de verificación, supervisión y observación crítica, que pretende identificar cambios en la situación que pudiesen generar nuevos riesgos, o afectar la eficacia del plan de Gestión de Riesgos. Cuando las condiciones cambian, las probabilidades de los riesgos, y los mismos riesgos, también cambian, es por ello que el monitoreo debe ser periódico con el fin de mitigar que cambie, crezca y se modifique.

(Fuente: <https://www.isotools.org/2017/05/14/10-pasos-para-implementar-un-plan-de-gestion-de-riesgos-de-acuerdo-a-iso-31000/>)

9.7. Auditorias y evaluación de plan de gestión del riesgo

El siguiente paso de cualquier proceso de implementación de un estándar de ISO, siempre será la auditoría de certificación. La auditoría, aunque se crea que es el final, en realidad es un nuevo comienzo.

El plan de Gestión de Riesgo, debe alimentarse, monitorearse, supervisarse y analizarse en forma continua, ya que los riesgos son dinámicos. Tanto sus causas como sus consecuencias pueden variar, y afectar la probabilidad y el impacto de ellos. (Fuente: <https://www.isotools.org/2017/05/14/10-pasos-para-implementar-un-plan-de-gestion-de-riesgos-de-acuerdo-a-iso-31000/>)

Auditoría interna y gestión de riesgos en ISO 31000 son dos conceptos que van de la mano. La auditoría interna debe evaluar y contribuir a la gestión de riesgos, aportando así a la mejora de los procesos de control, utilizando un enfoque sistemático y disciplinado. La auditoría interna es una actividad que suele proporcionar independencia a los gestores del sistema de gestión de riesgos, frente a la Alta Dirección. Esto garantiza que los riesgos comerciales de mayor impacto, se traten de forma adecuada y así mismo, el sistema de controles internos de la organización opere de forma efectiva y eficiente. Esto explica de manera precisa la importancia de la relación entre auditoría interna y gestión de riesgos en un sistema de gestión basado en la norma ISO 31000.

Auditoría interna y gestión de riesgos en ISO 31000 La gestión de riesgos es un proceso que promueve el logro rentable de la organización y el alcance de sus objetivos, asegurando que la Alta Dirección obtenga información confiable sobre el desempeño de las actividades relacionadas con el tratamiento y la gestión de riesgos. Dentro de este esquema, auditoría interna y gestión de riesgos, son procesos complementarios: apoyando el proceso de gestión de riesgos, la auditoría interna verifica que:

- 1-) Se aplique el proceso de gestión de riesgos en forma apropiada y que todos los elementos del proceso sean adecuados y suficientes.
- 2-) El proceso de gestión de riesgos está en consonancia con las necesidades estratégicas y la política de la organización.
- 3-) Todos los riesgos significativos han sido identificados y están siendo tratados.
- 4-) Los controles son diseñados e implementados de forma correcta, con el fin de mantener los objetivos del sistema de gestión de riesgos.
- 5-) Los controles críticos son adecuados y efectivos.
- 6-) Se están ejecutando planes para mejorar la gestión de riesgos.
- 7-) Existe un progreso apropiado, según lo previsto en el plan de gestión de riesgos.

Entonces, no es raro que la auditoría interna de una organización deba trabajar en estrecha cooperación con los encargados del sistema de gestión de riesgos. En algunas organizaciones, que no cuentan con un sistema de gestión de riesgos, la auditoría a menudo proporciona una visión sobre la gestión de riesgos más amplia que la que se puede obtener de un consultor externo, siempre que se presenten ciertas condiciones:

- 1-) Debe quedar claro que la Alta Dirección sigue siendo responsable de la gestión de riesgos. El plan de trabajo debe incluir una estrategia clara para que, en un periodo de tiempo definido, estas responsabilidades sean asumidas por un miembro de la Alta Dirección.

2-) La naturaleza y las condiciones en las que se preste el servicio de auditoría interna, debe documentarse dentro de la misma auditoría. Auditoría interna y gestión de riesgos – Consultoría externa. En áreas de mayor riesgo, en las que la Alta Dirección reconoce la necesidad de aumentar y mejorar los controles, existe la oportunidad para que la auditoría interna pueda agregar valor a la organización por medio de actividades de consultoría. Aunque estas actividades de asesoramiento y consultoría pueden ser una parte valiosa en un plan de auditoría, el alcance de esta práctica es limitado, y puede ajustarse a tres aspectos:

Aseguramiento del proceso de gestión de riesgos en sí.

Aseguramiento de riesgos significativos de alto impacto.

Seguimiento del estado del plan de tratamiento de riesgos.

La seguridad en el proceso de gestión del riesgo en sí, puede ser realizada para proporcionar una seguridad razonable a la Alta Dirección de que la gestión de riesgos de una organización está diseñada, documentada y puesta en práctica para lograr sus objetivos. (Fuente: <https://www.escuelaeuropeaexcelencia.com/2018/01/auditoria-interna-gestion-riesgos-iso-31000/>)

10. ANÁLISIS DE RESULTADOS

Se realizó un ejercicio de documentación y de análisis de información y de fuentes para de este modo contar con el material necesario y brindar una información útil a la necesidad del lector.

Fruto del proceso de consulta y recolección de la información se identificó el proceso requerido para implementar la norma de Gestión de Riesgos en diferentes organizaciones.

De acuerdo con lo definido en la Norma de gestión De riesgos se presentaron las diferentes modalidades de clasificación y administración de riesgos.

Se generó una guía útil para quienes deseen llevar a cabo la implementación de un modelo de Gestión de Riesgos pensando o no en llegar a obtener la certificación, lo ideal es poder acudir a esta información en cualquier momento para obtener conceptos que sean de ayuda.

11. CONCLUSIONES

- De acuerdo al estudio realizado podemos definir que los riesgos en las organizaciones se encuentran presentes en cada uno de los procesos de su actividad económica, es importante para el éxito de una organización que esta identifique, gestione y controle sus riesgos ya que los riesgos pueden ejercer impactos negativos o en algunos casos positivos dentro de una organización, por ello el éxito y que una organización perdure en el tiempo dependerá de que esta tenga control sobre los riesgos que la pueden afectar durante el desarrollo de su actividad económica.
- Es importante para el proceso de gestión del riesgo que todos los interesados de las organizaciones se involucren en el proceso de gestión de los riesgos, ya que por medio de los interesados no importa la relevancia que tenga dentro de la organización, podrán aportar por medio de sus experiencias por dentro o por fuera de la organización un panorama claro de los principales riesgos en los cuales las organizaciones se ven expuestas, es durante este proceso donde se identifican los verdaderos riesgos a los que se ve sometida una organización.
- Es un factor diferenciador y de ventaja competitiva el contar con un modelo eficiente de gestión de riesgos, esto permite a las organizaciones estar siempre alertas ante las eventualidades y circunstancias a las que se encuentran expuestas en su normal operación y que de una u otra manera terminarían afectando el patrimonio de la empresa y su desempeño.

- La correcta aplicación de la gestión de riesgos también cuenta con un componente social ya que ante una eventualidad o al materializarse un riesgo contemplado que pueda llevar a la parálisis del aparato productivo podría repercutir en un posible lucro cesante y por este medio y proceso de liquidación que afecta a sus Funcionarios, proveedores y acreedores generando un impacto económico mayor que el propio siniestro, el contar con protecciones correctas permiten recuperar el rumbo en tiempos prudentes y con resultados positivos para todos los interesados.
- Así como muchas organizaciones colocan un esfuerzo importante en desarrollar un programa de Responsabilidad Social Empresarial, del mismo modo la gestión de riesgos puede llevar beneficio a una comunidad que interactúa directamente con una organización o una industria, un ejemplo podría ser la de poblaciones que depende económicamente de una industria en particular, ¿qué sería de Barrancabermeja si Ecopetrol no contara con las debidas medidas de protección para su planta de refinamiento? El impacto económico y social sería terrible para la región, por tanto en la medida que se cuente con las debidas medidas se protege la industria, la sociedad, la infraestructura pública.
- La conclusión más importante es que los riesgos hacen parte intrínseca de cualquier operación, siempre estarán presentes y en la medida en que sepamos gestionarlos podremos hacer que la industria permanezca y mantenga la

estabilidad económica para los interesados y beneficie a las partes para generar la sinergia necesaria para seguir funcionando de la mejor manera posible.

12. REFERENCIAS

- <https://www.isotools.org/iso-31000-gestion-riesgos-cuales-directrices/>
2016/07/19/
- <https://www.bsigroup.com/es-ES/ISO-31000-Gestion-de-Riesgos/>
- <https://www.globalstd.com/posada-2017/la-nueva-iso-31000-2018>
- Norma NTC ISO 31000 Primera edición - Noviembre 15 de 2009
- <https://www.escuelaeuropeaexcelencia.com,> auditoria-interna-gestion-riesgos-iso-31000/ 2018/01.
- <https://calidadgestion.wordpress.com/gestion-del-riesgo-iso-31000>, 2016/10/28.
- <https://es.slideshare.net/Uro26/iso-31000>, 21/03/2010.
- GESTIÓN DE RIESGOS EN LA FASE DE DISEÑO PARA PROYECTOS DE CONSTRUCCIÓN UTILIZANDO LA GUIA PMBOK / María del Pilar, Narváez Rosero

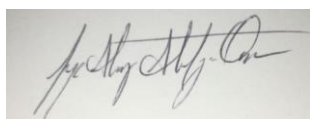
Nosotros: ADRIANA BUITRAGO ESPEJO, DEYMER PALENCIA GOMEZ Y JORGE ALONSO MONTOYA OSPINA, manifestamos en este documento nuestra voluntad de ceder a la Corporación Universitaria Unitec los derechos patrimoniales, consagrados en el artículo 72 de la Ley de 1982¹, de la investigación titulada:

IMPLEMENTACIÓN DE LA NORMA ISO 31000

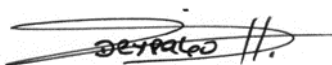
Producto de nuestra actividad académica, para optar por el título de ESPECIALISTAS EN GERENCIA DE PROYECTOS. La Corporación Universitaria Unitec entidad académica sin ánimo de lucro, queda por lo tanto facultada plenamente para ejercer los derechos anteriormente cedidos en su actividad ordinaria de investigación, docencia y publicación. La cesión otorgada se ajusta a lo que establece la Ley 23 de 1982. Con todo, en mi condición de autor me reservo los derechos morales de la obra antes citada con arreglo al Artículo 30 de la Ley 23 de 1982. En concordancia escribo este documento en el momento mismo que hago entrega del trabajo final a la Biblioteca General de la Corporación Universitaria Unitec.



ADRIANA BUITRAGO ESPEJO
Cédula: 52.759.094



JORGE ALONSO MONTOYA OSPINA
Cédula: 79953096



DEYMER JESUS PALENCIA GOMEZ
Cédula: 1.104.010.636

¹Los derechos del autor recaen sobre las obras científicas, literarias y artísticas en las cuales se comprenden las creaciones del espíritu en el campo científico, literario y artístico, cualquiera que sea el modo o la forma de expresión y cualquiera que sea su destinación, tales como: los libros, los folletos y otros escritos; las conferencias, alocuciones, sermones y otras obras de la misma naturaleza; las obras dramáticas o dramático musicales; las obras coreográficas y las pantomimas ; las composiciones musicales con letra o sin ella; las obras cinematográficas, a las cuales se asimilan las obras de dibujo, pintura, arquitectura, escultura, grabado, litografía; las obras fotográficas a las cuales se asimilan las expresas por procedimiento análogo a la fotografía, a la arquitectura, o a las ciencias, toda producción del dominio científico, literario o artístico que pueda reproducirse o definirse por cualquier forma de impresión o de reproducción, por fonograma, radiotelefonía o cualquier otro medio conocido o por conocer" (Artículo 72 de la Ley 23 de 1982)