APLICACIÓN DE LAS NORMAS ISO A LOS PRINCIPALES RIESGOS DE UNA EMPRESA MEDIANTE UN MODELO INTEGRAL DE GESTIÓN DE RIESGOS BASADO EN EL PROCESO DE LA GESTIÓN DE RIESGOS PRESENTADO EN LA ISO 31000

IVONNE JULIETE SÁNCHEZ DUARTE

MONOGRAFÍA DE GRADO PARA OPTAR EL TÍTULO DE ESPECIALISTA EN GERENCIA DE EMPRESAS

ASESOR
ANDRÉS RUEDA
INGENIERO INDUSTRIAL

FUNDACIÓN UNIVERSIDAD DE AMÉRICA
FACULTAD DE CIENCIAS ECONÓMICAS Y ADMINISTRATIVAS
ESPECIALIZACIÓN EN GERENCIA DE EMPRESAS
BOGOTÁ D.C.
2021

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____

Firma del Director de la Especialización

_____

Firma del Calificador

Bogotá D.C., mayo de 2021

DIRECTIVAS DE LA UNIVERSIDAD

Presidente de la Universidad y Rector del claustro

Dr. Mario Posada García Peña

Consejero Institucional

Dr. Luis Jaime Posada García Peña

Vicerrectora Académica y de Investigaciones

Dra. Alexandra Mejía Guzmán

Vicerrector Administrativo y Financiero

Ricardo Alfonso Peñaranda Castro

Secretario General

Dr. José Luis Macias Rodríguez

Decano Ciencias económicas y administrativas

Dr. Marcel Hofstette Gascon

Director Especialización en Gerencia de Empresas

Dr. Andrés Rueda

Las directivas de la Universidad de América, los jurados calificadores y el cuerpo docente no son responsables por los criterios e ideas expuestas en el presente documento. Estos datos corresponden únicamente al autor

AGRADECIMIENTOS

Agradezco principalmente a Dios por permitirnos estar con vida a pesar de la pandemia y contraer COVID-19. En segundo lugar, agradezco a mi mamá, que con sus múltiples esfuerzos logró sacar adelante mis estudios y me permitió convertirme en la profesional que soy y futura especialista. Finalmente, agradezco a mi novia que me apoyó y ayudó a finalizar este extenso trabajo y a los profesores y compañeros que me aportaron un poco de sí mismos a lo largo de las clases.

DEDICATORIA

Dedico este trabajo y próximo título de especialista a mi mamá, ya que sin ella nada de esto podría ser posible y es ella mi motor y para quien serán todos mis logros.

TABLA DE CONTENIDO

pág.

RESUMEN

La gestión de los riesgos se ha convertido en un tema de gran importancia con el avance del tiempo, ya que prevenir los riesgos resulta mucho más beneficioso a futuro para las empresas. Por esto, la Organización Internacional de Normalización (ISO, por sus siglas en inglés), desarrolló una norma pionera para la gestión de riesgos en una organización, denominada la ISO 31000. Esta norma contiene el conjunto de parámetros para gestionar efectivamente los riesgos. Sin embargo, su información es muy global y solo con su lectura e implementación quedan faltando datos para desarrollar parámetros como la identificación de los riesgos, el análisis, el tratamiento, entre otras. Por esto, en el presente documento se complementó esta información faltante con otras normas ISO que hacen referencia a otros tipos de sistemas de gestión en las organizaciones, tales como el sistema de gestión ambiental, el sistema de gestión de la salud y seguridad en el trabajo, el sistema de gestión de la seguridad de la información y el sistema de gestión de la cadena de suministro, y con documentos que contenían información de las fuentes de los riesgos, su análisis y tratamiento, desarrollando un modelo integral que contiene todos los apartados estipulados por la norma ISO 31000, lo estipulado por las normas ISO 14001, 45001, 27001 y 28000 referente a los mismos apartados, y la información de interés expuesta en otros documentos.

Palabras claves: gestión, riesgos, normas ISO, ambiental, salud y seguridad en el trabajo, cadena de abastecimiento y seguridad de la información.

INTRODUCCIÓN

En la presente monografía de grado se abarcará el tema de la Gestión de Riesgos empresariales que ha venido tomando un grado de relevancia importante a lo largo del tiempo. Para comenzar se desarrollará un marco teórico donde se explicarán los orígenes del término riesgo, así como su trascendencia para la sociedad, tomando como referencia el texto El Concepto del Riesgo del autor Saúl Chávez López; esto, con el fin de brindar el contexto del término que se desarrollará. Posteriormente se explicará la gestión del riesgo tal como se presenta en la norma ISO 31000, la cual es la base fundamental para el desarrollo del documento; en este apartado se presentará a profundidad cada paso para la implementación de la gestión de riesgo efectiva en una organización, como también los procesos de identificación, evaluación y control del riesgo.

Más adelante, en el capítulo 2, se realizará un marco teórico de los tipos de riesgo, a los cuales se relacionarán las normas ISO correspondientes, de manera que se contemplen todas las disposiciones de las normas junto con la definición de cada riesgo, para así lograr tener un marco conceptual amplio, el cual en el capítulo 3 servirá como fundamento, junto con lo expuesto en el capítulo 1, para llevar a cabo un modelo integrado para la gestión de riesgos, el cual contendrá información de beneficio para las empresas que quieran mitigar el riesgo pero en todos los aspectos, es decir, en todos los campos que contengan una posible presentación de riesgos que puedan afectar los objetivos de la organización.

También, se explicará a profundidad el uso y la información que contendrán las matrices, contemplando igualmente las normas asociadas y los aspectos indispensables para la correcta implementación del modelo.

OBJETIVOS

Objetivo General

Aplicar las normas ISO a los principales riesgos de una empresa mediante un modelo dinámico de gestión de riesgos basándose en el proceso de la gestión de riesgos presentado en la ISO 31000.

Objetivos Específicos

- Establecer un marco de referencia del riesgo, sus características y sus ámbitos de aplicación.
- Relacionar los diferentes tipos de riesgo identificados mediante las normas ISO.
- Proponer un modelo que integre los principales riesgos de una empresa y las normas ISO aplicando el proceso presentado en la ISO 31000.

1. GENERALIDADES DEL RIESGO

1.1 Conceptualización del Riesgo

El término *riesgo* ha existido desde la antigüedad, sin embargo, según Chávez (2018) no siempre hizo parte del vocabulario de la sociedad. El autor realiza la recopilación de diferentes definiciones del riesgo en su documento *El Concepto del Riesgo*, destacando inicialmente que según Luhmann (1996) citado en Chávez (2018) antiguamente se resaltaba el peligro, integrándose el término de riesgo por la sociedad moderna como una respuesta a la necesidad de la conceptualización de una situación específica. Existen diferentes autores que dan su perspectiva del origen del término tales como Peretti, Serrano, Pérez y Gardey, entre otros, quienes relacionan sus inicios con el término peligro. Por su parte, Briones (2005) citado en Chávez (2018) explica que el concepto se origina a finales de la Edad Media, pero hasta el siglo XVII se desarrolla en conjunción con las ideas de prudencia y seguridad. Además, Luhmann (1991) citado en Chávez (2018) expresa que el término riesgo fue mencionado para hacer referencia a decisiones vinculadas con el tiempo.

Chávez explica que se presentaron cambios en las ideologías dominantes, ya que según Serrano (2010) citado en Chávez (2018), cualquier fenómeno desastroso que existiera se le atribuía a Dios como un castigo, siendo hasta 1655 cuando Pascal desarrolló la teoría de la probabilidad. Por otra parte, según Briones (2005) citado en Chávez (2018), se comienza a desarrollar el concepto de riesgo en el siglo XVII el cual estaría ligado con la idea de prudencia y seguridad y la posibilidad que tienen las personas de elegir su destino. De igual manera, ECON-IT, explica que uno de los trabajos que influenciaron mayormente en el desarrollo de este término es el trabajo de La Place, donde se calcularon las probabilidades de esperanza de vida con y sin la aplicación de la vacuna de la viruela. De esta manera, se dio inicio al uso de métodos estadísticos para la medición de riesgos en diferentes contextos de salud y economía.

Posteriormente, en la segunda mitad del siglo XVIII inicia la Revolución Industrial dando cabida a la creación y el manejo de situaciones de riesgo, los cuales según Rousseau serían responsabilidad del hombre, y los elementos de probabilidad y decisión que integran al concepto de riesgo se convierten en aspectos de gran relevancia debido a los accidentes

ocasionados por la maquinaria. De esta manera, Chávez explica que “la lógica capitalista del liberalismo económico que se presenta desde el siglo XIX, hacen que las teorías de probabilidad en la economía sean una de las disciplinas pioneras en el cálculo del riesgo.” (p. 36).

En concordancia con la relevancia que se ha adquirido de la percepción del riesgo, Chávez expone que Aneas (2000) citado en Chávez (2018) explica que desde finales del siglo XIX, existía un mayor avance en los estudios de las causas físicas de los riesgos naturales pero aún no la respuesta de las personas ante estos. Asimismo, Aneas menciona que el sociólogo Samuel Prince en 1917, realizó la documentación de la explosión de un buque con municiones, ocasionando 2,000 muertos, miles de heridos y daños materiales, con lo que planteó algunos “principios básicos de conducta basados en el rechazo y la minimización del riesgo” (p. 37). También, en Chicago se llevó a cabo un estudio conocido como el *Paradigma de la Escuela de Chicago* el cual contenía trabajos sobre procesos naturales que incorporan riesgo y las razones de su desenlace catastrófico (p. 37).

De igual manera, en Estados Unidos a inicios del siglo XX se llevaron a cabo investigaciones destinadas al estudio de los riesgos naturales, las cuales hasta 1960, utilizaron métodos característicos de las Ciencias Económicas. Así, en 1970 se alcanzó cierto gradode madurez en los estudios sobre riesgos ambientales, a partir de la publicación de diversos libros por parte de la escuela de White (p. 37). Posteriormente, Chávez expone que de 1980 a 1990, según Calvo (2001) citado en Chávez (2018) y Casagrande (2002) citado en Chávez (2018), la percepción del riesgo adquiere mayor importancia debido a la influencia de movimientos ecologistas, y se expone por primera vez el *Principio de Precaución* gracias al contexto medio ambiental, generándose la Ley Barnier y propagándose a los ámbitos alimenticios y de salubridad. En congruencia, según Tricart (1982) citado en Chávez (2018) la conciencia del riesgo y la decisión política, toman mayor importancia que conocer y diagnosticar el problema.

Asimismo, según Wilches (1993) citado en Chávez (2018), Calvo (2001) citado en Chávez (2018), Briones (2005) citado en Chávez (2018) y Soldano (2009) citado en Chávez (2018), debido al crecimiento en el número de publicaciones en la década de los ochenta, se crea una conciencia en las personas de la diversidad de riesgos y su impacto que enfrentan, de tal manera que Georges Yves Kervern desarrolla el neologismo Cindyniques en 1987, con

el fin de establecerse como una disciplina que estudia los riesgos y se conoce como "la ciencia del peligro". De igual forma, se realiza un mayor hincapié en el estudio de los desastres naturales y se genera la necesidad de entenderlos y promover su mitigación mediante diferentes organismos tales como Naciones Unidas. Entonces, explica Chávez que frente a la situación los estudios acerca del riesgo se reconocen **"**como una evaluación compleja que debe ser abordada mediante el análisis transversal para poder obtener una visión integral de la problemática de una zona bajo estudio; esto mediante la gestión del riesgo, la cual se resume como la anticipación del desastre." (p.39).

Con base en este contexto, el autor continúa haciendo un recorrido por las definiciones contemporáneas de riesgo, iniciando con la definición de la Real Academia Española (1992) citado en Chávez (2018) donde lo definen como "contingencia o proximidad de un daño"; en donde contingencia se define como: "la posibilidad de que algo suceda o no suceda", en especial un problema que se presenta imprevistamente. De igual manera, explica que para autores como White (1974) citado en Chávez (2018)**,** Varnes (1984) citado en Chávez (2018), Cardona (1993) citado en Chávez (2018), Aneas (2000) citado en Chávez (2018), Díaz (2004) citado en Chávez (2018), entre otros definen el riesgo de manera cuantitativa, lo cual resume como "la estimación de costos debido a las pérdidas esperadas por la ocurrencia de un fenómeno natural o inducido por el hombre" (p.39). Chávez explica que estos autores coinciden en que estudiar el riesgo es una evaluación compleja, pero el del peligro hace referencia a una descripción de un fenómeno o proceso que tiene alto potencial dañino para la vida o las tareas de la sociedad (p.39).

Debido a este pensamiento, se justificó durante un largo periodo la gestión del riesgo en términos cuantitativos, lo cual se transforma en la corriente alternativa y cuya perspectiva adquiere otra dimensión desde la geografía y las ciencias sociales a partir de la crítica de Kenneth Hewitt llamada la visión dominante de los desastres y la ecuación de Gilbert White (1974) citado en Chávez (2018), en la que se incluye a la vulnerabilidad como factor clave (p.39).

Por otra parte, para algunos autores como Hewitt (1983) citado en Chávez (2018), Luhmann (1991) citado en Chávez (2018), Wilches (1993) citado en Chávez (2018), entre otros, el riesgo es más que un concepto estadístico de gestión descrito en términos

cuantitativos porque implica un problema de la sociedad, donde interviene la decisión racional del hombre y se conoce como construcción social del riesgo (p.40).

Así, Luhmann (1991) citado en Chávez (2018) explica que el riesgo es la consecuencia de tomar una decisión racional y este depende de la decisión y del peligro del entorno. Para Briones (2005) citado en Chávez (2018) el peligro está asociado con algo específico, y el riesgo es el margen de incertidumbre sobre el posible daño, de manera que es un concepto cualitativo que depende de otros factores como el contexto social y cultural. De esta forma, Chávez (2018) explica que es relevante destacar las principales definiciones de vulnerabilidad, ya que está estrechamente relacionada con el riesgo. En primer lugar, el diccionario de la lengua española (1992) citado en Chávez (2018), define el término como la posibilidad de ser herido o recibir una lesión tanto física o moral; mientras que dependiendo del autor pueden encontrarse conceptos relativamente sencillos como el de Soldano (2009) citado en Chávez (2018), quien define la vulnerabilidad como: capacidad respuesta - daño de la sociedad ante un evento potencialmente catastrófico; o bien con mayor detalle como Wilches (1993) citado en Chávez (2018), quien refiere la vulnerabilidad como global, que constituye un sistema dinámico de diferentes "vulnerabilidades", es decir, que surge como consecuencia de la interacción de una serie de factores y características (internas y externas) que convergen en una comunidad particular; y la resume como: incapacidad de una comunidad para absorber mediante el autoajuste, los efectos de un determinado cambio en su medio ambiente, o sea, la inflexibilidad o incapacidad para adaptarse a ese cambio.

Finalmente, el autor explica que principalmente se tiende a confundir los términos de riesgo y peligro, y que tal como afirma Mary Douglas, el riesgo es producto del conocimiento y la aceptación la cual está ligada a lo que se perciba de este. Concordando con Briones (2005) citado en Chávez (2018), lo que se concibe como riesgo proviene de diversas perspectivas de las disciplinas, las cuales reflejan "las formas de apropiación y percepción del entorno de distintas culturas y tiempos históricos" (p.47).

Por otra parte, para la obtención de una visión integral, se debe abarcar desde la gestión del riesgo. De esta manera, el grado de detalle y la complejidad del resultado del análisis del riesgo, que se realiza en la gestión del riesgo, corresponderá a las metodologías que se usen, ya que de aquí resultarán los "escenarios de riesgo, planes de contingencia y

(…) las medidas con la finalidad de planificar, prevenir y o mitigar las consecuencias de los riesgos a los que se encuentra expuesta la población para evitar un desastre" (p.48).

1.2 Gestión del Riesgo

Con base en el estudio previo para comprender de dónde proviene el término de riesgo, se ha establecido una de las normas pioneras en el ámbito de la Gestión de los Riesgos en una organización, la cual es la norma ISO 31000 (2011) que contiene las directrices generales para realizar una gestión eficaz de los riesgos que se puedan evidenciar en una empresa. Para comenzar, esta norma provee una introducción que se conecta con la importancia que se ha generado a lo largo del tiempo en el ámbito de entender y prevenir los riesgos, explicando que "las organizaciones de todo tipo y tamaño enfrentan factores e influencias, internas y externas, que crean incertidumbre sobre si ellas lograrán o no sus objetivos. El efecto que esta incertidumbre tiene en los objetivos de una organización es el "riesgo"" (Instituto Colombiano de Normas Técnicas y Certificación, NTC-ISO, 2011, p. 1).

Además, indica que todas las organizaciones gestionan el riesgo de diversas maneras, pero que se establecen ciertas directrices y procedimientos para su debido desarrollo, donde la característica clave es el *establecimiento del contexto* de las organizaciones que la implementen, donde se evidenciarán sus objetivos, "el entorno en el cual ella persigue sus objetivos, sus partes involucradas y la diversidad de criterios de riesgo; todo en conjunto ayudará a revelar y evaluar la naturaleza y la complejidad de sus riesgos" (Instituto Colombiano de Normas Técnicas y Certificación, NTC-ISO, 2011 p. 1).

Posteriormente, indica las ventajas de aplicar la norma en una organización, las cuales son:

> aumentar la probabilidad de alcanzar los objetivos; fomentar la gestión proactiva; ser consciente de la necesidad de identificar y tratar los riesgos en toda la organización; cumplir con los requisitos legales y reglamentarios pertinentes y con las normas internacionales; mejorar la presentación de informes obligatorios y voluntarios; mejorar el gobierno; mejorar la confianza y honestidad de las partes involucradas; establecer una base confiable para la toma de decisiones y la planificación; mejorar los controles; asignar y usar eficazmente los recursos para el tratamiento del riesgo;

> mejorar la eficacia y la eficiencia operativa; incrementar el desempeño de la salud y la seguridad, así como la protección ambiental; mejorar la prevención de pérdidas y la gestión de incidentes; minimizar las pérdidas; mejorar el aprendizaje organizacional; y mejorar la flexibilidad organizacional (Instituto Colombiano de Normas Técnicas y Certificación, NTC-ISO, 2011, p. 2).

Además, relaciona el objetivo de satisfacer las necesidades de las partes interesadas, de quien hacen parte:

> aquellos responsables del desarrollo de la política de gestión del riesgo dentro de la organización; aquellos responsables de garantizar que el riesgo se gestiona eficazmente dentro de la organización como unidad o dentro de un área, proyecto o actividad específicos; aquellos que necesitan evaluar la eficacia de una organización en cuanto a la gestión del riesgo; y aquellos que desarrollan normas, guías, procedimientos y códigos de práctica que, parcial o totalmente, establecen la manera de gestionar el riesgo dentro del contexto específico de estos documentos (Instituto Colombiano de Normas Técnicas y Certificación, NTC-ISO, 2011, p. 2).

De esta manera, se da inicio el capítulo 3 donde se establecen los principios que se deben cumplir por parte de las organizaciones para una gestión de riesgo eficaz, los cuales son (p. 9):

a) **La gestión del riesgo crea y protege el valor:** ya que favorece el cumplimiento de los objetivos y contribuye a una mejora del desempeño en todas las áreas que competen tanto interna como externamente a la organización.

b) **La gestión del riesgo es una parte integral de todos los procesos de la organización:** ya que no es una actividad independiente, sino que es responsabilidad de la dirección y una parte integral de todos los procesos de la organización.

c) **La gestión del riesgo es parte de la toma de decisiones:** ya que ayuda a quienes toman las decisiones de manera que pueden elegir informadamente y así dar prioridad a acciones y tomar otros caminos si se requiere.

d) La gestión del **riesgo aborda explícitamente la incertidumbre:** ya que considera la incertidumbre, su naturaleza y la forma en que se puede tratar.

e) **La gestión del riesgo es sistemática, estructurada y oportuna:** lo cual contribuye a la eficiencia y a resultados consistentes, comparables y confiables.

f) **La gestión del riesgo se basa en la mejor información disponible:** con fuentes de información tales como datos históricos, experiencia, retroalimentación de las partes involucradas, observación, previsiones y examen de expertos, como también las limitaciones de los datos o de los modelos utilizados, o la posibilidad de divergencia entre los expertos.

g) **La gestión del riesgo está adaptada:** alineándose con el contexto externo e interno y el perfil de riesgo de la organización.

h) **La gestión del riesgo toma en consideración los factores humanos y culturales:** reconociendo las capacidades, percepciones e intenciones de las personas externas e internas, que puedan facilitar o dificultar el logro de los objetivos de la organización.

i) **La gestión del riesgo es transparente e inclusiva:** de manera que las partes involucradas y quienes toman las decisiones en todos los niveles de la organización, intervienen garantizando una gestión pertinente y actualizada.

j) **La gestión del riesgo es dinámica, reiterativa y receptiva al cambio:** sintiendo y respondiendo continuamente al cambio, eventos externos e internos, el contexto y el conocimiento, monitoreando y la revisando los riesgos, si existen nuevos, cambian o desaparecen.

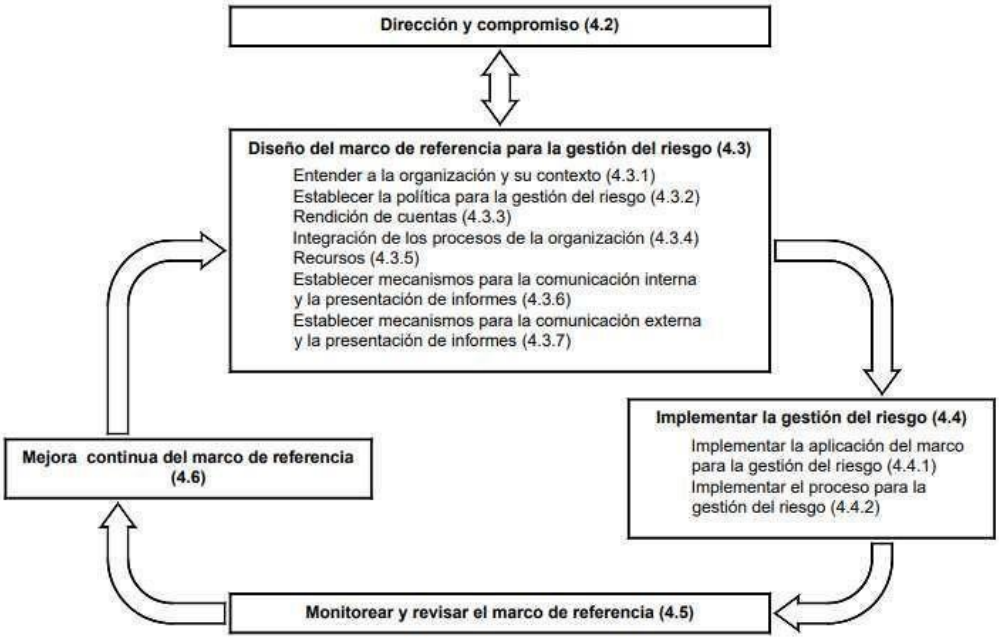
k) **La gestión del riesgo facilita la mejora continua de la organización:** debiendo las organizaciones desarrollar e implementar estrategias para mejorar la madurez de su gestión de riesgos junto con todos los otros aspectos de su organización.

Posteriormente, la norma establece el primer paso para efectuar la gestión del riesgo, lo cual compone el capítulo 4 en el establecimiento del marco de referencia. De esta forma se abordarán los aspectos mencionados en la norma y las figuras pertinentes que los representan.

Para comenzar, se especifica que dependiendo de la eficacia del marco de referencia se logrará el éxito de la gestión del riesgo, ya que este aporta las bases y las disposiciones que se introducirán en todos los niveles de la organización. Así, se garantiza que la información que se obtiene del riesgo y se deriva del proceso para la gestión del riesgo (el cual se expone en el capítulo 5 de la norma) sea reportado de manera adecuada y usado como base para tomar las decisiones y rendir las cuentas en todos los niveles de la organización. Teniendo esto en cuenta, la norma presenta la Figura 2 en la cual se resume la relación entre los componentes del marco de referencia en la gestión de riesgos, aclarando que es muy general para las organizaciones y que en caso de que se quiera aplicar se debe acomodar a las necesidades de cada empresa o si ya existe un modelo adoptado, se debe examinar con respecto a la norma (p. 11).

Figura 1.

Relación entre los componentes del marco de referencia para la gestión del riesgo.



Nota: en esta figura se estipulan los lineamientos para desarrollar, implementar, monitorear y mejorar el marco de referencia. Tomado de: Instituto Colombiano de Normas Técnicas y Certificación -ICONTEC- (2011). Relación entre los componentes del marco de referencia para la gestión del riesgo. El Instituto.

- **Dirección y Compromiso**: por parte de la dirección de las organizaciones, donde sus deberes se encuentran especificados, siendo estos:

> definir y aprobar la política para la gestión del riesgo; garantizar que la cultura de la organización y la política para la gestión del riesgo están alineadas; determinar indicadores del desempeño de la gestión para el riesgo que estén acordes con los indicadores del desempeño de la organización; alinear los objetivos de la gestión del riesgo con los objetivos y las estrategias de la organización; garantizar la conformidad legal y reglamentaria; asignar obligaciones y responsabilidades en los niveles respectivos dentro de la organización; garantizar que se asignan los recursos necesarios para la gestión del riesgo; comunicar los beneficios de la gestión del riesgo a todas las partes involucradas; y garantizar que el marco de referencia para gestionar el riesgo sigue siendo adecuado (Instituto Colombiano de Normas Técnicas y Certificación, NTC-ISO, 2011, p. 12).

- **Marco de referencia:** se debe comenzar por entender a la organización y su contexto, lo cual comprende el apartado 4.3.1 de la norma, donde se especifica que es relevante realizar una evaluación y comprensión del contexto tanto interno como externo ya que puede influir significativamente en el diseño. También propone algunos aspectos externos que se pueden incluir, tales como (p. 12):

> el ambiente social y cultural, político, legal, reglamentario, financiero, tecnológico, económico, natural y competitivo, bien sea internacional, nacional, regional o local; b) impulsores clave y tendencias que tienen impacto en los objetivos de la organización; y c) las relaciones con las partes involucradas externas, y sus percepciones y valores (Instituto Colombiano de Normas Técnicas y Certificación, NTC-ISO, 2011, p. 13).

Y algunos aspectos internos tales como:

> Gobierno, estructura organizacional, funciones y obligaciones; políticas, objetivos y estrategias que se han implementado para lograrlos; capacidades, entendidas en términos de recursos y conocimiento (por ejemplo capital, tiempo, personas, procesos, sistemas y tecnologías); sistemas de información, flujos de información y procesos de toma de decisiones (tanto formales como informales); relaciones con las partes involucradas internas y sus percepciones y valores; la cultura de la organización; normas, directrices y modelos adoptados por la organización; y forma y extensión de las relaciones contractuales (p.13).

- **Política para la gestión del riesgo**: debería contemplar los objetivos de la organización para gestionar el riesgo, su compromiso e incluir:

> la justificación de la organización para gestionar el riesgo; los vínculos entre los objetivos y las políticas de la organización y la política para la gestión del riesgo; las obligaciones y responsabilidades para gestionar el riesgo; la forma de tratar los conflictos de intereses; el compromiso para poner a disposición los recursos

necesarios con el fin de ayudar a los responsables de la gestión del riesgo y de rendir cuentas con respecto a ésta; la forma en la cual se va a medir y a reportar el desempeño de la gestión del riesgo; y el compromiso para revisar y mejorar periódicamente la política y el marco de la gestión del riesgo y en respuesta a un evento o un cambio en las circunstancias (p.13).

- **Rendición de cuentas**: las organizaciones deben asegurar que existe responsabilidad, autoridad y competencia adecuadas para la gestión del riesgo, donde se debe incluir la implementación y mantenimiento del proceso para la gestión y garantizar la idoneidad, eficacia y eficiencia de todos los controles, lo cual se podría facilitar a través del establecimiento de: los propietarios del riesgo, a quienes se rendiría las cuentas y tienen autoridad para gestionarlos; la persona encargada del desarrollo, implementación y mantenimiento del marco para la gestión; responsabilidades de los individuos en todos los niveles de la organización; medición del desempeño, proceso de escalamiento y reporte; y niveles adecuados de conocimiento (p. 13).

  Posteriormente, se procede a uno de los apartados de mayor relevancia, en concordancia con el principio b) el cual explica que la gestión de riesgos no es una actividad independiente, sino que está ligada a las actividades de la organización.

- **Integración**: la gestión del riesgo se debe incluir en todas las prácticas y los procesosde la organización de manera pertinente, eficaz y eficiente, convirtiéndose en parte de los procesos de la organización, particularmente en el desarrollo de la política, la planificación estratégica y del negocio, la revisión y en los procesos de gestión del cambio. También, se debe planear de manera que cubra toda la organización para garantizar que se está implementando e incluyendo en las prácticas y procesos (p. 14).

- **Recursos**: que se deberían proveer por parte de la Dirección, entre los cuales se debe considerar:

personas, habilidades, experiencia y competencia; recursos necesarios para cada paso del proceso de gestión del riesgo; los procesos, métodos y herramientas de la organización que se van a utilizar para gestionar el riesgo; procesos y procedimientos documentados; sistemas de gestión de la información y el conocimiento; y programas de entrenamiento (p.14).

- **Mecanismos para la comunicación interna y la presentación de informes**: con el fin de favorecer y fomentar la rendición de cuentas y la importancia del riesgo, específicamente garantizando que:

  los componentes clave del marco para la gestión del riesgo y todas las modificaciones posteriores se comunican de manera correcta; existe un reporte interno adecuado acerca del marco, su eficacia y resultados; la información pertinente derivada de la aplicación de la gestión del riesgo está disponible en los niveles y los momentos convenientes; y existen procesos para la consulta con las partes involucradas internas (p.15).

  Además, incluir, cuando corresponda, los procesos para tener en cuenta información del riesgo que provenga de diversas fuentes como también la sensibilidad de la información (p. 15).

- **Mecanismos para la comunicación externa y la presentación de informes**: la organización debe desarrollar e implementar un plan para la comunicación con las partes involucradas externas, el cual debe incluir:

  involucrar apropiadamente las partes interesadas externas y garantizar un intercambio efectivo de la información; reporte externo para cumplir con los requisitos legales, reglamentarios y del gobierno; brindar retroalimentación e informes sobre la comunicación y las consultas; usar la comunicación para crear confianza en la organización; y comunicarse con las partes involucradas en el evento de una crisis o contingencia (p.15).

Además, al igual que en el apartado anterior si es pertinente se deben considerar los procesos para tener en cuenta la información del riesgo que provenga de diferentes fuentes y la sensibilidad de la información (p.15).

- **Implementar el marco de referencia**: se procede al capítulo 4.4 para la implementación de la gestión del riesgo, donde la primera tarea que se debe realizar es implementar el marco de referencia establecido en el anterior capítulo. De estamanera, se especifica que la organización debe:

  definir el tiempo y la estrategia adecuados para la implementación del marco de referencia; aplicar el proceso y la política para la gestión del riesgo a los procesos de la organización; cumplir con los requisitos legales y reglamentarios; garantizar que la toma de decisiones, incluyendo el desarrollo y establecimiento de objetivos, estar en línea con los resultados de los procesos para la gestión del riesgo; llevar a cabo sesiones de información y entrenamiento; y comunicarse y consultar a las partes involucradas para garantizar que el marco para la gestión del riesgo sigue siendo adecuado (p.15).

- **Implementación del proceso para la gestión del riesgo**: a través de un plan que abarque todos los niveles y las funciones de la organización como parte de sus prácticas y procesos, el cual se explicará más adelante en el capítulo 5 de la norma (p. 15).

En continuidad con el marco de referencia, este, tal como lo explica el apartado 4.5, se debe monitorear y revisar para garantizar que la gestión del riesgo es eficaz, de manera que la organización debe (p.16):

medir el desempeño de la gestión del riesgo frente a los indicadores, los cuales se revisan periódicamente para determinar su idoneidad; medir periódicamente el progreso frente al plan para la gestión del riesgo y las desviaciones con respecto a éste; revisar periódicamente si el marco de referencia, la política y el plan para la

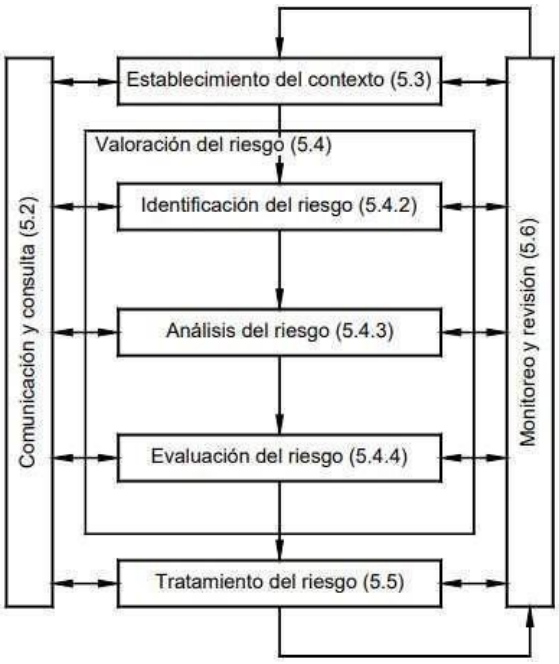
gestión del riesgo siguen siendo adecuados, según el contexto externo e interno de la organización; presentar informes sobre el riesgo, el progreso con el plan para la gestión del riesgo y sobre que tanto se cumple la política para la gestión del riesgo; y revisar la eficacia del marco de referencia para la gestión del riesgo (p.16).

- **Mejora continua:** este marco de referencia se debe mejorar continuamente, basándose en los resultados del apartado anterior y tomando decisiones sobre cómo se podría mejorar el marco, la política y el plan para la gestión del riesgo, las cuales generarían mejoras en la gestión y en la cultura (p.16).

Finalmente, el capítulo 5 de la norma ISO 31000 (2011) explica el proceso de gestión del riesgo mediante la Figura 3 que explica de manera resumida los pasos de este, la cual se implementará en el capítulo 3 del presente documento.

Figura 2

Proceso para la gestión del riesgo



Nota: en esta figura se representan los pasos para realizar la gestión de losriesgos.

Tomado de: Instituto Colombiano de Normas Técnicas y Certificación -ICONTEC- (2011). Proceso para la gestión del riesgo. El Instituto.

- **Comunicación y consulta de las partes involucradas**: tanto externas como internas, se debe realizar durante todas las etapas del proceso para la gestión del riesgo. De esta manera, se deben llevar a cabo en primer lugar los planes para garantizar la comunicación y la consulta, en los cuales se debe contemplar aspectos relacionados con el riesgo, sus causas, sus consecuencias (si se dispone esta información), y las medidas que se emplean para tratarlo. También debe ser eficaz para garantizar el entendimiento de las bases que se tienen en cuenta para la toma de decisiones y las razones para realizar acciones particulares, de tal forma que se pueda:

  > ayudar a establecer correctamente el contexto; garantizar que se entienden y se toman en consideración los intereses de las partes involucradas; ayudar a garantizar que los riesgos estén correctamente identificados; reunir diferentes áreas de experticia para analizar los riesgos; garantizar que los diversos puntos de vista se toman en consideración adecuadamente al definir los criterios del riesgo y al evaluar los riesgos; asegurar la aprobación y el soporte para el plan de tratamiento; fomentar la gestión adecuada del cambio durante el proceso para la gestión del riesgo; y desarrollar un plan adecuado de comunicación y consulta externo e interno (Instituto Colombiano de Normas Técnicas y Certificación, NTC-ISO, 2011, p.17).

  En concordancia, la norma establece que la comunicación y la consulta son relevantes ya que se emite la opinión de las partes interesadas, y pueden generar un alto impacto en las decisiones, como también el intercambio de información veraz, pertinente, preciso y de fácil entendimiento (p.17).

- **Establecimiento del contexto**: la organización articula sus objetivos, define los parámetros externos e internos a considerar y establece el alcance y los criterios del riesgo para el proceso de gestión; asimismo, la norma explica que aunque estos parámetros son similares a los establecidos en el diseño del marco de referencia, al establecerlos en este proceso se deben contemplar más detalladamente y sobre todo la manera como se relacionan con el alcance del proceso (p.18).

- **Contexto externo**: se definiría como el ambiente externo en el cual la organización busca alcanzar sus objetivos. Se considera de gran importancia ya que garantiza que los objetivos y los requisitos de las partes involucradas externas sean considerados al momento de desarrollar los criterios del riesgo. También se deben detallar los requisitos legales y reglamentarios, las percepciones de las partes involucradas y otros aspectos específicos para el alcance de la gestión. De igual manera puede incluir (p.18):

  > el ambiente social y cultural, político, legal, reglamentario, financiero, tecnológico, económico, natural y competitivo, bien sea internacional, nacional, regional o local; los impulsores clave y las tendencias que tienen impacto en los objetivos de la organización; y las relaciones con las partes involucradas externas y sus percepciones y valores (p.18).

- **Contexto interno**: se define como el ambiente interno en el cual la organización busca alcanzar sus objetivos, y debe contemplar la cultura, los procesos, la estructura y la estrategia de la organización ya que la gestión del riesgo debe ir alineada con estos. También, todo aquello dentro de la organización que pueda tener influencia en la forma en que la organización gestionará el riesgo, y debe establecerse ya que:

  > a) la gestión del riesgo tiene lugar en el contexto de los objetivos de la organización; b) los objetivos y los criterios de un proyecto, proceso o actividad en particular se deberían considerar a la luz de los objetivos de la organización como un todo; y c) algunas organizaciones fracasan en reconocer las oportunidades para alcanzar sus objetivos estratégicos, del proyecto o el negocio, y esto afecta la continuidad del compromiso, la credibilidad, la confianza y el valor de la organización (Instituto Colombiano de Normas Técnicas y Certificación, NTC-ISO, 2011, p.19).

  También, puede incluir:

gobierno, estructura de la organización, funciones y responsabilidades; políticas, objetivos y las estrategias implementadas para lograrlos; capacidades, entendidas en términos de recursos y conocimientos (por ejemplo capital, tiempo, personas, procesos, sistemas y tecnologías); las relaciones con las partes involucradas internas y sus percepciones y valores; la cultura de la organización; sistemas de información, flujos de información y procesos de toma de decisiones (tanto formales como informales); normas, directrices y modelos adoptados por la organización; y forma y extensión de las relaciones contractuales (p.19).

- **Establecimiento del contexto del proceso para la gestión del riesgo**: la norma recomienda establecer los objetivos, las estrategias, el alcance y los parámetros de las actividades de la organización (o de las partes donde se gestionará el riesgo), como también los recursos necesarios, las responsabilidades y autoridades, y los registros que se deben conservar. Asimismo, se puede realizar:

  definición de las metas y los objetivos de las actividades de gestión del riesgo; definición de las responsabilidades del proceso para la gestión del riesgo y dentro de este; definición del alcance, así como de la profundidad y extensión de las actividades de gestión del riesgo que se van a llevar a cabo, incluyendo las exclusiones e inclusiones específicas; definir actividad, proceso, función, proyecto, producto, servicio o activo en términos de tiempo y ubicación; definición de las relaciones entre el proyecto, el proceso o la actividad particulares y otros proyectos, procesos o actividades de la organización; definición de las metodologías para la valoración del riesgo; definición de la forma de evaluar el desempeño y la eficacia en la gestión del riesgo; identificación y especificación de las decisiones que se deben tomar; e identificación, establecimiento del alcance o el marco de los estudios necesarios, su extensión y objetivos, y los recursos necesarios para tales estudios (Instituto Colombiano de Normas Técnicas y Certificación, NTC-ISO, 2011, p.20).

- **Criterios del riesgo**: que se implementarán para evaluar su importancia. Estos deben reflejar los valores, objetivos y recursos de la organización, como también los requisitos

legales y demás que estén impuestos. De igual manera deben ser consecuentes con la política para la gestión del riesgo y se deben definir en primera instancia y revisarse continuamente. Entre estos se deben incluir (p.20):

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

- **Valorar el riesgo:** se define como el proceso total de identificación, análisis y evaluación del riesgo y se contempla en el apartado 5.4. Inicialmente propone la identificación del riesgo, explicando que se deben: "identificar las fuentes de riesgo, las áreas de impacto, los eventos (incluyendo los cambios en las circunstancias) y sus causas y consecuencias potenciales" (Instituto Colombiano de Normas Técnicas y Certificación, NTC-ISO, 2011, p.21), teniendo como objetivo crear una lista completa y correctamente realizada de riesgos, basándose en los eventos que puedan crear, aumentar, prevenir, degradar, acelerar o retrasar el logro de los objetivos. También, indica que "Es importante identificar los riesgos asociados a la no búsqueda de una oportunidad" (p.21), y que se debe realizar una identificación exhaustiva, ya que los riesgos que no se reporten en esta fase no recibirán el análisis posterior (p.21).

- **Identificación de riesgos:** se deben incluir los riesgos sin importar si la fuente de estos está o no bajo control por parte de la organización, ni si el origen o las causas son evidentes. También, se debe examinar los efectos colaterales de consecuencias particulares, incluyendo efectos en cascada y acumulativos, considerando un amplio rango de consecuencias, así el origen o causa del riesgo no sean evidentes, identificando así lo que podría suceder y teniendo en consideración todas las causas y consecuencias significativas (p.21).

Asimismo, la norma explica que las organizaciones deben aplicar herramientas y técnicas para identificar los riesgos que sean pertinentes para sus objetivos, capacidades y tipos de riesgo que enfrentan, donde la información pertinente y actualizada puede favorecer a la identificación de los riesgos y que sea realizado por personal con conocimiento apropiado (p.21).

- **Análisis de riesgos:** explicado en el apartado 5.4.3, donde se define como análisis el desarrollo y la comprensión del riesgo, el cual representa una entrada para evaluar el riesgo y tomar la decisión se si se debe o no tratar y cuáles serían las estrategias y métodos más adecuados. Se involucra también la consideración de las causas y las fuentes de riesgo, sus consecuencias tanto positivas y negativas, y la probabilidad de que estas puedan ocurrir. En cuanto se analiza el riesgo, se debe identificar los factores que afectan a las consecuencias y a la probabilidad, teniendo en cuenta que pueden existir consecuencias y afectaciones múltiples a partir de un evento y se deben considerar la eficacia y eficiencia de los controles existentes (p.21).

También, la forma de expresar y combinar las consecuencias y la probabilidad deben reflejar el tipo de riesgo, la información disponible y el propósito para el cual se va a usar la valoración, siendo consistente con los criterios del riesgo seleccionados y considerando la interdependencia entre los riesgos y sus fuentes. Asimismo, la confianza y sensibilidad en la determinación del riesgo debe ser consideradas y comunicadas eficazmente a los encargados de tomar las decisiones o a las partes involucradas, como también los "factores tales como la divergencia de opinión entre los expertos, la incertidumbre, la disponibilidad, la calidad, la cantidad y la pertinencia continua de la información, o los limitantes en el modelado se deberían establecer y se pueden enfatizar" (Instituto Colombiano de Normas Técnicas y Certificación, NTC-ISO, 2011, p.22).

La norma explica que el análisis puede ser efectuado con diferentes grados de detalle, los cuales dependen del riesgo, el propósito de su análisis y la información y los datos

y recursos que estén disponibles, como también puede ser cualitativo, semicuantitativo o cuantitativo, o una combinación de ellos, lo que depende de las circunstancias (p.22).

De igual manera, indica que las consecuencias y su probabilidad pueden determinarse mediante el modelamiento de los resultados de un evento o un grupo de sucesos, o a través de la extrapolación basada en estudios experimentales o datos disponibles. Asimismo, las consecuencias pueden ser expresadas en términos de impactos tangibles e intangibles, requiriéndose en algunos casos "más de un valor numérico o descriptor para especificar las consecuencias y su probabilidad en diferentes momentos, lugares, grupos o situaciones." (p.22).

- **Evaluar los riesgos:** el propósito de evaluar los riesgos es facilitar la toma de decisiones, basándose en los resultados del análisis, determinando cuáles necesitan tratamiento y la prioridad que requieren. De esta manera, la evaluación implica comparar el nivel de riesgo observado durante el análisis y los criterios del riesgo establecidos y así se puede considerar la necesidad de tratamiento (p.22).

  De igual forma, la norma explica que al tomar decisiones se debe tener en cuenta el contexto más amplio del riesgo y la tolerancia de los riesgos que acarrean otras partes diferentes de la organización que se benefician de estos, como también considerando los requisitos legales, reglamentarios y otros. Asimismo, puede tener lugar la decisión de emprender un análisis adicional, al igual que la decisión de no tratar el riesgo de ninguna manera diferente del mantenimiento de los controles existentes, por lo cual existirá una influencia por la actitud de la organización hacia el riesgo y por los criterios del riesgo que se han establecido (p.22).

- **Tratar el riesgo:** selección de una o más opciones para modificar los riesgos y su implementación, para seguidamente suministrar o modificar los controles. De esta manera, al tratar el riesgo se ve implicado un proceso cíclico de: "valoración del tratamiento del riesgo; decisión sobre si los niveles de riesgo residual son tolerables; si no son tolerables, generación de un nuevo tratamiento para el riesgo; y valoración de la

eficacia de dicho tratamiento." (Instituto Colombiano de Normas Técnicas y Certificación, NTC-ISO, 2011, p.22).

Estas opciones para el tratamiento no necesariamente son mutuamente excluyentes ni adecuadas en todas las circunstancias y hacen parte de estas:

> a) evitar el riesgo al decidir no iniciar o continuar la actividad que lo originó; b) tomar o incrementar el riesgo para perseguir una oportunidad; c) retirar la fuente de riesgo; d) cambiar la probabilidad; e) cambiar las consecuencias; f) compartir el riesgo con una o varias de las partes, (incluyendo los contratos y la financiación del riesgo); y g) retener el riesgo mediante una decisión informada (Instituto Colombiano de Normas Técnicas y Certificación, NTC-ISO, 2011, p.23).

Para seleccionar las opciones más adecuadas para el tratamiento del riesgo se debe mantener un equilibrio en los costos y los esfuerzos de la implementación frente a los beneficios derivados con respecto a los requisitos legales, reglamentarios y otros, tales como la responsabilidad social y la protección del ambiente. También, "en las decisiones se deberían considerar los riesgos que pueden ameritar el tratamiento que no es justificable en términos económicos, por ejemplo, los riesgos graves (consecuencia negativa alta) pero raros (baja probabilidad)" (p.23).

Se pueden seleccionar y aplicar las opciones que sean necesarias ya sea individualmente o en combinación, pero normalmente las organizaciones se pueden beneficiar adoptando una combinación de opciones de tratamiento. Cuando estas se seleccionen, se deben considerar los valores y las percepciones de las partes involucradas y su correcta y adecuada comunicación. De igual forma, si las opciones seleccionadas "pueden tener impacto en el riesgo en otras partes de la organización o para otras partes involucradas, estas opciones se deberían incluir en la decisión." (Instituto Colombiano de Normas Técnicas y Certificación, NTC-ISO, 2011, p.23).

Entonces, se debe crear un plan de tratamiento en el cual se debe identificar claramente el orden de prioridad para la implementación de los tratamientos individuales. Se debe considerar que el tratamiento en sí mismo puede introducir riesgos, tales como la falla o la ineficacia de las medidas del tratamiento por lo cual es necesario que el monitoreo sea parte integral del plan, para garantizar que las medidas sigan siendo eficaces. También puede introducir riesgos secundarios que se deben valorar, tratar, monitorear y revisar e incorporar en el mismo plan y no ser tratados como riesgos nuevos, siendo recomendable identificar y mantener el vínculo entre los dos riesgos (p.24).

Seguido a esto, se deben preparar e implementar estos planes, considerando que su propósito es documentar la forma en que se van a implementar las opciones de tratamiento seleccionadas. Estos deben incluir:

> las razones para la selección de las opciones de tratamiento, que incluyan los beneficios que se espera obtener; aquellos que son responsables de aprobar el plan y los responsables de implementarlo; acciones propuestas; requisitos de recursos, incluyendo las contingencias; medidas y restricciones de desempeño; requisitos de monitoreo y reporte; y tiempo y cronograma (Instituto Colombiano de Normas Técnicas y Certificación, NTC-ISO, 2011, p.24).

También, se deben integrar con los procesos de gestión de la organización y comunicar con las partes involucradas, quienes deberían conocer la naturaleza y la extensión del riesgo residual, el cual se debe documentar, monitorear, revisión y si es necesario tratar adicionalmente (p.24).

- **Monitoreo y revisión del riesgo**: este paso debe hacer parte de la planificación del proceso para la gestión del riesgo e incluir verificación o vigilancia continuas en los plazos que se consideren necesarios, estando las responsabilidades involucradas claramente definidas, y se deberán comprender todos los aspectos del proceso para la gestión del riesgo con el fin de:

> garantizar que los controles son eficaces y eficientes tanto en el diseño como en la operación; obtener información adicional para mejorar la valoración del riesgo; analizar y aprender lecciones a partir de los eventos (incluyendo los cuasi accidentes), los cambios, las tendencias, los éxitos y los fracasos; detectar cambios en el contexto externo e interno, incluyendo los cambios en los criterios del riesgo y en el riesgo mismo que puedan exigir revisión de los tratamientos del riesgo y las prioridades; e identificar los riesgos emergentes (Instituto Colombiano de Normas Técnicas y Certificación, NTC-ISO, 2011, p.24).

Por otra parte, los avances presentados en la implementación de los planes para tratamiento del riesgo generan una medida de desempeño, donde estos resultados pueden ser incorporados en las actividades globales de gestión del desempeño, medición y reporte externo e interno de la organización, como también ser registrados y reportados interna y externamente y usados como una entrada para la revisión del marco de referencia para la gestión del riesgo (p.25).

Como última medida, según la norma, se deberá registrar el proceso para la gestión del riesgo, de manera que las actividades para la gestión del riesgo tengan trazabilidad mediante los registros efectuados en el proceso para la gestión del riesgo funcionando como una base para la mejora de los métodos y las herramientas, así como del proceso global. En este paso, para la creación de registros se debería tener en cuenta (p. 25):

> las necesidades de la organización con respecto al aprendizaje continuo; los beneficios de reutilizar la información con propósitos de gestión; los costos y esfuerzos involucrados en la creación y el mantenimiento de los registros; las necesidades legales, reglamentarias y operativas para los registros; los métodos de acceso, la facilidad de recuperación y los medios de almacenamiento; el periodo de retención; y la sensibilidad de la información (Instituto Colombiano de Normas Técnicas y Certificación, NTC-ISO, 2011, p.25).

De esta manera finaliza la norma y sus especificaciones, las cuales se abarcarán en el tercer capítulo del presente documento, para realizar su aplicación y conjunción con las demás normas ISO que se retomarán en el modelo a construir

2. TIPOS DE RIESGO Y NORMAS ISO

A continuación, se presentarán los tipos de riesgo existentes y las respectivas normas ISO que abarcan su contexto, de manera que se implementará como marco referencial para el desarrollo del modelo final donde se establezcan todos los riesgos que se mencionarán, lo que especifica las normas y la aplicación del modelo de gestión de riesgos propuesto por la ISO 31000 explicada anteriormente.

2.1 Riesgo Ambiental

Para comenzar, se indagará en el riesgo ambiental que existe o puede llegar a existir en una organización. Según la revista Daphnia (1999), identificar y conocer los riesgos medioambientales que pueden estar asociados a las actividades productivas de una organización es la piedra angular para cualquier decisión, acción o actividad que se relacione con el cuidado y protección del medioambiente. Diariamente incrementa la importancia de conocer, con el mayor rigor posible, cuál es el impacto ambiental que generan o podrían generar las empresas, existiendo una presión continua por parte de numerosas iniciativas legislativas, económicas o formativas, cuyo eje de desarrollo es el concepto de riesgo medioambiental, para lograr su reducción o eliminación.

De igual manera, el artículo relaciona que la intervención sindical en el centro de trabajo, acerca de la identificación de riesgos medioambientales, encamina las actuaciones para conseguir empresas cuyo impacto en el medio ambiente sea sostenible, elaborando "Mapas de riesgos, de Buenas Prácticas y de Planes de Prevención" (Daphnia, 1999) que funcionen como medios de presión y participación de los empleados, "hasta la negociación, en los casos en que sea preciso, de una transición justa en aquellas empresas o sectores que requieran una reconversión ecológica de la producción" (Daphnia, 1999), como también presentando propuestas de implantación de sistemas de gestión medioambiental y haciendo partícipes a los trabajadores en estos. En congruencia, el artículo defiende que debido a intereses y percepciones distintas en la empresa, tales como la rentabilidad económica y la reducción de costos, la identificación y valoración de los riesgos debe hacerse autónomamente por parte de los empleados y así establecer la estrategia a seguir.

Posteriormente, se define el riesgo medioambiental como “toda circunstancia o factor que conlleva la posibilidad de un daño para el medio ambiente” (Daphnia, 1999). De esta forma, explica que “cualquier propiedad, condición o circunstancia en que una sustancia, un producto, una instalación, un equipo o un proceso puede ocasionar un daño directo a la cantidad o a la calidad del suelo, del agua, del aire, de los ecosistemas o indirecto a personas o bienes como consecuencia de los anteriores.” (Daphnia, 1999), es lo que generaría un riesgo medioambiental. Así, fundamenta que los trabajadores deberían contemplar entre sus funciones “aplicar los conocimientos y experiencias existentes a la realidad concreta de su centro de trabajo” (Daphnia, 1999).

El artículo presenta también una manera de identificar y evaluar un determinado riesgo, entre las cuales está conocer:

a) Las fuentes de riesgo presentes: esto a través de medios como “publicaciones, estudios, diagnósticos emitidos por expertos o consultores especializados, normas y disposiciones de carácter legal, etc.” (Daphnia, 1999).

b) Los identificadores del riesgo: los cuales “indican dónde y cómo actúan las fuentes de riesgo en las condiciones concretas de una empresa” (Daphnia, 1999).

c) Los efectos o consecuencias del riesgo: que reflejan “los daños que puedan ocasionar en el medio natural” (Daphnia, 1999).

Para la valoración del riesgo, el artículo presenta la forma tradicional que está dada por la fórmula: Riesgo = Probabilidad x Daño, de manera que, al igual que se explica en la norma ISO 31000, el valor del riesgo depende de los valores de probabilidad y daño escogidos en el sistema de evaluación. También es necesario considerar:

> la probabilidad de accidente, la exposición prolongada, los posibles escenarios en que se producen los sucesos anteriores y las consecuencias valorando: la intensidad (grado de incidencia en el medio por cantidad o peligrosidad), la extensión (área de influencia), la persistencia (tiempo que dura el efecto), la reversibilidad (posibilidad

de recuperar las condiciones iniciales) y las características del medio (el valor medioambiental del medio donde se produce) (Daphnia, 1999).

Un dato de gran relevancia presentado en el artículo de la revista Daphnia (1999) es que los riesgos medioambientales se identifican en el lugar de trabajo basándose en la formación específica y el conocimiento de los procesos productivos, las instalaciones, los productos usados, el tratamiento de los residuos, entre otros. Por otra parte, existe personal encargado de identificarlos, tales como: consultores externos cualificados para ello y que ofrecen este servicio mediante auditoría normalmente, técnicos de la propia empresa que se especialicen en gestión medioambiental, delegados de prevención, quienes tienen la ventaja de conocer los procedimientos, tener acceso a la información y conocer bien el lugar de trabajo. Por otra parte, existen sindicatos que han desarrollado metodologías propias para identificar y evaluar los riesgos medioambientales.

También, el artículo explica que se realiza un análisis de riesgo cruzando las fuentes, que están asociadas a las instalaciones y procesos de producción, con los elementos que componen el entorno natural y humano de la empresa. Este análisis puede ser: Integral, cuando está "destinado a conocer el impacto ambiental global de una instalación, a partir del estudio de todos los peligros asociados a la planta. Este es el procedimiento necesario para implantar sistemas de gestión medioambiental, realizar las evaluaciones de impacto ambiental, etc." (Daphnia, 1999), o Parcial, cuando se pretende "conocer los riesgos asociados a una o varias fuentes de riesgo importantes. Puede ser suficiente para PYMES o empresas cuyos procesos productivos sean sencillos" (Daphnia, 1999).

Respecto a las fuentes de riesgo, se informa que están asociadas a:

Peligros relacionados con materias primas, subproductos del proceso y productos finales. Hay que conocer la naturaleza y características de toxicidad de las sustancias (inflamable, explosivo, corrosivo, daña la capa de ozono, afecta a las especies acuáticas, etc.), las cantidades utilizadas, su almacenamiento y envasado.

Peligros relacionados con el almacenamiento. Hay que conocer las áreas dedicadas a almacenamiento, que sustancias son almacenadas y como, las formas de transporte y los efectos que pueden producirse en caso de accidente, fuga o desperfectos.

Peligros relacionados con los procesos de producción o con la prestación de servicios. Hay que conocer el uso y trasiego de las sustancias peligrosas, los efectos del mal funcionamiento de componentes y equipos, fallo de los sistemas de seguridad, control y mantenimiento, etc.

Peligros relacionados con la gestión de la empresa. Hay que conocer las deficiencias de formación, de información, de documentación, de organización del trabajo, así como los incumplimientos de la legislación vigente.

Peligros relacionados con los residuos, vertidos y emisiones. Hay que conocer el impacto en el medio, las autorizaciones, el tratamiento, la caracterización, inventario, colectores, chimeneas, control y mecanismos de vigilancia, etc.

Peligros de otras instalaciones o infraestructuras. Hay que conocer los procesos de refrigeración, la alimentación eléctrica, las plantas de depuración, y cualquier función auxiliar que se necesite para la actividad principal de la planta.

Peligros relacionados con los productos o servicios objeto de la actividad de la empresa. Ciclo de vida. Los elementos que componen el entorno natural y humano son:

a. Medio Inerte. Hay que conocer los efectos sobre las condiciones climáticas locales y regionales, sobre la calidad del aire, sobre la calidad y cantidad de los recursos hídricos, tanto superficiales como subterráneos y sobre la calidad y el uso de los suelos.

b. Medio biótico. Hay que conocer los efectos sobre la fauna, flora y sobre la estructura y diversidad de los distintos ecosistemas presentes en el entorno.

c. Otros aspectos importantes son las afecciones al paisaje y a los espacios naturales protegidos.

d. Entorno humano. Hay que conocer la influencia sobre la población, las actividades económicas con incidencia ambiental (agricultura, ganadería, minería), infraestructuras (canalización de agua, tratamiento local de

> residuos, redes eléctricas y de transporte), salud pública y sobre el patrimonio histórico, artístico y cultural (Daphnia, 1999).

En congruencia, el artículo expone la metodología de identificación de riesgos medioambientales SAT, la cual no es una auditoría normalizada, pero si se garantiza un correcto conocimiento del lugar de trabajo, los procesos de producción que se realicen y cómo está organizado; "La formación medioambiental adquirida. La información documentada en la empresa y de su acceso a ella. La posibilidad de apoyo técnico externo. La colaboración de la dirección de la empresa" (Daphnia, 1999), de manera que se podrán garantizar resultados de gran calidad similares a los de una auditoría. De esta manera, se pueden realizar evaluaciones globales o parciales.

En la evaluación global se deberá indagar en la disponibilidad de la información relacionada con los permisos necesarios, la legislación que se deba cumplir, los datos generales de la instalación, el consumo de agua, energía, materias primas, el análisis de vertidos y emisiones, residuos producidos, etc., al igual que aprovechar la experiencia laboral de los trabajadores para averiguar en los puestos de trabajo más significativos: "Las materias utilizadas, sus características contaminantes y las cantidades empleadas y los productos y subproductos, los residuos, vertidos y emisiones gaseosas." (Daphnia, 1999). De esta manera, se obtendrá como resultado un mapa de riesgos como un informe documentado, en el cual se indica la fuente de riesgo, "su localización en la empresa (sección, puesto de trabajo…), su valoración cuantitativa y cualitativa y los efectos o repercusiones que puede tener en el medio ambiente y en la salud laboral" (Daphnia, 1999).

Por otra parte, según Daphnia (1999), en la *evaluación parcial* se deben seleccionar los factores de riesgo sobre los que se actuará, recolectar la información disponible sobre estos, y realizar el seguimiento del itinerario de los estos en la empresa, entre lo cual se contempla desde la adquisición o aparición de los mismo hasta la salida de los procesos, ya sea como producto final o como subproductos residuales.

Más adelante, se exponen los elementos de esta metodología explicada, entre los cuales están:

> La sensibilización social medioambiental con el fin de incentivar la responsabilidad de cada empleado en la protección del medio natural, desde desempeñar sus obligaciones hasta modificar sus actitudes y comportamientos; aprovechar la experiencia y conocimiento de los empleados para la identificación de riesgos; motivar la participación activa y consciente por parte de los empleados en los planes acordados mediante: "asambleas, reparto de boletines, hojas informativas…, cursos de formación y reuniones y grupos de trabajo de comités y delegados de prevención (Daphnia, 1999).

La evaluación de riesgos laborales, y ya que existe una profunda relación entre la salud laboral y el medioambiente, se deben considerar para la identificación de riesgos medioambientales que: muchas sustancias que son nocivas para el ser humano son también contaminantes del medio natural; los procedimientos de evaluación son similares, por loque se puede indagar en otras metodologías, y que existe una propuesta de integrar la gestión medioambiental con la gestión de la calidad, de la seguridad industrial y de la salud ocupacional. De esta manera, se podría realizar una evaluación de los riesgos cambiando los identificadores de riesgo en salud laboral por los de medio ambiente, y considerando aspectos como "el consumo excesivo de materias primas, agua y energía y el ciclo de vida de los productos o servicios que la empresa pone en el mercado" (Daphnia, 1999).

Y, finalmente los acuerdos voluntarios que se han empleado ya que muchas veces se torna insuficiente la legislación para el cumplimiento del cuidado del medioambiente. Estos, "exigen como requisito el compromiso de alcanzar una «mejora continua» de los resultados ambientales" (Daphnia, 1999). Así, el documento explica que esto se puede lograr mediante la sensibilización medioambiental donde se compromete a los empleados a participar en la identificación de riesgos y en las actuaciones sobre ellos.

Por último, el artículo expone los beneficios potenciales de identificar los riesgos medioambientales, los cuales se comprenden por los beneficios derivados de: la sensibilización, la identificación de riesgos y del cumplimiento del plan de prevención (Daphnia, 1999). Con respecto a las campañas de sensibilización, se ve incrementa la participación de los trabajadores en la protección del ambiente y fomenta o refuerza el compromiso empresarial.

Con respecto a la identificación, según Daphnia (1999) el reconocimiento de los riesgos ambientales y el compromiso de actuar sobre ellos generan mejoras del medio natural, de la calidad de vida y de las condiciones de trabajo y salud laboral, como también mejorar su imagen corporativa, la cual representa efectos inmediatos sobre los clientes, los proveedores, las compañías de seguros, las entidades financieras y las administraciones y, genera una base sólida para la implantación de gestión ambiental, facilitando la obtención de la certificación según las norma ISO 14001, entre otras entidades, donde se ven mayormente beneficiadas las PYMES, por su tamaño y las características de sus procesos productivos.

Y, con respecto a los beneficios del cumplimiento del plan de prevención, explica que este consta de medidas inmediatas para minimizar los peligros potenciales y el inicio del proceso investigativo para determinar las alternativas técnicas y organizativas que puedan eliminar estos riesgos. En las medidas inmediatas se encuentran las medidas de protección, para disminuir los riesgos medioambientales y algunos efectos positivos como la reducción de la probabilidad de accidentes, del riesgo de multas, etc., las medidas de buenas prácticas, para la reducción de costes debido al ahorro en el consumo de energía, de materias primas, de agua, mantenimiento, etc., como también optimizar la organización del trabajo (Daphnia, 1999).

Asimismo, se puede complementar esta información con las fuentes de riesgo expuestas por la Escuela Europea de Excelencia (2018), donde relacionan que se debe tener en cuenta:

> Los elementos externos a la instalación: infraestructuras y fuentes, estructura fábrica, agua, gas, electricidad, etc. Rasgos y características de las instalaciones cercanas. Naturales, tales como físicos (tornados, maremotos, erupciones, etc.). Biológicos (proliferación de algas, plagas, etc.) Socioeconómicos: vandalismo, sabotaje, terrorismo, etc.
>
> Las actividades e instalaciones: almacenajes de combustibles, productos acabados, productos semiacabados, recursos energéticos y materias primas. Procesos y elementos necesarios para la producción: equipos informáticos, maquinaria, etc., situación del proceso, uso de sustancias para la actividad empresarial, disposición, gestión del mantenimiento, etc., medidas de seguridad, situación del entorno.

Procesos e instalaciones auxiliares: producción de calor, protección contra incendios, producción de frío, producción de energía eléctrica, tratamiento de agua para procesos e instalaciones, ruidos y vibraciones, instalaciones para prevenir y tratar la contaminación, depuración de aguas residuales, tratamiento de emisiones a la atmósfera, almacenamiento y tratamiento de residuos.

El factor humano: En el ámbito organizativo, estructura, sistemas de gestión, cultura preventiva, procedimientos, comunicación interna y externa, condiciones ambientales del puesto de trabajo, ambiente laboral. En el ámbito individual, formación, entrenamiento, capacitación, errores humanos (Escuela Europea de Excelencia, 2018).

Además, se explica que una vez identificadas las causas y los peligros que se puedan encontrar, se procederá a identificar los sucesos iniciadores, ya que si estos se evidencian, se podrá "identificar y hallar una solución para el riesgo y determinar mejor el escenario accidental y sus posibles consecuencias obteniendo una gestión del riesgo más sencilla" (Escuela Europea de Excelencia, 2018).

Posterior a su identificación, se postularán los escenarios de accidentes, donde se valoran posibles sucesos y la probabilidad de que estos ocurran en diferentes escenarios de accidente, para con esta probabilidad calculada, se estimarán las consecuencias potencias en un árbol de sucesos. Seguido a esto, se procederá a asignar la probabilidad del escenario de accidente, lo cual resulta de combinar las probabilidades del árbol de sucesos. Respecto a esto, existen diferentes criterios, entre los cuales se encuentran los antecedentes del sector o la actividad, la bibliografía especializada, la información de los proveedores y fabricantes y los antecedentes de accidentes en la empresa. Así, la siguiente fase consiste en estimar las consecuencias asociadas al escenario de accidente, donde se calcularán los daños que cada escenario podría generar en el medio ambiente, a través de métodos cuantitativos o cualitativos, teniendo en cuenta el entorno natural, humano y socioeconómico. Finalmente, se procede a la fase de estimación del riesgo, en la cual se debe considerar la definición de riesgo, la identificación de los posibles escenarios de accidente, la asignación de la probabilidad de que ocurran y sus consecuencias (Escuela Europea de Excelencia, 2018).

2.2 Norma ISO 14001

Por otra parte, la norma ISO 14001 (2015) es la encargada de especificar los lineamientos acerca del sistema de Gestión Ambiental y sus requisitos. A continuación, se presentará un resumen de los principios establecidos en la norma, haciendo énfasis en el apartado de Planificación.

Inicialmente, esta norma plantea los requisitos para un sistema de gestión ambiental que pueden implementarse por una organización para mejorar su desempeño ambiental. De esta manera, ayuda a las organizaciones a lograr los resultados deseados, aportando al medio ambiente y a las partes interesadas, entre los cuales está contemplado: "la mejora del desempeño ambiental; el cumplimiento de los requisitos legales y otros requisitos; el logro de los objetivos ambientales" (Instituto Colombiano de Normas Técnicas y Certificación, NTC-ISO, 2015, p.1). También, se especifica que se puede aplicar a cualquier organización y a los aspectos ambientales de sus actividades, productos y servicios tomando en consideración una perspectiva de ciclo de vida (p. 1).

De esta manera, para comenzar se deben determinar las cuestiones externas e internas de la organización que son pertinentes para su propósito y afectan su capacidad para cumplir los resultados planteados en su sistema de gestión ambiental, incluyendo las condiciones ambientales que puedan afectar o verse afectadas por la organización. Asimismo, se debe garantizar la comprensión de las necesidades y expectativas de las partes interesadas, determinando: "las partes interesadas que son pertinentes al sistema de gestión ambiental; las necesidades y expectativas pertinentes (es decir, requisitos) de estas partes interesadas; cuáles de estas necesidades y expectativas se convierten en requisitos legales y otros requisitos" (Instituto Colombiano de Normas Técnicas y Certificación, NTC-ISO, 2015, p. 6).

De igual forma, la organización debe establecer los límites y la aplicabilidad del sistema de gestión ambiental determinando así el alcance, considerando también: los aspectos externos e internos; los requisitos legales y otros requisitos; "las unidades, funciones y límites físicos de la organización; sus actividades, productos y servicios; su autoridad y capacidad para ejercer control e influencia." (Instituto Colombiano de Normas Técnicas y Certificación, NTC-ISO, 2015, p. 6 y 7). Definido el alcance, se deben incluir todas las actividades, productos y servicios de la organización, que estén dentro de este, en el sistema de gestión

ambiental, y se deberá conservar y estar disponible como información documentada para las partes interesadas (p. 7).

Finalizando el apartado 4 de la norma, se indica que es necesario establecer, implementar, mantener y mejorar continuamente un sistema de gestión ambiental, con el fin de lograr los resultados previstos, incluyendo la mejora del desempeño ambiental, en el cual se incluyan los procesos necesarios y sus interacciones, como también el contexto y las partes interesadas de la organización, de acuerdo con los requisitos que se presentan en esta norma (p.7).

En el apartado 5 se relacionan todos los requisitos acerca del liderazgo, indicando inicialmente que debe existir liderazgo y compromiso por parte de la dirección, con respecto al sistema de gestión ambiental,

> asumiendo la responsabilidad y la rendición de cuentas con relación a la eficacia del sistema de gestión ambiental; asegurándose de que se establezcan la política ambiental y los objetivos ambientales, y que éstos sean compatibles con la dirección estratégica y el contexto de la organización; asegurándose de la integración de los requisitos del sistema de gestión ambiental en los procesos de negocio de la organización; asegurándose de que los recursos necesarios para el sistema de gestión ambiental estén disponibles; comunicando la importancia de una gestión ambiental eficaz y conforme con los requisitos del sistema de gestión ambiental; asegurándose de que el sistema de gestión ambiental logre los resultados previstos; dirigiendo y apoyando a las personas, para contribuir a la eficacia del sistema de gestión ambiental; promoviendo la mejora continua; apoyando otros roles pertinentes de la dirección, para demostrar su liderazgo en la forma en la que aplique a sus áreas de responsabilidad (Instituto Colombiano de Normas Técnicas y Certificación, NTC-ISO, 2015, p. 7).

En seguida, se establece uno de los aspectos más relevantes dentro de la organización el cual es la política ambiental, que acorde al sistema de gestión ambiental, se debe establecer, implementar y mantener, de manera que: esté acorde al propósito y contexto de la organización, incluyendo la naturaleza, magnitud e impactos ambientales de sus tareas,

productos y servicios; brinde un marco de referencia para establecer los objetivos ambientales; contenga un compromiso de protección del medio ambiente, como también la prevención de la contaminación y otros compromisos específicos correspondientes según el contexto de la organización, tales como el uso sostenible de recursos, la mitigación y adaptación al cambio climático y la protección de la biodiversidad y de los ecosistemas; contenga un compromiso de llevar a cabalidad los requisitos legales y otros requisitos; contenga un compromiso para mejorar continuamente el sistema de gestión ambiental con el fin de mejorar el desempeño ambiental (p. 8).

También, la dirección se debe asegurar de que las responsabilidades y autoridades que se establezcan sean comunicados dentro de la organización, incluyendo entre estas: el aseguramiento de que el sistema de gestión ambiental concuerda con los requisitos establecidos en esta norma, y que la información sea comunicada adecuadamente acerca del desempeño del sistema de gestión ambiental, incluyendo el desempeño ambiental (p. 8).

Posteriormente, en el apartado 6 se mencionan los aspectos pertinentes para el desarrollo de este capítulo y el complemento para la aplicación de la norma ISO 31000 en los riesgos ambientales. De esta manera, se indica que al momento de planear el sistema de gestión ambiental, además de considerar todos los requisitos mencionados anteriormente, se deben determinar los riesgos y oportunidades relacionados con los aspectos ambientales, los requisitos legales y otros requisitos, los cuales se mencionarán más adelante, de forma que se asegure que el sistema de gestión ambiental pueda lograr los resultados previstos; que se puedan prevenir o reducir los efectos no deseados, como también la posibilidad de que condiciones ambientales externas influyan en la organización y que se logre la mejora continua. Asimismo, dentro del alcance del sistema de gestión ambiental se deben determinar las situaciones de emergencia potenciales, incluyendo las que puedan generar un impacto ambiental (p. 9).

Con respecto a los aspectos ambientales mencionados, se deben considerar los relacionados a las actividades, productos y servicios que pueda controlar la organización, como también en los que puede influir y su impacto ambiental desde la perspectiva del ciclo de vida. Estos se deben incluir dentro del alcance definido del sistema de gestión ambiental. Asimismo, se debe considerar si hay cambios o modificaciones en las actividades, productos y servicios, las condiciones anormales y las situaciones de emergencia que sean previsibles.

Además, se deberán considerar los aspectos que tengan o puedan tener un impacto ambiental significativo (aspectos ambientales significativos), mediante el uso de los criterios estipulados (p. 10).

Con respecto a los requisitos legales y otros requisitos mencionados, la organización deberá: determinar y tener acceso a los requisitos legales y otros requisitos relacionados con sus aspectos ambientales; determinar cómo estos requisitos legales y otros requisitos se aplican a la organización; tener en cuenta estos requisitos legales y otros requisitos cuando se establezca, implemente, mantenga y mejore continuamente su sistema de gestión ambiental (p. 10).

Posteriormente, la norma indica que la organización debe planificar las acciones que se van a tomar para abordar los aspectos ambientales significativos, los requisitos legales y otros requisitos y los riesgos y oportunidades que se identificaron anteriormente; también, la manera en que se integrarán e implementarán acciones en los procesos del sistema de gestión ambiental y demás procesos y cómo se evaluará la eficacia de estas. Una vez finalizada la etapa de planificación, se deberán considerar las opciones tecnológicas y sus requisitos financieros, operacionales y de negocio (p. 10).

En el apartado 6.2 se explican los objetivos ambientales y la planificación para lograrlos, dando inicio con que estos deben establecerse para las funciones y niveles pertinentes, considerando los aspectos ambientales significativo, los requisitos legales y otros requisitos asociados, y teniendo en cuenta sus riesgos y oportunidades. Estos objetivos deben: "ser coherentes con la política ambiental; ser medibles (si es factible); ser objeto de seguimiento; comunicarse; actualizarse, según corresponda" (Instituto Colombiano de Normas Técnicas y Certificación, NTC-ISO, 2015, p. 11).

Respecto a la planeación de las acciones para lograrlos, la organización debe determinar: "qué se va a hacer; qué recursos se requerirán; quién será responsable; cuándo se finalizará; cómo se evaluarán los resultados, incluidos los indicadores de seguimiento de los avances para el logro de sus objetivos ambientales medibles" (Instituto Colombiano de Normas Técnicas y Certificación, NTC-ISO, 2015, p. 11). Además, se debe considerar cómo integrar las acciones a los procesos de negocio de la organización (p. 11).

Por otra parte, en el apartado 7 de la norma se explican el apoyo que se debe brindar por parte de la organización, comenzando por "determinar y proporcionar los recursos

necesarios para el establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión ambiental" (p. 11). También, debe determinar la competencia necesaria de las personas que pueda afectar el desempeño ambiental y sus capacidades para cumplir los requisitos, asegurar su competencia (educación, experiencia), establecer las necesidades de formación asociadas con los aspectos ambientales y el sistema y adquirir la competencia necesaria (por ejemplo la formación, tutoría o reasignación de los empleados o la contratación o subcontratación de personal competentes) y evaluar la eficacia de las acciones ejercidas (p. 12).

Asimismo, la organización debe asegurarse de que las personas sean conscientes de:

> la política ambiental, los aspectos ambientales significativos y los impactos ambientales reales o potenciales relacionados, asociados con su trabajo; su contribución a la eficacia del sistema de gestión ambiental, incluidos los beneficios de una mejora del desempeño ambiental; las implicaciones de no satisfacer los requisitos del sistema de gestión ambiental, incluido el incumplimiento de los requisitos legales y otros requisitos de la organización (Instituto Colombiano de Normas Técnicas y Certificación, NTC-ISO, 2015, p. 12).

Posteriormente, se debe establecer, implementar y mantener la comunicación interna y externa pertinentes al sistema de gestión ambiental, indicando qué se debe comunicar, cuándo, a quién y cómo, y garantizar que la información sea coherente y fiable con la información generada dentro del sistema de gestión ambiental. Con respecto a la comunicación interna, se debe: "comunicar internamente la información pertinente del sistema de gestión ambiental entre los diversos niveles y funciones de la organización, incluidos los cambios en el sistema de gestión ambiental" (p.13), como también en la comunicación externa, y "asegurarse de que sus procesos de comunicación permitan que las personas que realicen trabajos bajo el control de la organización contribuyan a la mejora continua." (Instituto Colombiano de Normas Técnicas y Certificación, NTC-ISO, 2015, p. 13).

También, se deberá mantener toda la información documentada de los requisitos expuestos en todos los apartados de la norma, de manera que al momento de crear y actualizar

la información, se asegure la identificación y descripción, el formato y los medios de soporte y la revisión y aprobación. Asimismo, se debe controlar esta información, asegurando que "esté disponible y sea idónea para su uso, dónde y cuándo se necesite; esté protegida adecuadamente (por ejemplo, contra pérdida de confidencialidad, uso inadecuado, o pérdida de integridad)." (Instituto Colombiano de Normas Técnicas y Certificación, NTC-ISO, 2015, p.13). De manera que se aborde su "distribución, acceso, recuperación y uso; almacenamiento y preservación, incluida la preservación de la legibilidad; control de cambios (por ejemplo, control de versión); conservación y disposición" p. 13).

Por otra parte, en el apartado 8 se relacionan los requisitos correspondientes a la operación. Inicialmente se debe establecer, implementar, controlar y mantener los procesos pertinentes para cumplir los requisitos del sistema de gestión ambiental e implementar las acciones determinadas en el apartado 6, realizándolo a través del establecimiento de criterios de operación para los procesos y la implementación del control de los procesos de acuerdo con los criterios de operación. Asimismo, se deben controlar los cambios planificados y examinar las consecuencias de cambios que no sean previstos, tomando acciones para eliminar los efectos adversos. De igual forma, los procesos que sean contratados externamente deben estar controlados o se debe tener influencia sobre ellos, estableciendo dentro del sistema de gestión ambiental el tipo y grado de control o influencia que se va a aplicar (p.14 y 15).

En congruencia a la perspectiva del ciclo de vida, la organización debe

> establecer los controles, según corresponda, para asegurarse de que sus requisitos ambientales se aborden en el proceso de diseño y desarrollo del producto o servicio, considerando cada etapa de su ciclo de vida; determinar sus requisitos ambientales para la compra de productos y servicios, según corresponda; comunicar sus requisitos ambientales pertinentes a los proveedores externos, incluidos los contratistas; considerar la necesidad de suministrar información acerca de los impactos ambientales potenciales significativos asociados con el transporte o la entrega, el uso, el tratamiento al fin de la vida útil y la disposición final de sus productos o servicios (Instituto Colombiano de Normas Técnicas y Certificación, NTC-ISO, 2015, p. 15).

Además, la organización debe establecer, implementar y mantener los procesos necesarios para la preparación y respuesta ante situaciones potenciales de emergencia identificadas en el apartado 6, de manera que esté preparada para responder, a través de la planeación de las acciones para prevenir o mitigar los impactos ambientales ajenos generados por situaciones de emergencia, ante situaciones reales, tomando acciones para prevenir o mitigar las consecuencias de estas situaciones, que sean apropiadas a su magnitude impacto ambiental potencial, probando periódicamente las acciones de respuesta planificadas, evaluando y revisando continuamente los procesos y acciones, en especial después de que hayan ocurrido o se hayan realizado pruebas, e informando y formando segúncorresponda a las partes interesadas pertinentes, incluidas las personas que trabajan bajo su control (p. 15).

En el apartado 9 se mencionan los requisitos para la evaluación del desempeño ambiental y la eficacia del sistema de gestión ambiental, explicando que la organización debe realizar seguimiento, medir, analizar y evaluar su desempeño ambiental, determinando qué aspectos requieren seguimiento y medición, cuáles métodos de seguimiento, medición, análisis y evaluación se implementarán para asegurar resultados acertados, contra qué criterios se evaluará el desempeño ambiental y sus respectivos indicadores, las fechas en que se llevarán a cabo el seguimiento y la medición y cuándo se analizarán y evaluarán estos resultados. También, se debe asegurar de que los equipos de seguimiento y medición que se usan estén calibrados o verificados. En congruencia al anterior apartado, se debe garantizar la comunicación externa e interna del desempeño ambiental según los procesos de comunicación y los requisitos. De esta manera, se debe establecer, implementar y mantener los procesos necesarios para la evaluación del cumplimiento de losrequisitos, determinando la frecuencia con que se evaluará, realizando las acciones necesarias y conociendo y comprendiendo su estado, manteniendo esta evaluación documentada (p. 16).

Más adelante, en el apartado 9.2 se destaca que las organizaciones deberán implementar auditorías internas en intervalos planeados para garantizar que el sistema de gestión se encuentra en conformidad con los requisitos propios para este y los requisitos de la norma, y que se implementa y mantiene de manera eficaz. Respecto al programa, este deberá incluir la frecuencia, los métodos, las responsabilidades, los requisitos de planificación y la elaboración de informes, considerando la importancia ambiental de los procesos involucrados, los cambios que afectan a la organización y los resultados de las

auditorías previas. Así, se deben: "definir los criterios de auditoría y el alcance para cada auditoría; seleccionar los auditores y llevar a cabo auditorías para asegurarse de la objetividad y la imparcialidad del proceso de auditoría; asegurarse de que los resultados de las auditorías se informen" (Instituto Colombiano de Normas Técnicas y Certificación, NTC-ISO, 2015, p. 17).

Posteriormente, la dirección deberá revisar el sistema de gestión en los intervalos planeados, para asegurar su conveniencia, adecuación y eficacia continuas, considerando también el estado de las acciones que se tomaron en revisiones previas, los cambios en los aspectos internos y externos que tengan relevancia en el sistema, las prioridades de las partes interesadas y los requisitos tanto legales como de diferente índole, los aspectos ambientales significativos, los riesgos y las oportunidades, el grado de cumplimiento y logro de los objetivos ambientales, la información acerca del desempeño ambiental, incluyendo las tendencias relativas a: "no conformidades y acciones correctivas; resultados de seguimiento y medición; cumplimiento de los requisitos legales y otros requisitos; resultados de las auditorías" (Instituto Colombiano de Normas Técnicas y Certificación, NTC-ISO, 2015, p. 18), que los recursos sean adecuados, la correcta comunicación (incluyendo quejas) y las oportunidades de mejora continua. Como salidas de esta revisión, se incluirán:

> las conclusiones sobre la conveniencia, adecuación y eficacia continuas del sistema de gestión ambiental; las decisiones relacionadas con las oportunidades de mejora continua; las decisiones relacionadas con cualquier necesidad de cambio en el sistema de gestión ambiental, incluidas los recursos; las acciones necesarias cuando no se hayan logrado los objetivos ambientales; las oportunidades de mejorar la integración del sistema de gestión ambiental a otros procesos de negocio, si fuera necesario; cualquier implicación para la dirección estratégica de la organización (Instituto Colombiano de Normas Técnicas y Certificación, NTC-ISO, 2015, p. 18).

Finalmente, en el apartado 10 se especifican los aspectos para las oportunidades de mejora identificadas en el apartado 9 e implementar las acciones para lograr los resultados previstos en el sistema de gestión. De esta manera, cuando ocurra una no conformidad se deberá reaccionar a esta, tomando acciones para controlarla y corregirla, afrontar las

consecuencias (también la mitigación del impacto ambiental), evaluar si se requiere tomar acciones para eliminar sus causas, para que no vuelva a ocurrir, revisarla, determinar sus causas, identificar si existen similares o que puedan ocurrir de la misma forma, llevar a cabo las acciones necesarias y revisar su eficacia y si es necesario realizar modificaciones al sistema de gestión ambiental. Asimismo, se deberá mejorar continuamente la conveniencia, adecuación y eficacia del sistema de gestión ambiental para mejorar el desempeño ambiental (p. 19).

Para concluir con el marco de referencia del riesgo ambiental, en los anexos del presente documento se recolectarán algunas de las normativas generales en Colombia que respectan a la protección del medio ambiente.

2.3 Riesgo en la Salud y Seguridad en el Trabajo

En este apartado se tomarán los parámetros dados por la Oficina Internacional del Trabajo, en un documento donde se explica la importancia de la salud y seguridad en el trabajo, los riesgos que se corren, la manera de identificar las causas y las problemáticas que se generan al no considerar y tratar estos riesgos.

Para comenzar, la OIT (s.f.) indica que la salud y seguridad en el trabajo es una disciplina que tiende a: fomentar y mantener el mayor bienestar posible tanto físico y mental como social de los empleados, independientemente de su ocupación, prevenir las condiciones negativas en la salud de los trabajadores que se puedan desarrollar por su labor, proteger a los empleados de los riesgos que puedan conllevar efectos en la salud, ubicar y mantener a los trabajadores en un espacio laboral que se adapte a sus necesidades físicas o mentales y adaptar las actividades para que las pueda desarrollar una persona. Asimismo, indica que para el logro de estos objetivos competen se requiere la colaboración y la participación de directivos y empleados en programas de salud y seguridad, en los cuales se deben considerar los aspectos que se en la medicina laboral, la higiene industrial, la toxicología, la formación, la seguridad técnica, la ergonomía, la psicología, entre otros, y que también se abarca el tema de la seguridad laboral en su aspecto más amplio (p.2).

Teniendo en cuenta esta definición y los responsables, posteriormente se explican los aspectos generales de cómo las malas condiciones laborales influyen en la salud yseguridad

de los empleados, exponiendo que estas se pueden dar en cualquier contexto y ambiente, y que en los casos en que el entorno laboral es el mismo donde viven los empleados, se pueden presentar afectaciones no solo a estos, sino que también a sus familias y personas que los rodean. En consideración, la salud y seguridad laboral tiene como objeto evitar los accidentes y las enfermedades laborales, teniendo en cuenta también el lugar donde se desempeña el trabajo y el entorno fuera de este (p. 3).

La importancia de la salud y seguridad en el trabajo es el fundamento de esta disciplina, de manera que se expone que la mayoría de los empleados trabajan al menos 8 horas al día en el espacio que se les ha dispuesto, lo cual hace significativo que su permanencia en la oficina, un taller industrial, etc., sea seguro y sano, en especial cuando se exponen a polvos, gases, ruidos, vibraciones y temperaturas extremadas. Sin embargo, según la OIT, los empleadores no siempre conocen que tienen la responsabilidad de garantizar la salud y seguridad de sus empleados en el área de trabajo; así, los riesgos a los que se exponen constantemente es la razón de que abunden los accidentes y las enfermedades profesionales (p. 3).

Adicional al riesgo que se corre con estos accidentes, existe una implicación económica para los empresarios, ya que estos, como se expone en el documento, "son muy costosos y pueden tener muchas consecuencias graves, tanto directas como indirectas, en las vidas de los trabajadores y de sus familias" (OIT, s.f., p. 3). De esta manera, algunos costos directos que pueden tener los empleados son: "el dolor y el padecimiento de la lesión o la enfermedad, la pérdida de ingresos, la posible pérdida de un empleo y los costos queacarrea la atención médica" (OIT, s.f., p. 4). En adición, respecto a los costos indirectos, según la OIT (s.f.) pueden ser hasta diez veces (o más) mayores que los directos, y que, por ejemplo, el padecimiento de la familia del empleado no puede ser remunerado con dinero.

Para los empleadores, se incluyen entre los costos directos:

> pagar un trabajo no realizado, los pagos que hay que efectuar en concepto de tratamiento médico e indemnización, la reparación o la sustitución de máquinas y equipos dañados, la disminución o la interrupción temporal de la producción, el aumento de los gastos en formación y administración, la posible disminución de la

> calidad del trabajo y las consecuencias negativas en la moral de otros trabajadores (OIT, s.f., p. 4).

Y, respecto a los indirectos son:

> sustituir al trabajador lesionado o enfermo, hay que formar a un nuevo trabajador y darle tiempo para que se acostumbre al puesto de trabajo, lleva tiempo hasta que el nuevo trabajador produce al ritmo del anterior, se debe dedicar tiempo a las obligadas averiguaciones, a redactar informes y a cumplimentar formularios, a menudo, los accidentes suscitan preocupación en los colegas del accidentado e influyen negativamente en las relaciones laborales, las malas condiciones sanitarias y de seguridad en el lugar de trabajo también pueden influir negativamente en la imagen pública de la empresa (OIT, s.f., p. 4).

Con base en esta información, presentar estos datos tan superficiales de lo que implicaría suplir un accidente laboral, representa suficiente razón para prevenir y mitigar estos riesgos. Sin embargo, en el documento se explica que “a escala nacional, los costos estimados de los accidentes y enfermedades laborales pueden ascender al 3 o 4 por ciento del producto interno bruto de un país” (OIT, s.f., p. 4).

Debido a esto, y como se mencionó en el apartado de los riesgos ambientales, la OIT explica también que es de gran importancia que los empresarios, los empleados y los sindicatos pretendan mejorar las condiciones de salud y seguridad, de forma que se puedan controlar los riesgos (en su fuente), se implemente un continuo registro de exposición a productos nocivos, se conozcan de manera oportuna los riesgos que existen en el lugar de trabajo, se cuente con un ente regulador de salud y seguridad conformado por losempleados y los directivos, se tenga siempre presente y se realicen los esfuerzos para asegurar la salud y la seguridad de los trabajadores. Esto, implica que se puedan salvar vidas, se influya positivamente en la moral y productividad de los empleados y se ahorre una gran cantidad de dinero (p. 5).

Por otra parte, la OIT explica que los países industrializados, en su gran mayoría, presentan una menor cantidad de accidentes laborales gracias a sus eficientes programas de

salud y seguridad laboral, mejores servicios de primeros auxilios, médicos y a la constante participación de los empleados en la toma de decisiones sobre las problemáticasrespectivas. Por el contrario, en los países en desarrollo se presenta una deficiencia en la detección y reconocimiento de los accidentes y enfermedades, los registros que se realizan y los mecanismos de comunicación. También, se explica que las industrias con mayor índice de accidentalidad son: la minería, la agricultura (silvicultura y explotación forestal) y la construcción (p. 6).

En esta medida, es necesario identificar las fuentes o causas de los accidentes. Respecto a esto, la OIT explica que algunas veces es sencillo determinar la causa de un accidente laboral, pero que frecuentemente existe una "cadena oculta de hechos que han producido el accidente que ha provocado la lesión del trabajador" (OIT, s.f., p. 6). También explica que muchas veces estas causas se deben a que los empresarios no forman de manera correcta a sus empleados o que las instrucciones, brindadas por un proveedor, de uso de un producto no son correctas o son erróneas; postula también que esto genera la necesidad de programas preventivos correctos para evitar los accidentes, al igual que existan médicos "que detecten las enfermedades profesionales en sus primeras fases" (p. 6).

Posteriormente, habla de las enfermedades que se pueden generar debido a la presencia de los riesgos en el sitio de trabajo y la exposición de los empleados a estos. Indica que existen enfermedades conocidas las cuales dependen del tipo de riesgo, la vía de la exposición, la dosis, etc., siendo las más conocidas:

> la asbestosis (causada por el asbesto o amianto, material utilizado habitualmente en aislamientos, guarniciones de frenos de automóviles, etc.), la silicosis (ocasionada por el sílice, habitual en la minería, el pulimentado con chorro de arena, etc.), el saturnismo (causado por el plomo, material habitual en las fábricas de pilas y baterías, de pinturas, etc.) y la pérdida de audición provocada por el ruido (habitual en muchos lugares de trabajo, entre ellos los aeropuertos, y en lugares de trabajo en que se utilizan máquinas ruidosas, como prensas o taladradoras, etc.) (OIT, s.f., p. 6).

Adicionalmente, explica que existen enfermedades preexistentes en los empleados que se pueden agravar por las malas condiciones de su lugar de trabajo, siendo algunas de

estas: “las enfermedades cardíacas, las enfermedades del sistema óseo muscular, por ejemplo, lesiones permanentes de la espalda o trastornos musculares, las alergias, los problemas de la función reproductora y los trastornos que provoca la tensión” (OIT, s.f., p. 7). Esto implica que es necesario reportar a los empleadores estas enfermedades ya existentes en los empleados con el fin de que exista mayor precaución al momento de encargarles tareas y de ubicarlos en su área de trabajo.

Por otro lado, la OIT explica que muchas enfermedades provocadas por el trabajo no son reportadas oportunamente, ya que no existen o no son eficientes los mecanismos de transmisión de informes, por la inexistencia de servicios de sanidad laboral y por la falta de capacidad de los médicos para detectarlas (p.7).

En congruencia con lo expuesto, en el documento se explica que muchas veces el motivo por el que no se identifican las causas de las enfermedades que tienen relación con el trabajo, es que los efectos que provoca no se presentan en seguida, sino que puede presentarse un periodo de latencia y cuando ya se detecta es muy tarde para tratarla o identificar a qué riesgos estuvo expuesto el empleado. Indica también que aunque muchos de estos riesgosya se conocen, a medida que avanza el tiempo van existiendo nuevos productos químicos o tecnologías que implican diferentes tipos de riesgo a menudo desconocidos. De esta manera, según la OIT hay un número ilimitado de riesgos en el área de trabajo. Inicialmente existen riesgos en zonas donde no esté protegida la maquinaria, donde el suelo sea deslizante o donde no existan precauciones en caso de un incendio; también hay riesgos que son peligrosos pero que no resaltan a la vista, al igual que:

> los riesgos químicos a que dan lugar líquidos, sólidos, polvos, humos, vapores y gases; los riesgos físicos, como los ruidos, las vibraciones, la insuficiente iluminación, las radiaciones y las temperaturas extremadas; los riesgos biológicos, como las bacterias, los virus, los desechos infecciosos y las infestaciones; los riesgos psicológicos provocados por la tensión y la presión; y los riesgos que produce la no aplicación de los principios de la ergonomía, por ejemplo, el mal diseño de las máquinas, los instrumentos y las herramientas que utilizan los trabajadores, eldiseño erróneo de los asientos y el lugar de trabajo o unas malas prácticas laborales (OIT, s.f., p. 8).

Adicionalmente, en el documento se resalta que el empleado no es quien crea el riesgo, sino que muchas veces el riesgo ya existe en su lugar de trabajo; así, "la solución consiste en suprimir los riesgos, no en esforzarse en que los trabajadores se adapten a unas condiciones inseguras" (OIT, s.f., p. 9). De esta forma, tal como se mencionó en el apartado del riesgo ambiental, la OIT señala que es relevante que los sindicatos concuerden con lo estipulado anteriormente, ya que muchas veces los empleadores culpan a los empleados por la causa de un accidente, señalando su negligencia y dando a entender que si el trabajador hubiese tenido una actitud distinta, no hubiese ocurrido el accidente. Sin embargo, se destaca que todos cometen errores, y que por el no control de los riesgos en el lugar de trabajo, un empleado no puede pagar con su vida por un error; si bien es cierto que se deben capacitar y ser conscientes de los riesgos, esto no implica que dejen de ocurrir accidentes, la forma más adecuada de prevenirlos es implementando una gestión de riesgo eficaz y unas condiciones de seguridad apropiadas en el puesto de trabajo (p. 9).

De esta manera, se explica que si existe un gran compromiso de la dirección y los empleados, el programa de salud y seguridad que se implemente será exitoso. En el caso de la dirección, deberá considerar todos los riesgos que existan y no exclusivamente los que estén en el reglamento; se debe priorizar la salud y la seguridad de sus empleados, de forma que exista una constante comunicación con estos y estableciendo el orden jerárquico de los empleados que sean responsables de este aspecto, capacitándolos y formándolos para que puedan "reconocer los signos/síntomas tempranos de las posibles enfermedades laborales antes de que se conviertan en crónicas; evaluar el entorno laboral; insistir en que la dirección efectúe cambios antes de que surjan situaciones peligrosas" (OIT, s.f., p. 11). Adicionalmente, la persona delegada para implementar el programa de salud y seguridad deberá pronunciarse a diario para garantizar el bienestar de los empleados; estas acciones pueden ser llevadas a cabo fomentando activamente que la dirección controle o elimine los riesgos. Asimismo, puede generar una mejor gestión si conoce todos los riesgos en las áreas de trabajo y la forma de eliminarlos o controlarlos, en colaboración con el sindicato y el empleado y compartiendo esta información con todas las partes involucradas para garantizar una mayor seguridad (p. 11).

Finalmente, en el documento se exponen los principales riesgos a los que se enfrentan los empleados, entre los cuales se destacan: el trabajo del soldador, quien está expuesto a quemaduras, luz intensa y humos; el mecánico se expone a cortes, caídas, riesgos químicos (grasas, disolventes, amianto y humos de evacuación) y problemas ergonómicos; en el caso de un trabajador portuario puede estar expuesto a riesgos ergonómicos por una mala indicación en los pesos y lo que se debe cargar, fugas o unas bolsas rajadas, caídas, cortes, accidentes de tránsito y otros elementos de carga (carretillas, elevadoras); en las textilerías, los riesgos son las máquinas en movimiento y desprotegidas, incendios, ruido y vibraciones, algunos materiales contaminantes para la salud humana (como el polvo y el algodón); respecto a los conductores de tractores, se enfrentan al riesgo de volcarse y que no haya una cabina de seguridad (exponiéndose a quedar aplastado), al ruido, vibraciones y entornos donde hayan herbicidas y plaguicidas químicos expulsados por el tractor; los agricultores se exponen a productos químicos peligrosos, plaguicidas y herbicidas que pueden afectar tanto la respiración como la piel; quienes trabajan en la oficina, a pesar de que muchas veces se considera que no están expuestos a ningún riesgo, enfrentan algunos como la tensión que genera el trabajo, mala iluminación, ruido y los asientos mal diseñados; los constructores se exponen a grandes riesgos como caerse, resbalarse, tropezarse, cortarse, que le caigan objetos a gran altura, no contar con un equipo apropiado para trabajar en alturas, problemas ergonómicos y ruido; los mineros se exponen al polvo, incendios, explosiones, electrocutarse, fuertes vibraciones, temperaturas elevadas, ruido, caídas, entre otros (p. 16).

2.4 Norma ISO 45001

Esta norma es la pionera en la salud y seguridad de los riesgos laborales, y se implementará de igual manera en el presente documento para complementar y profundizar los aspectos mencionados anteriormente. Para comenzar, en la introducción de esta norma se explica que “La adopción de un sistema de gestión de la SST tiene como objetivo permitir a una organización proporcionar lugares de trabajo seguros y saludables, prevenir lesiones y deterioro de la salud, relacionados con el trabajo y mejorar continuamente su desempeño de la SST” (Instituto Colombiano de Normas Técnicas y Certificación, ISO, 2018, p. 7), con lo que da cuenta de que se busca gestionar activamente los riesgos para proporcionar un

ambiente seguro para los empleados. De esta forma, esta es una de las normas que más se relaciona y se ve influenciada por la gestión de riesgos, ya que como se menciona posteriormente, "es de importancia crítica para la organización eliminar los peligros y minimizar los riesgos para la SST tomando medidas de prevención y protección eficaces" (Instituto Colombiano de Normas Técnicas y Certificación, ISO, 2018, p. 7). Por consiguiente, se procederá a resumir la norma y profundizar en los apartados mayormente relacionados con la gestión del riesgo, con el fin de implementarlos en las matrices presentadas en el capítulo 3.

Principalmente, entre los factores de éxito que expone la norma para lograr una eficaz implementación del SST, se encuentra el liderazgo y compromiso de la alta dirección, el desarrollo de una cultura en apoyo al SST, la comunicación, la integración de los trabajadores o sus representantes, los recursos que se asignen, la compatibilidad entre las políticas de la SST y los objetivos, "los procesos eficaces paraidentificar los peligros, controlar los riesgos para la SST y aprovechar las oportunidades para la SST" (Instituto Colombiano de Normas Técnicas y Certificación, ISO, 2018, p. 7), evaluar continuamente el desempeño y seguimiento de la gestión del SST para mejorar su desempeño, integrar el sistema de gestión en los procesos de la organización, cumplir los requisitos legales y demás. Con base en esto se garantizará una gestión efectiva de la Salud y Seguridad en el Trabajo.

Posteriormente, la norma da inicio con la contextualización de la organización, en la cual se deben conocer las cuestiones externas e internas que hacen parte de su propósito y que pueden interferir para alcanzar los resultados deseados del sistema de gestión de la SST (p.9). Seguido a esto, se deben determinar las partes interesadas entre las cuales se encuentran los trabajadores y quienes tengan relación con el sistema de gestión de la SST, como también sus necesidades y expectativas. A continuación, se debe establecer los límites y la aplicabilidad del sistema de gestión con el fin de establecer su alcance, considerando en este el contexto de la organización, los requisitos y expectativas de las partes interesadas y "las actividades relacionadas con el trabajo, planificadas o realizadas" (Instituto Colombiano de Normas Técnicas y Certificación, ISO, 2018, p. 10) sobre las cuales la organización tenga control o influencia y que puedan impactar el desempeño del sistema de gestión. Y, en lo que respecta al sistema de gestión de la SST, se debe "establecer, implementar, mantener y mejorar continuamente, (…) incluidos los procesos necesarios y sus interacciones" (Instituto

Colombiano de Normas Técnicas y Certificación, ISO, 2018, p. 10) de acuerdo con lo establecido en esta norma.

En el apartado 5 de la norma se abarcan los temas del liderazgo, compromiso y participación tanto de los directivos como de los empleados. En primer lugar, se explica que los directivos de la organización deben asumir la responsabilidad y rendir cuentas para prevenir "las lesiones y el deterioro de la salud relacionados con el trabajo, así como la provisión de actividades y lugares de trabajo seguros y saludables" (Instituto Colombiano de Normas Técnicas y Certificación, ISO, 2018, p. 10); deben también: asegurar que la política de la SST y sus objetivos tengan compatibilidad con la dirección estratégica; asegurar la integración de los requisitos del sistema SST en los procesos de la organización; asegurar la disponibilidad de los recursos que se requieran para el establecimiento, la implementación, el mantenimiento y mejoramiento del sistema SST; mantener una comunicación de la importancia de este sistema; asegurar el alcance de los resultados previstos; dirigir y apoyar a los miembros para aportar a la eficiencia del sistema; asegurar y promover la mejora continua; apoyar a otras partes que lideren áreas de responsabilidad; desarrollar, liderar y promover la cultura organizacional en apoyo al sistema; proteger "a los trabajadores de represalias al informar de incidentes, peligros, riesgos y oportunidades" (Instituto Colombiano de Normas Técnicas y Certificación, ISO, 2018, p. 11); asegurar el establecimiento de procesos para la consulta y la participación de los trabajadores; apoyar el funcionamiento y establecimiento de comités de seguridad y salud.

Por otra parte, en lo que respecta a la anteriormente mencionada política de la SST, por parte de la dirección se debe incluir el debido compromiso con los empleados para mantener seguras y saludables sus condiciones de trabajo, previniendo las lesiones y el deterioro de su salud, y que tenga en cuenta el tamaño y contexto de la organización, como también la naturaleza de los riesgos y sus oportunidades. Adicionalmente, deberá proporcionar un marco de referencia para establecer los objetivos de la SST, incluir el compromiso de cumplimiento de los requisitos, de la eliminación de peligros y reducción de riesgos, de la mejora continua del sistema y, de la consulta y participación de los empleados (p. 11).

- **Participación de los empleados:** la organización debe proporcionar: "los mecanismos, el tiempo, la formación y los recursos necesarios, el acceso oportuno a información

clara, comprensible y pertinente sobre el sistema de gestión" (Instituto Colombiano de Normas Técnicas y Certificación, ISO, 2018, p. 12); eliminar los factores que impidan la participación o minimizarlos, incluir la opinión de los empleados para: determinar las necesidades y expectativas de las partes; establecer la política de la SST, los objetivos y la planificación para lograrlos; determinar los controles que existen para la contratación externa, compras y contratistas; determinar qué necesita seguimiento, medición y evaluación; planificar, establecer, implementar y mantener programas de auditoría; asegurar la mejora continua. También, determinar los mecanismos de consulta y participación; identificar peligros y evaluar riesgos y oportunidades; determinar acciones para eliminar los peligros y reducir los riesgos; determinar qué información se necesita comunicar y cómo; determinar medidas de control, su implementación y uso eficaces; investigar incidentes y no conformidades y determinar las acciones correctivas (p. 13).

En el apartado 6 se presenta una amplia información respecto a la identificación de riesgos, explicando que se deben identificar continua y proactivamente. Indica que se debe tener en cuenta: organización del trabajo, factores sociales "incluyendo la carga de trabajo, horas de trabajo, victimización y acoso (bullying) e intimidación" (Instituto Colombiano de Normas Técnicas y Certificación, ISO, 2018, p. 14), liderazgo y cultura; actividades y situaciones recurrentes y no recurrentes; peligros que provengan de:

> infraestructura, los equipos, los materiales, las sustancias y las condiciones físicas del lugar de trabajo; el diseño de productos y servicios, la investigación, el desarrollo, los ensayos, la producción, el montaje, la construcción, la prestación de servicios, el mantenimiento y la disposición; los factores humanos; cómo se realiza el trabajo; los incidentes pasados pertinentes internos o externos a la organización, incluyendo emergencias, y sus causas; las situaciones de emergencia potenciales (ISO, 2018, p. 15).

Se debe tener precaución también con las personas que tengan acceso a lugares de trabajo; lugares de trabajo que pueden afectarse por las actividades de la organización;

"trabajadores en una ubicación que no está bajo el control directo de la organización" (Instituto Colombiano de Normas Técnicas y Certificación, ISO, 2018, p. 15); también:

> el diseño de las áreas de trabajo, los procesos, las instalaciones, la maquinaria/equipos, los procedimientos operativos y la organización del trabajo, incluyendo su adaptación a las necesidades y capacidades de los trabajadores involucrados; las situaciones que ocurren en las inmediaciones del lugar de trabajo causadas por actividades relacionadas con el trabajo bajo el control de la organización; las situaciones no controladas por la organización y que ocurren en las inmediaciones del lugar de trabajo que pueden causar lesiones y deterioro de la salud a personas en el lugar de trabajo; los cambios reales o propuestos en la organización, operaciones, procesos, actividades y el sistema de gestión de la SST; los cambios en el conocimiento y la información sobre los peligros (Instituto Colombiano de Normas Técnicas y Certificación, ISO, 2018, p. 15).

En el capítulo 7 se menciona lo referente a recursos, toma de conciencia, comunicación externa y comunicación interna. Respecto a los recursos, la organización debe proporcionar los necesarios para establecer, implementar, mantener y mejorar el sistema de gestión.

- **Toma de conciencia:** sensibilizar a los empleados e informar acerca de: política y objetivos de la SST;

> su contribución a la eficacia del sistema de gestión de la SST, incluidos los beneficios de una mejora del desempeño de la SST; las implicaciones y las consecuencias potenciales de no cumplir los requisitos del sistema de gestión de la SST; los incidentes, y los resultados de investigaciones, que sean pertinentes para ellos; los peligros, los riesgos para la SST y las acciones determinadas, que sean pertinentes para ellos; la capacidad de alejarse de situaciones de trabajo que consideren que presentan un peligro inminente y serio para su vida o su salud, así como las

disposiciones para protegerles de las consecuencias indebidas de hacerlo (Instituto Colombiano de Normas Técnicas y Certificación, ISO, 2018, p. 18).

- **Comunicación:** respecto a la comunicación interna y externa, se debe transmitir:

  la información pertinente para el sistema de gestión de la SST entre los diversos niveles y funciones de la organización, incluyendo los cambios en el sistema de gestión de la SST; asegurarse de que sus procesos de comunicación permitan a los trabajadores contribuir a la mejora continua (Instituto Colombiano de Normas Técnicas y Certificación, ISO, 2018, p. 19).

En el apartado 8 se mencionan los parámetros para eliminar y reducir riesgos, lo cual se puede asociar al tratamiento de estos explicado en la ISO 31000.

- **Tratamiento de riesgos:** "eliminar el peligro; sustituir con procesos, operaciones, materiales o equipos menos peligrosos; utilizar controles de ingeniería y reorganización del trabajo; utilizar controles administrativos, incluyendo la formación; utilizar equipos de protección personal adecuados" (Instituto Colombiano de Normas Técnicas y Certificación, ISO, 2018, p. 21).

  También se deberá aplicar la gestión del cambio en caso de que se requiera para la reducción del riesgo, considerar si las compras que se hagan afectan el sistema SST, al igual que los contratistas y las contrataciones externas. De igual manera, se deben preparar respuestas ante emergencias que surjan.

  Con esto finalizan los apartados de interés de la norma ISO 45001 para complementar las matrices del presente trabajo.

2.5 Riesgo en la Seguridad de la Información

En el documento Gestión de riesgos emitido por el INCIBE (2015) se presenta un marco completo de la gestión del riesgo según la norma ISO 31000 y su aplicación en los riesgos en la seguridad de la información.

Gracias a la pandemia que se vive actualmente, las empresas se han visto obligadas a reinventarse, utilizando el internet como medio principal para crear nuevas relaciones con el cliente, para darse a conocer e incluso para conectar entre empleados. Dado al uso masivo del internet, es posible que se presente un posible fallo en el manejo de la información, por lo cual es necesario valorar los riesgos partiendo desde la identificación de estos.

Según INCIBE (2015) el propósito principal de la gestión de riesgos de seguridad de la información es proteger la información, tanto digital como de cualquier otro soporte, teniendo en cuenta todo el ciclo de la vida de esta. En la guía se explica que también se debe considerar "la infraestructura informática, los equipos auxiliares, las redes de comunicaciones, las instalaciones y las personas" (INCIBE, 2015). Explica que la seguridad de la información consiste en la protección de riesgos que pueden afectar una o varias de las principales propiedades: confidencialidad (solo las personas autorizadas pueden tener acceso a la información), integridad (la información no debe ser manipulada por terceros) y disponibilidad (los autorizados siempre deben tener acceso a la información).

De esta forma, se indica que hay tres causas por las que se puede ver amenazada la información. En primer lugar, se explican las causas naturales en las cuales se incluyen "inundaciones, terremotos, incendios, rayos, fallos de la infraestructura auxiliar: fallos de suministro eléctrico, refrigeración, contaminación." (p.15), también se puede ver amenazada por fallos de los sistemas informáticos y de comunicaciones, las cuales incluyen fallos en las aplicaciones o en el hardware, y por último la información se puede ver amenazada por error humano.

Para gestionar los riesgos, la guía indica que inicialmente se debe establecer el contexto en el cual se definen los criterios básicos; este se puede establecer desde un enfoque global o uno detallado. Además, se deben considerar la normatividad que compete a la organización.

En lo que respecta la identificación de riesgos, la guía propone que se deben identificar los elementos a los cuales se les debe garantizar su seguridad, siendo los primarios:

> Información: estratégica, de carácter personal o que esté sujeta a legislación que la proteja, esencial para el desarrollo del negocio, de difícil o muy costosa reposición, etc. Actividades y procesos de negocio: que tienen que ver con propiedad intelectual, los que si se degradan hacen imposible la ejecución de las tareas de la empresa, los necesarios para el cumplimiento legal o contractual, etc. (p.17).

y los de soporte: "hardware: PC, portátiles, servidores, impresoras, discos, documentos en papel. Software: sistemas operativos, paquetes, aplicaciones. Redes: conmutadores, cableado, puntos de acceso. Personal: usuarios, desarrolladores, responsables. Edificios, salas, y sus servicios. Estructura organizativa: responsables, áreas, contratistas" (p.17).

Para la valoración de los daños en la información, se le puede preguntar a los propietarios de los activos, usuarios expertos las siguientes preguntas:

> ¿Qué valor tiene este activo para la empresa?, ¿Cuánto cuesta su mantenimiento, ¿Cómo repercute en los beneficios de la empresa?, ¿Cuánto valdría para la competencia?, ¿Cuánto costaría recuperarlo o volverlo a generar?, ¿Cuánto costó adquirirlo o su desarrollo?, ¿A qué responsabilidades legales o contractuales nos enfrentamos si se ve comprometido? (p.18).

Por otro lado, en el texto se mencionan tres métodos para analizar las amenazas: "entrevistas con usuarios y cuestionarios, inspección físicas y uso de herramientas para el escaneo automatizado" (p.18).

Para la estimación de riesgos, se determinaron una serie de criterios los cuales sirven para medir el impacto de la pérdida de "confidencialidad, integridad y disponibilidad de los activos" (INCIBE,2015). Estos riesgos se pueden estimar cualitativa o cuantitativamente e incluyen: "pérdidas financieras, costes de reparación o sustitución, interrupción del servicio, pérdida de reputación y confianza de los clientes, disminución del rendimiento, infracciones legales o ruptura de condiciones contractuales, pérdida de ventaja competitiva y daños personales" (p.19). En la siguiente tabla recuperada de la guía, se pueden ver ejemplos de los criterios descritos anteriormente.

Figura 3

Ejemplo de niveles de clasificación de los impactos de un incidente

Rango impacto / Descripción		Descripción	Pérdidas financieras	Pérdida del activo(s)	Reputación e imagen	Disminución de rendimiento
5	Catastrófico	> 6 % del presupuesto	Total	Mayor que un mes	Alta y muy extendida	> 50 % de variación en los indicadores
4	Desastroso	6% del Presupuesto	Muy gran impacto	De una semana a un mes	Media y muy extendida	25-50 % variación en los indicadores
3	Serio	2% del presupuesto	Gran impacto	De un día a una semana	Media y poco extendida	10-25% variación en los indicadores
2	Menor	1% del presupuesto	Impacto menor	½ día o 1 día	Baja y muy extendida	5-10 % variación en los indicadores
1	Insignificante	< 0,5 % del presupuesto	Casi sin impacto	Menor de ½ día	Baja y poco extendida	Hasta 5% variación en los indicadores

Nota: ejemplo para clasificar un riesgo. Tomado de: INCIBE (2015). Ejemplo de niveles de clasificación de los impactos de un incidente. Una guía de aproximación para el empresario. Gestión de riesgos. Instituto Nacional de Ciberseguridad.

Según la guía, para la estimación cualitativa de los riesgos mencionados anteriormente, "se califican las potenciales consecuencias y la probabilidad según niveles (alto, medio, bajo) subjetivos" (p.20), mientras que para la estimación cuantitativa se "utiliza una escala con valores numéricos, apoyándose en datos de distintas fuentes" (p.20). Se debe determinar la probabilidad de que ocurran los incidentes mediante: estadísticas de los incidentes en el pasado, de estudios o del sector, factores geográficos o estacionales, motivaciones de los posibles atacantes, vulnerabilidades existentes medidas que ya se han tomado y su resultado (INCIBE, 2015). Se deben multiplicar los resultados obtenidos para calcular el riesgo, los cuales se deben comparar con los criterios de aceptación de riesgo. En la tabla que se muestra a continuación, se da un ejemplo donde se comparan las valoraciones realizadas.

Figura 4

Estimación del producto «probabilidad x impacto» para evaluar riesgos

Nota: ejemplo de análisis de un riesgo. Tomado de: INCIBE (2015). Estimación del producto «probabilidad x impacto» para evaluar riesgos. Gestión de riesgos. Una guía de aproximación para el empresario. Instituto Nacional de Ciberseguridad.

Según (INCIBE, 2015) se sitúa cada riesgo antes y después de considerar como han afectado las medidas, además, esta tabla sirve para estimar el tratamiento de cada uno de los riesgos, por ejemplo, los riesgos en la zona blanca son soportables mientras que los que se encuentran en rojo son inaceptables (p.21).

Por último, para el tratamiento de los riesgos, INCIBE sugiere que se debe hacer una lista con estos, donde se decida si el riesgo se evita, reduce o mitiga, se transfiere o se acepta, teniendo en cuenta la valoración obtenida para cada riesgo y el coste del tratamiento. En el texto se hace un ejemplo de cómo se debe realizar esta lista en la siguiente tabla.

Figura 5

Ejemplo criterios para el tratamiento de riesgos

Coste-Beneficio	Tratamiento
El coste del tratamiento es muy superior a los beneficios.	**Evitar el riesgo**, por ejemplo, dejando de realizar esa actividad.
El coste del tratamiento es adecuado a los beneficios.	**Reducir o mitigar el riesgo**: seleccionando e implementando los controles o medidas adecuadas que hagan que se reduzca la probabilidad o el impacto.
El coste del tratamiento por terceros es más beneficioso que el tratamiento directo.	**Transferir el riesgo, por ejemplo**, contratando un seguro o subcontratando el servicio.
El nivel de riesgo está muy alejado del nivel de tolerancia.	**Retener o aceptar el riesgo** sin implementar controles adicionales. Monitorizarlo para confirmar que no se incrementa.

Nota: ejemplo de opciones de tratamiento para los riesgos según la relación costo/beneficio. Tomado de: INCIBE (2015). Ejemplo criterios para el tratamiento de riesgos. Gestión de riesgos. Una guía de aproximación para el empresario. Instituto Nacional de Ciberseguridad.

El tratamiento de los riesgos se puede implementar con: "instalar productos o contratar servicios, establecer controles de seguridad, mejorar los procedimientos, cambiar el entorno, incluir métodos de detección temprana, implantar un plan de contingencia y continuidad, realizar formación y sensibilización" INCIBE (2015).

Con lo mencionado anteriormente se obtiene un plan de tratamiento de riesgos, a los que se le añade una relación de riesgos residuales, es decir, los riesgos que aún existen a pesar de las medidas tomadas.

Además de todo esto, el autor concluye diciendo que es necesario estar monitoreando los riesgos ya que estos no son estáticos y pueden cambiar radicalmente, por lo que es necesario detectar: "nuevos activos o modificaciones en el valor de los activos, nuevas amenazas, cambios o aparición de nuevas vulnerabilidades, aumento de las consecuencias o impactos, incidentes de seguridad de la información" (p.23). Además, se revisará el proceso de gestión de riesgos para adecuarlo al contexto afectando: "las categorías de activos, los

criterios de evaluación de riesgos, los niveles de clasificación de los impactos, las escalas de aceptación de riesgos y los recursos necesarios" (p.23).

2.6 Norma ISO 27001

Posterior a lo expuesto por el INCIBE, se complementará esta información por lo establecido en la norma que respecta al tema de Seguridad de la Información, la cual es la norma ISO 27001. Se tomarán los aspectos más relevantes de la norma para el desarrollo del modelo expuesto en el capítulo 3.

- **Política de SGSI:** se debe definir dependiendo de las características del negocio, la organización, su ubicación, sus activos y tecnología (Instituto Colombiano de Normas Técnicas y Certificación, NTC-ISO, 2006) e incluir:

  marco de referencia para fijar objetivos y establecer un sentido general de dirección y principios para la acción con relación a la seguridad de la información; tener en cuenta los requisitos del negocio, los legales o reglamentarios, y las obligaciones de seguridad contractuales; estar alineada con el contexto organizacional estratégico de gestión del riesgo en el cual tendrá lugar el establecimiento y mantenimiento del SGSI; establecer los criterios contra los cuales se evaluará el riesgo y; haber sido aprobada por la dirección (p.4).

- **Valoración de riesgo:** se debe definir el enfoque organizacional identificando:

  una metodología de valoración del riesgo que sea adecuada al sistema y a los requisitos reglamentarios, legales y de seguridad de la información del negocio, identificados; desarrollando criterios para la aceptación de riesgos, e identificando los niveles de riesgo aceptables. La metodología seleccionada para valoración deriesgos debe asegurar que dichas valoraciones producen resultados comparables y reproducibles (p.5).

- **Identificar los riesgos:** se debe identificar "los activos dentro del alcance del SGSI y los propietarios de estos activos; las amenazas a estos activos; las vulnerabilidadesque podrían ser aprovechadas por las amenazas; los impactos que la pérdida de confidencialidad, integridad y disponibilidad puede tener sobre estos activos" (Instituto Colombiano de Normas Técnicas y Certificación, NTC-ISO, 2006).

- **Analizar y evaluar los riesgos:** la organización debe:

  Valorar el impacto de negocios que podría causar una falla en la seguridad, sobre la organización, teniendo en cuenta las consecuencias de la pérdida de confidencialidad, integridad o disponibilidad de los activos; valorar la posibilidad realista de que ocurra una falla en la seguridad, considerando las amenazas, las vulnerabilidades, los impactos asociados con estos activos, y los controles implementados actualmente; estimar los niveles de los riesgos; determinar la aceptación del riesgo o la necesidad de su tratamiento a partir de los criterios establecidos en la valoración de riesgo (p.5).

- **Tratar los riesgos:** para esto se puede: "Aplicar los controles apropiados; aceptar los riesgos con conocimiento y objetividad, siempre y cuando satisfagan claramente la política y los criterios de la organización para la aceptación de riesgos; evitar riesgos, y transferir a otras partes los riesgos asociados con el negocio" (Instituto Colombiano de Normas Técnicas y Certificación, NTC-ISO, 2006).

- **Seguimiento y revisión:** esto se realiza mediante: la detección oportuna de errores en los resultados del procesamiento; la identificación de incidentes e intentos de violación a la seguridad (sean exitosos o hayan fracasado); la verificación del cumplimiento de las actividades de seguridad; la detección de actividades de seguridad y determinar si las acciones tomadas para solucionar un problema de violación a la seguridad fueron eficaces; revisar la eficacia del sistema; cumplimiento de los requisitos de seguridad. Adicionalmente, se debe:

Revisar las valoraciones de los riesgos a intervalos planificados, y revisar el nivel de riesgo residual y riesgo aceptable identificado, teniendo en cuenta los cambios en: la organización, la tecnología, los objetivos y procesos del negocio, las amenazas identificadas, la eficacia de los controles implementados, y eventos externos, tales como cambios en el entorno legal o reglamentario, en las obligaciones contractuales, y en el clima social (p.7).

- **Comunicación:** la organización debe comunicar y documentar:

Política y objetivos del SGSI; el alcance del SGSI; los procedimientos y controles que apoyan el SGSI; una descripción de la metodología de valoración de riesgos; el informe de valoración de riesgos; el plan de tratamiento de riesgos; los procedimientos documentados que necesita la organización para asegurar la eficacia de la planificación operación y control de sus procesos de seguridad de la información, y para describir cómo medir la eficacia de los controles; los registros exigidos por esta norma, y la declaración de aplicabilidad (Instituto Colombiano de Normas Técnicas y Certificación, NTC-ISO, 2006).

- **Compromiso de la dirección:** la organización se debe comprometer estableciendo: una política del sistema; sus objetivos y planes; las funciones y responsabilidades de seguridad de la información; la comunicación de la importancia de cumplir los objetivos y la política establecidos; los recursos necesarios; los criterios para aceptación de riesgos, y los niveles de riesgo aceptables; la realización de auditorías internas; las revisiones por la dirección (p.10).

- **Formación, toma de conciencia y competencia:** la organización debe asegurar que el personal cumpla con sus responsabilidades a través de: "La determinación de las competencias necesarias para el personal; el suministro de formación o realización de otras para satisfacer estas necesidades; la evaluación de la eficacia de las acciones emprendidas, y el mantenimiento de registros de la educación, formación, habilidades,

experiencia y calificaciones" (Instituto Colombiano de Normas Técnicas y Certificación, NTC-ISO, 2006).

- **Recurso:** se debe proveer los recursos que se requieran para: el establecimiento, implementación, operación, seguimiento, revisión y mejoría del sistema; aseguramiento de que los procedimientos de seguridad son de apoyo para los requisitos; cumplir los requisitos legales y reglamentarios y las obligaciones de seguridad; el mantenimiento de la seguridad apropiada a través de los controles seleccionados; el seguimiento, la revisión y corrección de los aspectos encontrados; y la mejora y eficacia del sistema donde sea pertinente (p.11).

2.7 Riesgo en la Cadena de Abastecimiento

Se abarcará también el riesgo en la cadena de abastecimiento, ya que este es uno de los aspectos que puede tener más repercusiones sobre los demás procesos, en especial para las empresas que trabajan con suministros o que dependen de proveedores. Según el Centro Latinoamericano de Innovación en Logística (2010) "los riesgos en la cadena de suministro corresponden a cualquier situación que pueda afectar o interrumpir el flujo de componentes y productos a través de la cadena de suministros".

De esta forma, el CLI propone una clasificación de los riesgos de la cadena de suministro, subdividiéndolos así:

1. Riesgos operacionales: definiéndolos como aquellos que provienen de las operaciones propias de una organización, pudiendo ser inherentes a las operaciones o asociados a las decisiones de directivos (p. 21).

2. Riesgos dentro de la cadena de suministro: son aquellos que provienen de las interacciones entre miembros de la cadena de suministro (proveedores y/o clientes) (p. 21).

3. Riesgos Externos: son aquellos que provienen de las interacciones de las cadenas de abastecimiento con su entorno (p. 21).

Debido a que la cadena de suministro se ve fuertemente asociada con el ámbito externo, esta depende de aspectos económicos, geopolíticos, ambientales, sociales y tecnológicos, de forma que cuando estos fluctúan pueden afectarla. Por esto, en el documento presentado por el CLI, indica que según un estudio de Accenture (2006) citado en CLI (2010), los riesgos más importantes son: escasez de mano de obra calificada, inestabilidad geopolítica, lead times bastante altos, operaciones de importación y demoras en las aduanas, interrupciones en el suministro de materias primas.

Por otra parte, en el documento se presentan las pautas para la identificación de riesgos, indicando que se debe (p. 31):

1. Definir el proceso general de la cadena de suministros
2. Dividir el proceso en grupos de operaciones relacionadas
3. Considerar sistemáticamente los detalles de cada operación
4. Identificar el riesgo en cada operación y resaltar sus principales características
5. Describir en un registro los riesgos más significativos.

Para identificar estos riesgos, existen herramientas, entre las cuales se encuentran: análisis de eventos pasados: los 5 por qué, diagramas de Causa – Efecto, análisis de Pareto, listas de Verificación (Checklists); análisis de operaciones: diagramas de proceso, procesos de Control, gestión de eventos de la cadena de suministro (SCEM).

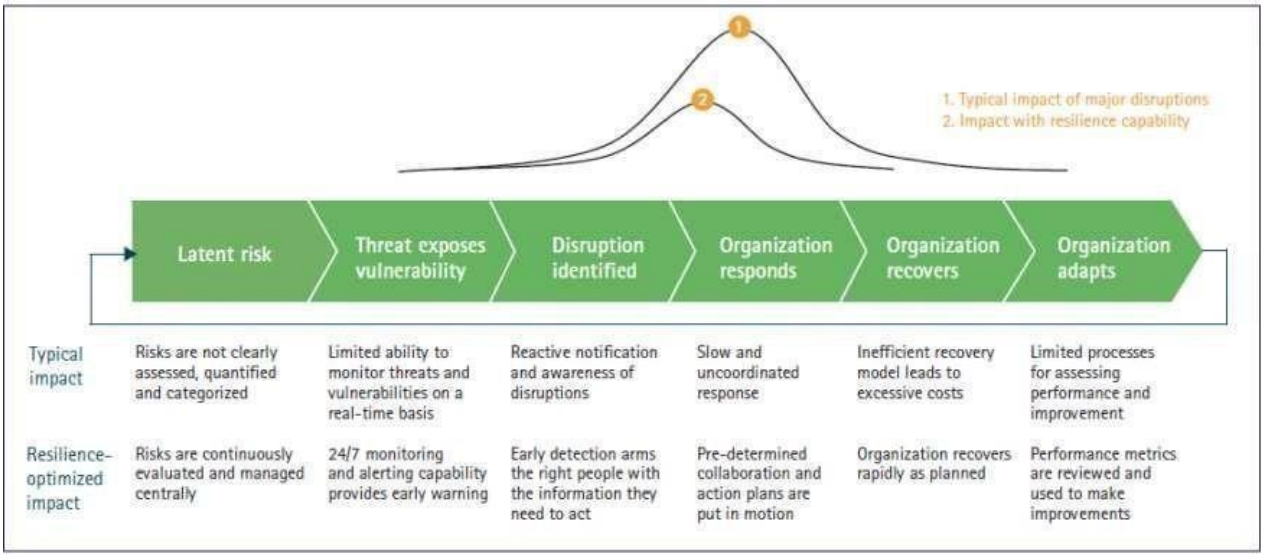
En lo que compete el análisis de los riesgos, las herramientas más frecuentes son: para categorizar el riego: mapas de riesgos, matrices de probabilidad – impacto; para analizarlo: análisis de modo y efecto de falla, análisis de escenarios, simulación, modelos de red.

Finalmente, respecto al tratamiento de estos riesgos se puede: ignorar o aceptar el riesgo, reducir la probabilidad del riesgo, reducir o limitar las consecuencias, transferir, compartir o desviar el riesgo, realizar planes de contingencia, adaptarse al riesgo, oponerse a un cambio, trasladarse a otro entorno.

Como información adicional, el documento presenta los pasos para establecer una cadena de abastecimiento resiliente, los cuales son:

Figura 6

Riesgo en la cadena de abastecimiento



Fuente: ***Keeping ahead of supply chain risk and uncertainty (2008)***

Nota: ejemplo para conformar una cadena de abastecimiento resiliente. Tomado de: CLI (2010). Riesgo en la cadena de abastecimiento. LOGYCA

2.8 Norma ISO 28000

Por otra parte, esta información se puede complementar y estandarizar con lo establecido en la norma ISO 28000, la cual establece los parámetros para garantizar la seguridad de la cadena de abastecimiento de una organización.

Inicialmente, el primer apartado de interés expuesto corresponde al desarrollo de la política de gestión de la seguridad, la cual deberá:

> ser coherente con otras políticas organizacionales; proporcionar el marco de referencia para establecer objetivos, metas y programas específicos de gestión de la seguridad; ser coherente con la estructura de la gestión de amenazas y riesgos de la seguridad general de la organización; ser apropiada para las amenazas de la organización y la naturaleza y escala de sus operaciones; determinar claramente los objetivos generales/amplios de gestión de la seguridad; incluir un compromiso con la mejora continua del proceso de gestión de la seguridad; incluir un compromiso de cumplir con la legislación actual aplicable, los requisitos de reglamentación y

estatutarios y otros requisitos que suscribe la organización; tener el respaldo visible de la alta dirección; ser documentada, implementada y mantenida; comunicarse a todos los empleados y terceras partes pertinentes, incluidos los contratistas y visitantes, con la intención de que estas personas sean conscientes de sus obligaciones individuales relacionadas con la gestión de la seguridad; estar disponible para las partes interesadas, cuando resulte apropiado; poderse revisar en caso de adquisición o fusión con otras organizaciones, u otro cambio en el alcance del negocio de la organización que pueda afectar la continuidad o pertinencia del sistema de gestión de la seguridad (Instituto Colombiano de Normas Técnicas y Certificación, NTC-ISO, 2008).

- **Identificación de riesgos:** se deben identificar los riesgos provenientes de:

amenazas y riesgos de falla física, tales como falla funcional, daño incidental, daño malicioso o terrorista o acción criminal; amenazas y riesgos operacionales, incluidos el control de la seguridad, los factores humanos y otras actividades que afectan el desempeño, la condición o la seguridad de las organizaciones; eventos del medio ambiente natural (tormentas, inundaciones, etc.) que pueden hacer que las medidas y equipos de seguridad resulten ineficaces; factores por fuera del control de la organización, tales como fallas en el equipo y servicios suministrados externamente; amenazas y riesgos de las partes involucradas, tales como falla en cumplir los requisitos de reglamentación o daño a la reputación o la marca; diseño e instalación del equipo de seguridad, incluido su reemplazo, mantenimiento, etc.; gestión de datos e información y comunicaciones; una amenaza a la continuidad de las operaciones (Instituto Colombiano de Normas Técnicas y Certificación, NTC-ISO, 2008).

Por otra parte, la norma indica que se debe "establecer y mantener una estructura organizacional de funciones, responsabilidades y autoridad" (Instituto Colombiano de Normas Técnicas y Certificación, NTC-ISO, 2008), que sea acorde al logro de la política y los objetivos.

- **Dirección y compromiso:** las directivas deberán: estipular los responsables del sistema de gestión y definir su autoridad y responsabilidades; establecer y cumplir los requisitos y expectativas de las partes interesadas; disponer los recursos necesarios; tener en cuenta el impacto que puedan generar los parámetros como la política, los objetivos, las metas, los programas, del sistema de gestión sobre otros aspectos de la organización; asegurar que otros programas de seguridad que se implementen se complementen con este; transmitir la importancia de cumplir los requisitos para cumplir la política; asegurarse de que los riesgos y amenazas identificados se evalúen y se incluyan en evaluaciones de amenazas y riesgos; asegurarse de que los objetivos, metas y programas establecidos sean viables (p. 9).

- **Toma de conciencia y capacitación**: se debe asegurar que los empleados que trabajen en áreas como diseño, operación y gestión de equipos y procesos de seguridad sea competente. Por otra parte, debe garantizar la concientización de:

  > la importancia del cumplimiento de la política y procedimientos de gestión de la seguridad y los requisitos del sistema de gestión de la seguridad; sus funciones y responsabilidades en el logro de la conformidad con la política y procedimientos de gestión de la seguridad y con los requisitos del sistema de gestión de la seguridad, incluidos los requisitos de preparación y respuesta ante emergencias; las consecuencias potenciales que tiene para la seguridad de la organización desviarse de los procedimientos de operación especificados (Instituto Colombiano de Normas Técnicas y Certificación, NTC-ISO, 2008).

Respecto a la comunicación, la norma indica que se deben tener procedimientos para garantizar que "la información pertinente de gestión de la seguridad se comunica hacia y desde los empleados relevantes, contratistas y otras partes interesadas" (Instituto Colombiano de Normas Técnicas y Certificación, NTC-ISO, 2008). Adicionalmente, "debido a la naturaleza confidencial de alguna información relacionada con la seguridad, se debería considerar adecuadamente la sensibilidad de la información antes

de su divulgación" (Instituto Colombiano de Normas Técnicas y Certificación, NTC-ISO, 2008).

- **Seguimiento y control:** se debe medir el desempeño del sistema planteado, mediante: medidas (cualitativas o cuantitativas) según los requerimientos; cumplimiento de la política, los objetivos y las metas (p. 12);

  > medidas proactivas de desempeño para hacer el seguimiento a la conformidad con los programas de gestión de la seguridad, los criterios de control operacionales y la legislación aplicable, los requisitos estatutarios y otros requisitos de reglamentación sobre seguridad; medidas reactivas de desempeño para hacer el seguimiento de deterioro, fallas, incidentes, no conformidades (incluidas las fallas que estuvieron a punto de ocurrir y las falsas alarmas) relacionadas con la seguridad y otra evidencia histórica de desempeño deficiente del sistema de gestión de la seguridad; registro de datos y resultados de seguimiento y medición suficientes para facilitar el análisis de las acciones preventivas y correctivas posteriores. Si se requiere equipo de seguimiento para el desempeño, y la medición o seguimiento, o todos ellos, la organización debe exigir que se establezcan y mantengan procedimientos para la calibración y mantenimiento de dicho equipo. Se deben conservar registros de las actividades de calibración y mantenimiento durante tiempo suficiente, para cumplir con la legislación y la política de la organización (Instituto Colombiano de Normas Técnicas y Certificación, NTC-ISO, 2008).

Con este finalizan los apartados de interés de la norma ISO 28000, de manera que se proseguirá al almacenamiento de toda esta información en el modelo integral.

3. MODELO INTEGRADO PARA LA GESTIÓN DE RIESGOS

La información recolectada anteriormente se implementará para desarrollar un modelo integral, que abarcará los riesgos ambientales, de salud y seguridad en el trabajo, de la seguridad de la información y de la cadena de abastecimiento, tomando los principales aspectos de cada una de las normas correspondientes, tales como: establecimiento del contexto, dirección y compromiso, políticas, toma de conciencia, recursos y mecanismos de comunicación, y conjugándolos en un modelo fácil de entender que recopila toda esta información. A continuación, se explicará cómo funciona el modelo, qué aspectos se deben considerar al momento de aplicarla, y en qué partes de los anteriores capítulos se puede ampliar la información ofrecida.

3.1 Modelo Integral

En las hojas de cálculo de Excel adjuntas al presente documento, se evidencia la recopilación de la información más relevante del capítulo 1 y 2. Principalmente, en la hoja llamada Introducción se exponen las ventajas de gestionar los riesgos, los principios de la gestión de riesgos y las convenciones que se implementaron.

En la hoja llamada Modelo inicial MR, se muestra la Figura 2 de la norma ISO 31000 que indica cómo se debe desarrollar el marco de referencia. Sin embargo, ya que la intención del presente documento es conjugar las normas de cada riesgo seleccionado enfocándolas o complementando lo expuesto en la norma ISO 31000, en las hojas posteriores a este modelo inicial, se presentará la información de cada norma respecto a cada apartado que menciona la ISO 31000 en la figura 2.

En primer lugar, se encuentra la dirección y compromiso. Cada una de las normas complementarias (ISO 14001, 45001, 28000, 27001) contiene información de distinta índole acerca de este tema, por lo cual se desarrolló una figura que represente esta información, de manera que quien la vaya a usar al momento de desarrollar el marco de referencia para la gestión de cualquiera de estos riesgos, pueda complementar la información de la ISO 31000 con lo que dice la ISO de cualquiera de los demás sistemas de gestión/riesgos.

Es decir, se debe considerar que además de implementar lo que dice la norma ISO 31000, cuando se vaya a gestionar cualquiera de los riesgos se desarrollará también cada uno de los sistemas de gestión que propone cada una de sus normas (sistema de gestión ambiental, sistema de gestión de la salud y seguridad en el trabajo, sistema de gestión de la seguridad de la información y sistema de gestión de la cadena de abastecimiento). Por ejemplo, si como empresario me interesa gestionar el riesgo ambiental, en cada uno de los ítems mencionados en la figura 2 de la norma ISO 31000, si sigo e implemento la información brindada en el modelo de esta monografía, estaré desarrollando también el sistema de gestión ambiental.

Entiéndase que cuando se habla de los sistemas de gestión, se hace referencia al establecimiento de: el contexto interno y externo, el compromiso de la alta dirección, las políticas, la toma de conciencia, los recursos necesarios y los mecanismos decomunicación; es decir, cada una de las hojas del modelo de Excel contienen la información para desarrollar, además de la gestión de los riesgos, los demás sistemas de gestión.

Por consiguiente, en cada una de estas hojas se deberá seguir o implementar la información que estos proveen. Después de establecer e implementar el marco de referencia, se prosigue a la hoja: Modelo inicial GR, en la cual se muestra la figura 3 de la norma ISO 31000, y contiene los pasos o ítems para gestionar cada uno de los riesgos.

De esta manera, en cada una de las hojas que lleva por título gestión de riesgos ambientales, de salud y seguridad en el trabajo, de seguridad de la información y de la cadena de abastecimiento, se muestran cada uno de los pasos a seguir para la gestión de cada uno de estos riesgos. En la parte de comunicación y consulta, se especifica que esta es la misma establecida anteriormente cuando se definieron los mecanismos de comunicación, pero que se hará con el fin de: ayudar a establecer correctamente el contexto; garantizar que se entienden y se toman en consideración los intereses de las partes involucradas; ayudar a garantizar que los riesgos estén correctamente identificados; reunir diferentes áreas de experticia para analizar los riesgos; garantizar que los diversos puntos de vista se toman en consideración adecuadamente al definir los criterios del riesgo y al evaluar los riesgos; asegurar la aprobación y el soporte para el plan de tratamiento; fomentar la gestión adecuada del cambio durante el proceso para la gestión del riesgo; y desarrollar un plan adecuado de comunicación y consulta externo e interno.

Una vez se culminen cada uno de los pasos, considerando lo establecido en el marco de referencia, se podrá dar por sentado que se gestionaron este tipo de riesgos en la empresa, con lo cual se debe proseguir a implementar lo desarrollado en el modelo.

3.2 Hoja de instrucciones

1. Tener en cuenta los principios expuestos en la hoja llamada Introducción, ya que estos son el pilar para garantizar una correcta gestión de los riesgos, y tener claras las convenciones usadas para cada riesgo.

2. Los ítems de la figura presentada en la hoja: Modelo inicial MR serán los que se abarquen para establecer el marco de referencia para gestionar cada uno de los riesgos.

3. En las hojas llamadas: Dirección y compromiso, Contexto int y ext, Políticas, Integración-Toma de conciencia, Recursos y Mecanismos de comunicación, contienen en el centro del círculo lo que respecta a la norma ISO 31000 (azul), lo cual se debe desarrollar y complementar con la información de las demás normas del riesgo que se quiera gestionar. Por ejemplo, voy a gestionar el riesgo de la salud y seguridad en el trabajo, por consiguiente, en todas estas hojas voy a hacer lo que dice la ISO 31000 (azul) y lo que dice la ISO 45001 (verde).

4. En la hoja del Contexto int y ext no hay información de las normas ISO 28000 y 27001, por lo cual el contexto que se establezca según lo que dice la ISO 31000 será el que se usará también para estos dos riesgos.

5. En la hoja llamada Rendición de cuentas, lo que se establezca allí será aplicado para el marco de referencia de todos los riesgos.

6. En la hoja: Implementación del MR, están cada uno de los pasos para implementar lo desarrollado en cada uno de los anteriores ítems para la gestión del riesgo.

7. La hoja: Modelo inicial GR contiene los pasos o ítems para gestionar cada uno de los riesgos.

8. En las siguientes hojas: GR ambiental, GR salud y seguridad, GR seguridad de la información y GR cadena de abastecimiento, se implementa la figura del paso anterior para gestionar el riesgo, por lo cual se debe seguir paso a paso lo que especifique cada ítem, desde el contexto hasta el monitoreo.

9. En cada una de estas hojas de GR, se presentan convenciones de diferentes colores para cada uno de los riesgos, y a lo largo de cada uno de los pasos, también se ven estas convenciones, los cuales hacen referencia a la información adicional que hay de cada riesgo, como sus fuentes, su tratamiento, su análisis, etc.

10. Desarrollar lo que dice cada ítem para así gestionar los riesgos.

A continuación, se presenta el link que llevará directamente al modelo desarrollado en Excel para la gestión de riesgos:

MODELO

4. CONCLUSIONES

Principalmente, la norma ISO 31000 contiene información muy detallada de cómo gestionar los riesgos efectivamente, pero lo hace de forma muy general de manera que se tuvo que investigar a fondo para complementar la información referente a cada uno de los tipos de riesgos seleccionados, completando sobre todo los apartados de la identificación en la parte de las fuentes, el análisis en la parte de cálculo del riesgo, y el tratamiento en la parte de herramientas o posibles tratamientos, con información proveniente de las normas ISO y otras fuentes.

Respecto a los objetivos específicos planteados, se estableció todo el contexto de la proveniencia del término riesgo a lo largo del tiempo, se mencionaron sus características, los tipos de riesgo que existen y la importancia de su gestión, complementando esta información con lo establecido en la norma ISO 31000.

Por otra parte, se definieron los riesgos ambientales, los riegos en la salud y seguridad en el trabajo, los riesgos en la seguridad de la información y los riesgos en la cadena de abastecimiento, brindando un marco amplio para su identificación y tratamiento, para posteriormente complementar esta información con lo que especifican las normas ISO respecto a los riesgos.

Finalmente, se generó un modelo integral compuesto por 15 hojas de Excel que contienen toda la información necesaria para desarrollar un marco de referencia para la gestión de riesgos, complementada esta información con las normas ISO respectivas, y para gestionar efectivamente el riesgo con información completa de fuentes, análisis y tratamientos de los riesgos.

A modo de recomendación, se evidenció que:

1. Se recomienda aplicar esta misma propuesta de modelo integral para otros riesgos que se consideran de gran importancia en las empresas.
2. Se recomienda también indagar más en las normativas referentes a cada uno de los riesgos, es decir, los requisitos legales que existen para brindar una información más completa.

BIBLIOGRAFIA

Chávez, S. (2018). El concepto de riesgo. Recursos Naturales y Sociedad. https://doi.org/10.18846.

Centro Latinoamericano de Innovación en Logística, CLI. (2010). Riesgo en cadena de abastecimiento. https://www.icesi.edu.co/blogs/bitacorariesgointegral1010/files/2010/11/gestion-de-riesgos-en-la-sch.pdf.

Daphnia (1999). Riesgos medioambientales en la empresa. Número 16. https://www.daphnia.es/revista/16/articulo/382/Riesgos-medioambientales-en-la-empresa.

Escuela Europea de Excelencia (2018). Riesgo ambiental y análisis de los riesgos según la ISO 14001 2015. Nueva ISO 14001:2015. https://www.nueva-iso-14001.com/2018/04/riesgo-ambiental-segun-la-iso-14001-2015/.

Instituto Colombiano de Normas Técnicas y Certificación (2018). Sistemas de gestión de la seguridad y salud en el trabajo – Requisitos con orientación para su uso. NTC-ISO 45001. El Instituto. https://ergosourcing.com.co/wp-content/uploads/2018/05/iso-45001-norma-Internacional.pdf.

Instituto Colombiano de Normas Técnicas y Certificación. (2006). Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos. NTC-ISO 27000. El Instituto. http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf.

Instituto Colombiano de Normas Técnicas y Certificación (2011). Gestión del Riesgo. Principios y Directrices. NTC-ISO 31000. El Instituto. https://sitios.ces.edu.co/Documentos/NTC-ISO31000_Gestion_del_riesgo.pdf.

Instituto Colombiano de Normas Técnicas y Certificación (2015). Sistemas de Gestión Ambiental. Requisitos con orientación para su uso. NTC-ISO 14001. El Instituto. https://informacion.unad.edu.co/images/control_interno/NTC_ISO_14001_2015.pdf

Instituto Colombiano de Normas Técnicas y Certificación (2008). Sistemas de Gestión de la Seguridad Para la Cadena de Suministro. NTC-ISO 28000 https://www.timon.com.co/wp-content/uploads/ntc28000.pdf.

Instituto Nacional de Ciberseguridad, INCIBE (2015). Gestión de riesgos. Una guía de aproximación para el empresario. https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_gestion_riesgos_metad.pdf.

Oficina Internacional del Trabajo, OIT. (s.f.). La Salud y la Seguridad en el Trabajo. http://www.concesiones.cl/publicacionesyestudios/Documents/Prevencion_de_riesgos/La%20Salud%20y%20la%20Seguridad%20en%20el%20Trabajo%20Doc%20OIT.pdf.