Diseño e Implementación de Buenas Prácticas de un Modelo Integral de Gestión de Riesgos en una Empresa Pyme del Sector de Servicios de Consultoría

Edison Felipe Espinosa González

Trabajo de Grado para Optar al Título de Ingeniero Industrial

Director

Olmedo González Herrera

Magíster en Estadística

Universidad Industrial de Santander

Facultad de Ingenierías Fisicomecánicas

Escuela de Estudios Industriales y Empresariales

Ingeniería Industrial

Bucaramanga

2026

Dedicatoria

A Dios

Por acompañarme en cada paso de este proceso. Por brindarme sabiduría en medio de la incertidumbre y por enseñarme que cada logro alcanzado es fruto de confiar plenamente en Él.

A mis padres

Por ser el mayor ejemplo de amor, esfuerzo y perseverancia. Gracias a su sacrificio, dedicación y apoyo incondicional, hoy logro alcanzar esta meta. Todo lo que soy es reflejo de sus enseñanzas y valores; este logro también les pertenece.

A mi hermano

Por ser mi compañero incondicional y mi apoyo constante en cada etapa de este camino. Gracias por estar siempre a mi lado, por tu apoyo incondicional, tus consejos y por compartir conmigo tantos momentos que han dejado huella en mi vida.

A mi novia

Por ser ese apoyo incondicional que llegó a mi vida en el momento indicado. Gracias por el amor, la paciencia y por estar conmigo en cada etapa de este proceso, incluso en los momentos más difíciles. Que la vida nos permita seguir creciendo juntos y construyendo sueños compartidos.

Agradecimientos

A los directivos y al equipo de STRATEGY AM AND PSM S.A.S., por brindarme la oportunidad de hacer parte de la organización y permitirme desarrollar este trabajo en un entorno de aprendizaje autentico, retador y de gran valor académico. Su disposición para compartir conocimiento y su compromiso con la mejora continua hicieron posible la construcción de las buenas prácticas de un modelo de gestión de riesgos.

A mi director de proyecto, Olmedo González Herrera, por su guía académica, sus observaciones rigurosas y su orientación oportuna en cada etapa del proceso. Su experiencia y claridad metodológica fueron claves para darle solidez a este libro.

A la Escuela de Estudios Industriales y Empresariales y a la Universidad Industrial de Santander, por brindar el marco académico y las herramientas necesarias para el desarrollo de este trabajo, así como por fomentar una formación integral orientada a la investigación aplicada y al servicio a las organizaciones.

Tabla de contenido

Lista de tablas

Lista de figuras

Lista de apéndices

Los apéndices están adjuntos y puede visualizarlos en la base de datos de la biblioteca UIS

Apéndice A. Cuestionario cuantitativo nivel de madurez de la gestión de riesgos en STRATEGY

Apéndice B. Revisión documental interna norma ISO 31000

Apéndice C. AGC-FT-007-Matriz de riesgos y oportunidades

Apéndice D. CCS-FT-027-Matriz de riesgos y oportunidades VRF

Apéndice E. Manual de gestión de riesgos

Apéndice F. Instructivo de uso de matrices de riesgos y oportunidades

Apéndice G. Toolkit de herramientas

Apéndice H. Sistema de indicadores

Resumen

Título: Diseño e Implementación de Buenas Prácticas de un Modelo Integral de Gestión de Riesgos en una Empresa Pyme del Sector de Servicios de Consultoría*

Autor: Edison Felipe Espinosa González**

Palabras Clave: Gestión del Riesgo, ISO 31000:2018, Mejora Continua, Valoración del Riesgo.

Descripción:

El presente trabajo tiene como objetivo diseñar e implementar buenas prácticas de un modelo integral de gestión de riesgos en la empresa STRATEGY AM AND PSM S.A.S., una pyme del sector de servicios de consultoría, con el fin de fortalecer la gestión del riesgo organizacional frente a la falta de un sistema formalizado. Esta necesidad surge debido a la ausencia de metodologías estandarizadas y herramientas integradas que permitan identificar, analizar, evaluar, tratar y controlar los riesgos de manera sistemática, lo cual limita la toma de decisiones, la planificación estratégica y la resiliencia operativa de la empresa. Para estructurar el enfoque se tomó como referencia la norma ISO 31000:2018, que ofrece directrices internacionales para abordar el riesgo de forma integral y adaptable a cualquier tipo de organización, independientemente de su tamaño o sector.

La metodología empleada tuvo un enfoque aplicado y descriptivo, con orientación cualitativa, desarrollada en cinco etapas: diagnóstico inicial, diseño del modelo, implementación piloto, ajuste y socialización de resultados. En el diagnóstico se evidenció un bajo nivel de cumplimiento frente a los lineamientos de la ISO 31000, con debilidades en la formalización, comunicación y estandarización de la gestión de riesgos.

Como resultado, se diseñó un modelo adaptado al contexto de la organización, estructurado en los niveles estratégico, táctico y operativo, acompañado de un manual de gestión de riesgos, matrices de identificación y control, un toolkit de herramientas operativas y un sistema de indicadores para su seguimiento continuo. La implementación piloto permitió validar la aplicabilidad del modelo y generar ajustes para su mejora

* Trabajo de Grado

** Facultad de Ingenierías Fisicomecánicas. Escuela de Estudios Industriales y Empresariales. Director: Olmedo González Herrera Magíster en Estadística.

Abstract

Title: Design and Implementation of Good Practices for a Comprehensive Risk Management Model in an SME in the Consulting Services Sector.

Author: Edison Felipe Espinosa González

Keywords: Risk Management, ISO 31000:2018, Continuos Improvement, Risk Assessment

Description:

This work aims to design and implement best practices for a comprehensive risk management model at STRATEGY AM AND PSM S.A.S., a small and medium-sized enterprise (SME) in the consulting services sector, in order to strengthen organizational risk management in the face of the lack of a formalized system. This need arises due to the absence of standardized methodologies and integrated tools that allow for the systematic identification, analysis, evaluation, treatment, and control of risks, which limits decision-making, strategic planning, and the company's operational resilience. The approach was structured around ISO 31000:2018, which offers international guidelines for addressing risk in a comprehensive and adaptable manner for any type of organization, regardless of its size or sector.

The methodology employed was applied and descriptive, with a qualitative orientation, and was developed in five stages: initial diagnosis, model design, pilot implementation, adjustment, and dissemination of results. The diagnostic assessment revealed a low level of compliance with ISO 31000 guidelines, with weaknesses in the formalization, communication, and standardization of risk management.

As a result, a model adapted to the organization's context was designed, structured at the strategic, tactical, and operational levels. This model was accompanied by a risk management manual, identification and control matrices, a toolkit of operational tools, and a system of indicators for continuous monitoring. The pilot implementation validated the model's applicability and allowed for adjustments to be made for its improvement.

* Degree Work

** Facultad de Ingenierías Fisicomecánicas. Escuela de Estudios Industriales y Empresariales. Director: Olmedo González Herrera Magíster en Estadística.

Introducción

STRATEGY AM AND PSM SAS es una firma de consultoría, especializada en Gestión de Activos, Seguridad de Procesos, Gestión del Conocimiento e Ingeniería de Mantenimiento y Confiabilidad. La firma dispone de un equipo de trabajo entre 15 – 20 empleados. Su modelo organizacional enfatiza el talento humano y la generación de valor a través de la transformación empresarial. Ubicada en la ciudad de Bogotá D.C con sede principal en la Carrera 7 # 156-10. El desarrollo de su objeto de negocio se ha enfocado a acompañar a diferentes organizaciones del sector minero energético del país en la implementación de metodologías y herramientas que facilitan la toma de decisiones, la gestión de activos y el mantenimiento y la confiabilidad. Grandes grupos empresariales del sector energético (Generación, Transmisión y Distribución de Energía Eléctrica, Minería, Transporte de Gas, Producción y Transporte de crudo) hacen parte del portafolio de clientes de STRATEGY AM AND PSM S.A.S. Los ingresos operacionales de la organización están en un rango de 500.000 – 1.000.000 USD anuales, consolidando su capacidad de generación de valor. Tal como se refleja en el mapa de procesos, es una compañía la cual cuenta con el cliente como núcleo central, alrededor del cual se articulan tres niveles de procesos interdependientes: soporte (comunicaciones, asesoría jurídica, contabilidad, tecnologías de la información, gestión de la calidad, seguridad y salud en el trabajo, así como gestión humana); misionales (consultoría, gestión comercial, academia y gestión del conocimiento); Finalmente, los procesos estratégicos (direccionamiento estratégico, gestión financiera, innovación y fortalecimiento del conocimiento) .

Al ser una firma de consultoría, STRATEGY AM AND PSM SAS la mayoría de los riesgos están relacionados a la gestión administrativa, el manejo de la información, la relación

con los clientes y en menor grado, la prestación ocasional de servicios en instalaciones industriales cuando esto es necesario. Sin embargo, estos riesgos, aunque de menor criticidad se alinean con los enfoques esenciales definidos por la organización: Financiero, Personas, Imagen y reputación.

Por lo anterior, el presente proyecto no tiene como finalidad implementar un sistema integral de gestión de riesgos bajo la totalidad de los lineamientos de la ISO 31000; en su lugar, se orienta al diseño e implementación de buenas prácticas, metodologías y herramientas de gestión de riesgos adaptadas al contexto y nivel de madurez de una empresa de consultoría. En este sentido, el proyecto se plantea como un proceso piloto con un horizonte de ejecución de seis meses, organizando en tres niveles organizacionales: estratégico (orientado a la gestión de riesgos del negocio, estratégicos y emergentes, integrados en el mapa de riesgos corporativo); táctico (enfocado en los riesgos asociados a los procesos organizacionales, registrados en las matrices de riesgos y controles por proceso) y a nivel operativo (dirigido a los riesgos propios de las actividades diarias y de la ejecución de un proyecto vigente en la compañía.) Esto con el fin de garantizar la identificación, monitoreo y mitigación de riesgos en el trabajo diario, con el propósito de anticiparse y abordar de manera sistemática dichas amenazas, garantizando una toma de decisiones más clara y acertada, asignando recursos de forma eficiente y fortaleciendo la resiliencia organizacional.

Este enfoque permitirá a la empresa anticipar y gestionar los riesgos de acuerdo con su contexto, fortalecer la toma de decisiones a partir de información confiable y promover una cultura orientada a la prevención y la mejora continua.

Adicionalmente, se busca definir una metodología junto con un conjunto de herramientas estandarizadas, las cuales serán consolidadas en un manual de gestión integral de riesgos que sirva como guía para la organización. Este manual reunirá y adaptará las metodologías y herramientas de gestión de riesgos al contexto específico de la empresa, facilitando su consulta y aplicación por parte de los diferentes actores involucrados.

1. Cumplimiento de objetivos

Tabla 1.

Cumplimiento de los objetivos específicos del proyecto

N°	Objetivos Específicos		Evidencia del Cumplimiento
1	Realizar un análisis diagnóstico que permita visualizar la situación actual de las buenas prácticas, metodologías y herramientas de gestión de riesgos para la empresa STRATEGY AM AND PSM SAS.	✓	Numeral 9
2	Diseñar y documentar un manual de gestión de riesgos (alineado ISO 31000 y contexto STRATEGY AM AND PSM S.A.S).	✓	Numeral 11.2.1 Apéndice E
3	Diseñar el instructivo de uso de matrices de riesgos y oportunidades para	✓	Numeral 11.2.3 Apéndice F

	procesos y proyectos (AGC-FT-007 y CCS-FT-027).			
4	Definir el toolkit de herramientas y lineamientos de aplicación (cuándo aplicarlas y salidas esperadas).	✓	Numeral 11.2.4 Apéndice G	
5	Diseñar e implementar un sistema de indicadores que permitan el seguimiento y medición de la eficacia de las propuestas de mejoras implementadas.	✓	Numeral 11.2.5 Apéndice H	
6	Desarrollar un programa de capacitación y aplicación a un proceso o un proyecto piloto.	✓	Numeral 11.2.6 Numeral 11.3	

2. Generalidades de la empresa

2.1. Información general de la empresa

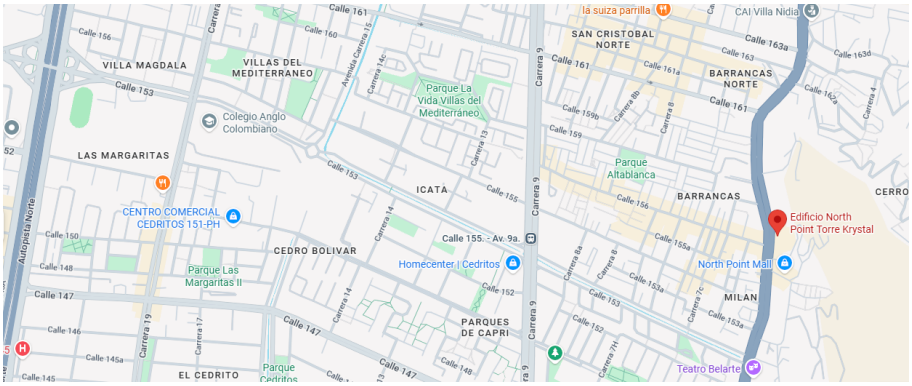
STRATEGY AM AND PSM S.A.S., identificada con el NIT 901.149.285-1 representada legalmente por Natalia Sanabria Jerez es una sociedad por acciones simplificada legalmente constituida en Colombia, con domicilio principal en Bogotá D.C. La empresa se dedica principalmente a actividades de consultoría de gestión bajo la clasificación del código económico 7020.

2.2. Localización

La empresa se encuentra ubicada en la Carrera 7 # 156-10 OF 1901 Torre Krystal. Bogotá, Colombia

Figura 1.

Localización de Strategy AM and PSM SAS



Nota. Mapa de la ubicación de Ak. 7 #156-10, Usaquén, Bogotá, Cundinamarca, Colombia [Captura de pantalla] (Google Maps, 2026)

2.3. Objeto social

Consultoría en Gestión de Activos (ISO 55000), Mantenimiento y Confiabilidad, Seguridad de Procesos, Ingeniería de Mantenimiento y Gestión del Conocimiento.

2.4. ¿Quiénes somos?

STRATEGY AM AND PSM S.A.S es una firma de consultoría, auditoría e implementación de sistemas en Gestión de Activos, Seguridad de Procesos, Gestión del Conocimiento y herramientas de Ingeniería de Mantenimiento y Confiabilidad. Su enfoque es el cambio centrado en el talento humano y la generación de valor a través de la transformación empresarial. (Strategy AM and PSM SAS, 2026)

2.5. Portafolio de productos

STRATEGY AM AND PSM S.A.S brinda una amplia gama de servicios de consultoría profesional, con enfoque en Gestión de Activos, Seguridad de Procesos, Gestión del Conocimiento e Ingeniería de Mantenimiento y Confiabilidad, apoyando a

organizaciones en la optimización de sus operaciones, la mejora continua y la generación de valor a través de la transformación empresarial.

Adicionalmente, la empresa cuenta con Strategy Academy, su área de formación especializada donde se dictan cursos en temas clave como preparación para certificaciones internacionales (por ejemplo, el curso Profesional CAMA2 para la certificación Certified Asset Management Assessor), fortalecimiento de competencias técnicas y programas orientados a elevar el nivel profesional en gestión de activos y mantenimiento (Strategy AM and PSM SAS, 2026).

2.6. Mercados que atiende

La organización presta servicios de consultoría, formación y apoyo en gestión empresarial especialmente para organizaciones intensivas en activos industriales que requieren optimizar la gestión de sus activos, fortalecer sus sistemas de mantenimiento y confiabilidad, mejorar la seguridad de procesos y desarrollar capacidades de gestión del conocimiento dentro de sus equipos. Su enfoque está dirigido a empresas que buscan transformación organizacional y cultural en estas áreas especializadas dentro del sector de consultoría de gestión.

2.7. Canales de distribución

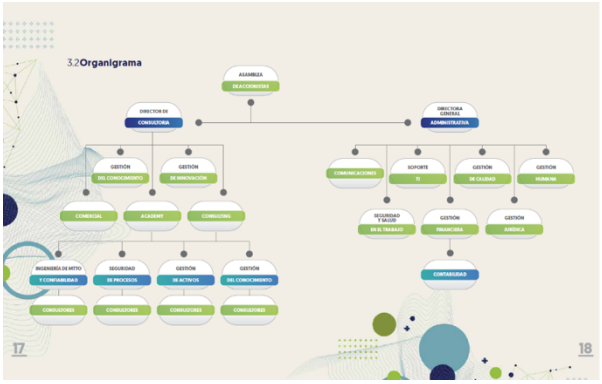
La empresa comercializa y entrega sus servicios principalmente a través de contacto directo con clientes corporativos, utilizando canales como su sitio web, comunicaciones por correo electrónico, llamadas telefónicas y reuniones personalizadas para gestión de proyectos y formación, congresos del sector y eventos promocionales, lo que permite establecer acuerdos de consultoría, ventas de cursos, rutas de formación y acompañamientos profesionales de manera directa con cada organización interesada.

2.8. Organigrama

La compañía muestra una estructura organizacional de tipo funcional encabezada por la Asamblea de Accionistas, de la cual se derivan dos áreas principales: la Dirección de Consultoría y la Dirección General Administrativa; la Dirección de Consultoría concentra las actividades misionales de la empresa, integrando la gestión del conocimiento y la innovación, así como las áreas comercial, academy y consulting, apoyadas por equipos de consultores especializados en ingeniería, seguridad de procesos, gestión de activos y del conocimiento, mientras que la Dirección General Administrativa agrupa las áreas de apoyo estratégico y operativo, tales como comunicaciones, soporte de tecnologías de la información, gestión de calidad y gestión humana, además de funciones transversales como seguridad y salud en el trabajo, gestión financiera, jurídica y contable, las cuales garantizan el adecuado funcionamiento y sostenibilidad de la organización.

Figura 2.

Organigrama STRATEGY AM AND PSM SAS



3. Planteamiento del problema

STRATEGY AM AND PSM S.A.S., como firma de consultoría especializada en gestión de activos, seguridad de procesos, gestión del conocimiento e ingeniería de mantenimiento y confiabilidad, desarrolla sus actividades en un entorno que demanda altos niveles de exigencia técnica, manejo confidencial de la información y toma de decisiones oportunas y fundamentadas. Si bien la organización no enfrenta de manera permanente riesgos operacionales de alta criticidad, sí se encuentra expuesta a diversos riesgos relacionados con la gestión administrativa, el manejo de la información, la relación con los clientes y la ejecución ocasional de proyectos en entornos industriales.

Actualmente, la gestión de riesgos se realiza de forma parcial y sin un enfoque estandarizado, apoyándose principalmente en la experiencia y el conocimiento del personal. Esta situación dificulta la identificación, el análisis, el seguimiento y el tratamiento sistemático de los riesgos. Asimismo, la ausencia de una política formal, lineamientos metodológicos claros y herramientas integradas puede generar inconsistencias en la toma de decisiones, un uso ineficiente de los recursos y una limitada capacidad de anticipación frente a eventos que puedan afectar los objetivos estratégicos, la reputación corporativa y la sostenibilidad financiera de la organización.

Desde esta perspectiva, surge la necesidad de diseñar e implementar un conjunto de buenas prácticas, metodologías y herramientas de gestión de riesgos ajustadas al entorno de una empresa de consultoría, que contribuyan al fortalecimiento de una cultura organizacional orientada a la prevención y la mejora continua, sin requerir la adopción completa de un sistema de gestión bajo el marco de la norma ISO 31000.

Desde el enfoque metodológico, se propone desarrollar un modelo piloto de gestión de riesgos aplicable a distintos niveles organizacionales, integrando herramientas existentes y adaptándolas a las particularidades de la empresa. Este enfoque puede constituirse como referencia para estudios y aplicaciones similares en organizaciones de servicios profesionales, en la medida en que una gestión de riesgos más estructurada contribuye a la sostenibilidad organizacional, al fortalecimiento del empleo y a la mejora en la calidad de los servicios prestados, generando un impacto positivo en el entorno económico y organizacional.

De igual forma, desde la pertinencia disciplinar, el proyecto aporta al fortalecimiento de áreas como la ingeniería industrial, la gestión organizacional y la gestión de la calidad, al incorporar principios de gestión de riesgos en procesos de consultoría, ampliando sus escenarios de aplicación y contribuyendo a la mejora de las prácticas profesionales asociadas.

En este contexto, el problema central que orienta el proyecto se resume en la siguiente pregunta: ¿Cómo diseñar e implementar, en un periodo de seis meses, buenas prácticas de gestión de riesgos adaptadas al contexto organizacional de la compañía, que permitan identificar, monitorear y gestionar de manera sistemática los riesgos estratégicos, tácticos y operativos, fortaleciendo la toma de decisiones, la asignación eficiente de recursos y la resiliencia organizacional?

4. Justificación

La gestión del riesgo se ha consolidado como un elemento clave para el adecuado funcionamiento de cualquier organización, ya que permite identificar, analizar y responder de forma anticipada a situaciones inciertas que pueden afectar el cumplimiento de los objetivos estratégicos y operativos. Este enfoque no solo contribuye a disminuir posibles

pérdidas, sino que también fortalece la capacidad organizacional para aprovechar oportunidades y adaptarse a cambios del entorno, incrementando su resiliencia. En el caso de las pequeñas y medianas empresas (PYMES), donde los recursos suelen ser limitados y la exposición a riesgos puede ser mayor, la adopción de buenas prácticas en gestión de riesgos favorece una toma de decisiones más sólida y una mayor estabilidad organizacional.

En este sentido, la implementación de buenas prácticas basadas en la norma ISO 31000 ofrece un enfoque estructurado y adaptable que puede integrarse a los procesos organizacionales, desde la planeación estratégica hasta las actividades operativas. Este marco proporciona directrices que facilitan la identificación, el análisis y la evaluación de riesgos, así como la definición de estrategias para su tratamiento, lo que se traduce en una mejor preparación frente a eventos adversos y en la protección del valor de la organización.

Por lo anterior, el presente proyecto de grado responde a la necesidad de brindar a la PYME objeto de estudio una propuesta concreta de buenas prácticas en gestión del riesgo, orientada a fortalecer su capacidad de anticipación y respuesta frente a posibles eventos adversos. Asimismo, busca promover una cultura organizacional basada en la prevención, la mejora continua y la sostenibilidad en el largo plazo. Al desarrollar e integrar estas prácticas, la organización podrá optimizar el uso de sus recursos, fortalecer la confianza de sus partes interesadas y mejorar su desempeño de manera estable y competitiva dentro de su sector.

5. Objetivos

5.1. Objetivo general

Diseñar e implementar un modelo de buenas prácticas, metodologías y herramientas de gestión de riesgos adaptadas al contexto de la empresa STRATEGY AM AND PSM SAS.

5.2. Objetivos específicos

- Realizar un análisis diagnóstico que permita visualizar la situación actual de las buenas prácticas, metodologías y herramientas de gestión de riesgos para la empresa STRATEGY AM AND PSM SAS.
- Diseñar y documentar un manual de gestión de riesgos (alineado ISO 31000 y contexto STRATEGY AM AND PSM S.A.S).
- Diseñar el instructivo de uso de matrices de riesgos y oportunidades para procesos y proyectos (AGC-FT-007 y CCS-FT-027).
- Definir el toolkit de herramientas y lineamientos de aplicación (cuándo aplicarlas y salidas esperadas).
- Diseñar e implementar un sistema de indicadores que permitan el seguimiento y medición de la eficacia de las propuestas de mejoras implementadas.
- Desarrollar un programa de capacitación y aplicación a un proceso o un proyecto piloto.

6. Resultados Esperados

- Se espera que al finalizar el proyecto se haya diseñado una metodología de gestión de riesgos adaptada al contexto de STRATEGY AM AND PSM SAS, alineada con los principios de la NTC-ISO 31000, que describa de manera clara y operativa el proceso completo de gestión de riesgos

- El proyecto permitirá la elaboración de un manual de gestión integral de riesgos que compile de forma estructurada la metodología, las herramientas, los roles y las responsabilidades asociadas, generando un documento para estandarizar la gestión de riesgos en STRATEGY AM AND PSM SAS.
- Se espera que al finalizar el piloto de la metodología y herramientas de gestión de riesgos en un proyecto de la compañía se hayan documentado los resultados operativos, los principales aprendizajes y los ajustes necesarios para optimizar el proceso, generando un informe de lecciones aprendidas que sirva como base para el despliegue de la metodología en el resto de la organización.
- Se desarrollará programa de capacitación y socialización dirigido al personal involucrado, para asegurar la apropiación de la metodología, las herramientas y los roles definidos en la gestión de riesgos.

7. Marco de Referencia

7.1. Marco de antecedentes

(Corredor Guerrero, 2017) desarrolla el trabajo titulado “Diseño y formulación de un sistema de gestión de riesgos basado en la norma NTC-ISO 31000:2011 para la Corporación CDT de Gas”, cuyo objetivo es diseñar, estructurar e implementar un sistema de gestión de riesgos alineado con dicha norma para una organización del sector energético. En su investigación, el autor parte de un diagnóstico inicial realizado mediante una matriz DOFA y una lista de chequeo contra los requisitos de la NTC-ISO 31000, identificando un nivel de cumplimiento del 7 % antes de la intervención. A partir de ese diagnóstico, procede a formular una política de riesgos, caracterizar los procesos organizacionales, diseñar formatos estandarizados (matrices FGR-01 a FGR-05), valorar los riesgos inherentes y residuales, y

definir planes de tratamiento, monitoreo, revisión y auditoría interna. El estudio concluye que la aplicación sistemática del modelo propuesto eleva el cumplimiento de la norma al 91 %, fortalece la cultura de gestión del riesgo y soporta la mejora continua a través de indicadores y auditorías periódicas. Este antecedente aporta de manera directa y contextualizada al mostrar cómo adaptar los lineamientos de la NTC-ISO 31000 a una entidad específica, combinando diagnóstico, diseño metodológico, herramientas documentales y un ciclo completo de implementación y auditoría, aspectos que guardan estrecha relación con el enfoque metodológico y estructural propuesto en el proyecto de la organización.

(Présiga Restrepo, Mejía Gómez, Londoño Giraldo , 2021) en su trabajo de grado "Análisis de la Gestión del Riesgo Financiero en las Pymes Manufactureras de Medellín", buscó analizar la importancia de la gestión del riesgo financiero en pequeñas y medianas empresas manufactureras mediante indicadores financieros que permiten identificar amenazas y debilidades organizacionales, aportando al entendimiento de cómo se pueden medir y mitigar factores de riesgo en contextos empresariales reales. Este estudio demuestra que más del 70 % de las empresas analizadas presentan riesgos financieros significativos y que la implementación de métodos claros de análisis contribuye a la toma de decisiones estratégicas para mitigar dichos riesgos, lo cual aporta al desarrollo de marcos metodológicos aplicables a entornos organizacionales diversos como STRATEGY AM AND PSM SAS.

(Ayala López, 2016) desarrolla el trabajo titulado "Diseño, estructuración e implementación de un sistema para la gestión integral del riesgo fundamentado en la norma NTC-ISO 31000 versión 2011 para la empresa La Muela S.A.S.", cuyo objetivo es diseñar, estructurar e implementar un sistema de gestión integral de riesgos alineado con la NTC-ISO

31000 para una pyme dedicada a la importación y distribución de insumos médicos y odontológicos. El proyecto se ejecuta en cinco etapas: primero, un diagnóstico inicial y análisis de contexto mediante una lista de chequeo frente a la ISO 31000 (identificando un nivel de cumplimiento del 9 %), análisis de mercado, contexto interno y matriz DOFA; segundo, la creación de manuales de funciones; tercero, el diseño del marco de trabajo que incluye la formulación de la política de riesgos, la definición de rendición de cuentas, el plan estratégico, el plan de recursos, y los planes de comunicación y formación; cuarto, la implementación del proceso de gestión de riesgos con etapas de identificación, valoración a través de una matriz de probabilidad–impacto y definición de niveles de aceptación; y quinto, el tratamiento de riesgos mediante matrices de tratamiento, monitoreo, definición de indicadores e integración con auditorías internas. El estudio concluye que el sistema diseñado permite incrementar el cumplimiento frente a los requisitos de la NTC-ISO 31000 del 9 % inicial al 90 %, fortalece la cultura organizacional en torno al riesgo, mejora la toma de decisiones y establece una base documental y procedimental para la mejora continua. Este antecedente demuestra que un enfoque por procesos y etapas es eficaz en pymes de servicios y comercio y aporta elementos metodológicos y estructurales que pueden ser adaptados en el proyecto de la organización para el diseño e implementación de una metodología de gestión de riesgos.

7.2. Marco Teórico

7.2.1. *Principios Gestión Del Riesgo*

(Internacional, 2018) El propósito de la gestión del riesgo es generar y proteger valor dentro de la organización. Asimismo, contribuye al mejoramiento del desempeño, al impulso de la innovación y al cumplimiento de los objetivos institucionales. Los principios

establecidos en la norma orientan las características de una gestión del riesgo eficaz y eficiente, al comunicar su finalidad, su valor y su alcance.

En ese sentido, dichos principios constituyen la base sobre la cual se estructura el marco de referencia y el proceso de gestión del riesgo, por lo que deben ser tenidos en cuenta en su diseño e implementación. Su aplicación permite a la organización fortalecer su capacidad para gestionar la incertidumbre y responder de manera adecuada a los efectos que esta pueda generar sobre sus objetivos.

Figura 3.

Principios de gestión integral de riesgos

Nota. Principios de gestión integral de riesgos [Captura de pantalla] (Internacional, 2018)

Integrada: La gestión del riesgo debe incorporarse de manera transversal en todas las actividades de la organización, formando parte de su cultura y de sus procesos en todos los niveles.

Estructurada y exhaustiva: La aplicación de un enfoque sistemático y completo permite obtener resultados consistentes, comparables y confiables en la identificación y tratamiento de los riesgos.

Personalizada: El marco y los procesos de gestión del riesgo deben ajustarse a las características del contexto interno y externo, así como a los objetivos específicos de cada organización.

Participativa: La participación oportuna de las partes interesadas aporta diferentes perspectivas y conocimientos, lo que enriquece el proceso y favorece una toma de decisiones más informada.

Dinámica: La gestión del riesgo debe ser capaz de anticipar, identificar y responder de manera ágil a cambios y riesgos emergentes que puedan impactar los objetivos organizacionales.

Basada en evidencia: Se fundamenta en el uso de información disponible histórica, actual y prospectiva reconociendo sus limitaciones y asegurando su acceso de manera clara y oportuna.

Sensible al factor humano: Considera la influencia del comportamiento de las personas y la cultura organizacional en todas las etapas del proceso de gestión del riesgo.

De mejora continua: Evoluciona de manera constante a partir del aprendizaje organizacional y la experiencia adquirida.

7.2.2. *Marco de referencia de la gestión integral de riesgos*

El éxito de la gestión del riesgo depende directamente de la efectividad del marco de referencia, ya que este establece las bases y directrices que orientan su aplicación en toda la organización. Dicho marco permite que la información asociada a los riesgos sea utilizada de manera adecuada, facilitando la toma de decisiones y la asignación de responsabilidades en los diferentes niveles organizacionales. Asimismo, facilita la integración de la gestión del riesgo dentro del sistema general de gestión, siempre que se adapte a las características y

necesidades particulares de la organización. En este sentido, los principios, el marco y el proceso de gestión del riesgo se encuentran estrechamente vinculados: los principios orientan la forma en que se comprende y valora el riesgo; el marco establece la estructura que permite desplegar la gestión en toda la entidad; y el proceso define las etapas prácticas para identificar, analizar, evaluar, tratar y supervisar los riesgos de manera sistemática y coherente.

Figura 4.

Marco de referencia de la gestión integral de riesgos

Nota. Marco de referencia de la gestión integral de riesgos [Captura de pantalla] (Internacional, 2018)

7.2.3. *Liderazgo y compromiso*

La alta dirección y los órganos de supervisión, cuando corresponda, deben garantizar que la gestión del riesgo se integre en todas las actividades de la organización, demostrando liderazgo y compromiso mediante:

- La adopción e implementación de todos los componentes del marco de referencia.
- La emisión de una declaración o política que defina el enfoque, las directrices o el plan de acción para la gestión del riesgo.

- La asignación de los recursos necesarios para el adecuado tratamiento y control de los riesgos.
- La determinación clara de la autoridad, las responsabilidades y las obligaciones de rendición de cuentas en los niveles pertinentes de la organización.

Esto permitirá a la organización alinear la gestión del riesgo con sus objetivos, estrategia y cultura; reconocer y atender tanto sus obligaciones como los compromisos voluntarios que asuma; y definir la magnitud y el tipo de riesgo que puede o no aceptar, orientando así el desarrollo de los criterios de riesgo y garantizando su adecuada comunicación a la organización y a las partes interesadas. Asimismo, contribuirá a comunicar el valor de la gestión del riesgo, fomentar el seguimiento sistemático de los riesgos y asegurar que el marco de referencia permanezca pertinente y ajustado al contexto organizacional.

7.2.4. *Integración*

Según (Internacional, 2018) la integración de la gestión del riesgo depende de la comprensión de las estructuras y el contexto de la organización. Las estructuras difieren dependiendo del propósito, las metas y la complejidad de la organización. El riesgo se gestiona en cada parte de la estructura de la organización. Todos los miembros de una organización tienen la responsabilidad de gestionar los riesgos.

La gobernanza define la dirección de la organización, establece sus relaciones tanto internas como externas y determina las reglas, procesos y prácticas necesarios para el cumplimiento de su propósito. A partir de esta orientación, las estructuras de gestión permiten traducir dichas directrices en estrategias y objetivos orientados al logro de un desempeño sostenible y a la viabilidad en el largo plazo. En este marco, la asignación clara de roles para

la rendición de cuentas y la supervisión de la gestión del riesgo constituye un elemento fundamental dentro de la gobernanza organizacional.

7.2.5. *Diseño*

La organización debe analizar su contexto interno y externo al diseñar el marco de gestión del riesgo, asegurando que este sea pertinente y actualizado.

El contexto externo comprende factores sociales, políticos, económicos, tecnológicos, legales y ambientales, así como las tendencias del entorno, las condiciones del mercado y las expectativas de las partes interesadas. También incluye aspectos como la competencia, las alianzas estratégicas, los recursos disponibles y otros elementos que pueden influir en el logro de los objetivos. La comprensión de este entorno permite anticipar riesgos y aprovechar oportunidades de manera oportuna.

Por su parte, el contexto interno abarca la misión, la visión, la estructura organizacional, así como los roles y responsabilidades definidos. Asimismo, considera la estrategia, la cultura organizacional y las políticas internas, junto con los recursos disponibles humanos, tecnológicos y financieros, los sistemas de información y los mecanismos de comunicación interna. Este análisis facilita la identificación de fortalezas y debilidades que inciden en la gestión del riesgo.

7.2.6. *Implementación*

La organización debe implementar el marco de referencia para la gestión del riesgo mediante la formulación de un plan que contemple de manera clara los plazos, los recursos y las responsabilidades. Asimismo, es necesario definir cómo, cuándo, dónde y quién toma las decisiones a lo largo de la organización, así como realizar los ajustes pertinentes en los procesos asociados a la toma de decisiones cuando sea necesario.

De igual forma, resulta fundamental asegurar que las disposiciones establecidas para la gestión del riesgo sean comprendidas y aplicadas de manera adecuada en todos los niveles organizacionales. La implementación efectiva del marco de referencia requiere el compromiso de la alta dirección y la participación activa de las partes interesadas, con el propósito de integrar la gestión de la incertidumbre en la toma de decisiones y considerar de manera oportuna los nuevos riesgos que puedan surgir.

7.2.7. *Valoración*

De acuerdo con la NTC-ISO 31000, la evaluación de la eficacia del marco de referencia implica la realización de mediciones periódicas de su desempeño, considerando su alineación con el propósito organizacional, los planes de implementación, los indicadores clave y los resultados esperados. Asimismo, es necesario verificar de manera continua su idoneidad para respaldar el cumplimiento de los objetivos estratégicos y operativos de la organización.

7.2.8. *Mejora*

La mejora se basa en un monitoreo constante y adaptaciones ante variaciones contextuales, optimizando el valor del marco de referencia. La norma promueve la mejora continua de su idoneidad, adecuación y eficacia, mediante la identificación de brechas, desarrollo de planes correctivos y su implementación responsable, lo que integra sólidamente el proceso de gestión del riesgo.

7.3. Proceso

7.3.1. *Generalidades*

El proceso de gestión del riesgo comprende la aplicación sistemática de políticas, procedimientos y prácticas en actividades como la comunicación y consulta, el

establecimiento del contexto, la evaluación y el tratamiento del riesgo, así como su seguimiento, revisión, registro e informe. Este proceso se representa de manera esquemática en la Figura 5.

Figura 5.

Proceso de la gestión integral de riesgos

Nota. Proceso de la gestión integral de riesgos [Captura de pantalla] (Internacional, 2018)

La comunicación y la consulta tienen como propósito principal facilitar que las partes interesadas comprendan los riesgos, los fundamentos de las decisiones adoptadas y la justificación de las acciones definidas. Mientras que la comunicación promueve la sensibilización y el entendimiento del riesgo, la consulta permite obtener aportes e información que fortalecen la toma de decisiones. Su adecuada integración favorece un flujo de información relevante, actual, precisa y accesible, garantizando al mismo tiempo la confidencialidad, la integridad de los datos y la protección de la privacidad.

7.3.2. *Comunicación y consulta*

La comunicación y consulta tienen como objetivo principal ayudar a las partes interesadas relevantes a entender los riesgos, los fundamentos de las decisiones adoptadas y la justificación de las medidas requeridas. Mientras la comunicación fomenta la

sensibilización y comprensión del riesgo, la consulta genera aportes y datos que fortalecen la toma de decisiones; su integración efectiva promueve un flujo de información factual, actual, relevante, precisa y accesible, respetando la confidencialidad, integridad de datos y privacidad individual.

Estas actividades deben ejecutarse de manera continua con stakeholders internos y externos en cada fase del proceso de gestión del riesgo. Sus beneficios incluyen:

- Integrar diversas especialidades en todas las etapas del proceso.
- Incorporar perspectivas variadas al definir criterios de riesgo y evaluar su magnitud.
- Suministrar datos suficientes para monitorear riesgos y respaldar decisiones.
- Fomentar inclusión y sentido de responsabilidad en los afectados.

7.3.3. *Alcance, Contexto y Criterios*

El establecimiento del alcance, el contexto y los criterios tiene como propósito adaptar el proceso de gestión del riesgo, de manera que permita realizar una evaluación eficaz y definir un tratamiento adecuado de los riesgos.

7.3.3.1. Definición del alcance. La organización debe establecer con precisión el alcance de sus actividades de gestión del riesgo. Dado que este proceso puede aplicarse en distintos niveles. Estratégico, operativo, de programas, de proyectos u otras actividades. Resulta fundamental definir claramente cuál es el ámbito considerado, los objetivos específicos que se deben abordar y la manera en que estos se articulan con los objetivos generales de la organización. Esta claridad permite asegurar coherencia, pertinencia y efectividad en la gestión del riesgo. En la planificación del enfoque se incluyen las siguientes consideraciones:

- Los objetivos y las decisiones que se necesitan tomar
- Los resultados esperados de las etapas a ejecutar en el proceso
- El tiempo, la ubicación, las inclusiones y las exclusiones especificas
- Las herramientas y las técnicas apropiadas de evaluación del riesgo
- Los recursos requeridos, responsabilidades y registros a conservar
- Las relaciones con otros proyectos, procesos y actividades

7.3.3.2. Contextos externo e interno. Los contextos hacen referencia al entorno en el cual la organización desarrolla sus actividades y persigue el cumplimiento de sus objetivos. En este sentido, el contexto específico del proceso surge del análisis de los entornos interno y externo, permitiendo reflejar de manera precisa las condiciones en las que se lleva a cabo la actividad. La comprensión del contexto es importante porque:

La gestión del riesgo tiene lugar en el contexto de los objetivos y las actividades de la organización

- Los factores organizacionales pueden ser una fuente de riesgo

- El propósito y alcance del proceso de la gestión del riesgo puede estar interrelacionado con los objetivos de la organización como un todo

7.3.3.3. Definición de los criterios del riesgo. La organización debe definir el nivel y el tipo de riesgo que está dispuesta a asumir en relación con sus objetivos, estableciendo criterios que permitan valorar su importancia y orientar la toma de decisiones. Estos criterios deben alinearse con el marco general de gestión del riesgo y adaptarse al contexto específico, reflejando los valores, recursos y políticas de la organización, así como las obligaciones y perspectivas de las partes interesadas.

Para establecer los criterios del riesgo, se debería considerar lo siguiente:

- Tipos y características de las incertidumbres que pueden influir en los resultados y metas.
- Definición y medición de consecuencias (positivas y negativas) y de la probabilidad.
- Consideración de los factores temporales dentro del análisis de riesgos.
- Asegurar consistencia en las mediciones utilizadas.
- Metodología para determinar el nivel de riesgo.
- Integración de combinaciones y secuencias de múltiples riesgos.

Evaluación de la capacidad de la organización para gestionar riesgos.

7.3.4. *Evaluación del riesgo*

La evaluación del riesgo comprende el proceso integral de identificación, análisis y valoración de los riesgos. Este proceso debe desarrollarse de manera sistemática, iterativa y participativa, incorporando el conocimiento y las perspectivas de las partes interesadas.

Asimismo, es fundamental basarse en la mejor información disponible, la cual puede ser complementada con estudios o análisis adicionales cuando sea necesario.

7.3.4.1. Identificación del riesgo. Su fin es detectar, caracterizar y especificar riesgos que faciliten u obstaculicen metas organizacionales, usando información actual y relevante. Se aplican técnicas variadas para mapear incertidumbres sobre objetivos, considerando interrelaciones entre:

- Las fuentes de riesgo tangibles e intangibles
- Las causas y los eventos
- Las amenazas y las oportunidades
- Las vulnerabilidades y las capacidades
- Los cambios en los contextos externo e interno
- Los indicadores de riesgos emergentes
- La naturaleza y el valor de los activos y los recursos
- Las consecuencias y sus impactos en los objetivos
- Las limitaciones de conocimiento y la confiabilidad de la información
- Los factores relacionados con el tiempo
- Los sesgos, los supuestos y las creencias de las personas involucradas

7.3.4.2. Análisis del riesgo. Su propósito es comprender la naturaleza del riesgo, así como sus principales características y, cuando sea posible, su nivel de magnitud. Para ello, se analizan las incertidumbres, sus causas y posibles consecuencias, junto con la probabilidad de ocurrencia, los escenarios asociados y los controles existentes, evaluando además su efectividad.

Un evento puede generar múltiples impactos en varios objetivos; el nivel de profundidad varía según datos disponibles, recursos y objetivos analíticos, combinando enfoques cualitativos, cuantitativos o mixtos.

El análisis del riesgo debería considerar factores tales como:

- La probabilidad de los eventos y de las consecuencias
- La naturaleza y la magnitud de las consecuencias
- La complejidad y la interconexión
- Los factores relacionados con el tiempo y la volatilidad
- La eficacia de los controles existentes
- Los niveles de sensibilidad y de confianza

7.3.4.3. Valoración del riesgo. De acuerdo con la NTC-ISO 31000, el propósito de la valoración del riesgo es apoyar la toma de decisiones. Este proceso implica comparar los resultados del análisis del riesgo con los criterios previamente establecidos, con el fin de determinar si es necesario implementar acciones adicionales. A partir de esta valoración, se pueden adoptar decisiones como:

- No hacer nada más
- Considerar opciones para el tratamiento del riesgo
- Realizar un análisis adicional para comprender mejor el riesgo

- Mantener los controles existentes
- Reconsiderar los objetivos

Las decisiones deberían tener en cuenta un contexto más amplio y las consecuencias reales y percibidas por las partes interesadas externas e internas.

7.3.4.4. Tratamiento del riesgo. El propósito del tratamiento del riesgo es identificar y aplicar las estrategias más adecuadas para reducir, transferir, aceptar o aprovechar los riesgos identificados, en coherencia con los objetivos organizacionales. Este proceso se desarrolla de manera iterativa, permitiendo ajustar continuamente las acciones implementadas para asegurar su alineación con la estrategia de la organización. En este sentido, el tratamiento del riesgo comprende:

- Formular y seleccionar opciones para el tratamiento del riesgo
- Planificar e implementar el tratamiento del riesgo
- Evaluar la eficacia de ese tratamiento
- Decidir si el riesgo residual es aceptable
- Si no es aceptable, efectuar tratamiento adicional

7.3.5. *Seguimiento y revisión*

El objetivo del seguimiento y la revisión en la gestión del riesgo es asegurar y mejorar de manera continua la calidad y la eficacia del diseño, la implementación y los resultados del proceso de gestión del riesgo. Este componente no debe abordarse de forma aislada, sino que debe planificarse como parte integral del proceso, con roles y responsabilidades claramente definidos.

El seguimiento y la revisión deben desarrollarse a lo largo de todas las etapas del proceso de gestión del riesgo e implican actividades como la planificación, la recopilación y

análisis de información, el registro de resultados y la retroalimentación al sistema, con el fin de facilitar la toma de decisiones informadas.

Asimismo, los resultados obtenidos deben integrarse en los mecanismos de evaluación del desempeño, en los sistemas de medición internos y en los informes organizacionales, garantizando que los procesos se mantengan alineados con los objetivos y se fortalezcan de manera continua.

7.3.6. *Registro e informe*

El proceso de gestión del riesgo, así como los resultados obtenidos durante su desarrollo, deben documentarse y comunicarse a través de los mecanismos establecidos por la organización. Esto permite garantizar la disponibilidad de información relevante, facilitar la toma de decisiones y fortalecer la gestión del riesgo en todos los niveles.

La documentación y los informes tienen varias finalidades importantes:

- Permitir que las actividades y resultados del proceso de gestión del riesgo se comuniquen a lo largo de toda la organización.
- Suministrar información útil que facilite la toma de decisiones en distintos niveles.
- Contribuir a la mejora continua de las prácticas de gestión del riesgo.
- Favorecer la interacción con las partes interesadas, especialmente con quienes tienen la responsabilidad de gestionar y rendir cuentas sobre los riesgos.

Además, las decisiones sobre la generación, conservación y tratamiento de la información registrada deben considerar factores como el uso previsto de la información, su sensibilidad y el contexto interno y externo de la organización.

7.3.7. *COSO ERM (2017): Integración riesgo con estrategia*

El marco (COSO ERM, 2017) resalta que la gestión del riesgo debe integrarse de manera directa en la formulación y ejecución de la estrategia organizacional, evitando que se trate como una actividad aislada. De igual forma enfatiza la necesidad de considerar los riesgos desde la definición de la estrategia y los objetivos, hasta su impacto en la toma de decisiones y el desempeño organizacional.

En este sentido, el modelo reconoce que los riesgos influyen tanto en la creación como en la preservación y generación de valor dentro de la organización. Por ello se busca fortalecer la alineación entre la gestión del riesgo, la estrategia y el desempeño, permitiendo una comprensión más integral de cómo los riesgos pueden afectar los objetivos estratégicos y las decisiones en todos los niveles organizacionales.

7.3.8. *ISO 31000:2018*

La norma internacional ISO 31000:2018 suministra principios y directrices para la gestión del riesgo en organizaciones de cualquier tamaño y sector, con énfasis en la creación y protección de valor mediante la integración sistemática del riesgo en los procesos decisorios. Publicada por la Organización Internacional de Normalización (ISO), esta edición enfatiza un enfoque estratégico y adaptable, reconociendo que el riesgo representa el efecto de la incertidumbre sobre los objetivos organizacionales, el cual puede manifestarse como desviaciones positivas o negativas respecto a lo esperado. (ISO, ISO 31000:2018 – Risk management — Guidelines, 2018)

7.3.9. *ISO 31010:*

La norma (ISO, Risk assessment techniques ISO 31010 , 2019) hace parte del conjunto de estándares relacionados con la gestión del riesgo y proporciona orientación para

la selección y aplicación de técnicas destinadas a la evaluación de riesgos, abarcando su identificación, análisis y valoración en diversos contextos organizacionales. (ISO, Risk assessment techniques ISO 31010 , 2019)

Según (ISO, Risk assessment techniques ISO 31010 , 2019), la identificación de riesgos se basa en técnicas que permiten detectar fuentes, causas y posibles eventos que podrían afectar los objetivos establecidos. Entre las técnicas más empleadas están: lluvia de ideas, entrevistas estructuradas o semiestructuradas, método Delphi, listas de verificación y técnicas más estructuradas como el Structured What-If Technique (SWIFT).

7.3.10. *Riesgo*

Según la norma internacional ISO 31000:2018, el concepto de riesgo se entiende como el efecto de la incertidumbre sobre los objetivos de una organización. Este enfoque destaca que el riesgo no se limita únicamente a resultados negativos, sino que también puede implicar desviaciones de lo esperado que sean positivas o negativas, dependiendo de las situaciones y del impacto que tengan sobre los objetivos planteados. En este sentido, el término “efecto” se refiere a una desviación respecto de lo esperado, lo cual puede manifestarse como una amenaza o como una oportunidad para la organización, y el riesgo suele expresarse mediante la combinación entre las consecuencias de un evento y la probabilidad de que dicho evento ocurra. (ICONTEC, 2018)

7.3.11. *Gestión del riesgo*

La gestión del riesgo se refiere a las actividades coordinadas para dirigir y controlar una organización con relación al riesgo. Este concepto implica que la gestión no es una acción aislada, sino un conjunto de procesos y decisiones que permiten identificar, analizar, evaluar y tratar los riesgos de manera sistemática, con el fin de apoyar el logro de los objetivos de la organización. (ICONTEC, 2018)

En los estudios de gestión de riesgos, el concepto de riesgo se relaciona directamente con la incertidumbre de eventos a largo plazo y sus consecuencias. En este sentido, diversos enfoques teóricos consideran que el riesgo no es un atributo aislado, sino una combinación de dos componentes fundamentales: la probabilidad de ocurrencia del evento y la magnitud de sus efectos. (Kent, 2016)

Dentro de este marco conceptual, la probabilidad se refiere a la posibilidad de que un evento de riesgo se materialice, mientras que el impacto corresponde a la magnitud de las consecuencias negativas que ese evento podría causar sobre los objetivos, recursos o resultados esperados. (OAP, 2016) Por su parte, el impacto refiere a la severidad de las consecuencias que tendría dicho evento sobre los objetivos, recursos o resultados de un proyecto si éste llegara a ocurrir. (Vazquez, 2024)

Dado lo anterior, el riesgo puede formularse matemáticamente como el producto de la probabilidad por el impacto, lo que permite cuantificar y priorizar los riesgos identificados. Esta relación se expresa mediante la siguiente ecuación:

$$Riesgo = Probabilidad * Impacto$$

La ecuación anterior propone que, cuanto mayor sea la probabilidad de que un evento ocurra y mayor sea el impacto de ese evento, mayor será el nivel de riesgo asociado. Este modelo es ampliamente utilizado en marcos de gestión de riesgos por su simplicidad y utilidad para orientar la evaluación y la toma de decisiones en proyectos y procesos organizacionales. (Kent, 2016)

7.3.12. *Matriz de probabilidad e impacto*

La matriz de probabilidad e impacto es una herramienta fundamental dentro del análisis cualitativo de riesgos en la gestión de proyectos. Esta matriz proporciona un enfoque

estructurado y visual para evaluar y priorizar los riesgos identificados, relacionando dos variables esenciales: la probabilidad de ocurrencia de un evento de riesgo y el impacto que dicho evento tendría sobre los objetivos del proyecto en caso de materializarse. (Banco Interamericano de Desarrollo, 2023)

Figura 6.

Matriz de probabilidad e impacto

Nota. Matriz de probabilidad e impacto Cox's risk matrix theorem and its implications for project risk management (Kailash, 2009)

La matriz se organiza como una tabla bidimensional en la que una dimensión corresponde a la probabilidad de que ocurra un evento y la otra al impacto que dicho evento tendría si se llegara a materializar. Cada una de estas dimensiones se escala, ya sea de manera cualitativa (por ejemplo, con categorías como bajo, medio y alto) o cuantitativa (utilizando valores numéricos). Esto posibilita ubicar cada riesgo en una celda concreta de la matriz según su nivel de probabilidad e impacto.

La principal ventaja de esta herramienta es que integra las dimensiones de probabilidad e impacto para ofrecer una representación visual de los riesgos y ayudar a identificar cuáles representan mayores amenazas para el desarrollo del proyecto. Los riesgos que se sitúan en zonas de alta probabilidad y alto impacto son considerados los más críticos

y, por ello, requieren la implementación de estrategias de mitigación más contundentes. Por el contrario, aquellos riesgos con baja probabilidad y bajo impacto pueden ser simplemente monitoreados o aceptados con menor prioridad.

7.3.13. *Análisis DOFA*

El análisis DOFA, también conocido como análisis SWOT por sus siglas en inglés (Strengths, Weaknesses, Opportunities, Threats), es una herramienta de planeación estratégica utilizada en la gestión de proyectos y en la formulación de estrategias organizacionales. Esta herramienta permite identificar, clasificar y evaluar los factores internos y externos que influyen en el logro de los objetivos establecidos. (Atlassian, 2026)

La matriz DOFA se estructura normalmente en un cuadro de cuatro cuadrantes, donde cada uno representa uno de los componentes mencionados. Esta representación permite al gestor del proyecto visualizar de forma clara y sistemática cómo interactúan los factores internos y externos, facilitando la identificación de áreas críticas que requieren atención estratégica. (Atlassian, 2026)

Figura 7.

Ejemplo de matriz DOFA

	Positivos	Negativos
Internos (factores de la empresa)	FORTALEZAS	DEBILIDADES
Externos (factores del ambiente)	OPORTUNIDADES	AMENAZAS

Nota. Matriz DOFA (Staff de Gerencia, 2018)

Además de su carácter descriptivo, el análisis DOFA permite formular estrategias orientadas a potenciar las fortalezas y aprovechar las oportunidades, al tiempo que facilita la mitigación de las debilidades y amenazas identificadas.

7.3.14. *Estructura organizacional*

En el análisis de la estructura organizacional, se reconoce que las decisiones, responsabilidades y funciones dentro de una entidad se distribuyen en tres niveles jerárquicos claramente definidos: estratégico, táctico y operativo. Esta clasificación permite comprender cómo se orienta y coordina el funcionamiento de la organización para el logro de sus objetivos, así como la manera en que se gestionan la toma de decisiones y la ejecución de las actividades diarias. (UNADM, 2025)

7.3.14.1. Nivel estratégico. El nivel estratégico concierne al nivel superior de la organización, donde se define la visión general, las políticas y los objetivos de largo plazo. En este nivel, directivos y alta dirección trazan las líneas maestras que orientan la gestión organizacional y establecen el rumbo general de la entidad. (UNADM, 2025)

7.3.14.2. nivel táctico. El nivel táctico, ubicado entre lo estratégico y lo operativo, se encarga de traducir las estrategias generales en planes específicos y acciones concretas para cada área o unidad funcional. Este nivel vincula las decisiones de alto nivel con las actividades que se ejecutarán, coordinando recursos y supervisando la operatividad de los procesos intermedios para asegurar que se cumplan los objetivos establecidos por la alta dirección. (UNADM, 2025)

7.3.14.3. nivel operativo. Por último, el nivel operativo es el nivel inferior de la jerarquía organizacional, donde se realizan las actividades y tareas diarias. Quienes se ubican en este nivel se centran en la ejecución directa de las acciones necesarias para atender las funciones rutinarias que hacen posible la operación de la organización y el cumplimiento de los planes desarrollados en los niveles superiores. (UNADM, 2025)

La representación de estos tres niveles suele hacerse mediante una estructura jerárquica o pirámide, en la cual el nivel estratégico está en la cúspide, seguido por el nivel táctico en la parte intermedia, y finalmente el nivel operativo en la base.

En relación con los roles organizacionales, cada nivel tiene funciones específicas: el nivel estratégico está asociado con la formulación de políticas y objetivos a largo plazo, el nivel táctico con la planificación y coordinación de procesos internos, y el nivel operativo con la ejecución y supervisión de las tareas rutinarias que sostienen la operación diaria de la entidad.

7.3.15. *Gestión del riesgo organizacional*

La gestión del riesgo organizacional compone un proceso fundamental para la sostenibilidad y el desempeño de las organizaciones, al permitir identificar, analizar y gestionar los eventos de incertidumbre que pueden afectar el cumplimiento de los objetivos estratégicos, tácticos y operativos. Según la norma ISO 31000:2018, el riesgo se define como el efecto de la incertidumbre sobre los objetivos, entendiendo dicho efecto como cualquier desviación, positiva o negativa, respecto a lo esperado (ISO, ISO 31000:2018 – Risk management — Guidelines, 2018)

Desde una perspectiva estratégica, la gestión del riesgo no se debe abortar únicamente como un mecanismo de control, sino como una herramienta de apoyo a la toma de decisiones y a la creación de valor. (Hopkin, 2018) señala que las organizaciones que integran la gestión del riesgo en sus procesos de planeación y operación presentan altos niveles de resiliencia y capacidad de adaptación frente a entornos variables. En este sentido, la gestión del riesgo se convierte en un componente transversal que apoya la eficiencia operativa, la protección de los activos y la continuidad del negocio.

7.3.16. *Parte interesada*

Según la norma ISO 31000:2018 (ICONTEC, 2018) Una parte interesada se entiende como cualquier persona u organización que puede influir, verse afectada o considerarse afectada por una decisión o actividad en el contexto de la gestión del riesgo. Este concepto incluye tanto a los actores que participan o inciden en los procesos de decisión, como a aquellos que experimentan sus efectos. En el marco de la norma, los términos en inglés *"interested party"* y *"stakeholder"* se traducen al español como "parte interesada", lo que favorece una interpretación uniforme en la literatura académica y profesional.

7.3.17. *Fuente de riesgo*

Según (ICONTEC, 2018), una fuente de riesgo se define como cualquier elemento que, de manera individual o en interacción con otros, tiene el potencial de generar situaciones que puedan afectar el logro de los objetivos organizacionales. Estas fuentes pueden originarse tanto en factores internos como externos a la organización, por lo que su identificación resulta fundamental dentro del proceso de gestión del riesgo. Reconocer las fuentes de riesgo permite comprender el origen de las incertidumbres que inciden en el cumplimiento de las metas y en la toma de decisiones. Asimismo, facilita la evaluación de posibles eventos y la definición de acciones adecuadas para prevenir o mitigar sus efectos. (ICONTEC, 2018)

8. Metodología

Para dar cumplimiento a los objetivos propuestos y garantizar el desarrollo del presente trabajo de grado en modalidad práctica empresarial, se implementó un conjunto de herramientas orientadas a promover el diseño e implementación de buenas prácticas de gestión de riesgos adaptadas al contexto de una firma de consultoría clasificada como PYME en Colombia. La metodología propuesta para la ejecución del proyecto se sustenta en un enfoque aplicado y descriptivo con orientación cualitativa, ya que se busca analizar y describir detalladamente el fenómeno de la gestión del riesgo dentro de la organización y cómo este se integra en su toma de decisiones y procesos cotidianos. El desarrollo metodológico se apoya principalmente en los lineamientos establecidos por la norma ISO 31000:2018, que proporciona un marco flexible y adaptable para integrar la gestión del riesgo en todas las funciones organizacionales y apoyar la toma de decisiones informadas,

mejorando así la capacidad de respuesta de la empresa frente a situaciones inciertas (Hopkin, 2018).

El proyecto se articula en cinco etapas secuenciales, diseñadas en congruencia con el cronograma de actividades y los objetivos propuestos. Esta estructura permite una ejecución ordenada y sistemática de las actividades a lo largo de un horizonte temporal de seis meses, garantizando el cumplimiento eficiente de las metas establecidas.

8.1. Introducción e identificación de la empresa

En la etapa inicial del proyecto se llevó a cabo un reconocimiento detallado de la empresa, mediante la recopilación de información relevante como datos generales, objeto social, portafolio de productos, mercados atendidos y canales de distribución. Este proceso se desarrolló a partir de la observación directa de la página web oficial de la organización, complementada con información proporcionada por el tutor empresarial.

8.2. Diagnóstico inicial de la empresa

Esta etapa es fundamental para el desarrollo del presente trabajo de grado, ya que permitió obtener un conocimiento detallado de cómo se están ejecutando actualmente las prácticas de gestión de riesgos en la empresa. Los resultados obtenidos a partir del diagnóstico inicial constituyen una parte clave para el avance de los objetivos planteados, al ofrecer una base sólida de información sobre el estado actual de la organización.

Como primera actividad, se realizó una revisión documental interna orientada a identificar el nivel de alineación y cumplimiento de la organización frente a los lineamientos de la NTC–ISO 31000 en materia de gestión del riesgo. Esta revisión incluyó el análisis de políticas y directrices existentes relacionadas con riesgo, calidad, seguridad y continuidad del negocio.

De manera complementaria, se llevaron a cabo conversatorios estructurados con la líder del área de Gestión de Calidad, con el propósito de analizar la percepción del riesgo dentro de la organización, identificar la existencia de prácticas formales o informales de gestión y documentar los criterios utilizados para priorizar y tratar los eventos de riesgo.

Finalmente, la metodología contempló el diseño y la aplicación de un cuestionario cuantitativo administrado de forma virtual, orientado a medir el nivel de madurez de la gestión del riesgo en la organización. Este instrumento se estructuró bajo una escala tipo Likert, permitiendo evaluar dimensiones clave como el conocimiento de políticas y lineamientos, la percepción de la importancia estratégica del riesgo, la capacidad de identificación y reporte, la comunicación interna y la existencia de canales formales de gestión. De esta manera, se integran enfoques cualitativos y cuantitativos en un diseño de investigación mixto, que permite obtener información confiable, válida y una visión integral del estado actual de la gestión del riesgo organizacional.

8.3. Formulación de las propuestas de mejoramiento

A partir del diagnóstico realizado en la organización, se procedió a seleccionar y analizar las propuestas de mejora más pertinentes, considerando tanto las necesidades identificadas como el nivel de madurez en gestión del riesgo y los recursos disponibles para su implementación.

En este contexto, la fase de implementación piloto se orientó a aplicar de manera controlada las buenas prácticas de un modelo de gestión del riesgo diseñado para la compañía, con el propósito de evaluar su viabilidad y pertinencia en un entorno real de operación.

8.4. Implementación propuesta de mejora

Una vez estructurada la propuesta de mejora de las buenas prácticas de un modelo integral de gestión de riesgos, se procedió a diseñar y ejecutar el plan de implementación, con el fin de materializar las acciones definidas y generar beneficios tangibles para la organización.

La implementación se centró en la ejecución controlada de los elementos incluidos en el modelo de gestión integral de riesgos, priorizando aquellos que respondían de manera directa a las necesidades críticas identificadas en el diagnóstico.

8.5. Control y evaluación de los resultados

Esta última etapa se realizó al finalizar la implementación de las respectivas propuestas de mejora que fueron aprobadas por la gerencia, se enfoca en el seguimiento y verificación del cumplimiento de los objetivos planteados.

Esta medición se realizó a través de una revisión documental empleando una matriz de evaluación estructurada basada en los elementos clave de la NTC-ISO 31000 (política de riesgos, responsabilidades, proceso de gestión de riesgos, comunicación y consulta, monitoreo y revisión) con el fin de observar el cambio e identificar el grado de cumplimiento de la organización con los lineamientos de la NTC–ISO 31000 en materia de gestión de riesgos.

Para finalizar, se presentaron a la gerencia de la compañía los resultados obtenidos del proceso de mejoramiento, los cuales evidenciaron los avances en la gestión de riesgos y el grado de cumplimiento con los lineamientos de la NTC-ISO 31000.

9. Diagnóstico de la empresa

9.1. Diagnóstico inicial

Con el propósito de conocer en profundidad el estado actual de la gestión de riesgos en la organización, se llevó a cabo un diagnóstico inicial que abarcó un periodo de aproximadamente dos meses (octubre y noviembre del año 2025), durante el cual se aplicaron un conjunto de herramientas, métodos y técnicas específicas para explorar sistemáticamente la realidad operativa, administrativa y estratégica de la organización. Entre las acciones realizadas destacan:

9.1.1. *Revisión documental*

Como parte del diagnóstico inicial, se llevó a cabo una revisión documental interna orientada a identificar el nivel de alineación y cumplimiento de la organización frente a los lineamientos de la NTC–ISO 31000 en materia de gestión del riesgo. Esta revisión incluyó el análisis de políticas y directrices existentes relacionadas con riesgo, calidad, seguridad y continuidad del negocio. (Ver Apéndice B).

Para el desarrollo del análisis, se empleó una matriz de evaluación estructurada con base en los elementos clave de la NTC-ISO 31000, tales como la política de riesgos, la asignación de responsabilidades, el proceso de gestión del riesgo, la comunicación y consulta, así como el monitoreo y la revisión.

Cada uno de estos componentes fue evaluado mediante un criterio de cumplimiento dicotómico, clasificándose como “Cumple” o “No cumple”, con el propósito de determinar el nivel de alineación de la organización frente a los lineamientos establecidos en el estándar. (Ver Apéndice B).

De igual manera, el análisis contempló la revisión de los formatos internos vigentes, entre los que se incluyen las matrices de riesgos AGC-FT-007 y CCS-FT-027 (ver Apéndices C y D)

Esta revisión se complementó con otros documentos que contienen información relevante de la organización, los cuales se encuentran disponibles en la carpeta asignada al practicante.

9.1.2. *Conversatorios*

Se organizaron reuniones con la líder del área de Gestión de Calidad, con el propósito de identificar la percepción del riesgo, la existencia de prácticas formales o informales de gestión y los criterios actualmente utilizados para priorizar y tratar los eventos de riesgo.

9.1.3. *Cuestionario cuantitativo*

Se diseñó y aplicó un cuestionario estructurado para medir el nivel de madurez de la gestión de riesgos en la organización, el cual fue administrado de manera virtual mediante Google Forms a un total de 12 colaboradores. Aunque el instrumento fue formulado bajo una lógica de percepción organizacional tipo Likert. El cuestionario incluyó ítems orientados a evaluar dimensiones clave como: conocimiento de lineamientos y políticas, percepción de la importancia estratégica del riesgo, capacidad de identificación y reporte, comunicación interna, existencia de canales formales y apoyo organizacional. El instrumento completo aplicado se presenta en el Apéndice A.

9.1.4. *Resultados del diagnóstico*

A continuación, se presentan los resultados del diagnóstico realizado en la organización, a través del cual se evaluó el estado actual de la gestión del riesgo. Estos resultados permiten identificar de manera clara las principales fortalezas, así como las

brechas y oportunidades de mejora, constituyéndose en la base para el diseño e implementación de un modelo de gestión del riesgo ajustado a la realidad de la empresa.

Los resultados del diagnóstico evidencian, en primer lugar, que la organización no cuenta actualmente un sistema de gestión de riesgos formalmente definido y documentado en la compañía, a pesar de que la organización reconoce la importancia del riesgo en sus enfoques financieros, de personas, imagen y reputación. Así mismo, en la revisión se evidenció que la organización aún no ha formalizado una política específica de gestión de riesgos ni un marco de referencia institucional que articule, de manera explícita, la identificación, evaluación, tratamiento, seguimiento y comunicación de los riesgos en los diferentes niveles de proceso.

Como resultado de la revisión documental basada en los elementos clave de la NTC–ISO 31000 (política de riesgos, responsabilidades, proceso de gestión de riesgos, comunicación y consulta, monitoreo y revisión), se evidenció que, de un total de 41 criterios evaluados (ver apéndice B), únicamente 8 cumplen con los lineamientos establecidos, lo que equivale a un 19,51% de cumplimiento. Por su parte, 33 criterios (80,49%) no cumplen con los requisitos evaluados.

Figura 8.

Revisión documental interna norma ISO 31000 estado inicial

Las reuniones sostenidas con la líder del área de Gestión de Calidad permitieron comprender el contexto interno y externo de la empresa, sus objetivos estratégicos y las partes interesadas relevantes, así como la percepción del riesgo, los controles implementados y la cultura organizacional asociada a la gestión de riesgos. Además, el objetivo fue levantar insumos clave para definir roles y responsabilidades, establecer el apetito y la tolerancia al riesgo, determinar el ciclo trimestral de revisión y establecer mecanismos de escalamiento.

Adicionalmente, los resultados del cuestionario cuantitativo aplicado al personal permitieron complementar los hallazgos obtenidos en la revisión documental y los conversatorios. La población objeto de estudio está conformada por un total de 12 trabajadores, desempeñando distintos cargos dentro de la organización, entre los que se encuentran consultores, socios en diferentes áreas y un profesional de comunicaciones. La caracterización sociodemográfica permite analizar variables como género, edad y cargo, las cuales son fundamentales para comprender la composición del talento humano y apoyar la toma de decisiones organizacionales .

En cuanto al género, se evidencia una distribución relativamente equilibrada, con 6 trabajadores de género masculino (50%) y 6 de género femenino (50%). Esto indica una participación equitativa entre hombres y mujeres dentro de la organización, lo cual puede favorecer la diversidad y el equilibrio en los equipos de trabajo.

Respecto a la edad, los trabajadores se encuentran en un rango entre los 23 y 53 años. La mayor concentración se ubica en edades entre los 25 y 34 años, lo que refleja una población laboral predominantemente joven adulta. También se identifican algunos casos de mayor experiencia, como un trabajador de 53 años, lo cual aporta diversidad generacional dentro del equipo.

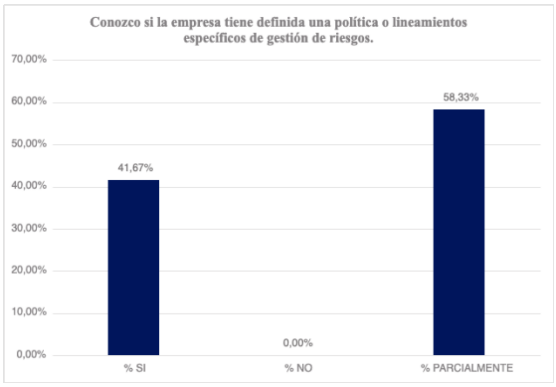
En relación con los cargos, se observa que la mayoría del personal corresponde al cargo de consultor, con un total de 7 trabajadores (58%). Adicionalmente, se identifican cargos estratégicos como socio de recursos humanos, socio de innovación, socio de calidad y socio de comunicación, así como un profesional de comunicaciones. Esta distribución evidencia una estructura organizacional donde predomina el rol operativo (consultores), acompañado de cargos directivos o estratégicos.

En conjunto, esta caracterización permite identificar que la organización cuenta con un equipo equilibrado en términos de género, con predominancia de personal joven y una estructura enfocada principalmente en actividades de consultoría, apoyada por roles estratégicos en áreas clave.

En cuanto al conocimiento de lineamientos formales en materia de gestión de riesgos, el 58,3% de los participantes señaló que únicamente tiene un conocimiento parcial sobre la existencia de una política o directrices específicas en la organización, mientras que el 41,67% manifestó conocerlas. Este comportamiento evidencia que, aunque algunos colaboradores perciben la presencia de lineamientos, estos no se encuentran formalmente consolidados ni comunicados de manera clara, uniforme y estructurada a todo el personal, lo que refleja una debilidad en la institucionalización del sistema de gestión de riesgos.

Figura 9.

Primer pregunta del cuestionario cuantitativo



No obstante, el 66,7% de los encuestados considera que la gestión de riesgos es un tema importante para el logro de los objetivos organizacionales, lo que demuestra una percepción positiva frente a la relevancia estratégica del riesgo. De igual manera, el 66,7% manifestó sentirse cómodo reportando riesgos o incidentes a sus superiores, lo cual representa una fortaleza cultural en términos de apertura y confianza.

Figura 10.

Segunda pregunta del cuestionario cuantitativo

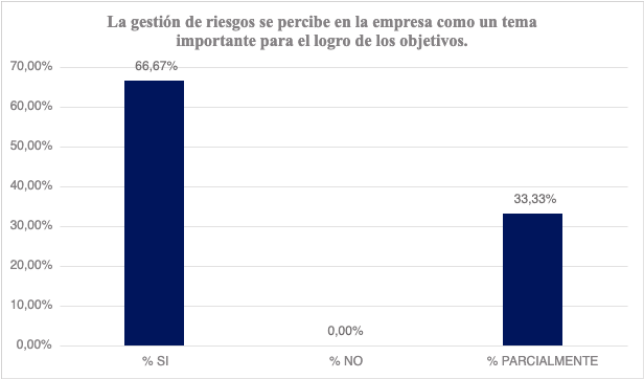
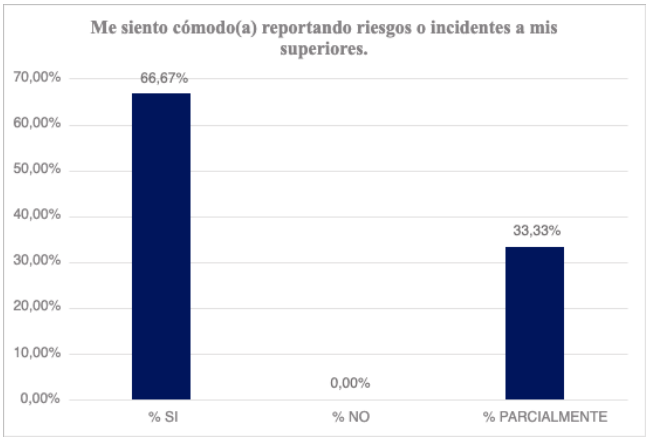


Figura 11.

Cuarta pregunta del cuestionario cuantitativo



En relación con el conocimiento operativo asociado a la gestión de riesgos, el 58,3% de los encuestados manifestó que conoce el procedimiento para identificar y reportar un riesgo; sin embargo, el 41,7% indicó que dicho conocimiento es únicamente parcial, lo que evidencia la ausencia de una estandarización clara y suficientemente difundida en los procesos internos. Esta situación se ve recalcada al analizar el reconocimiento del canal formal de reporte, donde el 41,67% afirmó no conocerlo, el 25% manifestó tener un conocimiento parcial y solo el 33,3% indicó conocerlo plenamente. Estos resultados representan una brecha significativa en la formalización, comunicación y apropiación de los mecanismos institucionales de reporte, aspecto que limita la efectividad del sistema de gestión de riesgos y su adecuada articulación en los niveles operativos de la organización.

Figura 12.

Tercer pregunta del cuestionario cuantitativo

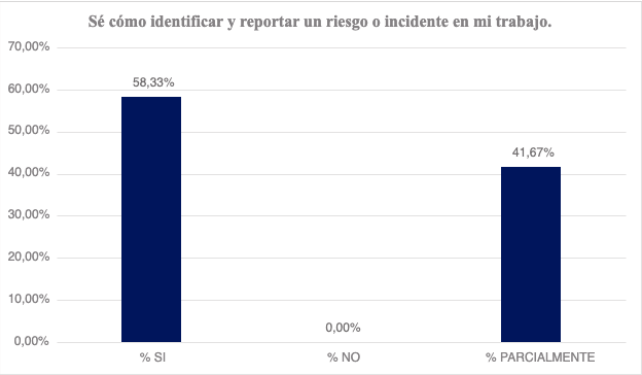
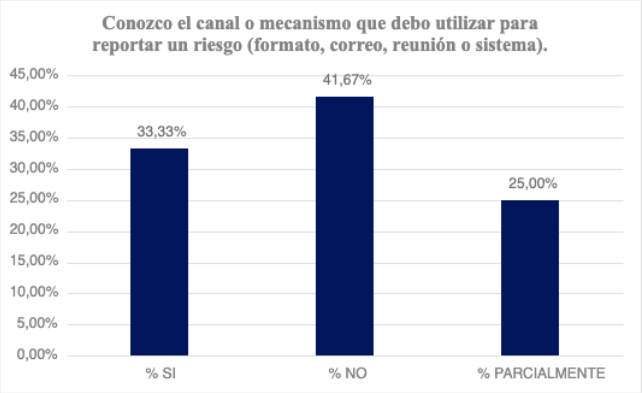


Figura 13.

Quinta pregunta del cuestionario cuantitativo



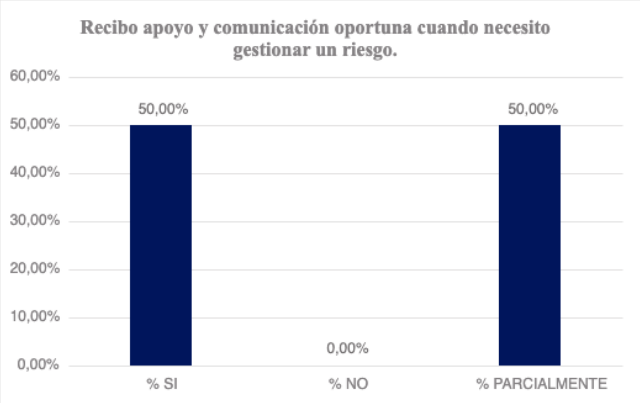
Respecto a la comunicación organizacional interna, el 58,3% considera que esta es solo parcialmente oportuna en materia de riesgos, y únicamente el 41,7% la percibe como adecuada. Asimismo, el 50% de los colaboradores manifestó recibir apoyo oportuno cuando necesita gestionar un riesgo, mientras que el otro 50% lo percibe solo parcialmente, lo que evidencia oportunidades de mejora en el acompañamiento institucional.

Figura 14.

Sexta pregunta del cuestionario cuantitativo

Figura 15.

Séptima pregunta del cuestionario cuantitativo



En conjunto, los resultados de la encuesta confirman que, si bien existe una percepción positiva frente a la importancia del riesgo y una disposición cultural favorable al reporte, la organización presenta debilidades estructurales en la formalización, documentación, comunicación y estandarización del sistema de gestión de riesgos. Estos hallazgos refuerzan la necesidad de diseñar e implementar buenas prácticas, metodologías y herramientas de gestión de riesgos adaptadas al contexto de la empresa, permitiendo avanzar hacia un mayor nivel de madurez organizacional en la gestión de riesgos.

9.2. Diagnóstico final

Como resultado del diseño e implementación de buenas prácticas del modelo de gestión de riesgos en la organización, se evidenció una mejora significativa en el nivel de

cumplimiento frente a los lineamientos establecidos en la norma ISO 31000 (ver apéndice B). Mientras que en el diagnóstico inicial se identificó un cumplimiento del 19,51%, posterior a la adopción de buenas prácticas, herramientas metodológicas y la estructuración del sistema, se alcanzó un nivel de cumplimiento del 73,17%, reflejando un avance sustancial en la madurez del proceso de gestión del riesgo.

Figura 16.

Revisión documental interna norma ISO 31000 estado final

Este incremento se logró mediante la definición e implementación de un enfoque estructurado, alineado con los principios, el marco y el proceso de la norma ISO 31000, la cual promueve la integración de la gestión del riesgo en todos los niveles organizacionales, desde lo estratégico hasta lo operativo, favoreciendo la toma de decisiones informadas y la protección del valor organizacional .

En este contexto, se desarrollaron e implementaron diversas herramientas y mecanismos que fortalecieron el sistema de gestión de riesgos. En primer lugar, se elaboró un manual de gestión de riesgos (ver apéndice E), en el cual se definieron los lineamientos, roles, responsabilidades, metodología y criterios para la identificación, análisis, evaluación, tratamiento, monitoreo y comunicación de los riesgos. Este documento constituye el eje central del sistema, asegurando su estandarización y trazabilidad.

Adicionalmente, se diseñó un sistema de indicadores (ver Apéndice H) orientado al seguimiento del desempeño de los riesgos y a la evaluación de la efectividad de los controles, lo cual permite analizar el comportamiento del riesgo residual y apoyar la toma de decisiones basada en datos. Asimismo, se desarrolló un programa de capacitación dirigido al proceso de soporte TI, con el propósito de fortalecer las competencias del personal en la identificación, análisis y gestión del riesgo, promoviendo una cultura organizacional enfocada en la prevención y la mejora continua.

Como parte fundamental del proceso, se construyó la matriz de riesgos y oportunidades (ver Apéndices C y D), en la cual se integraron los elementos requeridos por la metodología, tales como la identificación de amenazas, el origen del riesgo, su redacción estandarizada, el análisis de probabilidad e impacto, la evaluación del nivel de riesgo, la definición de controles, la asignación de responsables, los mecanismos de comunicación y la determinación del riesgo residual. Esta matriz se consolidó como una herramienta clave para la gestión sistemática y estructurada de los riesgos del proceso.

De igual manera, se aplicaron diversas herramientas que permitieron una comprensión integral del contexto organizacional y de los factores internos y externos que inciden en el proceso. Entre estas se destacan el análisis PESTEL, el análisis DOFA, el análisis Bow Tie y el diagrama de Ishikawa, los cuales facilitaron la identificación de causas, consecuencias y escenarios de riesgo, fortaleciendo la calidad del análisis y la toma de decisiones.

En cuanto al proceso de monitoreo y revisión, se establecieron mecanismos formales de seguimiento que permiten evaluar de manera continua la efectividad de los controles y el comportamiento de los riesgos, garantizando su actualización frente a los cambios del

entorno. Este enfoque se encuentra alineado con la ISO 31000, la cual establece que el monitoreo y la revisión deben ser procesos sistemáticos y continuos orientados a la mejora del desempeño y la adaptación de la gestión del riesgo a la evolución de la organización

10. Formulación de propuestas de mejoramiento

10.1. Etapa 1. Revisión documental y diagnóstico de la gestión de riesgos actual

En esta etapa se realiza una revisión documental de normas, modelos y buenas prácticas en gestión de riesgos, con énfasis en la norma ISO 31000:2018, el marco COSO ERM y literatura especializada en gestión del riesgo organizacional. El objetivo es establecer los fundamentos conceptuales y metodológicos que orientan el proyecto y garantizan la coherencia entre la propuesta metodológica y el marco teórico de igual manera, comprender el contexto interno y externo de la organización, así como identificar el nivel de madurez actual en la gestión de riesgos. Para ello, se analiza la estructura organizacional, el mapa de procesos, los objetivos estratégicos y los factores críticos asociados a los enfoques financiero, de personas, imagen y reputación.

Como producto de esta etapa se definen los criterios base para la gestión de riesgos en organizaciones de servicios y consultoría, así como los elementos mínimos necesarios para su adaptación al contexto de la organización.

10.1.1. *Técnicas e instrumentos*

- Revisión bibliográfica
- Análisis normativo
- Análisis comparativo de modelos.
- Conversatorios
- Análisis documental

10.1.2. *Resultado esperado*

Lineamientos conceptuales y metodológicos que soportan el diseño del modelo propuesto y Diagnóstico del estado actual de la gestión de riesgos y principales brechas identificadas.

10.2. Etapa 2. Diseño del modelo de gestión de riesgos adaptado a la organización

Con base en los resultados del diagnóstico, se diseña un modelo de gestión de riesgos ajustado al contexto de la compañía, tomando como referencia el proceso de gestión del riesgo propuesto por la norma ISO 31000: establecimiento del contexto, identificación, análisis, evaluación y tratamiento del riesgo.

El modelo se estructura para su aplicación en los tres niveles organizacionales:

10.2.1. *Nivel estratégico*

Definición de la política de riesgos, roles y responsabilidades, y criterios de aceptación del riesgo.

10.2.2. *Nivel táctico*

Integración de la gestión del riesgo en el proceso de gestión de la calidad.

10.2.3. *Nivel operativo*

Aplicación de herramientas de identificación y tratamiento de riesgos en la ejecución de un proyecto de un proceso de la compañía.

10.2.4. *Técnicas e instrumentos*

- Matrices de riesgos
- Definición de criterios
- Manual de gestión integral de riesgos

- Instructivo de uso de matrices de riesgos y oportunidades para procesos y proyectos (AGC-FT-007 y CCS-FT-027).
- Toolkit de herramientas y lineamientos de aplicación

10.2.5. *Resultado esperado*

Modelo de gestión de riesgos documentado y alineado con la estrategia organizacional.

10.3. Etapa 3. Implementación piloto del modelo de gestión de riesgos

En esta etapa se realiza la implementación piloto del modelo diseñado, aplicándolo de manera controlada en los procesos estratégicos, tácticos y operativos seleccionados. Se desarrollan sesiones de socialización y acompañamiento al personal involucrado, garantizando la correcta comprensión y aplicación de las herramientas propuestas.

Durante la implementación se realiza el seguimiento al comportamiento de los riesgos identificados y a la efectividad de los controles definidos, permitiendo recopilar información relevante para su posterior análisis.

- Técnicas e instrumentos
- Aplicación de matrices de riesgos
- Seguimiento de controles
- Registros de implementación.

10.3.1. *Resultado esperado*

- Modelo aplicado y validado de manera preliminar en la organización.
- Matrices diligenciadas en un proyecto actual y un proceso de la compañía

10.4. Etapa 4. Ajuste final versiones aprobables

En esta etapa se consolidan, revisan y ajustan todos los productos generados en las fases previas para conformar las versiones finales aptas para evaluación y aprobación por parte de los asesores y comités correspondientes. Este proceso incluye la integración de los comentarios y retroalimentación recibidos durante la ejecución piloto y las revisiones preliminares, de manera que el documento final muestre un trabajo riguroso, coherente y conforme a los criterios académicos institucionales

10.4.1. *Resultado esperado*

Se espera obtener un documento final consolidado y aprobado, que refleje de forma clara, coherente y académicamente sólida los resultados de la investigación y el modelo propuesto, listo para su presentación oficial, evaluación y eventual difusión institucional.

10.5. Etapa 5. Socialización de resultados

Finalmente, se evalúan los resultados obtenidos durante la implementación piloto, analizando la efectividad del modelo propuesto en términos de identificación, tratamiento y monitoreo de riesgos. La información recolectada es interpretada de forma cualitativa, comparando la situación inicial con el estado posterior a la implementación.

10.5.1. *Técnicas e instrumentos*

- Material visual y estructurado que sintetiza los principales hallazgos
- Sesión de socialización y retroalimentación

10.5.2. *Resultado esperado*

Se espera que, al finalizar la socialización de resultados, los participantes comprendan claramente los principales hallazgos del piloto, reconociendo las mejoras logradas en la

identificación, tratamiento y monitoreo de riesgos con respecto a la situación inicial, validen y aporten retroalimentación constructiva sobre los resultados presentados

11. Ejecución y resultado de propuestas de mejoramiento

11.1. Etapa 1. Revisión documental y diagnóstico de la gestión de riesgos actual

La ejecución de esta etapa inició con una revisión de la documentación teórica y normativa relacionada con gestión de riesgos, con énfasis en los lineamientos establecidos por la NTC-ISO 31000:2018 y el marco COSO ERM, así como literatura especializada en gestión del riesgo organizacional. Esta revisión permitió establecer una base conceptual sólida sobre las mejores prácticas y criterios metodológicos aplicables al diseño de un modelo de gestión de riesgos coherente con estándares reconocidos.

Posteriormente, se realizó un análisis del contexto interno de la organización, evaluando aspectos como la estructura organizacional, el mapa de procesos, los objetivos estratégicos y los factores críticos que inciden en la operación, con el fin de identificar su nivel de integración y las posibles brechas frente a las prácticas recomendadas en los marcos normativos revisados.

La recolección de información se llevó a cabo mediante conversatorios con la líder del área de gestión de calidad, la revisión de documentación interna y el análisis de los procesos estratégicos, tácticos y operativos. La información obtenida fue analizada de manera cualitativa, lo que permitió identificar brechas frente a las buenas prácticas establecidas en la literatura revisada.

Finalmente, el análisis de la información recopilada permitió reconocer fortalezas, debilidades y oportunidades de mejora en relación con los principios, criterios y elementos definidos en la NTC-ISO 31000:2018.

Como resultado del desarrollo de esta etapa, se obtuvo un diagnóstico del estado actual de la gestión del riesgo en la organización, el cual presenta una descripción detallada de su nivel de madurez, así como la identificación de los principales vacíos y oportunidades de mejora frente a estándares internacionales.

Identificación de brechas metodológicas y operativas, evidenciando aspectos que requieren intervención para alinear las prácticas internas con las mejores prácticas y lineamientos normativos revisados.

Lineamientos conceptuales y metodológicos base, que servirán como punto de partida para el diseño del modelo de gestión de riesgos adaptado al contexto de la organización. Estos lineamientos integran los criterios mínimos de gestión de riesgos para organizaciones de servicios y consultoría, asegurando coherencia técnica y teórica entre la propuesta metodológica y los marcos revisados.

Estos resultados constituyen que, en la actualidad, la organización no cuenta con un sistema formal de gestión de riesgos definido y documentado, a pesar de que reconoce la importancia de considerar los riesgos en sus enfoques financieros, de personas, así como en su imagen y reputación. Asimismo, la revisión documental y el análisis realizado permitieron evidenciar que no existe una política específica de gestión de riesgos ni un marco de referencia institucional que articule de forma explícita las fases del proceso identificación, evaluación, tratamiento, seguimiento y comunicación de los riesgos en los distintos niveles de la organización.

11.2. Etapa 2. Diseño del modelo de gestión de riesgos adaptado a la organización

Con base en los hallazgos del diagnóstico se diseñaron una serie de herramientas y prácticas necesarias para aplicar las metodologías de gestión de riesgos en la ejecución diaria

de los proyectos y procesos de la organización. Se priorizó la creación de instrumentos que faciliten la identificación, análisis y tratamiento de riesgos de manera sistemática, de forma que puedan ser aplicados de manera práctica en actividades concretas, mejorando la captación de información relevante y apoyando la toma de decisiones.

Durante esta etapa se desarrollaron diversas técnicas e instrumentos de apoyo, tales como:

11.2.1. *Manual de gestión integral de riesgos*

Se diseño un manual de gestión de riesgos ajustado al contexto de la organización, siguiendo las directrices del proceso de gestión de riesgos propuesto por la norma NTC-ISO 31000:2018, que comprende el establecimiento del contexto, la identificación, el análisis, la evaluación y el tratamiento de los riesgos, integrando también la comunicación, consulta, monitoreo y revisión dentro del ciclo de gestión, el cual se presenta en el apéndice E

La construcción del manual de gestión integral de riesgos se realizó de manera escalonada para asegurar que responda a las necesidades operativas y estratégicas de la organización. Inicialmente se definieron los principios y criterios generales del modelo alineados con los lineamientos propuestos por la norma NTC-ISO 31000:2018, adaptando las fases principales del proceso de gestión de riesgos a las realidades de los niveles estratégico, táctico y operativo de la empresa.

Para ello, se definieron los elementos de gobernanza del riesgo, incluyendo la asignación de roles y responsabilidades, así como los criterios de aceptación del riesgo, con el fin de orientar la toma de decisiones y asegurar su alineación con los objetivos corporativos.

11.2.2. *Matrices de riesgos y oportunidades*

Con base en los elementos establecidos en el manual de gestión integral de riesgos y los hallazgos obtenidos en el diagnóstico, se diseñaron las matrices de riesgos y de oportunidades que se presentan en los apéndice C y D**.** Estas matrices se constituyen en herramientas fundamentales para operacionalizar el proceso de gestión de riesgos en la organización, ya que permiten visualizar de forma sistemática los riesgos y oportunidades asociados a los procesos y proyectos, facilitando su evaluación y priorización para una toma de decisiones oportuna e informada.

11.2.3. *Instructivo para el uso de matrices de riesgos y oportunidades*

El instructivo para el uso de matrices de riesgos y oportunidades, presentado en el Apéndice F, constituye una herramienta metodológica orientada a la identificación, evaluación y seguimiento de riesgos y oportunidades en los procesos de la organización. Su estructura permite seleccionar el proceso objeto de análisis, registrar los eventos identificados y valorarlos mediante criterios de probabilidad e impacto, considerando dimensiones financieras, de personas e imagen.

Adicionalmente, incorpora elementos como controles, habilitadores, frecuencias de revisión, responsables y esquemas de comunicación, lo que fortalece la trazabilidad y el seguimiento de las acciones definidas. En conjunto, esta herramienta contribuye a estandarizar el análisis de eventos críticos, facilitando la priorización de acciones de mejora y promoviendo una gestión preventiva y el aprovechamiento de oportunidades dentro del sistema organizacional.

La herramienta inicia con una sección de selección del proceso, lo que permite adaptar la matriz al área específica que se desea analizar, como gestión de calidad,

innovación, dirección estratégica o soporte tecnológico. Posteriormente, el menú principal organiza el acceso a tres secciones: riesgos, oportunidades y matriz de impacto, facilitando una navegación estructurada y su aplicación por parte de los responsables.

En la sección de riesgos, se establecen lineamientos para registrar variables como la amenaza, su origen, los posibles efectos, la probabilidad de ocurrencia, el impacto en términos financieros, de personas e imagen, y el nivel de riesgo inherente. Asimismo, se contemplan los controles preventivos o de mitigación, la frecuencia de revisión, las fechas de seguimiento, los responsables y los mecanismos de comunicación, con el fin de asegurar la trazabilidad y el control periódico.

Por su parte, la sección de oportunidades mantiene una lógica similar, orientada a identificar condiciones favorables que puedan generar beneficios para el proceso. En ella se documentan aspectos como la oportunidad, su origen, el objeto de impacto, la probabilidad, el nivel de oportunidad inherente, los habilitadores o aceleradores, así como los mecanismos de seguimiento, responsables y comunicación.

Finalmente, la matriz de impacto funciona como base técnica para la valoración de riesgos y oportunidades, al definir los criterios de clasificación de la probabilidad y el impacto en las dimensiones financiera, de personas e imagen. Esto permite estimar el nivel de criticidad o beneficio potencial de cada evento, facilitando su priorización y contribuyendo a una toma de decisiones más objetiva y alineada con la mejora continua.

11.2.4. *Toolkit de herramientas y lineamientos de aplicación*

El Toolkit de herramientas y lineamientos de aplicación, presentado en el apéndice G, compone un conjunto integral de instrumentos metodológicos diseñados para apoyar la implementación operativa del modelo de gestión de riesgos y oportunidades en la

organización. Este compendio reúne formatos, guías, criterios y procedimientos que facilitan la identificación, análisis, valoración, tratamiento y monitoreo de riesgos y oportunidades en los distintos procesos, garantizando coherencia y estandarización en su aplicación.

El toolkit está organizado en una estructura de fácil acceso y actualización, alojado en una carpeta de SharePoint de la organización, lo que garantiza que todos los usuarios autorizados dispongan siempre de la versión vigente de los instrumentos y puedan consultar las guías asociadas a cada uno. La carpeta incluye, entre otros elementos, los siguientes archivos, que constituyen piezas centrales del toolkit:

- Plantillas de matrices de riesgos y oportunidades adaptadas a distintos tipos de procesos (por ejemplo, AGC-FT-007 y CCS-FT-027), que permiten identificar, evaluar, priorizar y dar seguimiento a eventos críticos y a condiciones favorables.
- Análisis DOFA, que facilita el análisis de factores externos e internos que pueden influir en el desempeño de los procesos.
- La herramienta PESTEL, que facilita el análisis de factores externos que pueden influir en el desempeño de los procesos.
- Plantillas de diagramas de Ishikawa, útiles para descomponer causas raíz de problemas o variaciones.
- Análisis de diagrama BowTie, que apoya la visualización de relaciones entre amenazas, eventos centrales, consecuencias, barreras y controles.
- Documentos de guía, como el instructivo de uso de matrices y el presente toolkit, que orientan a los usuarios sobre cuándo, cómo y con qué criterios aplicar cada herramienta.

En conjunto, este conjunto de herramientas funciona como una guía operativa que fortalece la consistencia del proceso de gestión del riesgo, promueve el análisis comparativo entre procesos y facilita la toma de decisiones a partir de información estructurada. Su diseño busca asegurar que los responsables dispongan de instrumentos claros, accesibles y estandarizados, que les permitan gestionar de manera efectiva tanto los eventos críticos como las oportunidades que pueden incidir en el desempeño organizacional.

11.2.5. *Sistema de indicadores*

El sistema de indicadores presentado en el Apéndice H corresponde a un conjunto estructurado de métricas diseñadas para evaluar el desempeño, la eficacia y el comportamiento del proceso de gestión de riesgos y oportunidades en la organización. Su propósito es proporcionar información objetiva y sistemática que facilite la toma de decisiones basada en evidencia, contribuya a la mejora continua y fortalezca el enfoque preventivo y estratégico de los procesos organizacionales.

Este sistema integra indicadores tanto cuantitativos como cualitativos, alineados con los objetivos estratégicos, operativos y de control interno. Cada indicador cuenta con una ficha técnica que define aspectos como su propósito, fórmula, unidad de medida, frecuencia de medición, responsables y fuentes de información, lo que garantiza consistencia metodológica en su aplicación y seguimiento.

Los indicadores se encuentran organizados en categorías clave, las cuales permiten evaluar diferentes dimensiones del sistema de gestión.

11.2.5.1. Indicadores de Riesgo. Permiten monitorear el comportamiento de los riesgos, la exposición inherente y la ocurrencia de incidentes relevantes.

- Nivel de Riesgo Inherente Promedio por Proceso y por Proyecto

- Número de Riesgos Materializados por Periodo

11.2.5.2. Indicadores de Oportunidades. Evalúan la identificación y aprovechamiento de oportunidades que generan valor o fortalecen el desempeño del proceso.

- Número de Oportunidades Identificadas por Proceso

11.2.5.3. Indicadores de Controles. Miden el avance en la implementación y efectividad de las barreras preventivas y mitigadoras definidas para cada riesgo.

- Porcentaje de Controles Preventivos y Mitigadores Implementados

11.2.5.4. Indicadores de Planes de Acción. Verifican la eficiencia, cumplimiento y trazabilidad de las acciones definidas para el tratamiento de riesgos y oportunidades.

- Porcentaje de Planes de Acción Cumplidos en el Tiempo Establecido
- Desviación Promedio en el Cumplimiento de Fechas

En conjunto, este sistema de indicadores permite monitorear la evolución del riesgo inherente y residual, identificar desviaciones significativas, evaluar la eficacia de los controles implementados y verificar el cumplimiento de los planes de acción asociados a eventos críticos. Su aplicación sistemática fortalece la gestión basada en datos, promueve la transparencia y facilita la integración de los resultados en los ciclos de evaluación y mejora continua del sistema organizacional.

11.2.6. *Programa de capacitación*

El Programa de Capacitación desarrollado para la organización constituye un componente clave para el fortalecimiento del Sistema de Gestión de Riesgos y Oportunidades, al asegurar que los colaboradores adquieran las competencias necesarias para comprender, aplicar y mantener actualizado el modelo implementado. Este programa fue diseñado con un enfoque didáctico y práctico, orientado a facilitar la apropiación del manual

de gestión del riesgo, el uso de las matrices y la correcta aplicación de los lineamientos definidos.

Como parte del proceso formativo, se incorporó el uso de la herramienta de inteligencia artificial Notebook, mediante la cual se elaboró un recurso de capacitación que explica de manera clara y secuencial los elementos del manual, su propósito, el procedimiento de gestión de riesgos y oportunidades, así como las responsabilidades asociadas a cada rol dentro de la organización. Este recurso audiovisual se diseñó como una guía permanente y de fácil acceso para los colaboradores, favoreciendo la estandarización del aprendizaje y la reducción de brechas de conocimiento entre los diferentes equipos de trabajo.

El material audiovisual y los recursos complementarios del programa fueron almacenados en la carpeta institucional de SharePoint bajo la denominación “Programa de Capacitación”, con el fin de garantizar su disponibilidad, trazabilidad y actualización continua. Desde este repositorio, los responsables pueden acceder al contenido, replicarlo en espacios formativos y emplearlo como herramienta de inducción para nuevos integrantes.

11.3. Etapa 3. Implementación piloto del modelo de gestión de riesgos

El proceso de Soporte TI desempeña un rol estratégico dentro de la organización, al asegurar la disponibilidad, continuidad y seguridad de la infraestructura tecnológica que respalda las operaciones corporativas. Su alcance abarca la atención de solicitudes de los colaboradores, la administración de equipos y plataformas digitales, la gestión de proveedores tecnológicos, así como la implementación de controles de seguridad, respaldo de la información y el seguimiento del desempeño del servicio.

Dado que este proceso incide directamente en la estabilidad operativa y en la protección de los activos de información, resulta fundamental identificar, evaluar y controlar los riesgos que puedan afectar la prestación del servicio, la seguridad de los datos, la continuidad tecnológica y el cumplimiento de los objetivos estratégicos. En este contexto, se desarrollará un piloto de aplicación del Manual de Gestión de Riesgos, con el propósito de validar su metodología, fortalecer la cultura preventiva y asegurar su alineación con estándares internacionales como la ISO 31000.

La ejecución del piloto permitirá identificar tanto amenazas como oportunidades asociadas al proceso, evaluar sus niveles de exposición, definir controles adecuados y generar información relevante para la toma de decisiones, la mejora continua y la actualización del sistema de gestión. Asimismo, facilitará la apropiación del método por parte de los responsables del proceso, promoviendo que la gestión del riesgo se consolide como una práctica sistemática, medible y sostenible dentro de la organización.

Este enfoque es coherente con los lineamientos de la ISO 31000, la cual establece que la gestión del riesgo debe integrarse en todas las actividades organizacionales y contribuir a la toma de decisiones y al fortalecimiento de la cultura organizacional .

A continuación, se presenta la metodología definida en el Manual de Gestión de Riesgos, la cual será aplicada durante el desarrollo del piloto en el proceso de Soporte TI.

11.3.1. *Proceso para la gestión de riesgos*

11.3.1.1. Comunicación y consulta. La comunicación y la consulta con las partes interesadas, tanto internas como externas, deben desarrollarse de manera efectiva para asegurar que quienes participan en la gestión del riesgo comprendan claramente los criterios y fundamentos utilizados para la toma de decisiones. Este intercambio de información debe mantenerse activo durante todas las fases del proceso de gestión del riesgo.

Con el fin de dar cumplimiento a esta etapa, se socializaron en cada uno de los procesos misionales los siguientes aspectos clave:

- El concepto de riesgo y los elementos que conforman su gestión.
- La definición del contexto interno de los procesos y del contexto externo que influye en ellos.
- La forma adecuada de identificar los riesgos asociados a cada proceso.

11.3.1.2. Alcance, contexto y criterios. El establecimiento del alcance, el contexto y los criterios del proceso de gestión del riesgo para el área de Soporte TI tiene como propósito adaptar la metodología institucional a las características particulares del proceso, permitiendo realizar una evaluación precisa y definir tratamientos adecuados frente a los riesgos tecnológicos, operativos y de seguridad de la información.

Este paso inicial permite determinar qué elementos del proceso serán analizados, comprender plenamente las condiciones internas y externas que pueden influir en él y definir los criterios que guiarán la valoración y priorización de los riesgos identificados.

Alcance

La organización debe establecer claramente el alcance de las actividades de gestión del riesgo aplicadas al proceso de Soporte TI. Dado que este proceso esta relacionado

directamente con otros procesos de la organización (TI, SG-SST, Gestión financiera, Consultoría, Contabilidad, I+D, Gestión de calidad, Gestión del conocimiento, Academy, Gestión comercial, Comunicación, Gestión Jurídica y Gestión Humana.)

Figura 17.

Diagrama de relaciones del proceso

Para la planificación del enfoque de gestión del riesgo en el proceso de Soporte TI se consideran los siguientes aspectos:

- Objetivos del proceso: asegurar la disponibilidad, funcionalidad y seguridad de los equipos, plataformas y servicios tecnológicos.

- Decisiones necesarias: definición de controles, priorización de riesgos, activación de acciones preventivas y de mitigación, frecuencia de revisión, entre otros.
- Resultados esperados: identificación precisa y completa de los riesgos asociados al proceso.
- Alcance específico: Incluye el alistamiento de equipos y elementos de trabajos, gestionar los equipos y herramientas tecnológicas, gestionar y configurar las plataformas digitales, gestión de centro de administración Microsoft 365.
- Herramientas y técnicas: matriz de riesgos, análisis causa efecto, revisión documental, indicadores del proceso y auditorías técnicas.
- Recursos y responsabilidades: líder de TI, proveedor de soporte, áreas usuarias, registros en SharePoint, informes técnicos, actas de entrega/devolución y reportes de administración de plataformas.

Contexto

El análisis de contexto define el entorno en el cual el proceso de Soporte TI desarrolla sus actividades y gestiona sus riesgos, permitiendo comprender los factores que pueden incidir en la operación, la disponibilidad tecnológica y la seguridad de la información. En este sentido, la identificación de los contextos interno y externo resulta fundamental para reconocer las condiciones que influyen en el cumplimiento de los objetivos del proceso.

Para complementar este análisis y estructurar la información de manera clara, se llevó a cabo un análisis DOFA, el cual permitió identificar las fortalezas y debilidades del contexto interno, así como las oportunidades y amenazas provenientes del entorno externo. Esta

herramienta facilita una visión integral del proceso y contribuye a una mejor toma de decisiones y a la definición de acciones estratégicas.

Este enfoque se encuentra alineado con los lineamientos de la ISO 31000, que establece la necesidad de analizar tanto factores internos como externos para definir el contexto del riesgo y garantizar una gestión adecuada y coherente con los objetivos organizacionales .

Tabla 2.

Análisis DOFA

Fortalezas (Contexto Interno)	**Oportunidades (Contexto Externo)**
Proceso estructurado con actividades definidas.	Avances tecnológicos constantes.
Uso de herramientas corporativas centralizadas como SharePoint.	Disponibilidad de proveedores especializados.
Relación formal con proveedores tecnológicos.	Tendencias de digitalización organizacional.
Controles de seguridad informática implementados.	Herramientas de automatización y monitoreo.
Documentación actualizada del proceso.	Estándares internacionales como ISO 27001 e ISO 9001.
Indicadores definidos para medir desempeño.	Servicios cloud que fortalecen continuidad operativa.
Capacidad interna para administrar plataformas digitales.	Acceso a formación y certificación tecnológica.

Acompañamiento y soporte a usuarios.	
Debilidades (Contexto Interno)	**Amenazas (Contexto Externo)**
Dependencia de proveedor externo para incidentes complejos.	Incremento global de ciberataques.
Limitación de recursos humanos internos.	Dependencia de terceros proveedores.
Equipos susceptibles a obsolescencia.	Obsolescencia acelerada en hardware y software.
Procesos manuales sin automatización completa.	Variabilidad de costos tecnológicos.
Capacidad limitada para auditorías internas avanzadas.	Cambios normativos constantes.
Retrasos en comunicación entre áreas.	Indisponibilidad temporal de servicios cloud.
Niveles desiguales de competencia digital en usuarios.	Ataques de ingeniería social cada vez más sofisticados.
Dependencia del presupuesto asignado.	

Criterios

La organización debe establecer los criterios que permitirán valorar los riesgos del proceso de Soporte TI y determinar el nivel aceptable de exposición. Estos criterios deben estar alineados con el marco institucional de gestión del riesgo, las políticas internas y los objetivos tecnológicos y de seguridad.

Los criterios definidos para el proceso consideran lo siguiente:

- Matriz de Riesgos RAM (Risk Assessment Matrix): La matriz RAM utilizada por la organización se fundamenta en la evaluación conjunta de la probabilidad de ocurrencia y la magnitud del impacto asociado a la materialización de los riesgos. Este instrumento clasifica ambos criterios en tres niveles de valoración, permitiendo una estimación sistemática y comparable. Los tres niveles de probabilidad y los tres niveles de impacto facilitan la asignación del nivel de riesgo resultante y proporcionan una base metodológica sólida para priorizar acciones de tratamiento y orientar la toma de decisiones dentro del proceso de gestión del riesgo.
- Redacción estandarizada de riesgos: Para asegurar claridad en la redacción, se adopta una fórmula estándar que integra estos tres elementos en una estructura coherente. Esta estructura permite expresar el riesgo de manera comprensible y sistemática, facilitando su análisis y tratamiento posterior. La redacción estandarizada se plantea de la siguiente forma: “Es posible que / pudiera ocurrir [riesgo], debido a [causa], afectando / produciendo [impacto].” Este formato favorece la identificación precisa de los factores que originan el riesgo y los efectos que podría generar, contribuyendo a una gestión del riesgo más consistente, objetiva y alineada con las buenas prácticas organizacionales.
- Criterios de probabilidad e impacto: Con el fin de valorar de manera estandarizada los riesgos identificados, se adopta una escala que clasifica la probabilidad de ocurrencia en tres niveles. El nivel Leve corresponde a situaciones en las que es improbable que el riesgo ocurra en condiciones

normales de operación, ubicándose en un rango de 0 % a 30 %, considerado como zona tolerable. El nivel Medio se presenta cuando existe una posibilidad significativa de ocurrencia del riesgo bajo ciertas circunstancias operacionales, con un rango superior al 30 % y hasta el 60 %. Finalmente, el nivel Alto refleja una probabilidad elevada de que el riesgo se materialice, ya sea por condiciones recurrentes, vulnerabilidades persistentes o antecedentes que respaldan dicha tendencia, ubicándose en un rango mayor al 60 % y hasta el 80 %. De igual forma se consideran tres dimensiones fundamentales para la organización: impacto financiero, impacto en las personas y el impacto en la imagen y reputación.

11.3.1.3. Evaluación del riesgo. La evaluación del riesgo es el proceso total de identificación del riesgo, análisis del riesgo y valoración del riesgo

11.3.1.3.1. ***Identificación de riesgos.*** El objeto de esta fase es generar una lista exhaustiva de riesgos con base en aquellos eventos que podrían crear, aumentar, prevenir, degradar, acelerar o retrasar el logro de los objetivos.

La identificación de riesgos se realizó mediante el análisis de las macro actividades del proceso de soporte TI, aplicando la metodología de la norma ISO 31000. Para cada actividad se evaluaron los posibles eventos que podrían afectar el cumplimiento de los objetivos del proceso, considerando los recursos utilizados, dependencias y posibles fallas. Se utilizó la técnica de análisis “What if”, formulando preguntas orientadas a identificar qué puede fallar, por qué y cuáles serían sus consecuencias, generando así una lista estructurada de riesgos por cada macro actividad.

Adicionalmente, en cada riesgo identificado se incorporó el origen del riesgo (causa), asimismo, se aplicó una redacción estandarizada de los riesgos bajo una estructura uniforme, garantizando claridad, coherencia y facilidad para su posterior análisis, evaluación y tratamiento dentro del sistema de gestión. Ver tabla 3

Tabla 3.

Identificación de riesgos

Nº	Amenaza	Origen	Redacción estandarizada
1	Entrega de equipos con fallas técnicas o mala configuración.	Externo	Es posible que se entreguen equipos con fallas técnicas o mala configuración, debido a una validación incompleta por parte del proveedor, afectando la continuidad operativa y la productividad del colaborador.
2	Instalación incompleta de software corporativo.	Ambos	Es posible que se realice una instalación incompleta de software corporativo, debido a errores en el proceso de alistamiento o falta de control, afectando el correcto funcionamiento de las herramientas.
3	Asignación incorrecta de equipos según el perfil del cargo.	Interno	Es posible que se asignen equipos incorrectos según el perfil del cargo, debido a una inadecuada definición de

			requerimientos técnicos, afectando el desempeño laboral.
4	Retrasos en la entrega de equipos a nuevos colaboradores.	Externo	Es posible que se presenten retrasos en la entrega de equipos a nuevos colaboradores, debido a demoras del proveedor o mala planificación, afectando el inicio oportuno de actividades.
5	Dependencia del proveedor para el alistamiento (demoras o errores).	Externo	Es posible que se generen demoras o errores en el alistamiento, debido a la dependencia del proveedor externo, afectando la disponibilidad de los equipos.
6	Falta de licenciamiento adecuado en software instalado.	Ambos	Es posible que se utilice software sin licenciamiento adecuado, debido a una gestión ineficiente de licencias, produciendo riesgos legales y operativos.
7	Equipos sin controles de seguridad (antivirus, políticas, etc.).	Interno	Es posible que se entreguen equipos sin controles de seguridad adecuados, debido a omisiones en la configuración inicial, afectando la seguridad de la información.

8	Desactualización del inventario de hardware y software.	Interno	Es posible que el inventario de hardware y software se encuentre desactualizado, debido a la falta de seguimiento y control, afectando la trazabilidad de los activos.
9	Pérdida, daño o uso inadecuado de equipos.	Interno	Es posible que se presenten pérdidas, daños o uso inadecuado de equipos, debido a un control insuficiente o uso indebido por parte de los usuarios, generando costos adicionales.
10	Falta de mantenimiento preventivo.	Ambos	Es posible que no se realicen mantenimientos preventivos, debido a una planificación deficiente, afectando la disponibilidad y vida útil de los equipos.
11	Obsolescencia tecnológica no controlada.	Interno	Es posible que ocurra obsolescencia tecnológica no controlada, debido a la falta de un plan de renovación, afectando la eficiencia operativa.
12	Baja trazabilidad en devoluciones o reasignaciones.	Interno	Es posible que exista baja trazabilidad en devoluciones o reasignaciones, debido a registros incompletos, afectando el control de activos.

13	Errores en la baja de activos (impacto contable).	Interno	Es posible que se presenten errores en la baja de activos, debido a una mala gestión o coordinación con contabilidad, produciendo inconsistencias financieras.
14	Falta de control sobre garantías y vida útil de equipos.	Interno	Es posible que no se controle adecuadamente la garantía y vida útil de los equipos, debido a la falta de seguimiento, afectando la toma de decisiones sobre reemplazo.
15	Caídas o indisponibilidad de plataformas	Externo	Es posible que se presenten caídas o indisponibilidad de plataformas, debido a fallas técnicas o del proveedor, afectando la continuidad del servicio.
16	Configuración incorrecta de plataformas.	Interno	Es posible que se configuren incorrectamente las plataformas, debido a errores humanos o falta de validación, afectando su funcionamiento.
17	Fallas en actualizaciones o cambios tecnológicos.	Ambos	Es posible que ocurran fallas en actualizaciones o cambios tecnológicos, debido a pruebas

			insuficientes, afectando la estabilidad de las plataformas.
18	Pérdida de información en plataformas digitales.	Ambos	Es posible que se pierda información en plataformas digitales, debido a fallas en respaldos o configuraciones, afectando la integridad de la información.
19	Dependencia de proveedores externos (hosting, soporte).	Externo	Es posible que exista dependencia de proveedores externos, debido a la tercerización del servicio, afectando la capacidad de respuesta ante incidentes.
20	Baja usabilidad o errores que afectan la experiencia del usuario.	Interno	Es posible que las plataformas presenten baja usabilidad o errores, debido a deficiencias en su diseño o configuración, afectando la experiencia del usuario.
21	Falta de monitoreo del rendimiento de plataformas.	Interno	Es posible que no se realice monitoreo del rendimiento de plataformas, debido a la falta de herramientas o seguimiento, afectando la detección oportuna de fallas.
22	Asignación incorrecta de permisos o roles.	Interno	Es posible que se asignen permisos o roles incorrectos, debido a errores en la

			administración de usuarios, afectando la seguridad de la información.
23	Accesos no autorizados a cuentas corporativas.	Ambos	Es posible que se presenten accesos no autorizados a cuentas corporativas, debido a controles de seguridad insuficientes, afectando la confidencialidad de la información.
24	Eliminación o modificación indebida de usuarios.	Interno	Es posible que se eliminen o modifiquen usuarios de manera indebida, debido a errores humanos o falta de control, afectando la continuidad del servicio.
25	Uso ineficiente o sobrecostos en licencias.	Interno	Es posible que se generen sobrecostos en licencias, debido a una mala gestión en su asignación, afectando el presupuesto del área.
26	Falta de control sobre autenticación (ej. MFA).	Interno	Es posible que no se implementen controles adecuados de autenticación, debido a configuraciones deficientes, afectando la seguridad del sistema.
27	Pérdida de información en correos o SharePoint.	Ambos	Es posible que se pierda información en correos o SharePoint, debido a fallas en

			la gestión o respaldo, afectando la disponibilidad de la información.
28	Incumplimiento de políticas de seguridad de la información.	Interno	Es posible que se incumplan políticas de seguridad de la información, debido a una débil administración de accesos, afectando la integridad y confidencialidad de los datos.

11.3.1.3.2. ***Análisis de riesgo.*** El análisis de riesgos se desarrolló con base en los lineamientos de la norma ISO 31000, la cual establece que el riesgo debe evaluarse considerando la probabilidad de ocurrencia y la magnitud de sus consecuencias, así como las causas y fuentes que lo originan.

En este contexto, se analizaron los factores que pueden incidir en la materialización de cada riesgo, tales como las dependencias tecnológicas, la intervención de terceros, los errores humanos y las condiciones operativas propias del proceso de soporte TI. Este análisis permitió comprender de manera integral las variables que influyen en la ocurrencia de los eventos y su posible impacto sobre los objetivos del proceso.

Para cada riesgo identificado se evaluaron sus causas, posibles consecuencias y la probabilidad de ocurrencia, permitiendo comprender su comportamiento y priorizar aquellos con mayor impacto sobre la disponibilidad, seguridad y funcionalidad de los servicios tecnológicos. Este análisis se desarrolló por macro actividades del proceso, facilitando la validación de los riesgos definidos y asegurando su alineación con los objetivos del proceso. Ver tabla 4, tabla 5.

Tabla 4.

Análisis de riesgos

Nº	Riesgo	Causas	Consecuencias
1	Entrega de equipos con fallas técnicas o mala configuración.	Falta de validación / errores del proveedor	Baja productividad, reprocesos
2	Instalación incompleta de software corporativo.	Falta de control en alistamiento	Interrupciones en el trabajo
3	Asignación incorrecta de equipos según el perfil del cargo.	Mala definición de requerimientos	Bajo desempeño del usuario
4	Retrasos en la entrega de equipos a nuevos colaboradores.	Dependencia del proveedor	Atrasos operativos
5	Dependencia del proveedor para el alistamiento (demoras o errores).	Tercerización del servicio	Demoras y baja calidad
6	Falta de licenciamiento adecuado en software instalado.	Mala gestión de software	Riesgos legales y fallas
7	Equipos sin controles de seguridad (antivirus, políticas, etc.).	Omisiones en configuración	Vulnerabilidad de información
8	Desactualización del inventario de hardware y software.	Falta de control	Pérdida de trazabilidad
9	Pérdida, daño o uso inadecuado de equipos.	Uso indebido / falta de control	Costos adicionales
10	Falta de mantenimiento preventivo.	Mala planificación	Fallas y paradas

11	Obsolescencia tecnológica no controlada.	Falta de renovación	Baja eficiencia
12	Baja trazabilidad en devoluciones o reasignaciones.	Registros incompletos	Descontrol de activos
13	Errores en la baja de activos (impacto contable).	Mala coordinación	Impacto contable
14	Falta de control sobre garantías y vida útil de equipos.	Falta de seguimiento	Pérdidas económicas
15	Caídas o indisponibilidad de plataformas	Fallas técnicas/proveedor	Interrupción del servicio
16	Configuración incorrecta de plataformas.	Error humano	Fallas funcionales
17	Fallas en actualizaciones o cambios tecnológicos.	Pruebas insuficientes	Inestabilidad
18	Pérdida de información en plataformas digitales.	Fallas en backups	Pérdida de datos
19	Dependencia de proveedores externos (hosting, soporte).	Servicios externos	Baja capacidad de respuesta
20	Baja usabilidad o errores que afectan la experiencia del usuario.	Mala configuración	Insatisfacción del usuario
21	Falta de monitoreo del rendimiento de plataformas.	Falta de herramientas	Fallas no detectadas

22	Asignación incorrecta de permisos o roles.	Mala gestión de usuarios	Riesgo de seguridad
23	Accesos no autorizados a cuentas corporativas.	Controles débiles	Fuga de información
24	Eliminación o modificación indebida de usuarios.	Error humano	Interrupciones
25	Uso ineficiente o sobrecostos en licencias.	Mala gestión	Impacto financiero
26	Falta de control sobre autenticación (ej. MFA).	Configuración deficiente	Vulnerabilidades
27	Pérdida de información en correos o SharePoint.	Fallas en respaldo	Afectación operativa
28	Incumplimiento de políticas de seguridad de la información.	Falta de control	Riesgos legales y reputacionales

Tabla 5.

Análisis de riesgos

Nº	**Probabilidad de ocurrencia**	**O_finanaciero**	**O_personas**	**O_imagen**
1	Medio	Medio		Medio
2	Medio	Medio		Medio
3	Medio	Medio		Medio
4	Alto	Medio		Alto

5	Alto	Alto		Alto
6	Medio	Alto		Alto
7	Alto	Alto	Leve	Alto
8	Alto	Medio		Medio
9	Medio	Medio		Medio
10	Alto	Alto		Medio
11	Medio	Medio		Medio
12	Medio	Medio		Medio
13	Leve	Leve		
14	Medio	Medio		Medio
15	Alto	Alto	Leve	Alto
16	Medio	Leve		Leve
17	Medio	Medio		Medio
18	Alto	Alto	Leve	Alto
19	Alto	Alto		Alto
20	Medio	Leve		Leve
21	Alto	Alto		Alto
22	Alto	Alto	Leve	Alto
23	Alto	Alto	Leve	Alto
24	Medio	Leve		Leve
25	Medio	Medio		Medio
26	Alto	Alto	Leve	Alto

27	Alto	Alto	Leve	Alto
28	Medio	Alto	Leve	Alto

11.3.1.3.3. ***Evaluación de riesgo.*** El propósito de la evaluación del riesgo es facilitar la toma de decisiones respecto a cuáles riesgos requieren tratamiento y establecer su nivel de prioridad para la implementación de acciones. Este proceso permite jerarquizar los riesgos identificados en función de su probabilidad de ocurrencia y la magnitud de sus consecuencias, orientando así la asignación eficiente de recursos y la definición de estrategias de mitigación adecuadas.

En este marco, para cada riesgo identificado se definieron controles orientados a su tratamiento, los cuales se clasifican en dos categorías: controles preventivos, diseñados para reducir la probabilidad de ocurrencia del evento, y controles de mitigación, enfocados en disminuir su impacto en caso de materializarse. Esta clasificación contribuye al fortalecimiento de la gestión del riesgo y a la continuidad operativa del proceso.

Por otra parte, la frecuencia de revisión de los riesgos se establece en función de su nivel de criticidad. Los riesgos clasificados como altos son objeto de seguimiento mensual; los de nivel medio se revisan de manera trimestral o semestral; y los riesgos bajos se evalúan anualmente. Este enfoque permite asegurar un monitoreo continuo, oportuno y proporcional al nivel de exposición, en concordancia con los lineamientos de la norma ISO 31000, la cual promueve una gestión del riesgo sistemática y orientada a la mejora continua.

Tabla 6.

Evaluación de riesgos

Controles	**Medidas de control**	**Tipo de control**	**Frecuencia de revisión (mes)**	**Fecha de última revisión (dd/mm/aaaa)**	**Fecha de próxima revisión**
Checklist de validación técnica antes de entrega	Se debe diseñar e implementar una lista de verificación técnica que incluya aspectos de hardware, software y seguridad, la cual deberá ser aplicada obligatoriamente antes de la entrega de cualquier equipo.	Preventivo	6	10/04/2026	10/10/2026
Uso de imágenes estándar automatizadas	Es necesario crear y mantener una imagen base corporativa que incluya el sistema operativo y el software autorizado, asegurando su	Preventivo	6	10/04/2026	10/10/2026

	despliegue automatizado en los equipos.				
Definición de perfiles tecnológicos por cargo	Se deben establecer y documentar los requerimientos tecnológicos específicos para cada rol dentro de la organización, asegurando que la asignación de equipos y software se realice conforme a dichos perfiles.	Preventivo	6	10/04/2026	10/10/2026
Acuerdos SLA con proveedores	Es fundamental definir acuerdos de nivel de servicio (SLA) con los proveedores, estableciendo tiempos claros de entrega, atención y soporte. Asimismo, se deben	De mitigación	3	10/04/2026	10/07/2026

	incluir cláusulas de penalización por incumplimiento y realizar un seguimiento continuo para verificar el cumplimiento de los compromisos establecidos.				
Proveedores alternos / plan de contingencia	Se debe contar con al menos dos proveedores para servicios o suministros críticos, con el fin de reducir la dependencia de un único tercero.	De mitigación	3	10/04/2026	10/07/2026
Auditorías periódicas de licencias	Se deben realizar auditorías periódicas para revisar el uso de licencias de software, garantizando el cumplimiento legal y contractual.	Preventivo	3	10/04/2026	10/07/2026

Implementación de políticas de seguridad automáticas	E deben implementar configuraciones de seguridad como antivirus, firewall y políticas de acceso de manera automatizada, preferiblemente mediante herramientas centralizadas como dominios.	Preventivo	1	10/04/2026	10/05/2026
Sistema automatizado de inventario (CMDB)	Es necesario implementar un sistema automatizado de inventario (CMDB) que registre todos los activos tecnológicos de la organización y se actualice en tiempo real.	Preventivo	3	10/04/2026	10/07/2026
Políticas de uso + actas de responsabilidad	Se deben definir políticas claras sobre el uso adecuado de los recursos tecnológicos	De mitigación	6	10/04/2026	10/10/2026

	y formalizar su aceptación mediante actas firmadas por los usuarios.				
Plan de mantenimiento preventivo programado	Se debe establecer un plan de mantenimiento preventivo que contemple revisiones periódicas de los equipos, registrando cada intervención realizada.	Preventivo	3	10/04/2026	10/07/2026
Plan de renovación tecnológica	Es necesario definir la vida útil de los equipos tecnológicos y planificar su reposición de manera anticipada.	Preventivo	6	10/04/2026	10/10/2026
Registro digital de movimientos de activos	Se debe implementar un control detallado de los movimientos de activos, incluyendo	Preventivo	6	10/04/2026	10/10/2026

	entregas, devoluciones y traslados.				
Validación contable previa a baja	Antes de dar de baja un activo, se debe validar su estado con el área contable, revisando aspectos como depreciación y valor en libros. La eliminación del activo debe contar con la debida autorización formal.	Preventivo	12	10/04/2026	10/04/2027
Base de datos de garantías y alertas	E debe mantener una base de datos actualizada con la información de garantías de los equipos, incluyendo fechas de vencimiento.	Preventivo	6	10/04/2026	10/10/2026
Plan de continuidad y	Se debe definir un plan de continuidad del negocio que	De mitigación	1	10/04/2026	10/05/2026

recuperación (DRP)	contemple escenarios de falla y estrategias de recuperación. Este plan debe ser probado periódicamente para asegurar su efectividad en situaciones reales.				
Procedimientos estandarizados de configuración	Es necesario documentar los procedimientos técnicos y operativos, asegurando que todo el personal esté capacitado en su aplicación.	Preventivo	12	10/04/2026	10/04/2027
Ambientes de pruebas antes de producción	Se deben establecer ambientes de prueba donde se validen cambios, actualizaciones o nuevas implementaciones	Preventivo	6	10/04/2026	10/10/2026

	antes de su paso a producción.				
Backups automáticos y redundancia	Se deben configurar copias de seguridad automáticas y periódicas, almacenadas en ubicaciones seguras.	De mitigación	1	10/04/2026	10/05/2026
Contratos con alta disponibilidad (HA)	Se deben contratar servicios que garanticen alta disponibilidad, incluyendo redundancia y tiempos mínimos de inactividad.	De mitigación	3	10/04/2026	10/07/2026
Pruebas de usuario (UX testing)	Antes de liberar sistemas o equipos, se deben realizar pruebas con usuarios finales para validar la funcionalidad y experiencia.	Preventivo	12	10/04/2026	10/04/2027

Herramientas de monitoreo en tiempo real	Se deben implementar herramientas de monitoreo que permitan supervisar la infraestructura en tiempo real, configurando alertas para la detección temprana de incidentes.	Preventivo	1	10/04/2026	10/05/2026
Modelo de control de accesos (RBAC)	Se deben definir roles y permisos de acceso basados en las funciones de cada usuario, asignando únicamente los privilegios necesarios.	Preventivo	1	10/04/2026	10/05/2026
Autenticación multifactor (MFA)	Se debe implementar autenticación multifactor (MFA) en los sistemas críticos, obligando su uso para todos los usuarios.	Preventivo	1	10/04/2026	10/05/2026

Flujo de aprobación para eliminación	Se debe establecer un flujo formal de aprobación para la eliminación de usuarios o activos, asegurando que toda acción esté validada previamente.	Preventivo	12	10/04/2026	10/04/2027
Control y seguimiento de uso	Se debe monitorear continuamente el consumo de licencias de software, identificando aquellas que no estén siendo utilizadas.	Preventivo	6	10/04/2026	10/10/2026
Implementación obligatoria de MFA	Se deben configurar políticas que obliguen el uso de MFA en toda la organización, asegurando su aplicación en todos los usuarios y sistemas.	Preventivo	1	10/04/2026	10/05/2026

Políticas de retención + backups	Se deben definir políticas de retención de información que establezcan tiempos claros de almacenamiento, junto con la automatización de respaldos.	De mitigación	1	10/04/2026	10/05/2026
Auditorías internas y capacitaciones	Se deben realizar auditorías periódicas para evaluar el cumplimiento de controles y procesos, complementadas con programas de capacitación dirigidos al personal.	Preventivo	3	10/04/2026	10/07/2026

11.3.1.4. ***Tratamiento de riesgo.*** En el desarrollo de la etapa de tratamiento de riesgos, además de la definición de los controles y la asignación de responsables, se establecieron los esquemas de comunicación asociados a cada control, con el fin de garantizar la adecuada gestión, seguimiento y trazabilidad de la información relacionada con los riesgos.

En este sentido, se definieron como mecanismos de comunicación los siguientes: informes, reuniones, correos electrónicos, minutas, gráficos, registros y herramientas colaborativas como Teams del proyecto, los cuales fueron seleccionados de acuerdo con la naturaleza del control, el nivel de criticidad del riesgo y la necesidad de información de los diferentes actores involucrados.

Estos esquemas permiten asegurar que la información relacionada con los riesgos sea oportuna, clara, verificable y accesible, facilitando la toma de decisiones y el monitoreo continuo del sistema. Asimismo, garantizan la participación de las partes interesadas y el flujo adecuado de la información entre los diferentes niveles de la organización.

Lo anterior se encuentra alineado con los lineamientos de la ISO 31000, la cual establece que la comunicación y consulta deben ser procesos continuos que permitan compartir información, generar entendimiento y apoyar la toma de decisiones en la gestión del riesgo .

De esta manera, la definición de esquemas de comunicación contribuye a fortalecer la efectividad de los controles implementados, asegurando no solo su ejecución, sino también su seguimiento, evaluación y mejora continua dentro del sistema de gestión de riesgos.

Tabla 7.

Tratamiento de riesgos

Riesgo residual	Responsable del control	Esquema de comunicación

Bajo	Dueño del riesgo	Registro
Bajo	Líder de área	Registro
Bajo	Líder de área	Reunión
Medio	Líder de área	Informe
Medio	Líder de área	Reunión
Bajo	Dueño del riesgo	Informe
Medio	Dueño del riesgo	Correo electrónico
Bajo	Líder de área	Registro
Bajo	Dueño del riesgo	Registro
Medio	Dueño del riesgo	Registro
Bajo	Dueño del riesgo	Informe
Bajo	Líder de área	Registro
Bajo	Líder de área	Correo electrónico
Bajo	Líder de área	Registro
Medio	Líder de área	Reunión
Bajo	Líder de área	Registro
Bajo	Líder de área	Registro
Medio	Líder de área	Registro
Medio	Líder de área	Informe
Bajo	Dueño del riesgo	Reunión
Medio	Dueño del riesgo	Grafico
Medio	Líder de área	Registro

Medio	Líder de área	Correo electrónico
Bajo	Líder de área	Teams del proyecto
Bajo	Líder de área	Informe
Medio	Líder de área	Correo electrónico
Medio	Dueño del riesgo	Correo electrónico
Bajo	Dueño del riesgo	Reunión

11.3.1.5. Monitoreo y revisión. De acuerdo con la norma ISO 31000, el monitoreo y la revisión constituyen una etapa esencial dentro del proceso de gestión del riesgo, cuyo propósito es asegurar y mejorar la calidad, pertinencia y efectividad del sistema implementado. Este proceso implica la recopilación, análisis y seguimiento continuo de la información, con el fin de evaluar el desempeño de los riesgos identificados, la eficacia de los controles establecidos y la necesidad de realizar ajustes en función de los cambios en el contexto organizacional.

En este sentido, la organización ha estructurado un esquema de monitoreo que permite verificar de manera sistemática la evolución de los riesgos, así como la efectividad de las medidas de tratamiento implementadas. Este esquema integra el seguimiento dentro de los procesos de gestión existentes, garantizando la trazabilidad de la información y el soporte necesario para la toma de decisiones.

Es importante señalar que el sistema de gestión de riesgos diseñado se encuentra en una fase inicial de implementación. Por lo tanto, aún no se dispone de un historial suficiente que permita evaluar de forma integral el comportamiento de los riesgos, la ocurrencia de eventos o la efectividad real de los controles definidos. No obstante, se han establecido los

lineamientos, criterios y mecanismos necesarios para el desarrollo del monitoreo y la revisión del sistema.

Estos lineamientos contemplan la definición de responsables, la periodicidad del seguimiento, el establecimiento de indicadores de gestión y la implementación de mecanismos de comunicación, los cuales facilitarán una evaluación estructurada en el corto y mediano plazo.

De esta manera, se busca asegurar que el sistema de gestión del riesgo evolucione de forma dinámica, permitiendo identificar desviaciones, fortalecer el proceso de mejora continua y adaptarse oportunamente a los cambios internos y externos que puedan afectar el logro de los objetivos organizacionales, en línea con el enfoque de revisión continua propuesto por la ISO 31000.

11.4. Etapa 4. Ajuste final versiones aprobables

La presente etapa de ajuste final representa una fase decisiva dentro del desarrollo de la propuesta de mejoramiento, ya que constituye el momento en el cual las versiones preliminares se transforman en un documento consolidado, coherente y apto para su evaluación formal. En esta etapa se procedió a consolidar, revisar y ajustar de manera integral todos los productos y documentos generados en las fases previas (diagnóstico, formulación, ejecución piloto y retroalimentación). Esto incluyó:

- Integración de comentarios recibidos durante las revisiones preliminares: Se reunieron las observaciones del tutor de la organización.
- Revisión sistemática de contenidos y coherencia interna: Se evaluó la coherencia entre objetivos, metodología, análisis de resultados y conclusiones, para garantizar un discurso lógico y académico.

- Ajuste de formato y estilo institucional: Se aplicaron los lineamientos de presentación requeridos por la institución.
- Consolidación de evidencias y apéndices: Se incorporaron evidencias de apoyo para fortalecer la claridad del diseño e implementación de buenas prácticas de la gestión integral de riesgos.
- Validación interna preliminar: Antes de la presentación oficial, el documento fue sometido a una revisión interna final por el equipo de trabajo para asegurar que las versiones ajustadas fuesen aptas para evaluación formal.
- Resultado del proceso ejecutivo: Como resultado de este proceso de ajustes y revisión rigurosa, se obtuvo una versión final consolidada y aprobable del manual de gestión de riesgos y sus herramientas de uso que: Cumple con los criterios académicos e institucionales además integra de manera clara y consistente los comentarios y retroalimentación recibidos en fases previas.

11.5. Etapa 5. Socialización de resultados

Una vez concluida la implementación piloto, se desarrolló la etapa de socialización de resultados, en la cual se presentaron y analizaron de manera estructurada los principales hallazgos del proyecto ante los grupos de interés institucionales, con especial énfasis en la alta gerencia de la organización.

Durante esta fase se realizaron reuniones formales con la alta dirección, en las que se expusieron detalladamente los resultados obtenidos, se verificó el cumplimiento de los objetivos definidos desde el inicio del proyecto y se analizó la contribución del modelo frente a las prioridades institucionales. Estos espacios facilitaron un diálogo constructivo con los

directivos, quienes valoraron de manera crítica los avances alcanzados, destacando las mejoras evidenciadas en la gestión de riesgos a partir de la implementación piloto.

Asimismo, se llevó a cabo la entrega formal del documento que consolida el alcance total del proyecto, incluyendo los productos desarrollados. Esta entrega se constituyó en un soporte documental relevante del proceso, favoreciendo la transparencia, la rendición de cuentas y la apropiación de los resultados por parte de la organización.

De igual manera, las actividades de socialización incorporaron el uso de material visual estructurado, que permitió presentar los principales hallazgos de forma clara, sintética y accesible para los asistentes.

12. Conclusiones

- A partir del diagnóstico realizado, se evidenció que la empresa STRATEGY AM AND PSM S.A.S. presentaba un bajo nivel de madurez en la gestión de riesgos, reflejado en la ausencia de metodologías estandarizadas, herramientas formales y lineamientos claros para su aplicación. Esta situación limitaba la identificación oportuna de riesgos y la toma de decisiones informadas, lo que justificó la necesidad de estructurar un modelo integral alineado con buenas prácticas internacionales.
- El desarrollo del proyecto permitió diseñar e implementar buenas prácticas orientadas a la estructuración de un modelo integral de gestión de riesgos, adaptado al contexto de la organización. Como resultado, se evidenció un incremento significativo en el nivel de cumplimiento frente a la ISO 31000:2018, pasando de un 19,51% en el diagnóstico inicial a un 73,17% en

la evaluación final, lo que demuestra un avance importante en la madurez organizacional en esta materia.

- El diseño del modelo de gestión de riesgos permitió consolidar un conjunto coherente de herramientas, metodologías y lineamientos alineados con la ISO 31000:2018, ajustados a las características de una pyme del sector de consultoría. La elaboración del manual de gestión de riesgos, las matrices, el toolkit y el sistema de indicadores representan un aporte metodológico relevante, al facilitar la integración de la gestión del riesgo en los niveles estratégico, táctico y operativo de la organización.
- La implementación piloto en el proceso de soporte TI permitió validar la aplicabilidad del enfoque propuesto en un contexto organizacional real. Durante su desarrollo, se identificaron 28 riesgos específicos, para los cuales se definieron e implementaron acciones orientadas a su tratamiento y mitigación.
- En términos generales, se concluye que la implementación de un modelo estructurado de gestión de riesgos, adaptado al contexto organizacional, contribuye a fortalecer la capacidad de anticipación, mejorar la toma de decisiones y aumentar la resiliencia empresarial. Asimismo, el estudio evidencia que es posible aplicar estándares internacionales como la ISO 31000 de manera flexible en pymes, generando valor sin requerir altos niveles de complejidad ni recursos elevados.

13. Recomendaciones

- Se recomienda que la organización establezca e institucionalice una política formal de gestión de riesgos que defina lineamientos, responsabilidades y criterios de actuación, con el fin de consolidar un enfoque estructurado y reducir la gestión empírica de los riesgos identificados.
- Se sugiere dar continuidad al modelo implementado mediante procesos periódicos de seguimiento y mejora continua, que permitan mantener y fortalecer el nivel de cumplimiento alcanzado, asegurando su sostenibilidad en el tiempo y su adaptación a los cambios del entorno organizacional.
- Se recomienda extender la aplicación del modelo de gestión de riesgos a otros procesos y proyectos de la organización, con el propósito de lograr una cobertura más amplia y garantizar mayor consistencia en la identificación, análisis y tratamiento de los riesgos a nivel organizacional.
- Se considera pertinente fortalecer los procesos de capacitación y sensibilización del talento humano en gestión de riesgos, con el fin de mejorar la apropiación del modelo, fomentar una cultura preventiva y asegurar la adecuada aplicación de las herramientas diseñadas.
- Se recomienda consolidar el sistema de indicadores diseñado, garantizando su seguimiento periódico y promoviendo su uso como herramienta de control y mejora, de manera que facilite la evaluación del modelo y apoye la toma de decisiones basada en información confiable.

Referencias bibliográficas

Atlassian. (2026). *(Strengths, Weaknesses, Opportunities, Threats) SWOT analysis*. Obtenido de https://www.atlassian.com/work-management/strategic-planning/swot-analysis?utm_source=chatgpt.com

Ayala López. (2016). *Diseño, estructuración e implementación de un sistema para la gestión integral del riesgo fundamentado en la norma NTC-ISO 31000 versión 2011 para la empresa La Muela S.A.S.*

Banco Interamericano de Desarrollo. (2023). *Guía teórica Gestión de riesgos para proyectos de desarrollo*. Obtenido de https://cursos.iadb.org/sites/default/files/GUIA%20TEORICA%20GRP%20-%20Gesti%C3%B3n%20de%20riesgos%20para%20proyectos%20de%20desarrollo.pdf.

Corredor Guerrero, A. (2017). *Diseño y formulación de un sistema de gestión de riesgos basado en la norma NTC-ISO 31000:2011 para la Corporación CDT de Gas.*

COSO ERM. (2017). *Enterprise Risk Management: Integrating with Strategy and Performance.*

EEIE, E. d. (2026). *Escuela de Estudios Industriales y Empresariales*. Obtenido de https://industrial.uis.edu.co/eisi/

Google Maps. (2026). *Google Maps*. Obtenido de Google Maps: https://www.google.com/maps

Hopkin. (2018). *Fundamentals of risk management.*

ICONTEC, I. C. (2018). *INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. Gestión del Riesgo. Directrices, Ginebra: ISO, 2018, 18 p. (ISO 310000, traducción oficial).*

Internacional, I. (2018). *NORMA TÉCNICA NTC-ISO COLOMBIANA 31000* . Bogotá, D.C.

ISO, I. O. (2018). *ISO 31000:2018 – Risk management — Guidelines.*

ISO, I. O. (2019). *Risk assessment techniques ISO 31010* .

Kailash. (01 de Julio de 2009). *Cox's risk matrix theorem and its implications for project risk management*. Obtenido de https://eight2late.com/2009/07/01/cox%E2%80%99s-risk-matrix-theorem-and-its-impl

Kent, J. (23 de Agosto de 2016). *Digital Magazine CIO.* Obtenido de https://www.cio.com/article/238969/risk-likelihood-x-impact.html

OAP, O. A. (27 de 04 de 2016). *Metodología de Administración de Riesgos Proceso Direccionamiento Estratégico.* Obtenido de unidadvictimas.gov.co: https://www.unidadvictimas.gov.co/wp-content/uploads/2016/05/metodologiaadministracionriesgosv3-1.pdf

Présiga Restrepo, Mejía Gómez, Londoño Giraldo . (2021). *Análisis de la Gestión del Riesgo Financiero en las Pymes Manufactureras de Medellín.*

SAS, S. A. (s.f.). *Strategy* . Obtenido de https://strategy.com.co/

Staff de Gerencia. (28 de Septiembre de 2018). *https://degerencia.com*. Obtenido de https://degerencia.com/articulo/que-es-la-matriz-dofa-foda-o-dafo/

Strategy AM and PSM SAS . (2025). *Cronograma Strategy AM and PSM SAS.*

Strategy AM and PSM SAS. (2026). Obtenido de https://strategy.com.co/

UNADM, U. A. (2025). *Administración para ingenieros Proceso de organización y dirección* . Obtenido de https://dmd.unadmexico.mx/contenidos/DCSBA/BLOQUE2/TA/06/TAIN/unidad_02/descargables/TAIN_U2_Contenido.pdf

Vazquez, D. (2024). *Boise State University*. Obtenido de Cybersecurity risk quantification (Module 3: Terminology & Concepts).: https://boisestate.pressbooks.pub/cybersecurityriskquantification/chapter/module-3-terminology-concepts/